



Win 2k Server Kompendium

<http://kickme.to/tiger/>

1 Einführung in Windows 2000

1.1 Windows 2000 als Netzwerkbetriebssystem

1.1.1 Betriebssysteme

1.1.2 Windows 2000 und Netzwerke

1.1.3 Netzwerksicherheit

1.1.4 Systemüberwachung

1.2 Die Windows 2000-Produktfamilie

1.2.1 Allgemeine Features

1.2.2 Windows 2000 Advanced Server

1.2.3 Windows 2000 Datacenter Server

Teil I Die Betriebssystemumgebung von Windows 2000

2 Architektur

2.1 Die Architektur der Teilsysteme und des Kernels

2.1.1 Benutzermodus und Kernelmodus

2.1.2 Die Hardwareabstraktionsschicht

2.1.3 Der Kernel

2.1.4 Die Windows 2000-Ausführungsschicht

2.1.5 Teilsysteme

2.1.6 Das Win32-Teilsystem

2.1.7 Das POSIX-Teilsystem

2.1.8 Das OS/2-Teilsystem

2.2 Das Speichermodell und die Speicherverwaltung

2.2.1 Das Speichermodell

2.2.2 Die Speicherverwaltung

3 Installation

3.1 Systemanforderungen

3.2 Die Hardwarekompatibilitätsliste

3.3 Überblick über den Installationsprozess

3.4 Der Installationsprozess im Detail

3.4.1 Windows 2000 starten

[3.4.2 Update-Informationen](#)

[3.4.3 Windows 2000 konfigurieren](#)

[3.4.4 Die Konfiguration der Netzwerkeinstellungen](#)

[3.4.5 Lizenzierungsmodelle](#)

[3.4.6 Szenario 1: Die Pro-Server-Lizenz](#)

[3.4.7 Szenario 2: Die Pro-Client-Lizenz](#)

[3.4.8 Lizenzen hinzufügen](#)

[3.5 Die unbeaufsichtigte Installation](#)

[3.6 Die Wiederherstellungskonsole installieren](#)

[3.7 Die Datei Boot.ini](#)

[3.8 Die Notfalldiskette](#)

[3.9 Migration von bereits bestehendem System](#)

[3.10 Hinweise zur Hardware](#)

[3.10.1 Interrupts](#)

[3.10.2 EIDE-Geräte](#)

[3.10.3 Windows-Update](#)

[3.10.4 Busse und Geräte](#)

4 Dateisysteme

[4.1 Betrachtungen zur Hardware](#)

[4.1.1 Festplattentechnologie](#)

[4.1.2 Festplattencontroller](#)

[4.1.3 Die SCSI-Prinzipien](#)

[4.1.4 Fortgeschrittene Controllertechnologie](#)

[4.2 Festplattenpartitionen](#)

[4.2.1 Der Systemstart](#)

[4.2.2 Basisfestplatten](#)

[4.2.3 Dynamische Festplatten](#)

[4.2.4 Basisfestplatten und normale Festplatten](#)

[4.3 Die Datenträgerverwaltung](#)

[4.3.1 Die Datenträgerverwaltung starten](#)

[4.3.2 Die Eigenschaften der Festplatte](#)

[4.3.3 Eigenschaften von Datenträgern oder Partitionen](#)

[4.3.4 Die Verwaltung von Partitionen und Datenträgern](#)

[4.3.5 Dynamische Festplatten](#)

[4.3.6 Kontingente einrichten](#)

[4.4 Dateisysteme](#)

[4.4.1 FAT](#)

[4.4.2 NTFS](#)

[4.4.3 Konvertierung von Formaten](#)

[4.4.4 Empfehlungen](#)

[4.5 Datenträger](#)

[4.5.1 Einfache Datenträger](#)

[4.5.2 Übergreifende Datenträger](#)

[4.5.3 Gespiegelte Datenträger](#)

[4.5.4 Stripesetdatenträger](#)

[4.5.5 RAID-5-Datenträger](#)

[4.5.6 Einige Hinweise zu Windows 2000-Datenträgern](#)

[4.6 Netzwerkfreigaben](#)

[4.6.1 Verzeichnisse freigeben](#)

[4.6.2 Auf freigegebene Verzeichnisse zugreifen](#)

[4.7 Verteiltes Dateisystem \(DFS\)](#)

[4.7.1 Konzepte des verteilten Dateisystems](#)

[4.7.2 Das verteilte Dateisystem einrichten](#)

[4.7.3 Das verteilte Dateisystem nutzen](#)

[4.8 Remotespeicher](#)

[4.8.1 Das Konzept des Remotespeichers](#)

[4.8.2 Remotespeicher einrichten](#)

[4.9 Die Wechselmedienverwaltung](#)

5 Netzwerke

[5.1 Microsofts Netzwerkkonzepte](#)

[5.1.1 Arbeitsgruppen und Domänen](#)

[5.1.2 Active Directory](#)

[5.1.3 Netzwerkdienste](#)

[5.2 Netzwerke \(Ihr LAN oder WAN\) und Netzwerke \(Segmentierung\)](#)

[5.2.1 Switched Ethernet](#)

[5.2.2 Mit Routern verbundene Segmente](#)

[5.3 RRAS](#)

[5.3.1 Der Remote-Zugriff](#)

[5.3.2 Multiprotokollrouting](#)

6 Drucken

[6.1 Druckkonzepte](#)

[6.1.1 Drucker](#)

[6.1.2 Schriftarten](#)

[6.1.3 Druckertreiber](#)

[6.1.4 Kommunikation mit Druckern](#)

[6.1.5 Der Ablauf eines Druckauftrags](#)

[6.2 Druckwarteschlangen einrichten](#)

[6.3 Die Druckerverwaltung](#)

[6.3.1 Die Befehle des Menüs Drucker](#)

[6.3.2 Die Eigenschaften des Druckers](#)

[6.3.3 Die Befehle des Menüs Dokument](#)

[6.3.4 Die Eigenschaften eines Druckauftrags](#)

[6.4 Warteschlangen über die Eigenschaften des Druckservers verwalten](#)

[6.4.1 Die Registerkarte Formulare](#)

[6.4.2 Die Registerkarte Anschlüsse](#)

[6.4.3 Die Registerkarte Treiber](#)

[6.4.4 Die Registerkarte Erweiterte Optionen](#)

[6.5 Problembehandlung](#)

[6.5.1 Probleme bei der Datenübertragung vom Client zum Server diagnostizieren](#)

[6.5.2 Probleme mit der Druckqualität diagnostizieren](#)

[6.5.3 Die Grenzen des Druckers kennen](#)

[6.5.4 Die Druckerspezifikationen kennen](#)

[6.5.5 Die Treiberversionen kennen](#)

[6.5.6 Sicherstellen, dass alles zusammenpasst](#)

7 Die Registrierung

[7.1 Was ist die Registrierung?](#)

[7.2 Die Struktur der Registrierung](#)

[7.2.1 Die Teilstruktur Classes](#)

[7.2.2 Die Teilstruktur Users](#)

[7.2.3 Die Teilstruktur Local Machine](#)

[7.2.4 Die Teilstruktur Current Configuration](#)

[7.3 Die Benutzung der Registrierung durch Anwendungen](#)

[7.4 Der Registrierungs-Editor](#)

[7.4.1 Wann sollte der Registrierungs-Editor benutzt werden?](#)

[7.4.2 Regedit benutzen](#)

[7.4.3 Änderungen der Registrierung mit Regedit finden](#)

[7.4.4 Den Registrierungs-Editor Regedt32 nutzen](#)

[7.5 Die letzte, als funktionierend bekannte Konfiguration benutzen](#)

8 TCP/IP-Netzwerke

[8.1 TCP/IP-Konzepte kurz und knapp](#)

[8.1.1 IP-Adressen](#)

[8.1.2 Subnetzmasken](#)

[8.1.3 Adressierung von Subnetzen](#)

[8.1.4 IP-Routing](#)

[8.1.5 TCP-Ports](#)

[8.2 Microsoft-TCP/IP](#)

[8.2.1 Einführung in Microsoft-TCP/IP](#)

[8.2.2 Installation von TCP/IP](#)

[8.2.3 Routing](#)

[8.2.4 DHCP](#)

[8.2.5 Einen Bereich einrichten](#)

[8.2.6 WINS](#)

[8.2.7 DDNS \(Dynamic Domain Name Service\)](#)

[8.2.8 Von WINS zu DNS migrieren](#)

[8.2.9 Einer Netzwerkkarte mehrere Adressen zuweisen](#)

Teil II Active Directory und Kontenverwaltung

9 Verzeichnis- und Zugriffskonzepte

9.1 Sicherheitskonzept

9.1.1 Kerberos

9.1.2 NTLM

9.1.3 Zugriffssteuerungsliste (ACL = Access Control List)

9.2 Active Directory-Steuerung

9.2.1 Arbeitsgruppen und Domänen

9.3 Active Directory- bzw. Domänenobjekte

9.4 Was kommt zuerst: Die Benutzer oder die Gruppen?

9.4.1 Erstellen von Objekten

9.5 Steuern des Benutzerzugriffs auf Ressourcen

9.5.1 Dateifreigabeberechtigungen

9.5.2 Druckerberechtigungen

10 Struktur des Active Directory

10.1 Standorte und Replikation

10.1.1 Standorte

10.1.2 Replikation

10.1.3 Erstellen von Standorten

10.2 Strukturstandards

10.2.1 Politische Struktur

10.2.2 Geografische Struktur

10.2.3 Gemischte Struktur

10.3 Organisationseinheiten

10.4 Dynamisches DNS

10.4.1 Funktionsweise der dynamischen Aktualisierung

10.4.2 Sichere dynamische Aktualisierung

11 Erstellen und Verwalten von Benutzerkonten

11.1 Benutzerkonten

11.1.1 Vordefinierte bzw. integrierte Benutzer

11.1.2 Richtlinien für die Vergabe von Namen und Kennwörtern

11.1.3 Erstellen von Benutzerkonten

11.1.4 Bedürfnisse der Benutzerumgebung

11.2 Datenträgerkontingente

11.3 Gruppen

11.3.1 Gruppenbereich

11.3.2 Erstellen einer neuen Gruppe

11.3.3 Vordefinierte Standardgruppen

12 IntelliMirror und Benutzersteuerung

12.1 Grundelemente von IntelliMirror

12.2 Steuerungskonzepte

12.2.1 Profile

12.2.2 Richtlinien: Eine allgemeine Einführung

12.3 Verwalten von Gruppenrichtlinien

12.3.1 Erstellen und Zuweisen von Gruppenrichtlinienobjekten

12.3.2 Ändern der Richtlinie

12.3.3 Gruppenrichtlinien-Administratoren

12.4 Windows Installer

12.4.1 WinInstaller

12.4.2 Verteilen der Pakete

12.5 Remoteinstallationsdienste

Teil III Netzwerkdienste

13 Durchsuchen des Netzwerks

13.1 Grundlagen zum Konzept

13.1.1 Suchdienstfunktionen für Server

13.1.2 Kriterien für die Auswahl eines Suchdienstes

13.1.3 Suchdienstwahl

13.2 Der Suchprozess

13.2.1 Suchdienstankündigungen

13.2.2 Der Hauptsuchdienst

13.2.3 Die Suchliste

13.2.4 Überlegungen zum Durchsuchen mehrerer Domänen und WANs

13.2.5 Ausfälle von Suchdiensten

13.2.6 Einen Windows 2000-Server so konfigurieren, dass er nie als Suchdienst eingesetzt wird

13.2.7 Überlegungen zum Suchdienst im Hinblick auf das Active Directory

14 Remotezugriff - RAS

14.1 Routing und RAS verstehen

14.2 Protokollunterstützung

14.2.1 TCP/IP

14.2.2 AppleTalk

14.2.3 NWLink IPX/SPX/NetBIOS-kompatibles Transportprotokoll

14.2.4 NetBEUI

14.3 Sicherheit beim Remotezugriff

14.4 Installieren von Routing und RAS

14.4.1 Konfigurieren des RAS-Servers

14.4.2 Erweiterte Konfiguration des RAS-Servers

14.4.3 Konfigurieren des Routing

14.4.4 Protokollunterstützung

14.4.5 Modem

14.4.6 Unterstützen von WANs

14.5 Authentifizierung

14.6 Fehlersuche

15 Multiprotokollumgebungen

15.1 Protokolle, die Windows 2000 unterstützt

15.1.1 Installieren eines neuen Protokolls

15.1.2 Lade sie alle!

15.1.3 Art der Verbindung

[15.1.4 TCP/IP](#)

[15.1.5 IPX/SPX](#)

[15.1.6 AppleTalk](#)

[15.1.7 NetBEUI](#)

[15.2 Routing- und RAS-Dienst](#)

[15.2.1 PPP](#)

[15.2.2 RIP](#)

[15.2.3 Fehlersuche](#)

16 Überlegungen zum Arbeitsplatzrechner

[16.1 Client-Dienste - ein kurzer Überblick](#)

[16.2 Betriebssysteme für Clients](#)

[16.2.1 Novell NetWare-Clients](#)

[16.2.2 DOS, OS/2, Windows 3.x und Windows für Workgroups](#)

[16.2.3 Macintosh](#)

[16.2.4 Verbindung zu UNIX](#)

Teil IV Verbindung zu anderen Betriebssystemen

17 Verbindung zu Novell NetWare

[17.1 Konzeptuelle Unterschiede](#)

[17.1.1 Sicherheit](#)

[17.1.2 Active Directory und NetWare Directory Services](#)

[17.1.3 Dateifreigaben](#)

[17.1.4 Drucken](#)

[17.2 Die Verbindung zu NetWare](#)

[17.2.1 Gateway Service für NetWare](#)

[17.2.2 File und Print Services für NetWare](#)

[17.2.3 Migrationsprogramm für den Verzeichnisdienst](#)

[17.2.4 NDS for NT \(von Novell\)](#)

18 Verbindung zwischen UNIX und Windows 2000 Server

18.1 Konzeptuelle Unterschiede zwischen Windows 2000 Server und UNIX-Betriebssystemen

18.1.1 Benutzerkonten

18.1.2 Sicherheit

18.1.3 Verzeichnisdienste

18.2 Unterschiedliche Varianten von UNIX

18.3 Einfache TCP/IP-Tools

18.3.1 Telnet

18.3.2 FTP

18.3.3 Die weniger bekannten Programme

18.4 Verbindung zwischen UNIX und Windows-Anwendungen

18.4.1 XWindows und Windows 2000

18.5 Zugriff auf NFS

18.6 Über Samba

18.7 Drucken in einer UNIX-Umgebung

18.8 Die Zukunft: Microsoft und UNIX

Teil V Kommunikation übers Internet

19 Internet Information Server (IIS)

19.1 Internet-Informationsdienste

19.2 Bevor Sie mit IIS beginnen

19.2.1 Systemanforderungen

19.2.2 Anbindung an das Internet

19.3 Installieren von IIS

19.4 Verwalten und Konfigurieren von IIS

19.4.1 Allgemeine IIS-Einstellungen

19.4.2 Verwalten der FTP-Site

19.4.3 Erweiterte Verwaltung der Website

19.4.4 Verwalten der Gopher-Site

19.4.5 Verwalten des Telnet-Dienstes

19.4.6 Erweiterte Sicherheitskonzepte

20 Virtuelle private Netzwerke

[20.1 Machen Sie das Internet zu Ihrem eigenen WAN](#)

[20.2 Was ist ein VPN, ein »Virtuelles privates Netzwerk«?](#)

[20.3 Sicherheit und Verschlüsselung](#)

[20.4 Tunnel-Server](#)

[20.5 VPN-Tunnel-Server und Firewalls](#)

[20.6 Verkehr mit Hilfe eines Tunnel-Servers filtern](#)

[20.7 Microsoft Windows 2000 VPN](#)

[20.7.1 IPSec](#)

[20.7.2 L2TP \(Layer 2 Tunneling Protocol\)](#)

[20.8 Synchrone und asynchrone Schlüssel](#)

[20.8.1 L2TP und IPSec](#)

[20.9 Einrichtung eines grundlegenden VPN in Windows 2000](#)

[20.10 Einrichtung eines Tunnel-Server-VPN mit Windows 2000](#)

[20.11 RRAS-Erweiterungen](#)

Teil VI Administration des Server

21 Serververwaltung

[21.1 Microsoft Management Console \(MMC\)](#)

[21.2 Dienstprogramme zur Serververwaltung](#)

[21.2.1 Ereignisse anzeigen](#)

[21.2.2 Protokolleinstellungen](#)

[21.2.3 Systeminformation](#)

[21.2.4 Geräte-Manager](#)

[21.3 SNMP](#)

22 Leistungsoptimierung und Tuning

[22.1 Windows 2000 Supporttools](#)

[22.2 Automatische Optimierung](#)

[22.2.1 Vermeiden von Fragmentierung](#)

[22.2.2 Multiprocessing](#)

[22.2.3 Priorisierte Prozesse und Threads](#)

[22.2.4 Festplattenanforderung in den Cache stellen](#)

[22.3 Stripesets und Auslagerungsdateien im virtuellen Speicher](#)

[22.3.1 Stripeset-Datenträger](#)

[22.3.2 Optimieren virtueller Speicherseiten](#)

[22.4 Der Systemmonitor](#)

[22.4.1 Objekte und Objektleistungsindikatoren](#)

[22.4.2 Ein Diagramm anlegen](#)

[22.4.3 Diagramme interpretieren](#)

[22.4.4 Berichte und Protokolle](#)

23 Dienstprogramme zur Sicherung des Servers

[23.1 Operatorberechtigungen für das Sicherungsprogramm von Windows 2000 Server](#)

[23.2 Sicherung von Windows 2000](#)

[23.2.1 Beaufsichtigte Operationen](#)

[23.2.2 Unbeaufsichtigte Operationen](#)

[23.2.3 Sicherung von der Eingabeaufforderung aus](#)

[23.3 Wiederherstellen einer Sicherung](#)

[23.3.1 Maßgebende Wiederherstellung](#)

[23.3.2 Wiederherstellung verschlüsselter Dateien](#)

[23.4 Unterstützte Sicherungsgeräte](#)

[23.5 Wiederherstellungskonsole](#)

[23.6 Notfalldisketten](#)

[23.7 Sicherungswerkzeuge von Drittanbietern](#)

24 Wiederherstellung nach Systemausfällen

[24.1 Machen Sie einen Plan und halten Sie sich daran](#)

[24.1.1 Dokumentation und Ereignisse](#)

[24.1.2 Katastrophenbeauftragte](#)

[24.1.3 Physische Betrachtungen](#)

[24.2 Wiederherstellung der Daten](#)

[24.2.1 Sicherungsoperationen](#)

[24.2.2 Zeitabhängige Sicherungspläne](#)

[24.3 Maßnahmen gegen Hardwareausfall](#)

[24.3.1 Hardware-RAID](#)

[24.3.2 Geclusterte Server](#)

Teil VII Anhang

A Problemlösungen/Fehlerliste

[A.1 Service Packs](#)

[A.2 STOP-Fehler](#)

[Was Sie bei der Anzeige von STOP-Bildschirmen im Kernelmodus tun können](#)

[Lösungen für STOP-Fehler](#)

B Inhalt der CD-ROM zum Buch

[B.1 Grundregeln im Umgang mit Free- und Shareware](#)

[Freeware](#)

[Shareware](#)

[B.2 Die Programme auf der CD-ROM im Detail](#)

~

Stichwortverzeichnis

© Copyright [Markt+Technik Verlag](#), ein Imprint der Pearson Education Deutschland GmbH
Elektronische Fassung des Titels: Windows 2000 Server Kompendium, ISBN: 3-8272-5611-9 Kapitel:
inhalt.htm

Satz und HTML-Erstellung: [reemers publishing services](#), Krefeld

Kapitel 1 Einführung in Windows 2000

Windows 2000 ist die aktuelle Version von Microsofts Betriebssystem Windows NT und bietet neueste Technologien. Dieses Kapitel führt Sie in die Windows 2000-Produktfamilie ein und bietet einen kurzen Gesamtüberblick über das Produkt. Sie erfahren, was neu ist, was verbessert wurde und wie bekannte Aufgaben auf neue Weise behandelt werden. Dieses Kapitel behandelt folgende Punkte:

- Windows 2000 als Netzwerkbetriebssystem
- Die Windows 2000-Produktfamilie
 - Allgemeine Merkmale
 - Windows 2000 Professional
 - Windows 2000 Server
 - Windows 2000 Advanced Server
 - Windows 2000 Datacenter Server

Windows 2000 ist die Zukunft der Betriebssystemserie von Microsoft. Dazu gehören die Workstationversion Windows 2000 Professional ebenso wie die Super-High-End-Version Windows 2000 Datacenter Server.

1.1 Windows 2000 als Netzwerkbetriebssystem

Was ist ein Netzwerkbetriebssystem? Auf einen ganz simplen Nenner gebracht: ein Betriebssystem für ein Netzwerk. Im Wesentlichen sollte ein Netzwerkbetriebssystem Ressourcen im gesamten Netzwerk koordinieren und zuordnen können. Um diesen Punkt etwas genauer zu beleuchten, wird nun zuerst veranschaulicht, was ein Betriebssystem ist und dann, warum Windows 2000 ein Netzwerkbetriebssystem ist. Ein effektives Netzwerkbetriebssystem benötigt eine effektive Sicherheits- und Leistungsüberwachung.

1.1.1 Betriebssysteme

In der Informatik ist die klassische Definition eines Betriebssystems sehr eng gehalten und definiert im Wesentlichen die Hauptaufgaben eines Betriebssystems: Die Zuordnung von Ressourcen und die Bereitstellung des Zugriffs auf Ressourcen. *Zuordnung von Ressourcen* bedeutet, dass das Betriebssystem der einzige Zuordnungsmechanismus für Ressourcen in einem System sein sollte, der jedem Client die angeforderten Ressourcen bereitstellt, wie z.B. Hauptspeicher, Festplattenspeicher oder Prozessorzeit. Das Betriebssystem muss mit mehreren Prozessen arbeiten und sicherstellen, dass die Hardware so effizient wie möglich genutzt wird. Eine ausführliche Beschreibung des Betriebssystems Windows 2000 finden Sie in Kapitel 2, in dem Themen wie die Speicherreservierung, das Prozessmodell und der Hardwarezugriff behandelt werden.

Microsofts Definition eines Betriebssystems geht von der Informatikdefinition aus und fügt mehrere hundert Megabyte an Benutzeroberfläche sowie einen Webbrowser, Texteditoren, Authentifizierungssysteme, Verzeichnisdienste, Internetdienste und viele weitere Dinge hinzu. Vieles ist einfach nur zur Zierde da oder um Chefs zu beeindrucken.

1.1.2 Windows 2000 und Netzwerke

Ein Netzwerkbetriebssystem verfügt über einige Merkmale, die über ein Standardbetriebssystem für den Einzelplatzcomputer hinausgehen. Es muss mit mehreren Computern zusammenarbeiten können und die Zuordnung von Ressourcen und das Job-Sharing behandeln. Das einfachste Beispiel hierfür ist die Speicherung von Dateien. Windows 2000 muss die Datenträgerressourcen zuordnen, damit Programme Daten lesen und schreiben können. Ein komplexeres Beispiel bieten die Sicherheitsdienste. Windows 2000 muss in der Lage sein festzustellen, ob ein Benutzer eine Datei an der gewünschten Stelle speichern darf.

Diese Art der Kooperation zwischen Computern macht ein Netzwerkbetriebssystem aus. Zu den Kernkonzepten, die Windows 2000 nutzt, um diesen Status zu erreichen, zählt der plattformübergreifende Zugriff. Windows 2000 kann mit den Systemen verschiedener Hersteller interagieren, die dadurch Dateien, Drucker und andere Netzwerkressourcen gemeinsam nutzen können. Windows 2000 Professional kann mit NetWare-Servern zusammenarbeiten und bietet eine Authentifizierung für NDS (Novell Directory Service), die Server-Produkte können mit NDS interagieren, indem sie als Gateways zwischen NetWare-Servern und Clients arbeiten, die von NetWare nicht authentifiziert werden. Weitere Informationen zur Verbindung mit NetWare-Systemen finden Sie in Kapitel 17.

UNIX ist das am weitesten verbreitete Serverbetriebssystem im Internet. Dieses Betriebssystem bietet ein hohes Maß an Zuverlässigkeit und eine bisher unerreichte Performance. Weil Microsoft Windows 2000 als Betriebssystem für das Internet positioniert hat, ist es sinnvoll, dass es mit Tools ausgestattet ist, um mit FTP, Telnet, SMTP und HTTP eine Verbindung zu UNIX herzustellen. Es sind außerdem zusätzliche Tools von Drittanbietern verfügbar, mit denen sogar ein Zugriff auf XWindows und NFS (Network File Services) möglich ist. In Kapitel 18 finden Sie hierzu alle wissenswerten Details.

Eines der interessantesten Features von Windows NT 4.0 war die Terminal Server Edition. Dieses Feature findet nun eine Fortsetzung in Windows 2000 Advanced Server und Windows 2000 Datacenter Server. Es bietet Clients die Möglichkeit, eine Verbindung zu Windows 2000 herzustellen, als säßen sie vor der Konsole des Servers. Die Clients selbst sind so schlank, dass sie auch auf älterer Hardware lauffähig sind und einen Zugriff auf extrem schnelle Server bieten. Außerdem gibt es neue Clients, sodass sogar über Handheld-PCs eine Verbindung zu diesen Servern hergestellt werden kann.

1.1.3 Netzwerksicherheit

Ohne Netzwerksicherheit ist der Datenfluss im Netzwerk vollständig offen und jeder kann darauf zugreifen. Die auf dem Server verfügbaren Ressourcen sind jedermann zugänglich und alle Anwender - vom Hausmeister bis zum Vorstandsvorsitzenden - haben die gleichen Zugriffsrechte. Dies mag zwar vielleicht der Traum eines jeden Hackers sein, ist jedoch der Alptraum sämtlicher Systemadministratoren. Netzwerksicherheit beinhaltet viele verschiedene Dinge. Aus der Betriebssystemperspektive beinhaltet sie die Authentifizierung von Benutzern und die Überprüfung der Zugriffsrechte.

Bei der Authentifizierung von Benutzern wird z.B. sichergestellt, dass die Benutzer diejenigen sind, die sie zu sein vorgeben. Windows 2000 bietet verschiedene Möglichkeiten, um dies zu gewährleisten. Die

traditionelle Kombination aus einem Benutzernamen und einem Kennwort hat sich bewährt, sie funktioniert jedoch nur so gut wie das Gedächtnis der Benutzer, das notorisch unzuverlässig ist. Windows 2000 implementiert ein Smartcard-Sicherheitssystem, bei dem der Benutzer eine Plastikkarte in einen Kartenleser einlegen muss. Auf diese Weise lässt sich ganz leicht sicherstellen, dass der Benutzer tatsächlich anwesend ist. Das wahrscheinlich neueste Authentifizierungsschema ist das biometrische Sicherheitssystem, das Finger- oder Handabdrücke, Gesichtsmuster oder andere Ähnlichkeitsmerkmale analysiert. Mit dem biometrischen Sicherheitssystem ist zumindest sichergestellt, dass niemand eine Smartcard umgehen kann oder ein Kennwort auf einen Klebezettel schreibt und diesen dann gedankenlos auf den Monitor klebt.

Die Überprüfung der Zugriffsrechte ist ein weiteres Problem der Netzwerksicherheit. Wie lässt sich verfolgen, welcher Benutzer Zugriff auf welche Dateien hat und wie lassen sich diese Dateien sichern? All das wird in Kapitel 4 behandelt.

Wie behandelt nun Windows 2000 die Überprüfung von Benutzern und die Freigabe des Zugriffs auf Ressourcen? Die wesentliche Änderung in Windows 2000 ist die Einführung von *Active Directory*. Active Directory ist eine Kombination aus einem Telefonbuch und einem Wachposten. Wenn sich ein Benutzer anmeldet, behandelt das Active Directory die Probleme der Authentifizierung von Benutzern. Dabei wird das Kennwort nicht über das Netzwerk übertragen, da dies ein Sicherheitsproblem darstellen würde. Active Directory verwendet ein spezielles Sicherheitssystem namens *Kerberos*, das am MIT (Massachusetts Institute of Technology) entwickelt wurde. Dieses System bietet eine Möglichkeit, die Echtheit des Benutzers sicherzustellen, ohne dass dieser dem Active Directory alles mitteilen muss, was er weiß. Außerdem verfügt das Active Directory über ein ausgefeiltes Replikationsschema, das die Verteilung von Daten im gesamten Unternehmensnetz ermöglicht und dem Benutzer erlaubt, sich überall anzumelden, wobei die Authentifizierung schnell und zuverlässig erfolgt.

1.1.4 Systemüberwachung

Zu den Aufgaben eines Betriebssystems gehört es, zu messen, was im Netzwerk und auf den einzelnen Computern im Netzwerk vor sich geht, um zu wissen, wie sich die Kapazität des Systems am besten erweitern lässt und wie sich Problembereiche ermitteln lassen. Windows 2000 verfügt über mehrere Tools, um die Systemleistung zu überwachen und Fehler zu finden.

Der bisherige Systemmonitor wurde durch eine gleichnamige MMC-Plug-In-Komponente (MMC = Microsoft Management Console) ersetzt. Der Systemmonitor stellt die statistischen Daten des Betriebssystems in Form von Diagrammen dar. Die Daten lassen sich so leicht analysieren. Eine ausführliche Beschreibung finden Sie in Kapitel 26.

Ein weiterer wichtiger Bestandteil der Leistungsüberwachung ist die Analyse der Vorgänge im Netzwerk. Windows 2000 enthält ein Produkt namens *Netzwerkmonitor*, mit dem sich alle eingehenden und ausgehenden Pakete bei einem lokalen Computer aufzeichnen lassen. Dieses Produkt wurde gegenüber der Vorgängerversion in Windows NT so verändert, dass alle Pakete angezeigt werden können. Andere Hardware- und Softwarelösungen bieten eine ähnliche Funktionalität.

1.2 Die Windows 2000-Produktfamilie

Um Windows 2000 Server besser vermarkten zu können, hat Microsoft das Produkt in drei verschiedene Pakete aufgeteilt, die sich im Funktionsumfang und ihrer Rolle in einem Netzwerk unterscheiden. Alle Produkte verfügen über dieselben Kernfunktionen, die im Wesentlichen Bestandteil des Betriebssystems sind. Windows 2000 Advanced Server ist mit zusätzlichen Features ausgestattet und hat dadurch eine höhere Kapazität, Windows 2000 Datacenter Server übersteigt diese Kapazität sogar noch.

1.2.1 Allgemeine Features

Alle Windows 2000 Server-Produkte beinhalten bestimmte Kernfunktionen. Diese lassen sich in die folgenden Bereiche unterteilen:

- Serververwaltung
- Active Directory
- Sicherheit
- Speicher und Dateisysteme
- Netzwerkfunktionen und Kommunikation
- Anwendungsdienste
- Unterstützung von SMP (Symmetric Multi Processing)
- Benutzeroberfläche
- Sicherung

Diese allgemeinen Features werden nachfolgend kurz beschrieben.

Serververwaltung

In Windows NT 4.0 beinhaltete die Serververwaltung die folgenden Anwendungen: Benutzer-Manager für Domänen, Server-Manager, Drucker-Manager, Festplatten-Administrator etc. In Windows 2000 gibt es eine neue Oberfläche namens *Microsoft Management Console* (MMC) und jede der erwähnten Anwendungen wurde durch ein Plug-In für die MMC ersetzt. Die Anwendungen lassen sich so wesentlich einfacher benutzen. So können Sie z.B. das MMC-Snap-In *Computerverwaltung* öffnen, indem Sie **Start/Einstellungen/Systemsteuerung** wählen, doppelt auf **Verwaltung** klicken und dann die Computerverwaltung starten (siehe Abbildung 1.1). Das Snap-In *Computerverwaltung* beinhaltet fast alle anderen Snap-Ins, wie z.B. die Benutzerverwaltung, die Datenträgerverwaltung, und bietet die Möglichkeit, Dienste zu starten und zu stoppen.

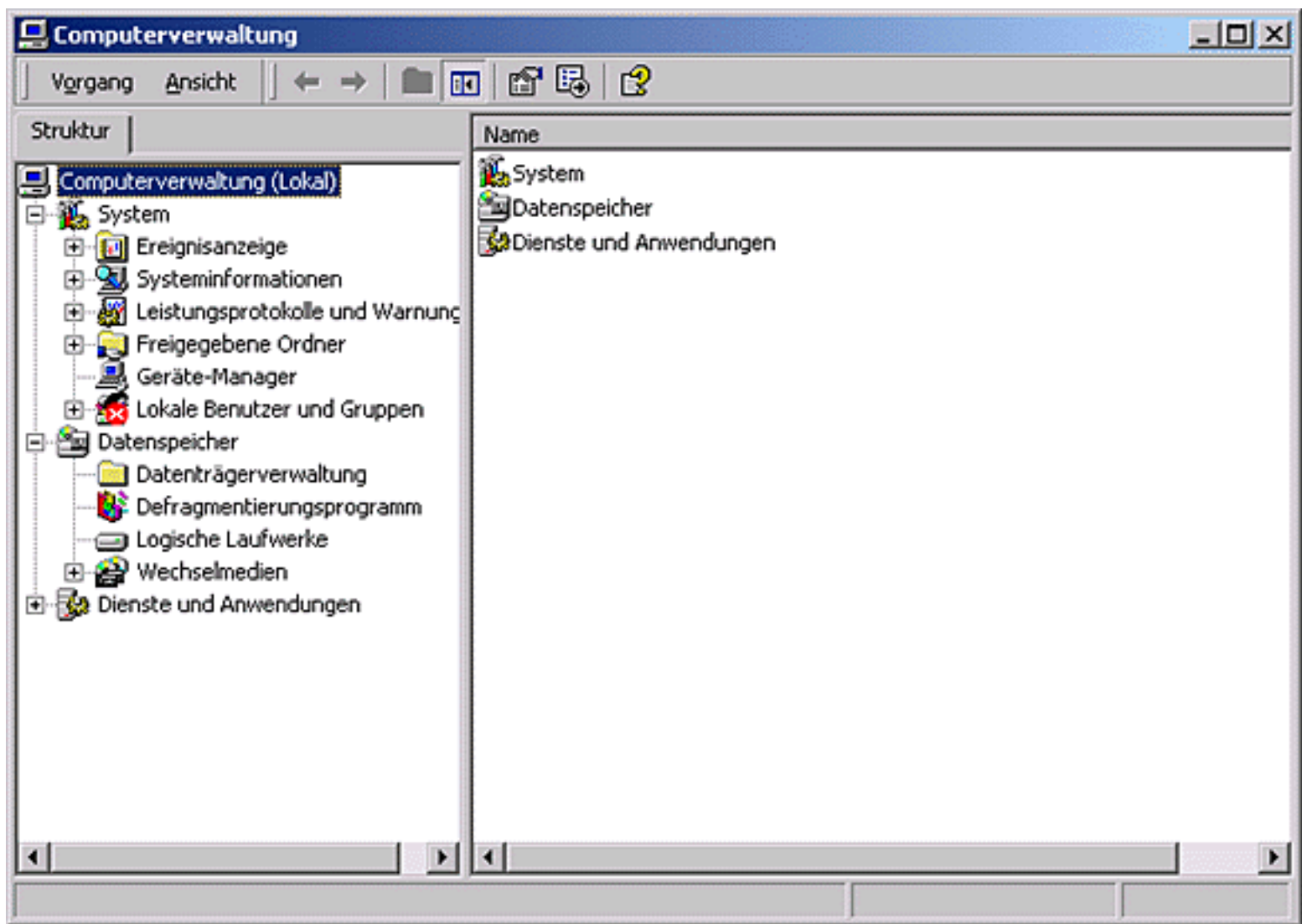


Bild 1.1: Die Microsoft Management Console (MMC) ist die Verwaltungsoberfläche von Windows 2000

Die MMC soll nun etwas genauer betrachtet werden. Sie besteht aus zwei Fensterbereichen. Auf der linken Seite wird eine Baumstruktur des Snap-Ins angezeigt und auf der rechten Seite die Daten. In diesem Bereich arbeiten Sie normalerweise auch. Klicken Sie z.B. im linken Fensterbereich auf den Eintrag **Datenspeicher** und dann auf **Datenträgerverwaltung**. Auf der rechten Seite des Fensters werden nun Tools für die Partitionierung der Festplatte angezeigt.

Ein weiteres großartiges Tool zur Verwaltung von Servern ist das Web-Based Enterprise Management (WBEM). Damit lassen sich Windows 2000-Server, auf denen der Internet Information Server-Dienst läuft, über jeden beliebigen Webbrowser verwalten.

Active Directory

Das Active Directory-System ist wahrscheinlich das wichtigste aller neuen Features in Windows 2000. Es integriert alle Daten von Benutzerkonten und Gruppen in einer dezentralisierten Datenbank. Außerdem integriert sich Active Directory in Microsoft Exchange Server. Auf diese Weise lassen sich doppelte Bemühungen vermeiden, die bei der Verwaltung von E-Mail-Verteilerlisten und Sicherheitsgruppen entstehen.

Windows NT nutzte ein Replikationsmodell mit einem primären Domänencontroller, was bedeutet, dass ein Server die gesamte Replikation der Sicherheitsdaten von Benutzern für alle Server im Netzwerk übernimmt, die Anmeldungen behandeln können. Bei Active Directory gibt es keinen primären Domänencontroller mehr, sondern alle Server können in gleicher Weise Änderungen speichern und vornehmen. Dadurch lässt sich das System leichter skalieren, weil nicht nur ein Server als zentraler Punkt für die Verteilung von Veränderungen dient. Dies bietet auch eine höhere Fehlertoleranz, weil jeder Server ein Domänencontroller sein kann und sich jeder Domänencontroller in einen Mitgliedsserver oder eigenständigen Server zurückstufen lässt.

Das Active Directory-System wurde als Konkurrenz zum Novell Directory Service (NDS) entwickelt. Beide Systeme basieren auf dem X.500-Standard und nutzen die Verzeichnisse über das Lightweight Directory Access Protocol (LDAP). Selbstverständlich sind diese beiden Verzeichnisdienste nicht kompatibel, weil dies uns das Leben viel zu leicht machen würde. Microsoft berücksichtigt dieses Problem und bietet Tools, mit denen sich NDS in Active Directory umwandeln lässt. Weitere Hinweise hierzu finden Sie in Kapitel 17.

Das Active Directory verwendet den X.500-Standard, der angibt, welche Arten von Informationen gespeichert werden und wie darauf zugegriffen wird. Die Informationen werden hierarchisch in Baumstrukturen gespeichert. Durch die Kombination von Baumstrukturen mit Directories wird das gesamte Active Directory-System extrem skalierbar, weil es von sehr großen Organisationen genutzt werden kann und trotzdem in kleinen Organisationen effizient arbeitet.

Active Directory ist so wichtig und so neu, dass ihm ein ganzer Teil des Buches gewidmet ist. Kapitel 9 beschreibt die Grundlagen der Sicherheit und Domänenstrukturen. Kapitel 10 behandelt das Design und die Konfiguration von Active Directory. Kapitel 11 behandelt die Erstellung und Verwaltung von Benutzerkonten und Kapitel 12 die Tools zur Verwaltung von Benutzern.



Sicherheit

Ein Punkt, der bisher bei allen Microsoft-Produkten bemängelt wurde, ist die Sicherheit sowie die Tatsache, wie leicht sich die vorhandenen Sicherheitsfunktionen umgehen lassen. Es gibt mindestens ein Programm, das verschlüsselte Kennwörter abfangen und entschlüsseln kann, die über das Netzwerk versandt werden. Außerdem gibt es zahlreiche andere Themen hinsichtlich der Verschlüsselung und Privatheit von Daten, die sich mit einer guten Verschlüsselungsgrundlage lösen lassen.

Windows 2000 behebt einen großen Teil der Sicherheitsprobleme, die in früheren Versionen von Windows vorhanden waren. Die passenden Netzwerkeinstellungen sorgen dafür, dass Windows 2000 keine verschlüsselten Kennwörter über das Netzwerk versendet, sondern Kerberos zur Authentifizierung verwendet. Kerberos benutzt ein Challenge-Response-System, bei dem kein Kennwort an den Server gesendet werden muss.

Das Kerberos-Sicherheitssystem

Kerberos ist ein Sicherheitssystem, das für die Verwendung unsicherer Kommunikationsmedien entwickelt wurde, wie z.B. ein WAN (Wide Area Network) wie das Internet oder auch ein LAN (Local Area Network), bei dem die Datensicherheit oberste Priorität hat.

Bei den traditionellen Systemen muss der Benutzer bei der Authentifizierung in einem Netzwerk einen Benutzernamen und ein Kennwort eingeben, die dann zu einem Server gesendet werden. Der Server gleicht den Benutzernamen und das Kennwort mit einer Liste ab. Höher entwickelte Systeme wie Windows NT übertragen noch immer das Kennwort, verschlüsseln dies aber vor der Übertragung. Bei beiden Verfahren wird das Kennwort über das Netzwerk zu einem Server gesendet. Selbst wenn das Kennwort verschlüsselt ist, besteht eine hohe Wahrscheinlichkeit, dass ein Mitarbeiter des Unternehmens die Netzwerkpakete, die Benutzernamen und Kennwort enthalten, abfängt und diese benutzt, indem sie entweder entschlüsselt oder die alten Pakete später zur Authentifizierung an einen Server gesendet werden.

Wenn Sie bezweifeln, dass eine Entschlüsselung der Kennwörter möglich ist, sollten Sie die Site www.l0pht.com aufsuchen. Dort finden Sie ein Programm namens *L0phtCrack*, das das Netzwerk überwacht, Pakete abfängt, die Kennwörter enthalten und diese dann mit einem Wörterbuch-Ansatz (bei dem geprüft wird, ob das Kennwort in einem Wörterbuch enthalten ist) und einem Brute-Force-Ansatz entschlüsseln. Das Programm ist sehr schnell und kann die meisten Kennwörter in wenigen Stunden entschlüsseln.

Wenn sich sowieso alle Kennwörter irgendwie entschlüsseln lassen, wie lässt sich ein Netzwerk dann sichern? Es läuft auf das folgende Problem hinaus: Die Workstation muss dem Server beweisen, dass sie das Kennwort kennt, ohne dieses über das Netzwerk übertragen zu müssen. Und wie funktioniert das? Die Workstation verwendet das Kennwort im Wesentlichen als Schlüssel für eine mathematische Funktion. Der Server sendet dann eine Frage über das Netzwerk zur Workstation. Die Workstation verwendet die mathematische Funktion, die sie mit dem Kennwort erzeugt hat und die Frage, die vom Server gestellt wurde, und übermittelt die resultierende Nummer an den Server. Es gibt natürlich noch zahlreiche Einzelheiten (Wie werden die Kennwörter verändert? Wie stellt der Server sicher, dass die Antwort von der richtigen Workstation stammt?), aber das Grundkonzept ist klar. Weitere Informationen bietet eine großartige, nicht sehr technisch gehaltene, leicht verständliche Beschreibung des gesamten Systems, die Sie unter dem folgenden URL finden:

<http://web.mit.edu/kerberos/www/dialogue.html>



Darüber hinaus implementiert Windows 2000 eine Public-Key-Verschlüsselung zur Verschlüsselung und Entschlüsselung von Daten. Bei der Public-Key-Verschlüsselung werden zwei Informationen benötigt, um eine Nachricht zu entschlüsseln: ein öffentlicher und ein privater Schlüssel. Der öffentliche Schlüssel wird veröffentlicht und ist allgemein verfügbar. Der private Schlüssel wird geheim gehalten. Wenn ein Benutzer eine Nachricht an einen anderen Benutzer senden möchte und nur dieser die Nachricht lesen können soll, muss er die Nachricht mit dem öffentlichen Schlüssel des Empfängers verschlüsseln. Wenn

der Benutzer dem Empfänger zeigen möchte, dass die Nachricht nicht gefälscht wurde, kann die Nachricht mit dem privaten Schlüssel des Senders verschlüsselt werden. Um die Nachricht zu entschlüsseln, benötigt der Empfänger dann den öffentlichen Schlüssel des Senders, mit dem sichergestellt wird, dass die Nachricht vom Empfänger stammt und seinen eigenen privaten Schlüssel, um die Nachricht zu entschlüsseln. Die Public-Key-Verschlüsselung stellt also sicher, dass Nachrichten weder unberechtigt gelesen noch gefälscht werden können.

Ein weiteres neues Feature ist das EFS (Encrypted File System). Eine Datei oder ein Verzeichnis lässt sich verschlüsseln. Anschließend kann nur der Benutzer darauf zugreifen, der es verschlüsselt hat. EFS steht nur auf Partitionen zur Verfügung, die mit dem Dateisystem NTFS formatiert wurden und funktioniert genauso wie die Komprimierungsfunktionen von NTFS. Mehr zu EFS finden Sie in Kapitel 4.

Windows 2000 implementiert Schnittstellen zu Smartcard-Lesegeräten. Dies bietet eine erhöhte Sicherheit, weil dann Benutzer nicht autorisiert werden, die einfach nur ein Kennwort kennen. Die Smartcard in Kombination mit einem Kennwort bietet ein hohes Maß an Sicherheit. Selbst dann, wenn eine Person das Kennwort ausspioniert hat und unberechtigt auf das System zugreifen möchte, benötigt sie zusätzlich noch die Smartcard. Ein Diebstahl der Smartcard alleine reicht ebenfalls nicht aus, da der Eindringling das korrekte Kennwort kennen muss. Smartcards haben eingebaute Sicherungen, die sie fälschungssicher machen. Sie lassen sich außerdem nur sehr schwer kopieren. In Windows 2000 ist eine Smartcard-Infrastruktur integriert und die Installation hängt von den Lesegeräten der verschiedenen Hersteller ab.

Ein weiteres neues Feature ist IPSec, das Internet Protocol Security-System. IP ist das Protokoll, auf das sowohl TCP als auch UDP aufsetzen. IPSec bietet eine End-to-End-Verschlüsselung und eine Überprüfung des Inhalts von Netzwerkpaketen. Weitere Informationen zu IPSec finden Sie in Kapitel 24.

Speicher und Dateisystem

Windows 2000 bietet verschiedene Funktionen für einen leichten Zugriff auf Speichermedien. Der Remotespeicher-Dienst erlaubt den Zugriff auf Archivierungsmedien wie Sicherungsbänder und optische Platten so, als wären sie online. Das System lädt dabei automatisch die korrekte Datei vom Archivierungsmedium.

Außerdem wurde die Unterstützung für Bibliotheken von Bandlaufwerken und Roboter-Medienwechsler verbessert. Der Remotespeicher-Dienst katalogisiert Cartridges und Bänder. Dadurch lassen sie sich später leicht finden. Dieses System arbeitet mit dem Remotespeicher-Server und dem verbesserten Sicherungsprogramm zusammen.

Windows 2000 führt ein einzigartiges und integriertes Datenträgerquotensystem ein. Dieses erlaubt die Zuweisung von Festplattenspeicher an Benutzer und Benutzergruppen. Wobei verschiedene Warnhinweise an jene Benutzer ausgegeben werden, die zu viel Festplattenspeicher verbrauchen. Außerdem werden den Benutzern verschiedene Beschränkungen auferlegt. Solche Systeme gibt es für UNIX und Novell NetWare bereits seit langem und wurden nun auch in Windows 2000 übernommen.

Das verteilte Dateisystem (DFS = Distributed File System) erlaubt die Verteilung von wichtigen und häufig benötigten Dateien über ein Netzwerk, wobei die Benutzer wie gewohnt auf die Dateien zugreifen können. Das heißt, eine Datei kann auf verschiedenen Servern im Netzwerk gespeichert werden, aber die

Benutzer greifen immer unter demselben Namen auf die Datei zu und benutzen die Datei, die auf dem nächst gelegenen Server liegt.

Kapitel 4 bietet eine ausführliche Beschreibung dieser Punkte. Dort wird gezeigt, wie ein hochleistungsfähiges Dateisystem eingerichtet und gewartet werden kann und auf welche Weise sich Features wie beispielsweise ein Remotespeicher-Server implementieren lassen.

Netzwerkfunktionen und Kommunikation

Was wäre ein Server ohne die Möglichkeit, mit Workstations zu kommunizieren? Ein Türstopper. Glücklicherweise implementiert Windows 2000 Server die üblichen Protokolle, die Windows 2000 Server unter den anderen Betriebssystemen hervorhebt. Selbstverständlich gibt es eine umfangreiche Unterstützung von Protokollen wie TCP/IP, IPX/SPX und sogar das »berüchtigte« NetBEUI. Außerdem lassen sich Protokolle von Drittanbietern und selten genutzte Protokolle leicht installieren, da Protokolle als installierbare Komponenten implementiert sind.

Windows 2000 enthält auch einen Multiprotocol-Routingmechanismus. Wenn mehrere Netzwerkgeräte in einem Server installiert sind, kann dieser als Router zwischen den verschiedenen Diensten agieren und Daten zwischen den Netzwerken verschieben.

Ein weiteres Feature, das stark verbessert wurde, ist RAS (Remote Access Services). Beispielsweise wurde diese Funktion um das so genannte Virtual Private Networking (VPN) erweitert. RAS bietet Windows 2000 Server die Möglichkeit, Verbindungen von anderen Quellen wie Modems, ISDN-Adapter und sogar Standard-Internetverbindungen entgegen-zunehmen. Der Computer auf der anderen Seite der Verbindung kann dann so agieren, als wäre er lokal verbunden. Bedingt durch die beschränkte Bandbreite ist die Verbindung jedoch etwas langsamer. VPN bietet die Möglichkeit, eine Verbindung von einem Punkt im Internet aus zu einem Windows 2000 Server-Computer herzustellen und auf die gleiche Weise auf die Netzwerkfunktionen zuzugreifen, als wäre der Computer in das lokale Netzwerk integriert. VPN verschlüsselt außerdem die Pakete, die an das Internet gesendet werden, um die Sicherheit zu erhöhen.

Windows 2000 unterstützt ATM-Adapter (ATM = Asynchronous Transfer Mode, dt. asynchroner Übertragungsmodus). ATM ist eine Netzwerktechnologie, um die Daten, die in Pakete aufgeteilt werden, in Echtzeit über das Netzwerk zu übertragen.

Die Netzwerkinfrastruktur von Windows 2000 unterstützt auch einen QoS-Zugangssteuerungsdienst (QoS = Quality of Service). Über diesen Dienst erhalten bestimmte Netzwerkadressen und Pakettypen eine höhere Priorität als andere Arten der Kommunikation. Das heißt, dass die eigentliche Arbeit, die in einem Unternehmen verrichtet wird, den Vortritt vor Video- und Musikdaten hat, die über das Internet in das Unternehmen hereinströmen.

Weitere Informationen zu Netzwerkfunktionen finden Sie in Kapitel 8 und in den Kapiteln 13 bis 16. Kapitel 13 beschreibt das lästige Thema der Suche im Netzwerk. Kapitel 14 erläutert Routing und RAS (RRAS = Routing and Remote Access Services). Kapitel 15 veranschaulicht die Arbeit mit Multiprotocol-Umgebungen und Kapitel 16 zeigt, wie Client-Workstations mit Servern interagieren.

Anwendungsdienste

Windows 2000 bietet einige Funktionen, dank derer sich Anwendungen intelligenter verhalten und die Daten schneller zurückliefern. *Windows Scripting Host* (WSH) ist ein Dienst, der Skripte ausführt, die in verschiedenen Skriptsprachen wie VBScript und JavaScript geschrieben sind. Die Skripte können remote ausgeführt werden, sodass der Server Aufgaben für die Client-Workstations verrichten kann. Außerdem bietet der *Indexdienst* einen zentralen Ort für die Suche nach Dokumenten, die bestimmte Informationen enthalten. Der Indexdienst durchsucht alle Dateien auf dem Server, protokolliert, was in den Dateien enthalten ist und organisiert die Informationen so, dass der Benutzer sie leicht finden kann.

Außerdem stellt Windows 2000 das weit verbreitete Win32-API mit allen entsprechenden Erweiterungen zur Verfügung, sodass sämtliche Win32-Anwendungen, die für frühere Windows-Versionen geschrieben wurden, unverändert unter Windows 2000 laufen. Besonders wichtig für die Benutzer von Windows 2000 Server ist, dass alle aktuellen BackOffice-Programme und andere Serveranwendungen wie SQL Server und Exchange Server problemlos funktionieren. Windows 2000 bietet sogar eine hohe Integration von Exchange, indem sich die Windows 2000-Benutzergruppen in Exchange-Verteilerlisten umwandeln lassen und umgekehrt.

Symmetric Multiprocessing (SMP)

Die gesamte Windows 2000-Produktlinie - von Windows 2000 Professional bis Windows 2000 Datacenter Server - unterstützt den Einsatz mehrerer Prozessoren:

- Windows 2000 Professional - 2 Prozessoren
- Windows 2000 Server - 4 Prozessoren
- Windows 2000 Advanced Server - 8 Prozessoren
- Windows 2000 Datacenter Server - 32 Prozessoren

Was bewirkt SMP? SMP sorgt nicht dafür, dass alles schneller läuft, sondern die Programme müssen auf die Verwendung mehrerer Prozessoren ausgelegt sein, um diese gleichzeitig nutzen zu können. Das herausragende Merkmal an SMP ist jedoch, dass ein Programm, das auf mehreren Prozessoren ausgeführt werden kann, nicht wissen muss, wie viele Prozessoren vorhanden sind und selbst auf Systemen läuft, die nur mit einem Prozessor ausgestattet sind. Deshalb müssen die Programme nicht neu geschrieben werden und in den meisten Fällen lässt sich eine Programmversion auf Systemen mit einem oder mehreren Prozessoren ausführen, ohne neu kompiliert werden zu müssen.

Einfache Bedienung durch Windows 95/98-Oberfläche

Die neue Benutzeroberfläche basiert auf der im Internet Explorer 5 eingebauten Technologie und wird konsistent in allen Versionen von Windows 2000 verwendet. Manche Features wurden aus Windows 95/98 übernommen, wie z.B. die sinnbildliche Darstellung eines Arbeitsplatzes mit einem **Start**-Menü. Es gibt aber auch Features, die es in Windows 95/98 nicht gibt, wie z.B. Menüs, die aus- und eingeblendet werden sowie der Schatten beim Mauszeiger, die von der Grafikkarte im Server abhängen.

Windows 2000 muss auch nicht so häufig neu gestartet (gebootet) werden wie frühere Versionen von Windows NT. In Windows NT 4.0 ist selbst bei der geringsten Änderung von Einstellungen ein Neustart erforderlich und Hardware lässt sich schon gar nicht in ein laufendes System einbauen. Windows 2000 reduziert die Anzahl der Neustarts und unterstützt Plug&Play-Technologien von PC Cards und USB bis

zu Hot-Plug-PCI-Slots.

Sicherung und Wiederherstellung von Daten

Windows 2000 verfügt über ein ganz neues Programm zur Sicherung und Wiederherstellung von Daten. Selbstverständlich bietet das Programm grundlegende Funktionalitäten, die von einem zeitgemäßen Programm zu erwarten sind, wie hohe Leistung, die Fähigkeit, mit Medienwechslern zusammenzuarbeiten und die Möglichkeit, vollständige, inkrementelle und differenzielle Sicherungen durchzuführen. Zu den Verbesserungen gehört die neue Speicherverwaltung von Remotespeicher, die im Wesentlichen Unterstützung für Medienwechsler und Bibliotheken für Bandlaufwerke bietet.

Diese Features haben alle Windows 2000 Server-Produkte gemeinsam, und sind entsprechend auch beim Produkt Windows 2000 Server vorhanden. Windows 2000 Advanced Server und Windows 2000 Datacenter Server bieten sogar eine noch höhere Funktionalität.

1.2.2 Windows 2000 Advanced Server

Windows 2000 Advanced Server weist einige Features auf, die umfangreiche Anwendungen oder Server benötigen, um ihr volles Potenzial auszuschöpfen. Windows 2000 Advanced Server ist mit einem Clusterdienst ausgestattet. Anwendungen lassen sich mit der Clusterverwaltung auf zwei Servern einrichten und werden auf einem Server ausgeführt. Bei einem Komplettausfall, der z.B. durch ein Hardware-Versagen, durch Probleme des Betriebssystems oder durch den Absturz einer Anwendung bedingt sein kann, übernimmt der zweite Server die Funktion des ersten und setzt die Datenverarbeitung fort.



Hier ein kleiner »historischer Rückblick«: Die Bezeichnung Advanced Server stammt ursprünglich von Windows NT 3.1 Advanced Server, der Serverversion von Windows NT 3.1. Die Workstationversion von Windows NT 3.1 hieß einfach Windows NT 3.1. Die meisten Leute, die seit damals mit Windows NT arbeiten, freuen sich darüber, dass die Bezeichnung Advanced Server nun wieder aufgegriffen wurde, fast genauso sehr, wie sie die Bezeichnung Windows 2000 ablehnen.

Außerdem bietet Windows 2000 Advanced Server einen Lastenausgleich in der Netzwerk- und der Komponentenschicht. Dies bedeutet, dass mehrere Netzwerkkarten in ein System eingebaut werden können und die Last zwischen diesen gleichmäßig verteilt wird. Mit der Microsoft Transaction Server-Technologie kann Windows 2000 Advanced Server auch mehrere Server nutzen, um die Arbeitslast des Servers auf mehrere Server zu verteilen.

Hardware-Skalierbarkeit

Windows 2000 Advanced Server unterstützt bis zu acht Prozessoren bei Hardware, die SMP unterstützt. Außerdem kann Windows 2000 Advanced Server bis zu 4 Gbyte RAM nutzen, und Anwendungen, die dies unterstützen, können bis zu 3 Gbyte des Anwendungsspeichers adressieren.

Windows-Terminaldienste

Die Terminaldienste, die in Windows 2000 Advanced Server enthalten sind, bieten »schlanken« Clients (oder veralteter Hardware) die Möglichkeit, auf Programme zuzugreifen, die auf dem Server ausgeführt

werden. Die Programme werden dabei genau gleich dargestellt wie auf dem Server. Viele dieser schlanken Geräte, die auch als *Windows-Terminals* bezeichnet werden, sind Computer ohne Festplatte, die lediglich mit einer Tastatur, einer Maus, einem Monitor und einer Netzwerkverbindung ausgestattet sind. Die eigentliche Datenverarbeitung erfolgt zentral auf dem Server. Es gibt verschiedene solcher schlanken Clients, wie die bereits erwähnten Windows-Terminals und Geräte, die unter Windows CE ausgeführt werden. Selbst normale PCs können von der Computerleistung profitieren, die auf einem Server verfügbar ist.

1.2.3 Windows 2000 Datacenter Server

Windows 2000 Datacenter Server ist die High-End-Version von Windows 2000 Server. Sie bietet alle Features von Windows 2000 Advanced Server, unterstützt aber bis zu 32 Prozessoren. Außerdem bietet Windows 2000 Datacenter Server eine fortgeschrittene Clusterverwaltung, die über die einfache Übernahme beim Systemausfall hinaus in den Bereich des echten Lastenausgleichs geht. Windows 2000 Datacenter Server wird erst im Anschluss an die Produkte Windows 2000 Server und Advanced Server verfügbar sein.

© Copyright [Markt+Technik Verlag](#), ein Imprint der Pearson Education Deutschland GmbH
Elektronische Fassung des Titels: Windows 2000 Server Kompendium, ISBN: 3-8272-5611-9 Kapitel:
Einführung in Windows 2000

Die Betriebssystemumgebung von Windows 2000

Teil I

2. [Architektur](#)
3. [Installation](#)
4. [Dateisysteme](#)
5. [Netzwerke](#)
6. [Drucken](#)
7. [Die Registrierung](#)
8. [TCP/IP-Netzwerke](#)

Kapitel 2 Architektur

Bestimmte Aufgaben müssen alle Betriebssysteme erfüllen. Ein Betriebssystem muss Speicherressourcen zuweisen, den Zugriff auf Treiber kontrollieren und den Wechsel zwischen Programmen behandeln, die momentan aktiv sind oder warten. Windows 2000 ist da keine Ausnahme. Der Prozess funktioniert bei der gesamten Windows 2000 Serverfamilie gleich. Deshalb bietet dieses Kapitel einen allgemeinen Überblick über die Funktionsweise des Betriebssystems - unabhängig von den Diensten und zum größten Teil unabhängig von der zugrunde liegenden Hardwareplattform. Um die Analyse zu erleichtern, wird das Betriebssystem dabei in kleinere Einheiten unterteilt:

- Die Architektur der Teilsysteme und des Kernels
- Die Dienste der Ausführungsschicht (Executive)
- Die Teilsysteme
- Das Speichermodell und die Speicherverwaltung

Werfen wir zunächst einen Blick auf die Architektur der Teilsysteme und des Kernels, dem Herzen von Windows 2000.

2.1 Die Architektur der Teilsysteme und des Kernels

Als das Betriebssystem noch in den Kinderschuhen steckte und »Windows NT 3.5« hieß, kämpften verschiedene Betriebssysteme um die Vorherrschaft. Windows NT war der Newcomer unter den Rivalen OS/2 und UNIX. Microsoft wusste auch, dass der Markt für 32-Bit-Windows-Anwendungen zunächst nur langsam wachsen würde. Deshalb war Windows NT ursprünglich auf den Betrieb verschiedener *Teilsysteme* oder Subsysteme ausgelegt, die die Ausführung von Programmen von verschiedenen Betriebssystemen aus ermöglichten. Windows NT erlaubt Programmen, die diese Teilsysteme verwenden, die gleichzeitige Ausführung und den gemeinsamen Zugriff auf Ressourcen wie die CPU-Zeit, Festplattenlaufwerke und Bildschirme, wobei dafür gesorgt wird, dass das fehlerhafte Verhalten eines Programms die anderen Programme nicht negativ beeinflusst.

Die Teilsysteme wurden so programmiert, dass sie, wenn ein Programm Gefahr lief, Amok zu laufen und die Integrität des Teilsystems des Hosts zu zerstören drohte, nicht das gesamte Betriebssystem zum Absturz bringen und die anderen Teilsysteme nicht beeinflussen sollten.

Damit die Teilsysteme unabhängig voneinander arbeiten können, muss es einen zentralen Zuweisungsmechanismus (oder *Kernel*) und zahlreiche andere Systeme geben, die zusammenarbeiten, um die grundlegenden Dienste bereitzustellen. Der Prozessor muss in der Lage sein zu verhindern, dass Anwendungen Speicher überschreiben, der vom Kernel und anderen Diensten genutzt wird. Dies wurde durch Implementierung eines Benutzer- und eines Kernelmodus erreicht. Um zu verhindern, dass der Kernel und die Ausführungsschicht Probleme bei der Hardware verursachen und um den Wechsel zwischen verschiedenen Prozessorarchitekturen zu erleichtern, muss die gesamte Interaktion mit der Hardware über die Hardwareabstraktionsschicht (HAL = Hardware Abstraction Layer) erfolgen. Außerdem muss der Kernel in der Lage sein, die Zeitplanung für Prozesse durchzuführen, Speicher zu

verwalten und die Steuerelemente für die Sicherheit zu verstärken. Schließlich haben die Teilsysteme auch noch die Dienste, die sie Anwendungen bereitstellen müssen und die Anwendungsprogrammierungsschnittstellen (API = Application Programming Interface), die sie benötigen, um mit dem Benutzer zu interagieren. Die Abbildung 2.1 bietet Ihnen einen Überblick über das, was in den nächsten Abschnitten behandelt wird.

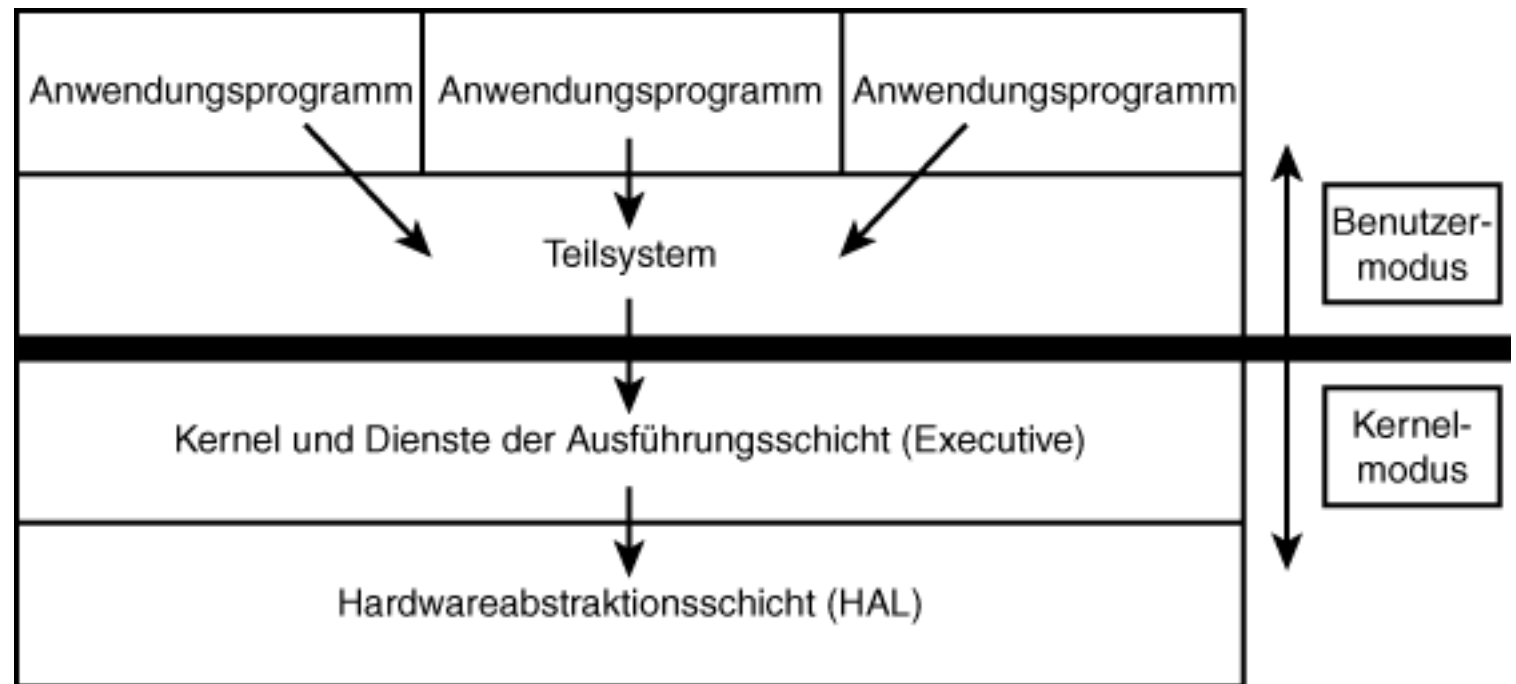


Abbildung 2.1: Die grundlegende Architektur von Windows 2000. Alle Schichten unterhalb der Anwendungsschicht werden in den nachfolgenden Abschnitten ausführlich beschrieben.

2.1.1 Benutzermodus und Kernelmodus

Windows 2000 benutzt zwei verschiedene Prozessormodi. Ein Modus namens *Kernelmodus* führt die Dienste der Ausführungsschicht aus und der andere Modus namens *Benutzermodus* führt die Anwendungsprogramme aus.

Die Dienste des Kernelmodus werden vom Prozessor geschützt. Die Dienste des Benutzermodus werden vom Betriebssystem geschützt. Dabei wird verhindert, dass Programme, die im Benutzermodus ausgeführt werden, Speicher überschreiben, der von Programmen benutzt wird, die im Kernelmodus ausgeführt werden. Der Prozessor verhindert, dass Programme, die im Kernelmodus ausgeführt werden, Daten in den Adressraum schreiben, in dem Programme gespeichert sind. Außerdem ruft der Prozessor eine Kernelmodus-Ausnahme hervor, die Windows 2000 in einen »blauen Bildschirm« (BSOD = Blue Screen of Death) umsetzt. Der blaue Bildschirm enthält Text, anhand dessen der Support von Microsoft herausfinden kann, was mit dem Computer los ist. Normalerweise wird ein blauer Bildschirm durch einen fehlerhaften Treiber verursacht, der versucht, Daten an eine unzulässige Stelle zu schreiben.



Wenn der Kernelmodus um so viel zuverlässiger ist, warum wird dann nicht alles im Kernelmodus ausgeführt? Die Antwort darauf ist einfach und einleuchtend zugleich: Die Programmierung von Komponenten, die im Kernelmodus ausgeführt werden, ist erheblich aufwändiger. Neue Releases würden dann noch später erscheinen als bisher. Ein Komödiant fragte einmal, »Warum besteht nicht das gesamte Flugzeug aus demselben Material wie der Flugschreiber?«. Wenn das Flugzeug aus diesem Material bestünde, wäre es zu schwer, um überhaupt fliegen zu können. Andere Frage, gleiche Antwort: Wenn alles im Kernelmodus ausgeführt würde, müssten Programme so umfangreich sein, um alle möglichen Ausnahmen zu behandeln, dass sie niemals erscheinen würden. Deshalb müssen wir uns damit abfinden, dass Programme eventuell abstürzen können.

Bei Windows 2000 wird so viel wie möglich im Benutzermodus ausgeführt. Dadurch reduziert sich die Menge des höchst kritischen Codes, der im Kernelmodus ausgeführt wird, und der Code wird leichter handhabbar. Der Unterschied zwischen einem Absturz eines Programms im Benutzermodus und einem im Kernelmodus ist, dass ein Benutzermodusprogramm ein Ereignis in das Ereignisprotokoll einträgt und die restlichen Programme davon unberührt bleiben. Wenn ein Kernelmodusprogramm ein Problem hat, bricht der Server mit einem blauen Bildschirm ab. Werfen Sie einen Blick auf Abbildung 2.1. Die Komponenten unterhalb der Linie werden im Benutzermodus ausgeführt.

Beginnend mit Windows NT 4.0 werden Teile des Win32-Teilsystems, insbesondere die Benutzer- und GDI-Teile, im Kernelmodus ausgeführt. Dies war eine etwas kontroverse Entscheidung, die im Abschnitt zum Win32-Teilsystem ausführlicher beschrieben wird.

Benutzermodusprogramme kommunizieren mit dem Kernel über spezifische Anwendungsprogrammierungsschnittstellen (APIs = Application Programming Interfaces). Diese APIs dienen dazu, einen stabilen Kommunikationsmodus zwischen den verschiedenen Programmen, die ausgeführt werden, und dem Betriebssystem zu definieren.

Der Rest des Kernelmodus ist in drei Teile aufgeteilt. Die Hardwareabstraktionsschicht (HAL = Hardware Abstraction Layer) bietet eine konsistente Schnittstelle zur Hardware, der Kernel ist der Motor des Ganzen und die Dienste der Ausführungsschicht (Executive Services) verwalten die grundlegenden Operationen wie die Sicherheit, die Zeitplanung für Tasks und den Speicher.

2.1.2 Die Hardwareabstraktionsschicht

Windows 2000 ist portierbar, was bedeutet, dass es auf verschiedenen Hardwareplattformen laufen kann. Windows NT war für Alpha-Systeme, MIPS und den PowerPC verfügbar. Die Nachfrage war jedoch nicht groß genug, um den Produktionsaufwand zu rechtfertigen.

Windows 2000 ist portierbar, weil es fast komplett in C++ geschrieben ist und C++-Compiler zu den ersten Compilern gehört, die für neue Prozessoren geschrieben werden. Die Teile von Windows 2000, die nicht in C++ geschrieben sind, sind in der Assemblersprache der Hardwareplattform geschrieben, auf die Windows 2000 portiert wurde. Diese Teile sind in der so genannten *Hardwareabstraktionsschicht* (HAL) enthalten.

Dabei handelt es sich um den einzigen Bestandteil des Betriebssystems, der direkt mit der Hardware interagiert. Die Interaktion erfolgt über eine feste Schnittstelle zum darüber liegenden Kernel und eine

Maskierung der Unregelmäßigkeiten der darunter liegenden Hardware. Deshalb muss der Kernel nichts über die Besonderheiten der Hardware wissen und auch nicht so stark geändert werden, wenn eine Portierung auf eine andere Hardwareplattform erfolgt.

Die Hardwareabstraktionsschicht präsentiert dem Kernel eine abstrakte Sicht der Hardware, sodass der Kernel nicht neu geschrieben werden muss, um einen anderen Prozessor nutzen zu können. Der Kernel muss nur wissen, wie er auf einen bestimmten Prozessortyp zugreift. Dies ist der Typ, den die Hardwareabstraktionsschicht bereitstellt. Die Hardwareabstraktionsschicht behandelt die Anforderungen des Kernels und wandelt diese in Anweisungen um, die der Prozessor verarbeiten kann.

Die Hardwareabstraktionsschicht bietet die Grundlage für die Unterstützung des symmetrischen Multiprocessing (SMP). Es weiß, wie der Prozessor benutzt wird und präsentiert dem Kernel einfach - falls vorhanden - mehrere Prozessoren. Wenn ein Computer mit mehreren Prozessoren ausgestattet wird, muss die Hardwareabstraktionsschicht ersetzt werden. Bei den meisten Systemen, insbesondere Serversystemen, ist eine Programmdiskette vorhanden, die eine vom Hardwarehersteller bereitgestellte Hardwareabstraktionsschicht installiert, um die Unterstützung von SMP zu aktivieren.

Noch ein wichtiger Hinweis:

Die Hardwareabstraktionsschicht ist der einzige Bestandteil des Systems, der direkt mit der Hardware kommunizieren kann, und der Kernel ist der einzige Teil des Systems, der direkt mit der Hardwareabstraktionsschicht kommuniziert. Dies reduziert die Probleme mit der Hardware und erhöht die Sicherheit, weil zerstörerische Anwendungen den Kernel und die Hardwareabstraktionsschicht umgehen müssen, um Probleme bei der Hardware zu verursachen.



2.1.3 Der Kernel

Der *Kernel* ist unter architektonischen Gesichtspunkten der zentrale Bestandteil des Betriebssystems. Bei Windows 2000 wird ein *Mikrokernel-Design* eingesetzt, was bedeutet, dass der Kernel nur ein Minimum der Funktionalität bereitstellt und darauf baut, dass andere Dienste zusätzliche Funktionalität liefern. Der Kernel ist hauptsächlich dafür verantwortlich festzulegen, was der Prozessor als Nächstes ausführt.

Wenn ein Programm ausgeführt wird, ist dies mit einem Prozess verknüpft und ein Prozess besitzt mindestens einen Thread. Ein *Prozess* besteht aus Speicherplatz und mindestens einem Thread. Der *Thread* ist das, was tatsächlich ausgeführt wird. Er ist der »Programm«-Teil der Anwendung und der Prozess setzt sich aus dem Programm und den Daten zusammen, mit denen das Programm arbeitet. Der Unterschied zwischen einem Prozess und einem Thread ist, dass nicht dem Prozess vom Betriebssystem Prozessorzeit zugeteilt wird, sondern dem Thread. Vereinfacht ausgedrückt bedeutet dies: Nicht Prozessen, sondern Threads wird vom Betriebssystem Ausführungszeit zugeteilt.

Der Kernel kennt drei Arten von Aufgaben. Erstens legt er die Zeitplanung für die Ausführung von Threads fest. Jedem Thread wird eine Priorität im Bereich zwischen 0 und 31 zugeordnet. Der Kernel nimmt den Thread mit der höchsten Priorität, der unbedingt ausgeführt werden muss, und gestattet, dass dieser Thread für eine bestimmte Zeitdauer auf einem Prozessor ausgeführt wird. Am Ende dieser Zeitdauer betrachtet der Kernel wieder die Threadliste und wählt den Thread mit der höchsten Priorität zur Ausführung aus. Enthält das System mehrere Prozessoren, wird für jeden Prozessor, basierend auf der Priorität, ein Thread ausgewählt.

Eine weitere Aufgabe des Kernels ist das *Interrupt Handling*. Wenn ein Gerät, wie z.B. eine Festplatte, aufgefordert wird, Daten zu lesen, wird die Anforderung an die Festplatte gesendet. Die Festplatte ruft die Daten ab und benachrichtigt dann den Kernel, indem sie veranlasst, dass ein Interruptsignal an einen Prozessor gesendet wird. Wenn ein Interrupt auftritt, unterbricht der Kernel automatisch den Prozess, der auf einem Prozessor ausgeführt wird, behandelt den Interrupt und liefert dann die Kontrolle wieder an den Prozess zurück, der unterbrochen (preempted) wurde.

Die dritte Art von Aufgaben, die das System behandeln muss, ist die Behandlung von *Kernelausnahmen*. Wenn etwas passiert und ein Programm, das im Kernelmodus ausgeführt wird, eine Schutzverletzung oder eine andere Art von Fehler verursacht, versucht der Kernel, den Fehler zu behandeln. In einigen Fällen kann der Kernel den Fehler problemlos beheben. Manchmal ist das aber auch nicht möglich, dann ist mal wieder BSOD-Zeit, d.h. der blaue Bildschirm mit dem Speicherabbild wird angezeigt.

2.1.4 Die Windows 2000-Ausführungsschicht

Ein Betriebssystem hat zahlreiche unterschiedliche Pflichten zu erfüllen, um Anwendungen eine entsprechende Ausführungsumgebung zu bieten. Das Mikrokernel-Design von Windows 2000 legt fest, dass der Kernel nur grundlegende Dienste wie den Taskwechsel behandelt. Die restlichen Dienste werden natürlich auch ausgeführt, nur nicht vom Kernel. Die meisten wurden in die Windows 2000-Ausführungsschicht (*Executive*) ausgelagert. Diese enthält entsprechend zahlreiche Dienste für die unterschiedlichsten Aufgaben.

Die Windows 2000-Ausführungsschicht wird im Kernelmodus ausgeführt. Sie hat uneingeschränkten Zugriff auf den Kernel und die E/A-Geräte. Die meisten Benutzeranwendungen greifen nicht direkt auf die Ausführungsschicht zu, sondern benutzen ein Teilsystem, wie z.B. das Win32-Teilsystem, das die Dienste der Ausführungsschicht aufruft. Die Abbildung 2.2 zeigt die verschiedenen Komponenten der Windows 2000-Ausführungsschicht.

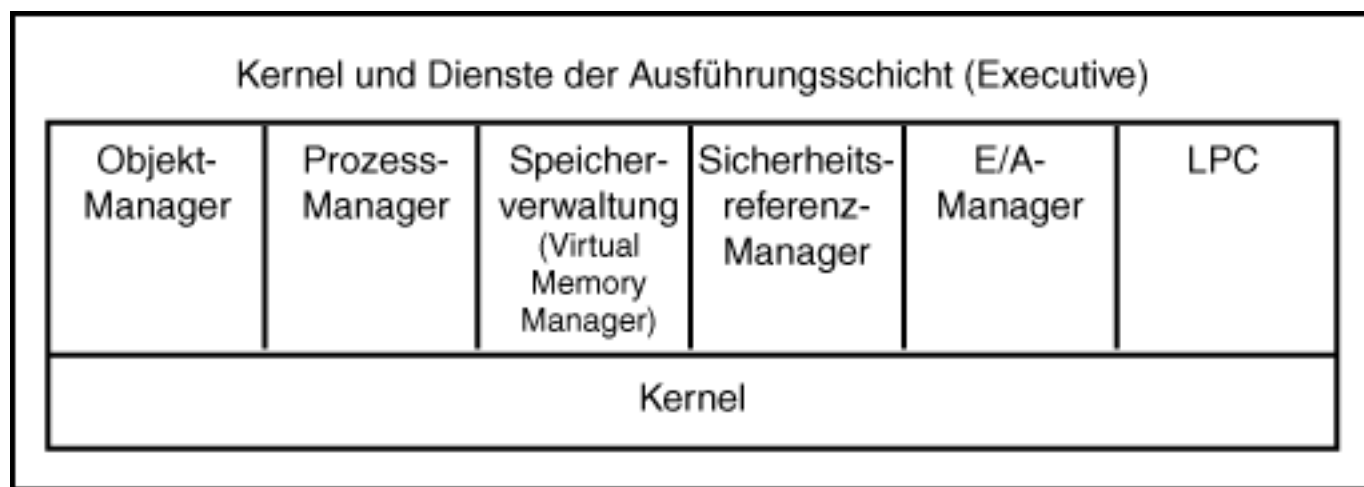


Abbildung 2.2: Diese Teile der Windows 2000-Ausführungsschicht stellen in ihrer Kombination die grundlegenden Betriebssystemdienste bereit

Die Ausführungsschicht behandelt die folgenden Dienste:

- Objekt-Manager
- Prozess-Manager

- Speicherverwaltung (Virtual Memory Manager)
- Sicherheitsreferenz-Manager
- E/A-Manager
- Funktionen für lokale Prozeduraufrufe (LPC = Local Procedure Call)

Die folgenden Abschnitte veranschaulichen die genaue Funktionsweise jedes dieser Dienste.

Der Objekt-Manager

Der Objekt-Manager ist sehr wichtig. Er dient dazu, Objekte zu erstellen, zu verwalten und zu löschen, die vom System benutzt werden. Der Objekt-Manager empfängt eine Anforderung für eine Ressource, wie z.B. ein serieller Anschluss (*Port*), und liefert ein Handle (Zugriffsnummer) für den seriellen Anschluss zurück. Das Handle beinhaltet eine Zugriffsmethode auf ein Objekt und Sicherheitsinformationen, die festlegen, wie der Zugriff auf das Objekt erfolgt.

Der Objekt-Manager liefert auch andere Arten von Handles zurück, wie z.B. Gerätehandles (für die seriellen und parallelen Anschlüsse), um Konflikte beim Zugriff auf die Geräte zu vermeiden.

Der Objekt-Manager kommuniziert extensiv mit dem Sicherheitsreferenz-Manager (SRM), der später besprochen wird. Der SRM erzeugt die Sicherheitsinformationen, die mit einem Handle verknüpft werden, bevor es an das aufrufende Programm zurückgeliefert wird.

Außerdem achtet der Objekt-Manager auf verwaiste Objekte. Wenn ein Programm auf einen seriellen Port zugreift und dann abstürzt, ist der Objekt-Manager dafür verantwortlich, das Handle zu finden, es zu schließen und die benutzten Ressourcen freizugeben.

Der Prozess-Manager

Der Prozess-Manager ist ein Vermittler zwischen dem Benutzer und dem Objekt-Manager. Seine Aufgabe besteht in erster Linie darin, Prozesse zu erzeugen und zu verwalten. Der Prozess-Manager nimmt Anforderungen für die Erzeugung von Prozessen entgegen, ruft den Objekt-Manager auf, um die Prozesse und ihre Threads zu erzeugen, und hält dann die Liste der Prozesse verfügbar.

Die Speicherverwaltung für den virtuellen Arbeitsspeicher

Wenn ein Prozess erzeugt wird, wird ihm ein 4-Gbyte-Adressraum zugewiesen. Dieser Adressraum beginnt bei 0 und endet bei 4 Gbyte. Bei Windows 2000 Professional und Windows 2000 Server werden 2 Gbyte Speicher für den Benutzeradressraum zugewiesen und 2 Gbyte für das System. Windows 2000 Advanced Server weist 3 Gbyte Benutzeradressraum und 1 Gbyte für das System zu.

Windows 2000 unterstützt den Speicherschutz wie folgt: Ein Programm kann keinen Speicher außerhalb des eigenen Adressraums adressieren. Wenn eine Anwendung einen Lesevorgang aus dem Speicher anfordert, behandelt die Speicherverwaltung (VMM = Virtual Memory Manager) den Mechanismus für den Abruf der Daten. Die virtuelle Speicherverwaltung unterhält eine Tabelle, um zu verfolgen, welche Teile des Adressraums eines Prozesses sich im physischen Arbeitsspeicher befinden und welche ausgelagert sind. Wenn ein Prozess Daten aus dem Speicher lesen muss, prüft die virtuelle Speicherverwaltung, ob sich die Daten tatsächlich im physischen Speicher befinden. Ist das nicht der

Fall, behandelt die virtuelle Speicherverwaltung den Abruf der Daten von der Festplatte. Der Abschnitt »Das Speichermodell und die Speicherverwaltung« weiter unten in diesem Kapitel geht näher auf die virtuelle Speicherverwaltung ein.

Der Sicherheitsreferenz-Manager

Der Sicherheitsreferenz-Manager (SRM) bildet die Grundlage für die Sicherheit in Windows 2000. Wenn sich ein Benutzer anmeldet, erzeugt der Anmeldeprozess ein Sicherheitstoken für den Benutzer. Immer dann, wenn der Benutzer den Zugriff auf ein Objekt anfordert, weist der Objekt-Manager den SRM an, das Token zu prüfen und festzustellen, welche Zugriffsberechtigungen der Benutzer erhalten soll. Der Objekt-Manager liefert das Handle auf das Objekt zurück, wobei die Zugriffsberechtigung Bestandteil des Handles ist.

Der E/A-Manager

Der E/A-Manager behandelt die Geräteein- und -ausgabe (E/A) für das System. Der E/A-Manager stellt seine Dienste Gerätetreibern und Anwendungen zur Verfügung, sodass die Gerätetreiber nicht wissen müssen, wie die Anwendungen sie benutzen werden. Und auch die Anwendungen müssen nicht wissen, wie die Geräte verwendet werden.

Der E/A-Manager behandelt beispielsweise alle Festplatten und Medien mit hoher Speicherkapazität als SCSI-Geräte. Wenn ein Hardwarehersteller dafür sorgen will, dass ein bestimmtes Gerät unter Windows 2000 läuft, muss er einen Treiber schreiben, den der E/A-Manager wie ein SCSI-Gerät behandeln kann, das eine stark standardisierte Schnittstelle bietet. Der Hersteller muss alle Aufrufe so übersetzen, dass die Hardware sie verstehen kann. Eine Anwendung muss nur wissen, wie das Teilsystem für einen Lesevorgang von der Festplatte aufgerufen wird. Das Teilsystem fordert dann den E/A-Manager auf, von der Festplatte zu lesen. Die Anwendung und das Teilsystem müssen nicht wissen, wie Daten von der Festplatte gelesen werden. Sie müssen nur wissen, was von der Festplatte gelesen werden soll.

Die Funktionen für lokale Prozeduraufrufe

Windows 2000 ist ein Client/Server-System. Was geschieht, wenn der Client und Serverprozesse auf demselben Computer ausgeführt werden? Eine Methode besteht in der Benutzung von entfernten Prozeduraufrufen (RPC = Remote Procedure Call), was einen ziemlich großen Overhead beinhaltet. Windows 2000 ist jedoch mit der Funktion der lokalen Prozeduraufrufe (LPC = Local Procedure Call) ausgestattet, was die Benutzung derselben Schnittstellen wie bei den RPCs gestattet, jedoch mit einem wesentlich geringeren Overhead. Dadurch kann das System schneller Antworten bieten, ohne die Schnittstelle ändern zu müssen.

2.1.5 Teilsysteme

Ein *Teilsystem* (auch *Subsystem* genannt) kann als Umgebung betrachtet werden, das zwischen dem Kernel und den Anwendungen sitzt und Programmen die Dienste und APIs zur Verfügung stellt, die diese erwarten. Dadurch können die Programme ausgeführt werden. Das Teilsystem benutzt die APIs gleichzeitig, um die benötigten Ressourcen beim Kernel anzufordern. Ein Teilsystem ist also im Wesentlichen ein Übersetzungsprogramm, das zwischen einer Gruppe von Anwendungen und dem Kernel sitzt.

Was ist ein API?

Ein API ist eine Anwendungsprogrammierungsschnittstelle (Application Programming Interface). Hilft Ihnen das noch immer nicht weiter? Ein API gestattet einem Programm die Kommunikation mit der Außenwelt. Ein Programm, das eine Verschlüsselung vornehmen muss, kann z.B. das CryptoAPI von Microsoft aufrufen, das Standardfunktionen für die Verschlüsselung enthält. Das Programm selbst muss nicht wissen, wie die Verschlüsselung durchgeführt wird. Diese wird vom API erledigt.

Ein API besteht aus einem Satz von Funktionen, die von Programmierern benutzt werden, um festzulegen, wie Programme interagieren. Der Einsatz eines API erlaubt es dem Hersteller der Schnittstelle (in diesem Fall Microsoft), deren Arbeitsweise zu ändern, ohne dass die Programme, die darauf zugreifen, geändert werden müssen.

Wenn Microsoft z.B. eine tolle neue Verschlüsselungsfunktion entwickelt, kann diese problemlos in das CryptoAPI integriert werden. Solange sich die Schnittstelle nicht ändert, können die Programme unverändert auf das CryptoAPI zugreifen.

Wichtig ist hier die Schnittstellenkonsistenz. Toaster haben z.B. eine konsistente Schnittstelle. Jeder Toaster verfügt über einen oder mehrere Schlitze, in die die Brotscheiben eingelegt werden, einen Aktivierungshebel und einen Schalter, um die Bräunungsstufe einzustellen. Einige Toaster sind vielleicht etwas aufwändiger und enthalten Sensoren, die feststellen, wann der Toast perfekt ist. Das Grundprinzip ist jedoch bei allen Toastern gleich und die Benutzer müssen nicht rätseln, wie ein Toaster benutzt wird.

Ein API funktioniert auf dieselbe Weise. Ein Programmierer kann eine bestimmte Version des API schreiben. Wenn jedoch ein neueres API erscheint, das mit zusätzlichen Funktionen ausgestattet ist, kann der Programmierer trotzdem weiterhin die gleichen Eingaben (Brot) verwenden und erhält das gleiche Ergebnis (Toast).

Gibt es eine neuere Version eines APIs, kann ein neues Programm dieselbe Schnittstelle benutzen, um eine neue Art von Eingaben (Vollkornbrot) machen und eine neue Art von Ausgabe (getoastetes Vollkornbrot) zu erhalten.

Nun sind Sie sicherlich hungrig. Gönnen Sie sich doch einen Toast. Das Buch ist noch da, wenn Sie zurückkommen.



Ein Teilsystem führt eine ganze Gruppe von Programmen aus und behandelt deren Zugriff auf den Kernel. Dies bedeutet, dass alle Hardwarezugriffe eines Programms über das Teilsystem laufen. Deshalb muss ein Programm, um Sound abspielen zu können, dies dem Teilsystem mitteilen. Das Teilsystem leitet diese Anforderung dann an den Kernel weiter und dieser an die Hardwareabstraktionsschicht. Die Hardwareabstraktionsschicht manipuliert die Hardware so, dass Sound abgespielt werden kann, woraufhin Sound abgespielt wird.

Es gibt zwei Arten von Teilsystemen. Das Win32-Teilsystem ist eine Klasse für sich. Alle anderen Teilsysteme sind im Wesentlichen Übersetzungsprogramme zwischen dem Teilsystem, das sie emulieren, und Win32. Das POSIX-Teilsystem ordnet die Funktionen des POSIX-API denen des Win32-API zu.

Wie sieht ein Teilsystem aus? Jedes Windows 2000-System ist mit ausführbaren Dateien ausgestattet, die Teilsysteme sind. Eines davon heißt Csrss.exe (Client/Server Resources Subsystem), das besser unter der

Bezeichnung Win32-Teilsystem bekannt ist.

2.1.6 Das Win32-Teilsystem

Das Win32-Teilsystem wird am häufigsten benutzt und ist das einzige kritische Teilsystem. Ursprünglich war das Win32-Teilsystem eines unter vielen. Weil alle Benutzerfunktionen des Betriebssystems Win32 verwenden, werden Teile des Win32-Teilsystems im Kernelmodus als Teil der Windows 2000-Ausführungsschicht ausgeführt. Dies sind die Teile, die die grafische Benutzeroberfläche und die Grafikausgabe steuern. Deshalb stürzt das gesamte Betriebssystem ab, wenn das Win32-Teilsystem abstürzt.



Wenn das Win32-Teilsystem unter Windows NT 3.51 abstürzte, resultierte dies selbstverständlich in einem blauen Bildschirm, obwohl die User- und GDI-Teile nicht Bestandteil des Kernels waren. Das Betriebssystem war so eingerichtet, dass ein blauer Bildschirm erzeugt wurde, wenn der Kernel keine Benutzeroberfläche hatte. Weil die gesamte Benutzeroberfläche auf der User und der GDI basiert, stürzt das Betriebssystem ab, wenn eine dieser Komponenten abstürzt. Diese Teile in die Ausführungsschicht zu verschieben, ist nicht so schlimm, wie es aussieht. Die Verlagerung erfolgte, weil sich jeder Wechsel zwischen dem Benutzer- und dem Kernelmodus negativ auf die Performance auswirkt. Durch die Reduktion dieser Kontextwechsel verbesserte sich die Performance von Win32-Anwendungen beträchtlich.

Das bedeutet natürlich nicht, dass Anwendungen im Kernelmodus ausgeführt werden, sondern nur Teile des Teilsystems. Deshalb sind das Teilsystem und das Betriebssystem vor schädlichen Anwendungen sicher. Das Betriebssystem entdeckt Schutzverletzungen und stoppt die schädliche Anwendung, bevor sie Schaden verursachen kann.

Das Win32-API deckt alle Operationen ab, die eine Windows-Anwendung bei der Ausführung benötigt. Dies reicht von Lese- und Schreibvorgängen in Dateien bis zu DirectX. Das Win32-API ist ein sehr komplexes API und enthält zahlreiche Funktionalitäten. Die Windows-Programmierung erfolgt heutzutage unter Zugriff auf das Win32-API. Abbildung 2.3 bietet einen Überblick über diese Teilsystemsicht.

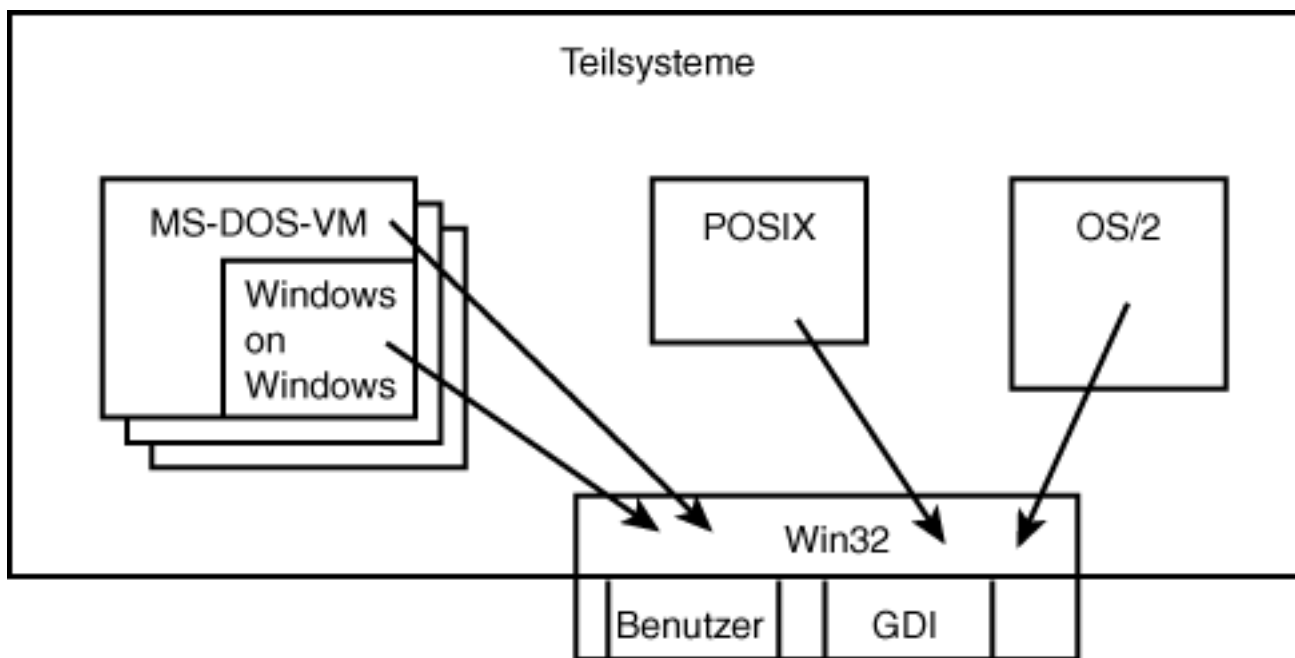


Abbildung 2.3: Die Teilsystemschiicht der Windows 2000-Architektur zeigt, wie die Teilsysteme mit dem Win32-Teilsystem interagieren, das als Einziges direkt mit der Ausführungsschicht interagiert.

Das Win32-Teilsystem enthält auch das MS-DOS- und das 16-Bit-Windows-Teilsystem (Windows 3.1 und Windows 3.11). Weil Windows 3.1 eigentlich kein echtes Betriebssystem ist, sondern vielmehr eine grafische Benutzeroberfläche, die auf MS-DOS aufsetzt, musste das System in erster Linie in der Lage sein, MS-DOS-Anwendungen auszuführen.

MS-DOS-Anwendungen werden in einem Programm namens *NT Virtual DOS Machine* (NTVDM) ausgeführt. Obwohl das Betriebssystem inzwischen Windows 2000 heißt, gibt es noch eine NTVDM. Die NTVDM führt alle DOS-Anwendungen aus, indem die MS-DOS-5.0-Umgebung emuliert wird. Jede DOS-Anwendung läuft in ihrer eigenen NTVDM und in ihrem eigenen Adressraum. Diese NTVDMs lassen sich so lange starten und benutzen, bis kein Systemspeicher mehr verfügbar ist. Die NTVDM stellt einen vollständigen Netzwerk-Redirector sowie eine Unterstützung der Maus und von CD-ROM-Laufwerken bereit und bietet immer noch genügend freien Speicher (620 Kbyte), um MS-DOS-Anwendungen passabel auszuführen.

Nachdem es eine Möglichkeit gibt, DOS-Anwendungen auszuführen, muss nur noch ein Weg gefunden werden, um Windows 3.1-Anwendungen auszuführen. Dazu dient ein System namens Windows on Windows (WOW). WOW bietet eine Schnittstelle zwischen der 16-Bit-Architektur von Windows 3.1 und der 32-Bit-Architektur des Win32-Teilsystems, indem Aufrufe von Diensten mit einem Prozess namens *Thunking* umgewandelt werden. Thunking ist eine Methode, um 32-Bit-Datenwerte ohne Datenverlust in 16-Bit-Datenwerte umzuwandeln (und umgekehrt). Der eigentliche Mechanismus des Thunking hängt von den Daten ab, die übergeben werden. Alle Aufrufe an die User-, GDI- und Kernelbibliotheken im Win32-API werden in die entsprechenden Aufrufe im Win32-API umgewandelt. Die Abbildung 2.4 veranschaulicht dies.

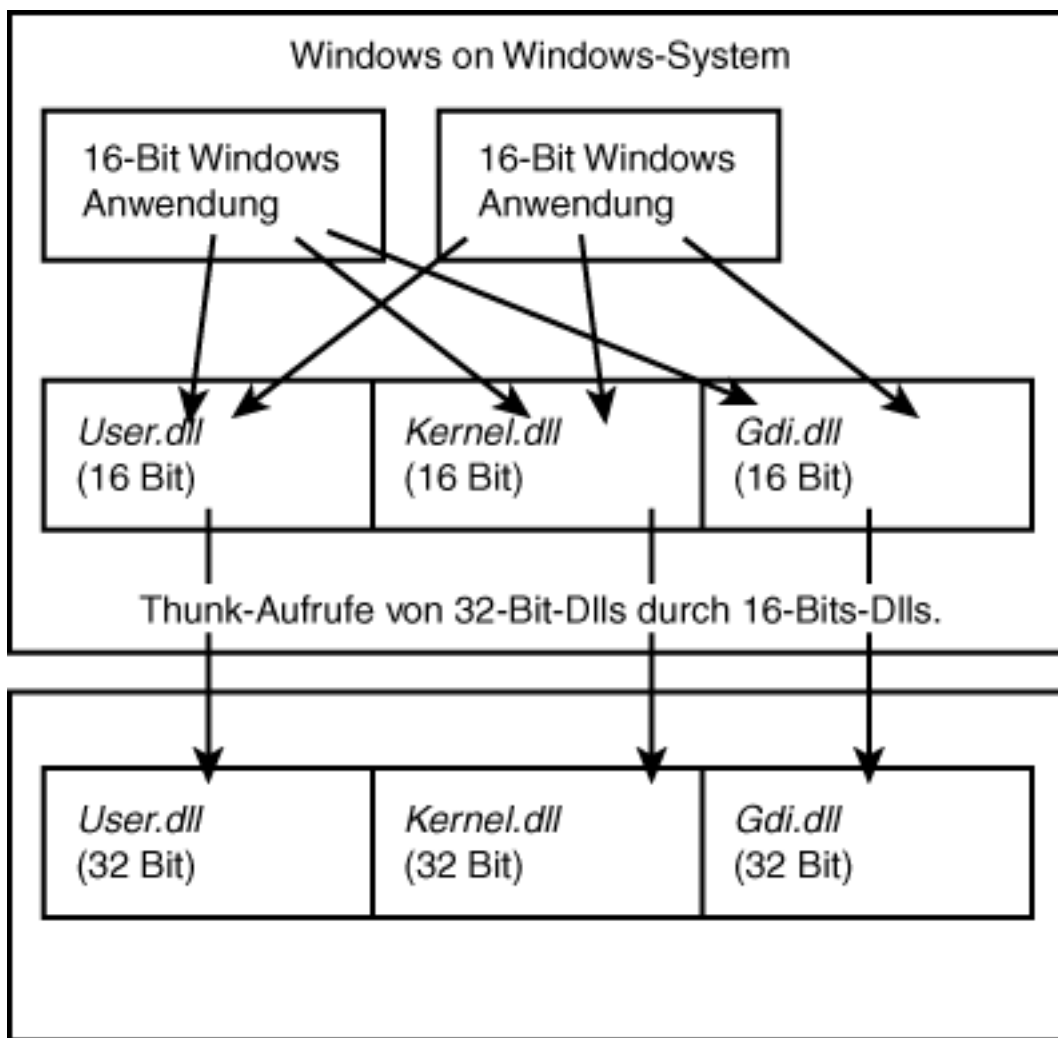


Abbildung 2.4: Die Bestandteile des Windows on Windows-Systems (WOW) und deren Interaktion mit dem Win32-Teilsystem

Programme, die im WOW ausgeführt werden, laufen alle in derselben Instanz von *Wowexec* (dem Programm, das die Systemaufrufe von Win16 zu Win32 behandelt). Dies geschieht, um den Overhead zu reduzieren (jede der *Wowexec*-Instanzen benutzt Speicher) und um OLE- und Ausschneiden- und -Einfügen-Operationen bei Win16-Programmen zu ermöglichen.

Windows 3.1 implementiert Multitasking mit einer Technik namens »kooperatives Multitasking«. Das Betriebssystem nimmt an, dass sich jedes Programm »gesittet« verhält und den Prozessor gelegentlich frei gibt, damit das nächste Programm ausgeführt werden kann. Selbstverständlich glauben alle Programmierer, dass ihr Programm das Wichtigste auf der Welt ist und niemals den Prozessor freigeben sollte. Deshalb gibt es unter Windows 3.1 viele Performanceprobleme. Windows 2000 nutzt ein »präemptives Multitasking«.

Bei diesem weist das Betriebssystem CPU-Zeit zu und unterbricht jedes laufende Programm, wenn die zugewiesene CPU-Zeit vorüber ist.

Der Threadplaner von Windows 2000 macht einige einzigartige Dinge, damit Win32-Anwendungen korrekt ausgeführt werden. Denken Sie daran, dass alle Threads im präemptiven Multitasking ausgeführt werden. Bei *Wowexec* kann immer nur der Thread ausgeführt werden, der auch beim letzten Mal ausgeführt wurde. Das heißt, bei jeder Instanz von *Wowexec* kann immer nur ein Thread aktiv sein und

dieser Thread muss den Prozessor freiwillig freigeben, bevor ein anderes 16-Bit-Windows-Programm ausgeführt werden kann. Das heißt, eine 16-Bit-Windows-Anwendung, die den Prozessor nicht freigibt, verhindert, dass andere 16-Bit-Anwendungen ausgeführt werden. Diese Richtlinie wurde implementiert, weil viele Win16-Anwendungen falsche Annahmen darüber treffen, wie sie in Relation zum Rest des Betriebssystems und anderen Windows 3.1-Anwendungen ausgeführt werden, um Daten zurückzuliefern. Wenn das Betriebssystem für die Anwendungen einen anderen Zeitplan entwickelt als echte Windows 3.1-Anwendungen, geht die Kompatibilität zu den Anwendungen verloren.

2.1.7 Das POSIX-Teilsystem

Laut Microsoft wurde das POSIX-Teilsystem entwickelt, damit Benutzer UNIX-Anwendungen unter Windows NT ausführen konnten. POSIX ist ein Standard, der verschiedene Betriebssystemdienste und API-Aufrufe spezifiziert, die Anwendungen zur Verfügung stehen müssen. POSIX steht für *Portable Operating System Interface for UNIX*.

Es gibt drei Ebenen von POSIX-Kompatibilität. Windows 2000 unterstützt nur die unterste Ebene namens *POSIX.1*. Diese Ebene spezifiziert einen minimalen Satz an Diensten und erfordert die Unterstützung der Unterscheidung von Groß-/Kleinschreibung bei Dateinamen, die Unterstützung harter Links und die Möglichkeit, Benutzer daran zu hindern, auf Dateien zuzugreifen, wenn sie keine Berechtigung zum Zugriff auf alle übergeordneten Verzeichnisse der Datei haben (*Traversal Checking*). Damit der Benutzer also die Datei *D:\Daten\Dokumente\Foo.doc* lesen kann, benötigt er Lesezugriff auf das Stammverzeichnis auf Laufwerk *D:*, auf das Verzeichnis *Daten*, auf das Verzeichnis *Dokumente* und auf die Datei *Foo.doc*.

Lange Zeit, insbesondere während der Entwurfsphase von Windows NT, war die POSIX-Kompatibilität eine Anforderung an jedes Betriebssystem, das von der Bundesregierung der USA gekauft wurde. Einige Zyniker behaupten sogar, dass Microsoft die POSIX-Kompatibilität nur aus diesem Grund in Windows NT aufgenommen habe. Diese Zyniker liegen vermutlich richtig.

POSIX.1 ist eine so geringe Kompatibilitätsebene, dass sie fast nutzlos ist. POSIX.1-kompatible Systeme müssen kein bestimmtes binäres Dateiformat nutzen. Deshalb können sie nicht notwendigerweise dieselben Programme ausführen. Das System ist auf der Ebene des POSIX.1-Standard so »schwammig«, dass die Portierung von Anwendungen auf ein anderes Betriebssystem mit sehr viel Mühe verbunden ist. Der POSIX.1-Standard spezifiziert keine Netzwerkschnittstelle. Deshalb haben Programme, die für das POSIX-Teilsystem entwickelt werden, keinen Netzwerkzugriff.

Das POSIX-Teilsystem funktioniert, indem die C-Aufrufe in Aufrufe des Win32-Teilsystems umgewandelt werden. Deshalb ist das POSIX-Teilsystem vom Win32-Teilsystem abhängig und kann nichts, was das Win32-Teilsystem nicht ebenfalls könnte. Außerdem führt der Overhead für die Übersetzung dieser Aufrufe dazu, dass POSIX-Anwendungen langsamer sind als entsprechende reine Win32-Programme. Auch hier könnten Zyniker sagen, dass dies ein weiterer Grund ist, Programme nur auf Win32 zu portieren und UNIX und POSIX ganz zu ignorieren.

2.1.8 Das OS/2-Teilsystem

Als Windows NT entwickelt wurde, war es von Microsoft als Ersatz für OS/2 gedacht. Microsoft fand heraus, dass die Windows-Oberfläche wesentlich beliebter war als der Presentation Manager von OS/2. Deshalb beschloss Microsoft, das neue Betriebssystem mit einer Windows-Oberfläche zu erstellen und das Produkt in Windows New Technology (oder Windows NT) umzubenennen.

Das OS/2-Teilsystem ist ein sehr beschränktes Teilsystem, das ursprünglich entwickelt wurde, um OS/2 1.x-Zeichenmodusanwendungen auszuführen. Es kann keine grafischen Anwendungen ausführen und auch keine OS/2 2.x-Programme oder höher. Das OS/2-Teilsystem basiert wie das POSIX-Teilsystem auf der Win32-API. Es konvertiert im Wesentlichen OS/2-API-Aufrufe in Win32-Aufrufe, enthält aber nur das Kern-API von OS/2 1.x und einige grundlegende LAN Manager-Netzwerkaufrufe, um Programmen Netzwerkzugriff zu bieten. Dadurch ist das System dem POSIX-Teilsystem einen Schritt voraus, das keine Netzwerkunterstützung bietet.

2.2 Das Speichermodell und die Speicherverwaltung

Eine der wichtigsten Aufgaben von Betriebssystemen besteht darin, den Speicher zuzuweisen und zu überwachen. Die Festlegung, wie der Speicher für verschiedene Prozesse zugewiesen wird und wie die Prozesse auf den Speicher zugreifen, ist Bestandteil des Speichermodells des Betriebssystems. Bestandteil der Speicherverwaltung ist die Behandlung des physischen Speichers und der Auslagerung von Seiten auf die Festplatte.

2.2.1 Das Speichermodell

Windows 2000 benutzt ein Prozess- und ein Taskmodell, um die Verarbeitung zu beschreiben. Ein *Prozess* ist ein Objekt, das eine Speicherreservierung und mehrere Tasks besitzt. Ein *Task* ist eine Ausführungseinheit (d.h. das, was der Kernel ausführt).

In Windows 2000 erhält jeder Prozess einen Speicherraum von `0x00000000` bis `0xFFFFFFFF`, den er adressieren kann und der 4 Gbyte Speicher in einem flachen Adressraum entspricht. Auf diese Weise erzeugt Windows 2000 den Speicherschutz.

Was hat es nun mit dem geschützten Speicher auf sich? Stellen Sie sich ein Betriebssystem, wie z.B. Windows 3.1, mit einem gemeinsam genutzten Speicherraum vor. Dies bedeutet, dass alle Programme im selben Adressraum ausgeführt werden. Stellen Sie sich weiterhin vor, dass ein Programmierer ein Programm erzeugt, das Dateien im Arbeitsspeicher ablegt und später aus diesem abrufen und anzeigt. Dieses Programm ist eine Textverarbeitung, die immer eine gesamte Datei in den Arbeitsspeicher einliest und sie dann anzeigt (dies ist vermutlich die ungünstigste Vorgehensweise, aber auf diese Weise arbeitet der Editor, *Notepad.exe* von Windows). Wenn ein Programm Speicher benötigt, bittet es das Betriebssystem darum. Das Betriebssystem liefert entweder einen Zeiger auf den Speicher zurück oder die Meldung »Ich kann Dir nicht mehr Speicher zur Verfügung stellen«. Wenn der Programmierer also 2 Kbyte Speicher anfordert und die Datei tatsächlich 3 Kbyte groß ist, wird die Datei in den Arbeitsspeicher eingelesen. Wenn die 2 Kbyte überschritten sind, wird die Datei trotzdem weiter

eingelassen. Das ist etwa so, als würden 15 kg Kunstdünger in einen 10-kg-Sack gestopft. Die restlichen 5 kg müssen irgendwo hin gelangen. Beim Kunstdünger werden sie auf dem ganzen Boden verstreut. Beim Speicher wird das 1 Kbyte mit Daten einfach in den weiteren Speicheradressraum geschrieben.

Bei einem solchen Speicherüberfluss gibt es nur zwei Optionen. Die Daten werden entweder in den Speicher geschrieben, den das Betriebssystem bisher noch nicht zugewiesen hat, oder sie werden in den Speicher geschrieben, den ein anderes Programm nutzt. Weil es keinen Speicherschutz gibt, merkt das Betriebssystem von diesem Problem nichts. In der Zwischenzeit wurden die Programmdaten des Programms, das im Adressraum neben der Textverarbeitung ausgeführt wird, einfach von den Daten aus der Textdatei überschrieben. Wenn das Programm nun ausgeführt werden soll, stürzt es ab. Wie es Murphys Gesetz voraussagt, wird im schlimmsten Fall das Betriebssystem überschrieben. Und das passiert normalerweise auch.

Dies ist nun allgemein bekannt, aber früher (Ende der achtziger und Anfang der neunziger Jahre) war dies bei PC-basierten Betriebssystemen ein großes Problem. Das einzige PC-orientierte Betriebssystem, das einen Speicherschutz bot, war OS/2, aber dieses Betriebssystem war nicht sehr beliebt.

Wenn eine Anwendung versucht, in einen fremden Speicherraum zu schreiben, resultiert dies in einer *Schutzverletzung*. Eine solche Schutzverletzung ist die *Allgemeine Schutzverletzung*, die bei den meisten Windows-Betriebssystemen üblich ist. Sie tritt auf, wenn eine Anwendung mit einem Lese- oder Schreibzugriff unberechtigt auf einen Speicherbereich zugreift.

Warum führen Schutzverletzungen zum Abbruch von Programmen? Eine weitere Möglichkeit wäre es, den Speicher vor dem Schreibzugriff zu schützen und das Programm weiterhin auszuführen. Angenommen, ein Benutzer verwendet dieses alternative Betriebssystem und erstellt in einer Textverarbeitung ein Dokument. Dann beginnt die Textverarbeitung, in einen unerlaubten Speicherbereich zu schreiben. Das Betriebssystem ignoriert den Schreibvorgang, weil dieser unzulässig ist, und der Benutzer versucht, den Text in eine Datei zu speichern. Aber die Datei befindet sich nicht im Speicher. In diesem Fall hat der Benutzer dann nicht nur eine kleine Datenmenge verloren, sondern vermutlich die Arbeit eines ganzen Nachmittags.

Warum kann das Betriebssystem das Programm nicht einfach darüber in Kenntnis setzen, dass es etwas falsch macht? So funktionieren Programme eben nicht, und selbst, wenn sie es täten, muss ein Programm ernsthafte Probleme haben, um eine Schutzverletzung zu verursachen. Und dies ist normalerweise schlechte Programmierung. Wenn ein Programm so schlecht programmiert ist, dass es eine Schutzverletzung verursacht, wird es dann mit einer Meldung des Betriebssystems etwas anfangen können, die besagt, dass es seine Vorgehensweise ändern soll? Es wird diese Meldung sehr wahrscheinlich einfach ignorieren und entweder abstürzen, weil das Betriebssystem seine Ausführung unterbricht, oder die Schutzverletzung komplett übergehen, was in einem Datenverlust resultiert. Auch diese Lösung ist sicherlich nicht wünschenswert. Deshalb bricht Windows 2000 ein Programm eher ab, als einen fortwährenden Datenverlust zu riskieren.

Eine Möglichkeit sicherzustellen, dass Programme nicht mehr Speicher benutzen als sie benötigen und damit ihre Speicherabbilder beschädigen, besteht darin, zu verhindern, dass sie auf die Adressräume anderer Programme zugreifen können. Wenn das Programm nur Adressen zwischen 0 und 4 Gbyte kennt, und dieser Raum zum Programm gehört, kann das Programm möglicherweise keine anderen Daten überschreiben. Auf diese Weise wird Speicher unter Windows 2000 verwaltet. Jeder Prozess erhält seinen eigenen virtuellen 4-Gbyte-Adressraum, und kann damit machen, was er möchte. In Abbildung

2.5 finden Sie ein Programm, das diese Funktionsweise veranschaulicht.

Programm 1	Programm 2	Programm 3	Adresse
Von Programm nutzbarer Adressraum	Von Programm nutzbarer Adressraum	Von Programm nutzbarer Adressraum	0xFFFFFFFF
			0x7FFFFFFF
Von System nutzbarer Adressraum	Von System nutzbarer Adressraum	Von System nutzbarer Adressraum	0x00000000

Abbildung 2.5: Das Speichermodell für den virtuellen Arbeitsspeicher. Jede Anwendung hat ihren eigenen Adressraum und weiß nichts von den Adressräumen anderer Anwendungen.

Prozesse müssen noch immer Speicher vom Betriebssystem anfordern, bevor sie diesen nutzen können, obwohl ihnen ein 4-Gbyte-Adressraum zur Verfügung steht. Dies hat einen einfachen Grund: Die Speicherverwaltung muss wissen, wie viel Speicher ein Prozess benötigt, um feststellen zu können, ob genügend Systemspeicher für die Ausführung des Programms vorhanden ist und damit die virtuelle Speicherverwaltung (VMM) weiß, wie der Speicher adressiert werden soll.

Für Prozesse gibt es eine weitere Beschränkung. Der 4-Gbyte-Adressraum ist nicht vollständig nutzbar. Ein Teil des Adressraums ist für das System reserviert. In Windows 2000 Professional und Windows 2000 Server liegt die Grenze bei 2 Gbyte für das System und die Anwendung. Bei Windows 2000 Advanced Server und Windows 2000 Datacenter liegt die Trennungslinie bei 3 Gbyte für die Anwendung und 1 Gbyte für das System. Diese Änderung wird über einen Schalter in der Datei *Boot.ini* ermöglicht. Werfen Sie einen Blick auf die nachfolgende *Boot.ini*-Datei. Die Einträge im Bereich [operating systems] zeigen, wie der /3GB-Schalter zum Start von Windows 2000 hinzugefügt wurde:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(2)\WINNT
[operating systems]
multi(0)disk(0)rdisk(0)partition(2)\WINNT=
    "Windows 2000 Advanced Server" /3GB
multi(0)disk(0)rdisk(0)partition(2)\WINNT=
    "Windows 2000 Advanced Server [VGA mode]" /basevideo /sos
```

Bei einer echten *Boot.ini*-Datei gibt es beim Gleichheitszeichen keinen Zeilenumbruch. Der Zeilenumbruch ist hier durch die geringe Seitenbreite des Buchs bedingt.

Damit eine Anwendung das neue Speichermodell nutzen kann, muss das Betriebssystem wissen, dass das Programm dazu in der Lage ist. Im Header der *.exe*-Datei wird ein Attribut namens *IMAGE_FILE_LARGE_ADDRESS_AWARE* aktiviert, d.h. auf den Wert 1 gesetzt. Im Ordner *Support* der Windows 2000 Advanced Server-CD finden Sie ein Programm namens *Imagecfg.exe*, das das Attribut bei ausführbaren Dateien setzt. Um z.B. dafür zu sorgen, dass die Datei *Accrvcv.exe* das neue Speichermodell nutzt, dient folgender Befehl.

```
Imagecfg -1 ACCRCV.EXE
```

Der Befehl kann mit dem Befehl `imagecfg -0` wieder rückgängig gemacht werden.

2.2.2 Die Speicherverwaltung

Die virtuelle Speicherverwaltung (VMM = Virtual Memory Manager) behandelt die Speicherzuweisung, die Auslagerung und die Übersetzung der Anforderungen von Anwendungen eines bestimmten Speicherblocks in eine Leseanweisung für einen bestimmten Block des physischen Speichers.

Bevor die Speicherverwaltung beschrieben wird, müssen noch ein paar wesentliche Punkte genannt werden. Windows 2000 versucht, jedes Bit des Systemspeichers auszunutzen. Für den Programmstart bleibt nur eine geringe Speichermenge verfügbar. Wenn dieser Speicher von keiner Anwendung genutzt wird, wird er vom Betriebssystem als Zwischenspeicher für die Festplatte genutzt. Wenn ein Computer als Dateiserver läuft, gibt es keine Möglichkeit, Windows 2000 mitzuteilen, dass Speicher als Zwischenspeicher genutzt werden soll - dies geschieht bereits.

Außerdem gibt es noch den physischen Arbeitsspeicher, d.h. die Chips im Computer und den virtuellen Arbeitsspeicher (der sich eigentlich auf der Festplatte befindet.). Der Arbeitsspeicher ist in Einheiten aufgeteilt, die *Seiten* genannt werden. Eine Seite besteht aus 4 Kbyte Arbeitsspeicher. In dieser Größe verschiebt die virtuelle Speicherverwaltung auch Arbeitsspeicher. Eine Seite existiert an mindestens einem von drei Orten: dem physischen Speicher, der Auslagerungsdatei oder in einer Liste der Seiten, die ausgelagert werden sollen (die sog. *Warteliste*).

Die virtuelle Speicherverwaltung muss einen Überblick über den gesamten virtuellen Arbeitsspeicher haben, der für einen Prozess reserviert ist, und auch den Status des Arbeitsspeichers prüfen und sehen, ob sich der Prozess tatsächlich im Arbeitsspeicher befindet oder auf die Festplatte ausgelagert wurde. Die virtuelle Speicherverwaltung zeichnet auch auf, ob eine einzelne Seite Code oder Daten enthält. Die virtuelle Speicherverwaltung kennt den Unterschied zwischen Code (ausführbare Programme, die in den Speicher geladen werden) und Daten (Informationen, die von Code benutzt werden). Code ist schreibgeschützt, auf Daten besteht ein Lese-/Schreibzugriff. Dies hilft der virtuellen Speicherverwaltung festzustellen, wenn ein Programm »verrückt spielt« und versucht, in einem unerlaubten Speicherbereich

zu schreiben. Die virtuelle Speicherverwaltung behandelt alle Lese- und Schreib Anforderungen an den Arbeitsspeicher und weiß somit, wenn ein Programm versucht, in schreibgeschützte Daten zu schreiben. Derartige Situationen lassen sich leicht verhindern.

Die virtuelle Speicherverwaltung führt auch Buch über den physischen Speicher im Computer: er zeichnet auf, welche Seiten zugewiesen wurden, zu welchen Prozessen diese Seiten gehören und wann die Seiten zuletzt benutzt wurden (d.h. gelesen oder beschrieben wurden).

Wenn die virtuelle Speicherverwaltung eine Anforderung erhält, Daten für ein Programm aus einem bestimmten Speicherbereich zu lesen, konsultiert die virtuelle Speicherverwaltung eine Tabelle, die eine Liste aller Seiten enthält, die zu dem Programm gehören, und ein Statusbit, das angibt, ob sich die Seite im physischen Speicher befindet. Ist dies der Fall, liefert die virtuelle Speicherverwaltung die angeforderten Daten direkt an das Teilsystem zurück. Befinden sich die Informationen nicht im physischen Speicher, prüft die virtuelle Speicherverwaltung seine Warteliste um festzustellen, ob die Seite dort verfügbar ist. Ist dies der Fall, wird versucht, die Seite von der Festplatte zu laden.

Wenn die virtuelle Speicherverwaltung die Seite nicht findet, resultiert daraus ein Seitenfehler. Es gibt zwei Arten von Seitenfehlern. Ein *harter Seitenfehler* tritt auf, wenn die virtuelle Speicherverwaltung die gesuchte Seite weder im physischen Speicher noch in der Warteliste findet. Ein *weicher Seitenfehler* tritt auf, wenn die virtuelle Speicherverwaltung die Seite zwar nicht im physischen Speicher findet, wohl aber in der Warteliste. Die virtuelle Speicherverwaltung ruft die Seite dann wieder in den physischen Speicher, ohne sie von der Festplatte lesen zu müssen.

Wenn die virtuelle Speicherverwaltung entweder Speicher als neuen Speicher für ein Programm zuweisen oder eine Seite von der Festplatte lesen muss, wird eine Tabelle überprüft, die eine Liste der freien Seiten enthält. Die Speicherverwaltung weist dann die benötigte Anzahl von Seiten im Speicher zu. Wenn der freie Arbeitsspeicher einen bestimmten Wert unterschreitet, startet die virtuelle Speicherverwaltung einen Prozess um festzustellen, welche Seiten ausgelagert werden können. Erinnern Sie sich daran, wie die virtuelle Speicherverwaltung feststellt, ob Seiten im physischen Speicher benutzt werden? Diese Informationen dienen auch dazu festzulegen, welche Seiten im physischen Speicher bleiben müssen und welche auf die Festplatte ausgelagert werden können.

Die virtuelle Speicherverwaltung bestimmt auf der Basis des Zeitpunkts der letzten Nutzung, welche Seiten auf die Warteliste gesetzt werden. Sie benutzt einen LRU-Algorithmus (LRU = Least Recently Used) um festzulegen, welche Seiten auf die Festplatte ausgelagert werden. Seiten, die schon eine Weile nicht benutzt wurden, werden ausgelagert, wohingegen häufig benutzte Seiten im Arbeitsspeicher bleiben.

Um diese Aktivität zu überwachen, stehen im Systemmonitor zahlreiche Attribute zur Verfügung. Eine ausführliche Beschreibung des Systemmonitors finden Sie in Kapitel 24.

Kapitel 3 Installation

Ein Rückblick auf die verschiedenen Versionen von Windows NT zeigt, dass bei jeder Version erwähnt wurde, wie einfach die Installationsprozedur ist. Windows 2000 wird erwartungsgemäß dieselben begeisterten Besprechungen erhalten, weil die Installationsprozedur sogar noch weiter verbessert wurde. Der Schlüssel zu einer erfolgreichen Installation ist jedoch noch immer die Berücksichtigung der Hardwarekompatibilitätsliste.

Dieses Kapitel beschreibt die verschiedenen Aspekte der Installation:

- Systemanforderungen
- Hardwarekompatibilitätsliste
- Installationsoptionen
- Lizenzoptionen
- Automatisierte Installation
- Installation der Wiederherstellungskonsole
- Die Datei *Boot.ini*
- Die Notfalldiskette
- Migration
- Hinweise zur Hardware

3.1 Systemanforderungen

Windows 2000 leistet mehr als Windows NT 4.0. Deshalb ist es ganz natürlich, dass die Hardwareanforderungen höher sind. Hier sind die minimalen Systemanforderungen von Windows 2000 für Intel-Systeme:

- Mindestens ein Pentium 166MHz-Prozessor oder höher. Pentium II-, Pentium III- und Xeon-Prozessoren sowie baugleiche Prozessoren der Hersteller Cyrix und AMD werden unterstützt. Die Verwendung mehrerer Prozessoren wird unterstützt.
- Mindestens 64 Mbyte RAM. Empfehlenswert sind 128 Mbyte. Mindestens 8 Gbyte Festplattenspeicher für Advanced Server und 4 Gbyte für Server.
- Eine Festplatte mit viel freiem Speicherplatz. Wie viel ist viel? 850 Mbyte für die Installation und jeweils 2 Mbyte je 1 Mbyte Hauptspeicher des Systems. Wenn das System 128 Mbyte RAM hat, benötigt die Installation 1.106 Mbyte ($850 \text{ Mbyte} + 128 \text{ Mbyte} * 2$) freien Festplattenspeicher. Erfolgt die Installation über ein Netzwerk anstatt von CD-ROM, werden zusätzlich 200 Mbyte Festplattenspeicher für die temporären Installationsdateien benötigt. Wenn es sich um ein Update eines bestehenden Domänencontrollers handelt und gleichzeitig der Active Directory-Dienst installiert wird, ist erheblich mehr freier Festplattenspeicher erforderlich, weil der Aktualisierungsprozess bis zu zehn Mal mehr Speicher beansprucht als die Benutzerkontendatenbank.
- Ein Monitor mit VGA-Auflösung oder besser.
- Eine Tastatur.
- Eine Maus oder ein anderes Zeigegerät ist optional. Ohne Maus ist die Bedienung jedoch schwierig.
- Für eine Installation von CD-ROM ist ein entsprechendes Laufwerk erforderlich, das zumindest eine 12-fache Geschwindigkeit aufweisen sollte. Nützlich ist auch ein 3,5«-Diskettenlaufwerk, falls das System nicht von CD-ROM booten kann.
- Für eine Installation über ein Netzwerk wird auch eine Netzwerkkarte benötigt, die auf der Hardwarekompatibilitätsliste enthalten ist und ein Server, auf dem die Windows 2000-Dateien vorhanden sind und von dem aus sie auf dem neuen Server installiert werden.

Falls nichts Anderes angegeben ist, handelt es sich bei den Angaben um Mindestanforderungen.

3.2 Die Hardwarekompatibilitätsliste

Der wahrscheinlich wichtigste Teil der Dokumentation zu Windows 2000 ist die Hardwarekompatibilitätsliste (HCL). In dieser Liste ist die gesamte Hardware aufgeführt, die von Windows 2000 unterstützt wird. Berücksichtigt werden Prozessoren, Netzwerkkarten, Festplattencontroller, Drucker und andere Geräte. Auf diese Geräteliste können Sie online unter der URL <http://www.microsoft.com/hwtest/hcl/> zugreifen.



Microsoft hat die unangenehme Angewohnheit, URLs zu veröffentlichen und dann den Inhalt an einer anderen Stelle abzulegen. Ungefähr die Hälfte der URLs in den Hilfedateien von SQL Server 7.0 funktionieren nicht, weil Microsoft das URL-Schema geändert hat. Wenn die Artikel, nach denen Sie suchen, nicht angezeigt werden, sollten Sie es einmal mit der Suchfunktion von Microsofts Website versuchen.

Die Hardwarekompatibilitätsliste repräsentiert eine Liste von Hardware, deren korrekte Funktionsweise unter Windows 2000 von Microsoft überprüft wurde. Normalerweise stellen die Hardwarehersteller Microsoft die Windows-Treiber zur Verfügung. Microsoft prüft diese und aktualisiert die Hardwarekompatibilitätsliste. Da die Aufnahme in die Hardwarekompatibilitätsliste für die Hersteller kostenpflichtig ist, verzichten einige Hersteller darauf und liefern einige ihre Treiber direkt mit der Hardware aus. Dies birgt für den Benutzer ein gewisses Risiko, da der Microsoft-Support leicht sagen kann, dass das Problem durch den fehlerhaften Treiber verursacht wird und nicht an Windows 2000 liegt. Um diese Art von Problemen zu vermeiden, sollten Sie nach Möglichkeit nur Hardware verwenden, die in der Hardwarekompatibilitätsliste enthalten ist.

3.3 Überblick über den Installationsprozess

Der Installationsprozess muss eine ganze Reihe von Abläufen gewährleisten. Er muss sicherstellen, dass die Systemdateien von Windows 2000 in die Systempartition kopiert werden. Dann muss er Windows 2000 so konfigurieren, dass es mit der Hardware des Systems zusammenarbeitet. Als Nächstes muss die Installation Windows 2000 für die Arbeit im Netzwerk konfigurieren (was wäre ein Server, der nicht in ein Netzwerk integriert ist). Dieser Abschnitt bietet einen Überblick über den Installationsprozess.

Als erstes muss das System Windows 2000 starten. Dies geschieht entweder über eine bootfähige Windows 2000-CD-ROM oder indem das Programm *Winnt32.exe* unter Windows NT oder Windows 9x oder das Programm *Winnt.exe* von einer Befehlszeile (DOS, Windows 3.x) aus ausgeführt wird. In allen Fällen richtet das Programm die Festplatte ein, um Windows 2000 zu starten (booten).

Wenn Sie die Windows 2000-Installation mit dem Programm *Winnt32.exe* oder *Winnt.exe* ausführen, können Sie den Installationsprozess mit Befehlszeilenoptionen beeinflussen. Hier sind die Befehlszeilenoptionen für das Programm *Winnt.exe*:

- */s*: [*Quellpfad*]. Der Pfad zu den Windows 2000-Dateien, wie z.B. *d:\i386*. Dies kann auch ein Netzwerkpfad sein, wie z.B. *\\intrepid\install\i386*. Wird kein Pfad angegeben, werden Sie vom Setup-Programm aufgefordert, diesen anzugeben.
- */t*: [*Temporärer Pfad*]. Der Pfad, in dem die temporären Dateien abgelegt werden. Diese Dateien werden benötigt, um Windows 2000 zu booten. Wurde diese Option nicht angegeben, versucht das Setup-Programm, ein Laufwerk zu finden, auf dem die Dateien abgelegt werden können.
- */u*: [*Antwortdatei*]. Der Name der »Antwortdatei«. Details hierzu finden Sie im nächsten Abschnitt zur automatisierten Installation.
- */udf:id[,UDF-Datei]*. Die ID dient dazu, eindeutige Informationen aus der UDF-Datei (UDF = Uniqueness Database File) zu beziehen. Die UDF-Datei enthält Antworten für alle Fragen, die bei der automatisierten Installation gestellt werden. Mehr zur automatisierten Installation erfahren Sie im nächsten Abschnitt.
- */r*: [*Ordner*]. Der Pfad zu einem Verzeichnis, das vom Setup-Programm installiert wird. Das Verzeichnis besteht auch nach der Installation und wird normalerweise benutzt, um nach der Installation von Windows spezielle Treiber auf der Festplatte zu installieren, um den Wechsel oder die nachträgliche Installation von Treibern zu erleichtern.

- `/rx`: [*Ordner*]. Der Pfad zu einem Ordner, der von der Installationsroutine eingerichtet, anschließend aber vollständig entfernt wird.
- `/e`: [*Befehl*]. Gibt einen Befehl an, der ausgeführt wird, nachdem der GUI-Teil (GUI = Graphical User Interface, Grafische Benutzeroberfläche) der Installation beendet ist.
- `/a`. Gibt an, dass die Eingabehilfen im Anschluss an die Installation aktiviert werden.

Das Programm *Winnt.exe* wurde für die Ausführung von einer Befehlszeile oder von MS-DOS entwickelt und ist deshalb mit anderen Optionen ausgestattet als das Programm *Winnt32.exe*, das von einer Eingabeaufforderung unter Windows 95, Windows 98, Windows NT oder Windows 2000 aus ausgeführt wird. Das Programm *Winnt32.exe* verfügt über folgende Befehlszeilenoptionen:

- `/s`: [*Quellpfad*]. Der Pfad zu den Windows 2000-Quelldateien (z.B. *D:\i386*).
- `/tempdrive`: [*Laufwerksbuchstabe*]. Das Laufwerk für die temporären Dateien.
- `/unattend`. Wird diese Option verwendet, führt das Installationsprogramm eine unbeaufsichtigte Installation durch. Hierbei wird die Anzeige des Endbenutzerlizenzvertrags (EULA) übergangen.
- `/unattend[id]`: [*Antwortdatei*]. Diese Option gibt die ID der UDF-Datei an, die für die Installation benutzt werden soll und den Pfad zu der Antwortdatei. Im nächsten Abschnitt finden Sie weitere Informationen zur unbeaufsichtigten Installation.
- `/copydir`: [*Ordnername*]. Diese Option erzeugt einen Ordner im Windows 2000-Verzeichnis, der nach der Installation bestehen bleibt. Sie entspricht der Option `/r` für das Programm *Winnt.exe*.
- `/copysource`: [*Ordnername*]. Diese Option erzeugt wie die Option `/copydir` einen Ordner, entfernt diesen aber nach dem Installationsprozess.
- `/cmd`: [*Befehlszeile*]. Eine vollständige Befehlszeile, die ausgeführt wird, nachdem der GUI-Teil des Setups beendet ist.
- `/debug[Ebene]`: [*Dateiname*]. Die Ebene, auf der Debuginformationen gehalten sein sollten, und die Datei, in die die Debuginformationen geschrieben werden sollten.
- `/udf:id[, UDB-Datei]`. Die ID der UDF-Datei, die für diesen Computer benutzt werden sollte. Im nächsten Abschnitt erfahren Sie mehr über die unbeaufsichtigte Installation.
- `/syspart`: [*Laufwerksbuchstabe*]. Wenn dieser Schalter angegeben wird, kopiert die Installationsroutine die benötigten Dateien in eine Partition der Festplatte, markiert die Partition als aktive Partition, sodass von ihr gebootet wird und stoppt dann die Installation. Die Festplatte kann dann entfernt und in einen anderen Computer eingesetzt werden, wo die Installation wieder aufgenommen wird. Dieser Schalter funktioniert nur unter Windows NT oder Windows 2000, nicht unter Windows 9x. Er muss in Kombination mit dem Schalter `/Tempdrive` eingesetzt werden.
- `/checkupgradeonly`. Dieser Schalter sorgt dafür, dass nichts installiert wird. Statt dessen prüft die Installationsroutine nur, ob vom aktuellen Betriebssystem ein Update auf Windows 2000 erfolgen kann. Bei einem Windows 9x-Computer wird ein Bericht in die Datei *Upgrade.txt* im Windows-Verzeichnis geschrieben. Bei Windows NT-Computern wird eine Datei *Winnt32.log* im Windows NT-Verzeichnis (normalerweise *\Winnt*) erzeugt.
- `/cmdcons`: . Installiert die Wiederherstellungskonsole. Diese wird nur benutzt, nachdem Windows 2000 erfolgreich installiert wurde.
- `/m`: [*Ordnername*]. Wenn dieser Schalter angegeben wird, ersetzt Windows 2000 die Windows 2000-Installation durch die Dateien im angegebenen Ordner.
- `/makelocalsource`. Durch diesen Schalter wird das Installationsverzeichnis auf die Festplatte des Computers kopiert, um später das Hinzufügen und Entfernen von Komponenten zu erleichtern.
- `/noreboot`. Dieser Schalter sorgt dafür, dass die Installationsroutine am Ende des Dateikopiervorgangs nicht automatisch neu bootet, sodass andere Befehle ausgeführt werden können.

Wenn Windows 2000 startet, wird geprüft, ob es sich um ein Update oder eine Neuinstallation handelt. Bei einer Neuinstallation werden Sie durch die Erstellung von Festplattenpartitionen und die Formatierung von mindestens einer Systempartition geführt, die Windows 2000 nutzen kann. Bei Updates muss das System die vorhandene Systempartition nutzen.

Die Windows 2000-Installation beginnt dann, die Dateien auf die Systempartition zu kopieren, und startet anschließend das System neu.

Wenn das System wieder bootet, wird Windows 2000 in einem Grafikmodus gestartet und Sie müssen zahlreiche Fragen beantworten, damit Windows 2000 korrekt konfiguriert werden kann. Dabei geht es um die Lizenzierung, die Pfade für die Installation usw. In dieser Phase führt Windows 2000 eine Installation der Geräte durch, die bis zu 15 Minuten dauern kann.

Nach der Installation und der Konfiguration der Geräte stellt Windows 2000 Ihnen weitere Fragen, um das Netzwerk einrichten zu können. Es gibt keine Fragen zur Aufnahme in eine Domain oder zur Art des Domänencontrollers, da alle Windows 2000-Server als eigenständige Server installiert werden. Erst im Anschluss an die Installation können Sie einen Server zum Domänencontroller machen. Dies stellt eine gewaltige Verbesserung gegenüber Windows NT dar, wo die Entscheidung einmal getroffen wird, und sich ein Wechsel vom eigenständigen Server zum Domänencontroller nur über eine Neuinstallation des Systems durchführen lässt.

Nach der Installation kann bei Bedarf die Mitgliedschaft in einer Domäne konfiguriert werden und das System gestattet die Installation und Konfiguration anderer Dienste.

Nun haben Sie einen Überblick über das, was Sie im nächsten Abschnitt erwartet. Es folgt nun eine ausführliche Beschreibung des gesamten Installationsprozesses.

3.4 Der Installationsprozess im Detail

Der Installationsprozess besteht aus dem Booten von Windows 2000, der Konfiguration von Windows 2000 sowie der Konfiguration des Netzwerkzugriffs.

3.4.1 Windows 2000 starten

Windows 2000 lässt sich von CD-ROM oder von der Festplatte aus installieren. Bei CD-ROM-Installationen braucht nur die CD-ROM in das Laufwerk eingelegt und ein Neustart des Systems durchgeführt zu werden. Die CD-ROM startet Windows 2000 und der Installationsprozess beginnt.

Bei der Installation von der Festplatte aus muss unter Windows 9x oder Windows NT das Programm *Winnt32.exe* oder unter MS-DOS oder Windows 3.x (an der Befehlszeile) das Programm *Winnt.exe* ausgeführt werden. Dabei wird eine Kopie der Dateien auf dem System erstellt, die normalerweise von CD-ROM gestartet werden. Anschließend erfolgt ein Systemneustart und die Installation beginnt am selben Punkt wie bei der Installation von CD-ROM. Bei der Installation von der Festplatte müssen Sie beachten, dass eine Systempartition existieren muss, bevor Windows 2000 installiert werden kann. Das Programm *Winnt* kopiert alle Dateien auf die Festplatte und diese Dateien können während der Installation nicht entfernt werden. Deshalb kann das System die Festplatten bei einer Installation von der Festplatte während der Installation nicht neu partitionieren.

Der Bootprozess von Windows 2000 muss herausfinden, von welcher Art von Datenträger aus die Installation durchgeführt werden kann. Im Wesentlichen müssen alle IDE- und SCSI-Adapter im System gefunden werden. Wenn der Adapter verfügbar war, als Windows 2000 ausgeliefert wurde, gibt es kein Problem. Der Adapter wird gefunden und die Installation beginnt. Ansonsten benötigen Sie eventuell eine Diskette vom Hardwarehersteller, um die Adaptertreiber während des Ladevorgangs zu laden. Am Anfang des Bootprozesses gibt es eine Stelle, an der Sie aufgefordert werden, die Taste (F6) zu drücken, um einen Adapter eines Drittanbieters zu installieren. Wenn der Adapter nicht vom Windows 2000-Installationsmedium aus installiert werden kann, *muss* diese Option verwendet werden, um die Treiber einzurichten, die zur Fertigstellung des Bootprozesses benötigt werden.

Wenn Windows 2000 nicht starten kann, bricht die Installation mit einer `INACCESSIBLE_BOOT_DEVICE`-Meldung ab. Die Meldung sollte nur auftreten, wenn der Adapter für den Datenträger nicht verfügbar ist oder wenn ein Eingriff vom Benutzer erfolgte, durch den die Installationspartition nicht mehr nutzbar war.

Den ersten Bildschirm im Installationsprozess, bei dem Sie etwas eingeben müssen, sehen Sie in Abbildung 3.1. Er bietet drei Optionen an. Die erste Option ist die Installation von Windows 2000, die Sie sehr wahrscheinlich nutzen wollen. Drücken Sie dazu die (Enter)-Taste. Die zweite Option dient dazu, eine beschädigte Installation zu reparieren. Diese

Installationsart wird über die (R)-Taste gestartet. Sie wird im Abschnitt über die Notfalldiskette ausführlicher beschrieben. Die letzte Option dient dazu, die Installation abubrechen. Drücken Sie dazu die (F3)-Taste.

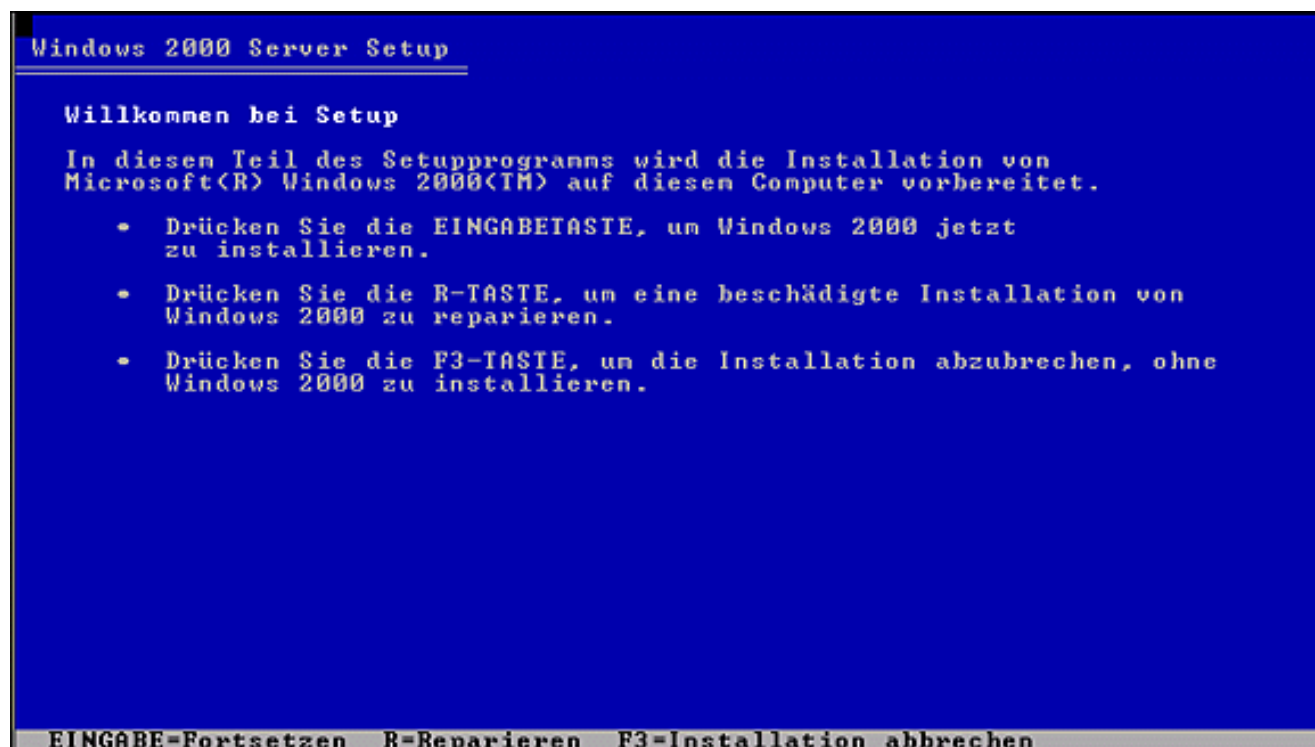


Abbildung 3.1: Dies ist der erste Bildschirm der Windows 2000-Installation, bei dem Sie eine Entscheidung treffen müssen. Drücken Sie die (Enter)-Taste, um fortzufahren.

Das Setup-Programm prüft dann, welche Datenträger für die Installation von Windows 2000 verfügbar sind. Zuerst wird festgestellt, ob überhaupt formatierte Partitionen verfügbar sind. Sind keine formatierten Partitionen vorhanden, werden Sie aufgefordert, dies zu bestätigen. Sind Datenträger verfügbar, prüft das Setup-Programm, ob es eine Systempartition gibt und ob auf dieser ein Betriebssystem installiert ist. Sie können wählen, ob Sie die Installation durchführen oder eine neue Partition für die Installation wählen möchten. Als Nächstes ermittelt das Setup-Programm, ob ein Update vom bestehenden Betriebssystem möglich ist. Sie werden gefragt, ob die bestehende Installation gelöscht und eine neue Installation durchgeführt werden oder ob die Installation in einem anderen Ordner erfolgen soll.

Als Nächstes wird Ihnen die Lizenzvereinbarung präsentiert, die Sie sich sorgfältig durchlesen sollten. Drücken Sie dann die (Bild¼)-Taste, um ans Ende der Lizenzvereinbarung zu gelangen, und drücken Sie die (F8)-Taste, um die Lizenzvereinbarung zu akzeptieren.

Bei einer Neuinstallation kommt noch ein Schritt hinzu, bei dem die Festplattenpartition eingerichtet wird, auf der Windows 2000 installiert werden soll (siehe Abbildung 3.2). In diesem Bildschirm erzeugen Sie über die (E)-Taste eine neue Partition. Um eine Partition zu löschen, markieren Sie diese und drücken dann die (L)-Taste.

Windows 2000 Server Setup

In der Liste unten sind die bestehenden Partitionen und nicht partitionierten Bereiche auf diesem Computer aufgeführt.

Verwenden Sie die NACH-OBEN- und NACH-UNTEN-TASTEN, um eine Partition oder einen nicht partitionierten Bereich in der Liste auszuwählen.

- Drücken Sie die EINGABETASTE, um Windows 2000 in der ausgewählten Partition zu installieren.
- Drücken Sie die E-TASTE, um eine Partition in dem unpartitionierten Bereich zu erstellen.
- Drücken Sie die L-TASTE, um die ausgewählte Partition zu löschen.

1000 MB Festplatte 0, ID=0, Bus=0 (an atapi)

Unpartitionierter Bereich 999 MB

EINGABE=Installieren E=Partition erstellen F3=Installation abbrechen

Abbildung 3.2: Das Setup-Programm muss wissen, wo das Betriebssystem installiert werden soll. Hier gibt es nur eine Festplatte. Drücken Sie die (E)-Taste, um eine Partition zu erstellen.

Layout der Festplattenpartitionen für die Installation

Es gibt Kontroversen darüber, welche Dateisysteme und Festplattenlayouts für die Installation von Windows 2000 am besten geeignet sind. Diese Meinungsverschiedenheiten rühren hauptsächlich daher, dass es nicht möglich ist, ein Betriebssystem zu booten, das auf Partitionen zugreifen kann, die mit dem Dateisystem NTFS formatiert sind. Es gibt sowohl Befürworter des NTFS- als auch des FAT-Dateisystems. Wenn Sie nicht wissen, was NTFS und FAT ist, sollten Sie den Abschnitt zu Dateisystemen in Kapitel 4 lesen.

Für das FAT-Dateisystem spricht, dass es zahlreiche Dienstprogramme für die Diagnose und Reparatur von FAT-Partitionen gibt, nicht aber für NTFS. Außerdem ist es ganz nützlich, von Diskette aus booten und Dateien ersetzen zu können, die benutzt werden, da einige Dateien nicht überschrieben werden können, wenn Windows 2000 ausgeführt wird. Da auf die Systempartition selten geschrieben wird, besteht kein großer Bedarf für den zusätzlichen Overhead der Protokollierung der Transaktionen, die beim Dateisystem NTFS erfolgt. Das Dateisystem FAT erhöht eigentlich die Performance.

Die Befürworter von NTFS stellen die Tatsache in den Vordergrund, dass die Bootpartition durch die NTFS-Dateiberechtigungen geschützt werden kann. Außerdem sagen sie, dass es ein wichtiges Sicherheitsmerkmal ist, dass NTFS während eines Bootvorgangs von Diskette nicht erreichbar ist, da dies den Fall ausschließt, dass Leute zum Server gehen, von Diskette booten und mit den ganzen Informationen wieder weggehen.

Allgemein wurde dieses Dilemma bisher dadurch gelöst, dass FAT bei Bootpartitionen auf Servern verwendet wurde, die physisch sicher sind, d.h., dass nur vertrauenswürdige Personen die Möglichkeit haben, von einer Diskette zu booten. NTFS sollte auf Servern verwendet werden, die zusätzlich gesichert werden müssen. Eine weitere Lösung für dieses Problem besteht darin, immer das NTFS-Dateisystem zu nutzen und zusätzlich die Wiederherstellungskonsole zu installieren, die später in diesem Kapitel beschrieben wird. Active Directory-Dienste lassen sich nur auf NTFS-Partitionen installieren. Die Frage ist also bei Servern, die Domänencontroller für ein Windows 2000 Active Directory sind, überflüssig.



Nachdem Sie die Systempartition ausgewählt haben, bereitet Windows 2000 das System auf die nächste Phase der Installation vor. Normalerweise muss bei einem Update die alte Version des Betriebssystems gelöscht werden. Dann können die neuen Systemdateien in das Windows 2000-Verzeichnis installiert werden (standardmäßig das Verzeichnis `C:\Winnt`). Während die Dateien kopiert werden, ist der in Abbildung 3.3 gezeigte Bildschirm sichtbar. Nach dem Kopiervorgang wird das System neu gebootet und die Konfigurationsphase beginnt.

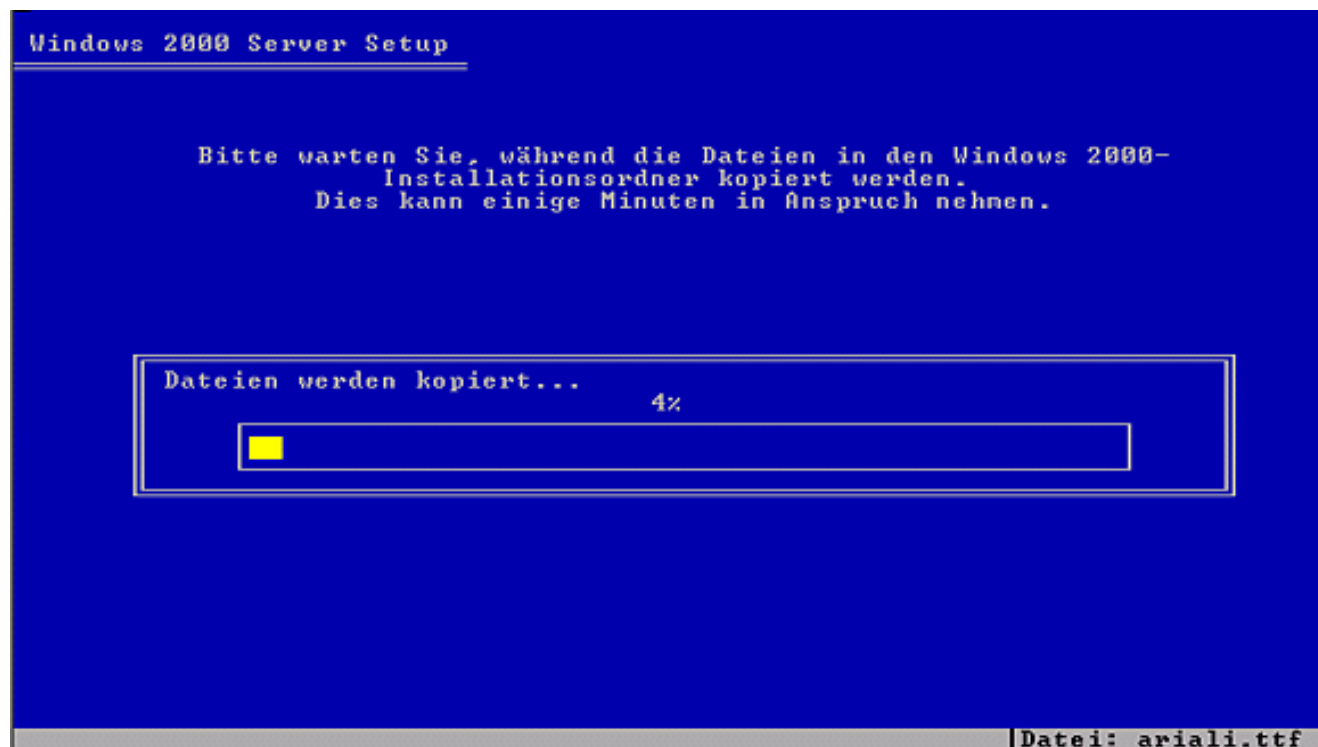


Abbildung 3.3: Der Kopiervorgang-Bildschirm erscheint, wenn das System die zur Ausführung von Windows 2000 benötigten Dateien auf die Festplatte kopiert.

3.4.2 Update-Informationen

Bei einer Update-Installation von Windows 2000 entfernt das System den größten Teil der Windows NT-Installation - zumindest, was die Systemdateien betrifft - und ersetzt die Systemdateien dann im Rahmen der Windows 2000-Installation. Die Benutzer- und Systemeinstellungen sowie die Registrierung der Anwendungen werden übernommen. Deshalb müssen die Anwendungen nach einem Update nicht neu installiert werden.

Die Treiber und Treiberkonfigurationen werden bei einem Update nicht übernommen. Wenn unter Windows NT 4.0 eine bestimmte Soundkarte installiert wurde und Windows 2000 diese nicht unterstützt, wird sie unter Windows 2000 nicht funktionieren, da Windows 2000 keine Treiber von Windows NT 4.0 nutzen kann. Dasselbe gilt für Updates von Windows 98.

Außerdem ändert sich die Lage einiger Dateien bei der Neuinstallation von Windows 2000 und bei Updates. Bei Windows NT 4.0 wurden Benutzerprofile im Verzeichnis `x:\Winnt\Profiles` gespeichert. Diese Informationen werden nun im Verzeichnis `x:\Dokumente und Einstellungen` abgelegt. Beim Update verschiebt Windows 2000 die Dateien jedoch nicht, sondern benutzt weiterhin das Verzeichnis `x:\Winnt\Profiles`.

3.4.3 Windows 2000 konfigurieren

Nachdem der Kopiervorgang im Textmodus beendet ist, wird das System neu gebootet und die Konfigurationsphase des Setups beginnt. Das System bootet, wie in Abbildung 3.4 gezeigt, in Windows 2000. Dann wird der Windows 2000-Setup-Assistent gestartet und die Phase der Systemkonfiguration beginnt.



Abbildung 3.4: Windows 2000 bootet das erste Mal im GUI-Modus

Nun beginnt Windows 2000 nach Geräten zu suchen. Wenn alle Geräte des Systems in der Windows 2000-Hardwarekompatibilitätsliste enthalten sind, gibt es keinen Grund zur Sorge. Die Hardware wird erkannt und die Hardwaretreiber werden konfiguriert. Dieser Prozess dauert eine gewisse Zeit (15 Minuten bis zu einer halben Stunde). Der Bildschirm flackert mehrmals auf, wenn das System versucht herauszufinden, welche Grafikkarte und welcher Monitor benutzt werden. Das System stoppt einige Male, wenn die seriellen Anschlüsse abgefragt werden, die lange Timeout-Intervalle haben. Besorgen Sie sich eine Tasse Kaffee, lehnen Sie sich zurück, entspannen Sie sich und betrachten Sie eine Weile die hübsch blinkenden Lichter.

Wenn das System unerklärlich lange ohne Festplattenaktivität hängt, die Maus sich nicht bewegen lässt und die Tastatur nicht reagiert, sollten Sie mindestens 15 Minuten warten, bevor Sie weitere Schritte unternehmen. Bei manchen Geräten dauert es sehr lange, bis diese erkannt und konfiguriert werden. Wenn es sich um eine Installation auf einem Laptop handelt, sollten Sie sicherstellen, dass das Diskettenlaufwerk korrekt angeschlossen ist, weil das System möglicherweise auf eine Reaktion vom Diskettenlaufwerk wartet, bevor es die Installation fortsetzt.

Als Nächstes folgen Fragen zum Gebietsschema. Standardmäßig ist Deutschland ausgewählt. Wollen Sie diese Einstellung verändern oder zusätzliche Gebiete und Sprachen auswählen, klicken Sie auf die Schaltfläche Anpassen (siehe Abbildung 3.5).



Abbildung 3.5: Hier können Sie das Gebietsschema ändern, um z.B. mehrere Spracheinstellungen zu nutzen

Im nächsten Bildschirm werden Ihre Benutzerinformationen abgefragt. Sie müssen hier den Namen und die Organisation angeben, für die die Software registriert werden soll. Dann erfolgt die Wahl des Lizenzierungsmodus. Einzelheiten hierzu finden Sie im Abschnitt »Lizenzierungsmodelle« weiter unten in diesem Kapitel. Wenn Sie nicht sicher sind, welchen Lizenzierungsmodus Sie wählen sollen, übernehmen Sie die Standardeinstellung Pro Server, da ein späterer Wechsel zum Lizenzierungsmodus Pro Arbeitsplatz möglich ist.

Als Nächstes müssen der Computernamen, das Administratorkennwort und die Kennwortbestätigung eingegeben werden (siehe Abbildung 3.6). Als Computernamen ist eine Kombination des Besitzernamens und einer Zufallszahl vorgegeben. Dadurch soll gewährleistet werden, dass alle Computer in einem Netzwerk eindeutige Namen tragen. Wählen Sie bei Bedarf einen anderen aussagekräftigen und eindeutigen Namen. Das Administratorkennwort ist das Kennwort für das lokale Konto des Administrators.

Windows 2000 Server Setup

Computernamen und Administratorkennwort
Geben Sie einen Namen und ein Administratorkennwort für den Computer ein.

Ein Computernamen wurde vorgeschlagen. Wenn sich der Computer in einem Netzwerk befindet, können Sie den Computernamen vom Netzwerkadministrator erhalten.

Computernamen:

Es wird ein Benutzerkonto mit Namen "Administrator" erstellt. Verwenden Sie dieses Konto, wenn Sie Vollzugriff auf den Computer benötigen.

Geben Sie ein Administratorkennwort ein.

Administratorkennwort:

Kennwortbestätigung:

< Zurück Weiter >

Abbildung 3.6: In dieses Dialogfeld müssen Sie einen eindeutigen Computernamen und ein Administratorkennwort eingeben

Zum Schluss gibt es noch einige optionale Komponenten. Diese sind in folgende Kategorien aufgeteilt:

Clusterdienste. Nur in der Version Advanced Server verfügbar. Diese Option installiert alle Programme, die benötigt werden, um das Windows 2000-Clustering zu ermöglichen.

Indextdienst. Dieser Dienst kann die Lage aller Dateien und Dateieigenschaften auf einem Server speichern, um die Suche nach Dateien zu beschleunigen.

Internet-Informationdienste (IIS). Gestattet Windows 2000, Internetdienste auf der Basis der installierten Unterkomponenten anzubieten.

- **Dokumentation.** Dokumentation aller Dienste (im HTML-Format).
- **FrontPage 2000-Servererweiterungen.** Erweiterungen, die für IIS-Server benötigt werden, um Webs veröffentlichen zu können, die mit FrontPage 2000 erstellt werden.
- **FTP-Server (File Transfer Protocol).** Implementiert das Standard-FTP-Protokoll, das Clients den Dateiversand und Empfang vom Server gestattet.
- **Gemeinsame Dateien.** Erforderlich für IIS-Server. Werden von vielen Komponenten benötigt.
- **Internetdienste-Manager (HTML).** HTML-basierte grafische Benutzeroberfläche für die Verwaltung der Internetdienste von IIS. Funktioniert nur, wenn der WWW-Server ausgeführt wird.
- **Internet-Informationdienste Snap-In.** Das IIS-Snap-In gestattet die Verwaltung von IIS-Server über die Microsoft Management-Konsole (MMC - Microsoft Management Console).
- **NNTP-Dienst.** Der Server kann als Network News Transfer-Server eingesetzt werden.
- **SMTP-Dienst.** Der Server kann den SMTP-Dienst anbieten, das Standard-Mail-System des Internets. Es lassen sich dann Mailboxen und Weiterleitungsdienste einrichten.
- **Unterstützung von Visual InterDev RAD Remote-Bereitstellung.** Ermöglicht Visual InterDev die Remote-Bereitstellung von Anwendungen (Komponenten und ASP-Seiten) auf dem Server.

- **WWW-Server.** Der Server kann Websites mit HTML-Seiten anbieten sowie ASP verarbeiten und anbieten.

Message Queuing-Dienst. Die Microsoft Message Queue (MMQ) steht nur unter Windows 2000 Advanced Server zur Verfügung. Ein sehr zuverlässiger Nachrichtenübermittlungsdienst für die Kommunikation im Netzwerk.

Netzwerkdienste. Die Dateien und Systeme, die für den Netzwerkzugriff erforderlich sind.

- **COM-Internetdiensteproxy.** Ermöglicht COM-Objekten die Kommunikation über das HTTP-Protokoll sowie das erfolgreiche Passieren zahlreicher Proxyserver und Firewalls.
- **DHCP-Protokoll (Dynamic Host Configuration Protocol).** Das Protokoll, mit dem IP-Adressen Arbeitsstationen im Netzwerk zugewiesen werden.
- **Directory Service-Migrationstool.** Das Tool, das zur Migration von Novells Directory Services zu Microsofts Active Directory erforderlich ist. Erfordert und installiert die Gateway Services für NetWare.
- **DNS-Server (Domain Name System).** Das Standardbenennungssystem im Internet, das nun für Active Directory benötigt wird. Der DNS-Server übersetzt Netzwerknamen (wie *www.microsoft.com*) in IP-Adressen (wie 207.46.130.50).
- **Einfache TCP/IP-Dienste.** Unterstützt einfache Dienste wie »Zitat des Tages«, »Zeichengenerator«, »Daytime«, »Discard« und »Echo«.
- **Internetauthentifizierungsdienst.** Gestattet die Authentifizierung eingehender VPN- und DFÜ-Netzwerkverbindungen über das RADIUS-Protokoll.
- **QoS-Zugangssteuerungsdienst.** Überwacht und misst den eingehenden Netzwerkverkehr. Für jedes Subnetz lässt sich die Verbindungsgüte angeben.
- **Site Server-ILS-Dienste.** Überwacht und unterhält Benutzerinformationen.
- **WINS (Windows Internet Name Services).** Ein Protokoll, das an Bedeutung verloren hat und durch das bei weitem überlegene Protokoll DNS ersetzt wurde.

Remoteinstallationsdienste. Erlaubt die Installation von Windows 2000 Professional auf Computern, die remotestartfähig sind.

Remotespeicher. Dienst dazu, selten benutzte Dateien auf Magnetband oder ein anderes wiederverwendbares Medium zu speichern. Mehr hierzu erfahren Sie in Kapitel 4.

Script Debugger. Skriptprogramme, die mit VBScript oder JScript erstellt wurden, lassen sich debuggen.

Terminaldienste und Terminaldienstelizenzen. Die Terminaldienste werden später in diesem Buch beschrieben. Sie stehen nur in der Advanced Server-Installation zur Verfügung.

Verwaltungs- und Überwachungsprogramme. Dies sind Programme zur Verwaltung von Windows 2000 und zur Überwachung der Netzwerkschnittstelle auf einem Windows 2000-Server.

- **Netzwerkmonitorprogramme.** Dies ist Microsofts Protokollanalysetool, das auch als *Packet Sniffer* bezeichnet wird. Es werden die übertragenen Datenpakete analysiert.
- **SNMP (Simple Network Management Protocol).** Das Protokoll, das für die Remote-Überwachung von Geräten und Servern über das Internet eingesetzt wird.
- **Verbindungs-Manager-Komponenten:** Das Verbindungs-Manager-Verwaltungskit und der Telefonbuchdienst.

Weitere Datei- und Druckdienste für das Netzwerk. Enthält Komponenten wie Datei- und Druckdienste für Macintosh und Druckdienste für Unix.

Windows Media-Dienste: Multimediainhalte lassen sich Netzwerkbenutzern verfügbar machen.

Zertifikatsdienste. Diese beiden Komponenten, der Webregistrierungssupport für Zertifikatsdienste und die Zertifizierungsstelle für Zertifikatsdienste, dienen dazu, Zertifikate für Sicherheitsanwendungen zu erstellen, die öffentliche Schlüssel verwenden.

Zubehör und Dienstprogramme. Diese Kategorie enthält die meisten Dienstprogramme von Windows 2000.

- **Eingabehilfen-Assistent.** Unterstützt Benutzer mit Körperbehinderungen bei der Bedienung des Computers.

- *Kommunikation*. Diese Komponente enthält drei Unterkomponenten:
- *HyperTerminal*. Der sehr dürftige Ersatz für Windows Terminal. HyperTerminal steuert Modems und DFÜ-Netzwerkverbindungen für die direkte Terminalkommunikation. Die Benutzeroberfläche ist jedoch nicht sehr gut gelungen.
- *Telefon*. Ein Programm, um mit anderen Windows-Benutzern über ein Netzwerk per Telefon zu kommunizieren.
- *Wählhilfe*. Wenn ein Modem an den Computer angeschlossen ist, ermöglicht die Wählhilfe die automatische Anwahl von Telefonnummern über das Modem.
- *Multimedia*. Programme zur Wiedergabe von Audio-, Animations- und Videodateien über ein CD-ROM-Laufwerk und eine Soundkarte. Bietet verschiedene Audiodateien, einen Audiorecorder, einen CD-Player, eine Lautstärkeregelung, den Media Player und Audioschemata.
- *Spiele*. Enthält vier klassische Windows-Spiele: FreeCell, Minesweeper, Pinball und Solitär.
- *Zubehör*. Diese Kategorie ist der wesentliche Bestandteil der Kategorie *Zubehör und Dienstprogramme*. Sie enthält die folgenden Komponenten:
 - *Desktop-Hintergrund*. Der Desktop-Hintergrund ist eine Sammlung von Hintergrundbildern für den Windows-Desktop.
 - *Dokumentvorlagen*. Vorlagen für WordPad.
 - *Mauszeiger*. Ein Paket mit animierten Mauszeigern und Mauszeigern mit unterschiedlichen Zeigergrößen und -formen. Um den Mauszeiger zu ändern, klicken Sie in der Systemsteuerung doppelt auf Maus und wählen dann den gewünschten Typ auf der Registerkarte Zeiger aus.
 - *Objekt-Manager*. Erzeugt verknüpfte Objekte und bettet diese in die verschiedenen Anwendungen des Systems ein.
 - *Paint*. Ein sehr einfaches Zeichenprogramm, um Grafiken zu erstellen, zu bearbeiten und anzuzeigen.
 - *Rechner*. Ein einfaches Rechnerprogramm, das sich sowohl für die einfache Addition als auch für die Berechnung von Netzwerkmasken als nützlich erweist.
 - *WordPad*. Eine einfache, aber sehr nützliche Textverarbeitung.
 - *Zeichentabelle*. Über die Zeichentabelle lassen sich Symbole und Zeichen in Dokumente einfügen.
- *Zwischenablagenansicht*. Ermöglicht es, Informationen in der Zwischenablage zu speichern und diese zu betrachten.

Wie Sie sehen, gibt es zahlreiche verschiedene Komponenten. Wurden Komponenten während des Setups nicht installiert, lassen sie sich nachträglich über die Systemsteuerung hinzufügen. Klicken Sie dazu in der Systemsteuerung doppelt auf Software, aktivieren Sie die Registerkarte Windows Setup und klicken Sie auf Hinzufügen. Bei einem Server ist außer WordPad und dem Rechner das meiste Zubehör deaktiviert. Andere Dienste werden nur bei Bedarf installiert und können sogar Probleme verursachen, wenn sie ohne Bedarf installiert werden (beispielsweise DHCP).

3.4.4 Die Konfiguration der Netzwerkeinstellungen

Der nächste Schritt im Installationsprozess ist die Konfiguration der Netzwerkeinstellungen. Die neuen Standardeinstellungen für Windows 2000 sind das TCP/IP-Transportprotokoll, die Datei- und Druckerfreigabe für Microsoft-Netzwerke und Clients für Microsoft-Netzwerke. TCP/IP wird standardmäßig über DHCP konfiguriert. Wenn sich diese Einstellungen für Ihre Umgebung eignen, können Sie die Option Standardeinstellungen wählen. Ansonsten wählen Sie die Option Benutzerdefinierte Einstellungen.

Die Konfiguration über Benutzerdefinierte Einstellungen beginnt zunächst mit der Installation der üblichen Einstellungen. Es können außerdem Komponenten hinzugefügt und entfernt werden und es lassen sich Eigenschaften von Komponenten verändern (siehe Abbildung 3.7).



Abbildung 3.7: Hier werden die Netzwerkeinstellungen bei der Installation festgelegt. Klicken Sie auf die Schaltfläche **Installieren**, um Komponenten hinzuzufügen.

Um Komponenten hinzuzufügen, klicken Sie auf die Schaltfläche **Installieren**. Es öffnet sich eine Liste mit den drei Komponententypen *Client*, *Dienst* und *Protokoll*. Ein *Client* ist eine Komponente, die einem angemeldeten Benutzer den Zugriff auf einen anderen Computer ermöglicht. Ein *Dienst* ist eine Ressource, die auf dem lokalen Computer installiert wird und auf die andere Computer über das Netzwerk zugreifen können. Ein *Protokoll* legt fest, wie der Zugriff auf den Computer erfolgt und wie die Clients des Computers mit den anderen Diensten des Computers kommunizieren. Ein Beispiel für einen Client ist der Client für Microsoft-Netzwerke, der anderen Computern gestattet, den lokalen Computer als Dateiserver zu benutzen. Ein Beispiel für ein Protokoll ist TCP/IP, das Servern die Kommunikation mit Clients erlaubt.

Klicken Sie auf die Art von Komponente, die Sie hinzufügen möchten, und klicken Sie dann auf die **Hinzufügen**-Schaltfläche. Wählen Sie anschließend in der Liste die gewünschte Komponente aus und klicken Sie auf **OK**. Einige Komponenten setzen andere Komponenten voraus (z.B. benötigt der Clientdienst für NetWare das NWLink-Protokoll). Das Setup-Programm installiert alle abhängigen Komponenten, damit die ausgewählte Komponente funktioniert.

Um eine bestehende Komponente zu konfigurieren, wählen Sie die Komponente in der Liste aus und klicken auf die Schaltfläche **Eigenschaften**. Die Komponente TCP/IP kann entweder automatisch über DHCP oder manuell konfiguriert werden. Beim Setup von TCP/IP müssen drei Werte eingestellt werden: die IP-Adresse, die Subnetzmaske und das Standard-Gateway. Die IP-Adresse muss innerhalb des Netzwerks eindeutig und numerisch sein. Ein Beispiel für eine IP-Adresse ist 10.1.1.3. Die Subnetzmaske identifiziert, welcher Teil der IP-Adresse das Netzwerk identifiziert und welcher den speziellen Computer. Eine Subnetzmaske von 255.0.0.0 bedeutet, dass der erste Teil der Adresse zur Identifikation des Netzwerks dient und der Rest zur Identifikation des individuellen Computers. Innerhalb eines Netzwerks müssen alle Subnetzmasken identisch sein. Weitere Informationen zu Subnetzmasken finden Sie in Kapitel 8. Das Standard-Gateway ist eine IP-Adresse eines Geräts im lokalen Subnet, das weiß, wie der Übergang zu anderen Subnets erfolgen kann. Dies ist die IP-Adresse des lokalen Routers.

Dies wirkt nun alles ziemlich kompliziert und ist eigentlich auch ein Verwaltungsalptraum. Deshalb hat Microsoft einen Standard namens *DHCP* (Dynamic Host Configuration Protocol) implementiert, der Computern gestattet, ihre Netzwerkinformationen von einem Server im Netzwerk zu beziehen, der dafür konfiguriert ist, diese Informationen bereitzustellen. Wählen Sie **IP-Adresse automatisch beziehen**, muss das System DHCP zur Konfiguration des Netzwerks verwenden.

Im Netzwerk gibt es außerdem wahrscheinlich mindestens einen DNS-Server. Ein DNS-Server wandelt IP-Adressen (wie 10.1.1.3) in verständliche Namen um. Die DNS-Serveradresse kann manuell eingegeben oder über DHCP bezogen werden.

Zu diesem Zeitpunkt können auch andere TCP/IP-bezogene Dienste installiert werden. Weitere Informationen über diese Dienste und ihre Installation erhalten Sie in Kapitel 8.



Während der Installation sollten Sie nur ein Minimum an Netzwerkprotokollen und Diensten installieren, um dafür zu sorgen, dass der Server online ist und mit anderen Servern im Netzwerk kommunizieren kann. Dadurch reduziert sich die Anzahl der Faktoren, die Sie prüfen müssen, wenn ein Problem bei der Installation auftritt. Je einfacher die Problembehandlung ist, desto besser. Protokolle und Dienste lassen sich immer nachträglich hinzufügen. In Kapitel 15 erfahren Sie mehr über die Installation von Protokollen.

Während des Setups werden auch andere Protokolle zur Installation angeboten. Das AppleTalk-Protokoll dient zur

Kommunikation mit Apple-Computern inklusive des Macintosh. Das DLC-Protokoll wird normalerweise benutzt, um eine Verbindung zu alten Druckservern herzustellen, wie z.B. ältere Versionen von HP JetDirect. Das Protokoll NetBEUI ist ein altes Protokoll, das (hoffentlich) als primäres LAN Manager-Protokoll ausstirbt. Das Network Monitor Driver-Protokoll nutzt der Microsoft Netzwerkmonitor, um den Versand der Datenpakete im Netzwerk zu beobachten.

Das NWLink-Protokoll ist Microsofts Implementierung von IPX/SPX. Das NetBIOS-API ist ebenfalls vorhanden. Dieses Protokoll dient zur Kommunikation mit Novell NetWare-Servern. Diese ganzen Protokolle werden in Kapitel 15 ausführlicher besprochen.

Standardmäßig installiert das System das TCP/IP-Protokoll. Anschließend wird der Dienst Datei- und Druckerfreigabe für Microsoft-Netzwerke hinzugefügt. Und der Client für Microsoft-Netzwerke bietet Zugriff auf andere Windows 2000- und Windows NT-Server, die im Netzwerk verfügbar sind.

Außerdem können optionale Dienste und Clientsoftware sowie zwei zusätzliche Dienste installiert werden. Der erste ist der QoS Packet Scheduler, der mit Routern zusammenarbeitet, um Quality of Services-Informationen zu übermitteln. Der SAP-Agent ist ein weiterer Dienst, der ebenfalls gemeinsam mit Novell NetWare eingesetzt wird und für die Kommunikation von Serverinformation nützlich ist.

Wenn alle Netzwerkinformationen ausgewählt sind, klicken Sie auf Weiter. Das System fordert Sie dann auf, die Rolle dieses Computers im Netzwerk anzugeben. Ein Server kann der einzige Server im Netzwerk oder Bestandteil einer Domäne sein. Wenn der Server nicht in ein Netzwerk integriert ist oder wenn es keine Domäne gibt, wählen Sie die Option Nein, ansonsten Ja. Geben Sie auf jeden Fall den Namen der Arbeitsgruppe oder Domäne in das Textfeld ein.

Wenn die Netzwerkkonfiguration beendet ist, richtet Windows 2000 den Rest des Betriebssystems ein. Dabei werden hauptsächlich Komponenten bei der Registrierung angemeldet und temporäre Dateien entfernt. Wenn die Systempartition mit NTFS formatiert wurde, richtet das Installationsprogramm die Berechtigungen für die Systemdateien so ein, dass Administratoren auf das, was sie benötigen, Zugriff haben, während die Systemdateien gesichert werden.

3.4.5 Lizenzierungsmodelle

Microsoft muss für die Software natürlich auch eine Bezahlung erhalten und dies geschieht, indem die Anzahl der Benutzer eines Servers aufgezeichnet werden. Die Lizenzierung ist ein sehr komplexes Thema und es geht dabei nicht nur um den juristischen Inhalt der Lizenz, sondern auch darum, für welches Lizenzierungsmodell sich eine Organisation entscheiden sollte. Um die Dinge noch verwirrender zu gestalten, hat Microsoft angekündigt, die Lizenzierung einfacher zu machen. Dies entspricht allerdings den Versprechungen der Regierung, die Steuergesetzgebung zu vereinfachen: Die Formulare werden immer länger und die meisten Leute zahlen am Ende mehr.

Bei Windows 2000 Server gibt es zwei Lizenzierungsmodelle. Die Serverlizenz ist eine Lizenz, bei der Windows 2000 Server auf einem Computer installiert werden kann. Eine Clientlizenz ermöglicht den Zugriff auf einen Windows 2000-Server von einem Computer im Netzwerk aus.

Bei der Lizenz von Windows 2000 Server handelt es sich um eine Datei- und Drucklizenz. Das heißt, wenn der Server als Datei- oder Druckserver verwendet wird, muss jeder Client, der auf den Server zugreift, eine Clientlizenz besitzen und jeder Server benötigt eine Serverlizenz. Wenn ein SQL Server oder Exchange Server auf dem Windows 2000-Server installiert wird, der Server aber nicht als Datei- oder Druckserver verwendet wird, sind keine Clientlizenzen für Windows 2000 Server erforderlich. Es werden jedoch eine Lizenz für Windows 2000 Server, eine Serverlizenz für SQL Server oder Exchange Server und Clientlizenzen für SQL Server oder Exchange Server benötigt.

Es gibt zwei Arten von Clientlizenzen. Eine *Pro-Arbeitsplatz*-Lizenz bedeutet, dass jeder Computer eine Lizenz benötigt und auf so viele Server zugreifen kann, wie er möchte. Eine *Pro-Server*-Lizenz bedeutet, dass jeder Server für die Anzahl der Clients, die gleichzeitig auf ihn zugreifen, Clientlizenzen benötigt. Microsoft schlägt die Verwendung der Pro Arbeitsplatz-Lizenz vor, weil das System sich leichter administrieren lässt und die Flexibilität höher ist, wenn jeder Client auf alle Server zugreifen kann. Die Pro Server-Lizenz ist erheblich komplizierter, weil darauf geachtet werden muss, wie viele Client jeweils mit einem Server verbunden sind. Preislich gibt es zwischen der Pro-Arbeitsplatz- und der Pro-Server-Lizenz keinen Unterschied und es ist möglich, einmalig von einer Pro-Server-Lizenz auf eine Pro-Arbeitsplatz-Lizenz zu wechseln. Dieser Wechsel kann nicht rückgängig gemacht werden. Wird ein Server als »Pro-Arbeitsplatz«-Server eingerichtet, ist kein Wechsel des Lizenzierungsmodells möglich.

In den nächsten Abschnitten wird anhand mehrerer Szenarios der Unterschied zwischen der Pro-Arbeitsplatz- und der Pro-Client-Lizenz erklärt.

3.4.6 Szenario 1: Die Pro-Server-Lizenz

Das Unternehmen XYZ betreibt ein Servicecenter und jeder Angestellte arbeitet an einem eigenen Computer. Das Servicecenter ist mit einem Server ausgestattet und es gibt 60 Mitarbeiter. Es ist jeweils nur ein Drittel der Computer in Benutzung. Das Unternehmen kann dann 10 Pro-Server-Lizenzen für den Server oder 60 Pro-Arbeitsplatz-Lizenzen kaufen.

3.4.7 Szenario 2: Die Pro-Client-Lizenz

Das Unternehmen XYZ erweitert die Rechnerkapazität des Servicecenters durch den Erwerb von drei zusätzlichen Servern, die als Datei- und Druckserver genutzt werden. Das Unternehmen kann nun entweder weitere Pro-Server-Lizenzen erwerben und benötigt dann weitere 60 Lizenzen für die Clients (insgesamt 80 Lizenzen) oder es kann zusätzlich 40 Lizenzen kaufen und dann alle Lizenzen in Pro-Arbeitsplatz-Lizenzen umwandeln. Durch den Umstieg auf die Pro-Arbeitsplatz-Lizenz kann jeder Client auf beliebig viele Server zugreifen. Es ist also ökonomischer, auf die Pro-Arbeitsplatz-Lizenz umzusteigen.

3.4.8 Lizenzen hinzufügen

Die Lizenzen werden über die Lizenzierung verwaltet, die Sie über den Menübefehl Start/Programme/Verwaltung/Lizenzierung öffnen. Bei der Installation müssen Sie sich zwischen der Pro-Server- und der Pro-Arbeitsplatz-Lizenz entscheiden (siehe Abbildung 3.8). Wenn Sie das Pro-Server-Lizenzierungsmodell wählen, müssen Sie die Anzahl der erworbenen Lizenzen über die Lizenzierung einrichten. Wurde das Pro-Arbeitsplatz-Lizenzierungsmodell gewählt, nutzt die Lizenzierung die Lizenzinformationen automatisch gemeinsam mit den anderen Servern in der Domäne. Wird die Anzahl der angemeldeten Lizenzen überschritten, werden die Warnhinweise im Ereignisprotokoll von Windows 2000 aufgezeichnet.

Um Pro-Server-Lizenzen hinzuzufügen, öffnen Sie in der Verwaltung die Lizenzierung, wählen auf der Registerkarte Produkte das Produkt, für das Sie weitere Lizenzen hinzufügen möchten, und klicken auf Lizenzen hinzufügen. Geben Sie unter Anzahl die Anzahl der Lizenzen ein, die das Unternehmen erworben hat, und klicken Sie auf OK. Über die Schaltfläche Lizenzen entfernen können Sie die Anzahl der Lizenzen reduzieren.

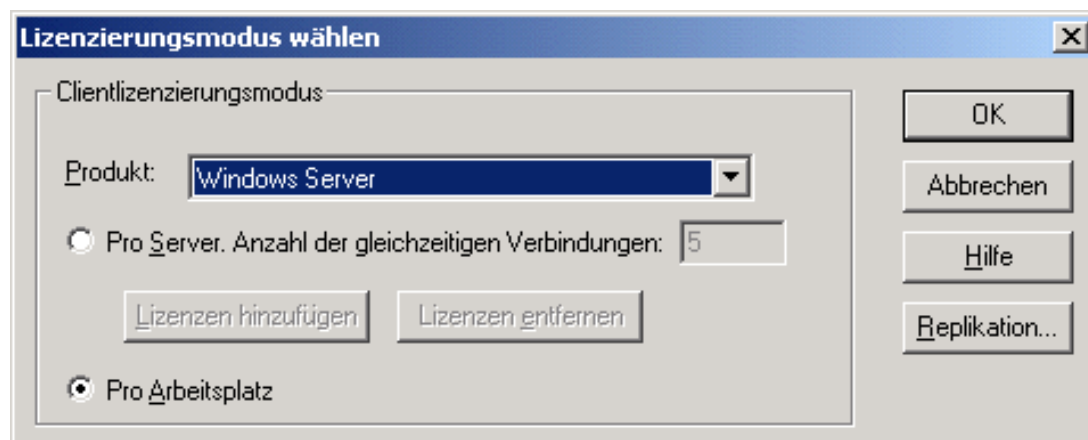


Abbildung 3.8: Die Lizenzierung. Klicken Sie auf Lizenzen hinzufügen. Um die Pro-Server-Lizenz einmalig in eine Pro-Arbeitsplatz-Lizenz umzuwandeln, wählen Sie die Option Pro Arbeitsplatz.

Um Lizenzen hinzuzufügen, öffnen Sie in der Systemsteuerung die Verwaltung und doppelklicken dort auf Lizenzierung. Wählen Sie auf der Registerkarte Produkte den Server aus, zu dem Sie Lizenzen hinzufügen möchten, und rufen Sie im Menü Lizenz den Befehl Neue Lizenz auf. Es öffnet sich das Dialogfeld Neue Clientzugriffslizenz. Geben Sie unter Anzahl die Anzahl der Clientzugriffslizenzen ein, die Sie hinzufügen möchten, und klicken Sie auf OK.

Über die Lizenzierung können Sie auch andere Produkte und Produktlizenzen verwalten. Öffnen Sie die Lizenzierung über

das Verwaltung-Symbol der Systemsteuerung. Auf der Registerkarte Erwerbsdatum sehen Sie das Datum, die Anzahl und den Administrator der erworbenen Lizenzen. Sie können hier Lizenzen hinzufügen oder entfernen. Auf der Registerkarte Produkte sehen Sie alle lizenzierbaren Produkte, die auf dem Server installiert wurden. Standardmäßig sind hier nur die Produkte *Windows Server* und *Microsoft BackOffice* aufgeführt. Eine BackOffice-Lizenz ist eine Clientzugriffslizenz für alle BackOffice-Produkte (Windows 2000, SQL Server, Exchange Server, Systems Management Server und SNA Server). Auf der Registerkarte Clients (Pro Arbeitsplatz) werden die Benutzer aufgeführt, die das Produkt im Pro-Arbeitsplatz-Modus verwendet haben. Auf der Registerkarte Server wird der Lizenzierungsmodus für Server innerhalb des Standortes und die Anzahl der Lizenzen im Pro-Server-Modus aufgeführt.



Bei einigen BackOffice-Produkten, wie z.B. der Systems Management Server, ist eine Pro- Arbeitsplatz-Lizenzierung erforderlich. Sie ist nicht mit der Pro-Server-Lizenzierung kompatibel.

Die Pro-Arbeitsplatz-Lizenzierung verhindert nicht den Zugriff auf die Anwendungen. Die Anwendungen können also weiterhin benutzt werden. Es werden jedoch Meldungen in das Ereignisprotokoll von Windows 2000 eingetragen.

3.5 Die unbeaufsichtigte Installation

Microsoft bietet Tools, um den Setup-Prozess zu automatisieren und die Software effizienter auf einer großen Anzahl von Computern installieren zu können. Für diesen Prozess müssen Sie zwei Dateien erstellen: eine Antwortdatei, die Antworten auf alle Fragen enthält, die das Setup-Programm stellt, und eine UDF-Datei (UDF = Uniqueness Database File), die die Antworten in der Antwortdatei mit bestimmten Einstellungen für einen Computer überschreibt, wie z.B. den Computernamen.

Microsoft stellt eine Datei namens *Unattend.txt* bereit, die eine Grundlage für die unbeaufsichtigte Installation bietet. Die Datei hat das grundlegende Format einer INI-Datei, bei dem die Abschnittsnamen in eckige Klammern gesetzt sind, denen eine Liste mit Wertenamen und Werten folgt. Zeilen, die mit einem Semikolon beginnen, sind Kommentare. Nachfolgend sehen Sie einen Ausschnitt.

```
[GuiUnattended]
; Setzt die Zeitzone auf mitteleuropäische Zeit.
; Setzt das Administrator Kennwort auf NULL.
; Setzt das AutoLogon auf ON und führt die
; Anmeldung einmal durch
TimeZone = "110"
AdminPassword = *
AutoLogon = Yes
AutoLogonCount = 1
```

Dieser Abschnitt heißt *GuiUnattended* und die nächsten vier Zeilen sind Kommentare, weil sie mit Semikolons beginnen. Danach folgen vier Eigenschaften. Die erste heißt *TimeZone* und hat den Wert »110«.

Auf der Website von Microsoft finden Sie im Supportbereich zahlreiche Optionen für die unbeaufsichtigte Installation. Klicken Sie einfach auf der Start-Webseite auf Support.

3.6 Die Wiederherstellungskonsole installieren

Die Wiederherstellungskonsole ist eine Bootoption von Windows 2000, die eine Eingabeaufforderung öffnet, welche Zugriff auf alle NTFS-Freigaben des Systems bietet und einige wichtige Operationen erlaubt, wie beispielsweise das Ersetzen von Dateien und den Wechsel von Bootoptionen. Dies ist sehr hilfreich, wenn der Server beim Booten wegen eines Treiberproblems stoppt oder wenn eine Datei während der Ausführung von Windows 2000 ersetzt werden muss.

Um die Wiederherstellungskonsole zu installieren, beenden Sie zunächst die Windows 2000-Installation. Öffnen Sie dann

die Eingabeaufforderung und wechseln Sie in das Verzeichnis, das das Windows 2000-Setup-Programm enthält (z.B. das Verzeichnis `\i386` auf der CD-ROM). Geben Sie anschließend den folgenden Befehl ein:

```
Winnt32 /cmdcons
```

Es öffnet sich das Dialogfeld Windows 2000 Setup (siehe Abbildung 3.9), über das Sie die Installation der Wiederherstellungskonsole starten können (siehe Abbildung 3.10). Wenn die Installation beendet ist, wird das Dialogfeld angezeigt, das Sie in Abbildung 3.11 sehen. Um die Wiederherstellungskonsole zu starten, wählen Sie beim Start des Computers aus den Startoptionen die Windows 2000-Wiederherstellungskonsole aus.

Um die Wiederherstellungskonsole zu benutzen, starten Sie Windows neu und wählen unter den Startoptionen Microsoft Windows 2000-Wiederherstellungskonsole (siehe Abbildung 3.12). Die Wiederherstellungskonsole wird nun geöffnet.

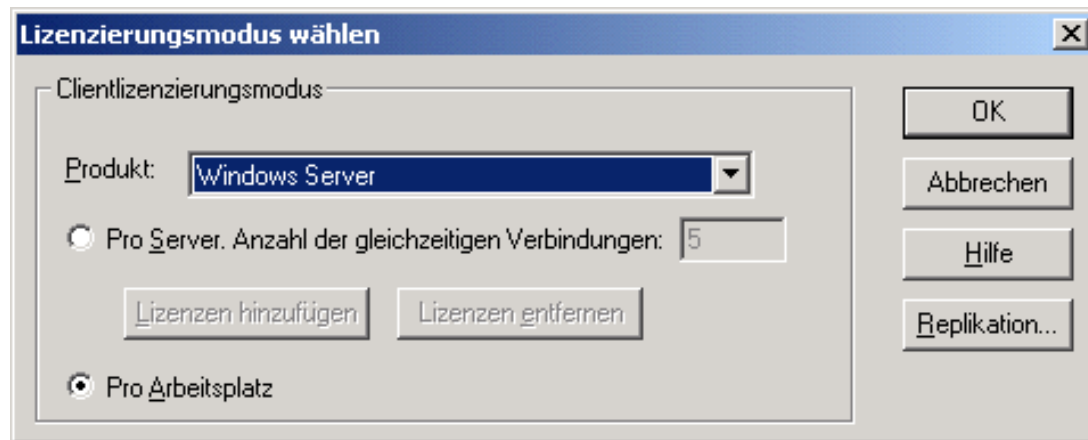


Abbildung 3.9: Starten Sie hier die Installation der Wiederherstellungskonsole



Abbildung 3.10: Zur Installation der Wiederherstellungskonsole benötigt das Setup-Programm ungefähr 7 Mbyte Festplattenspeicher

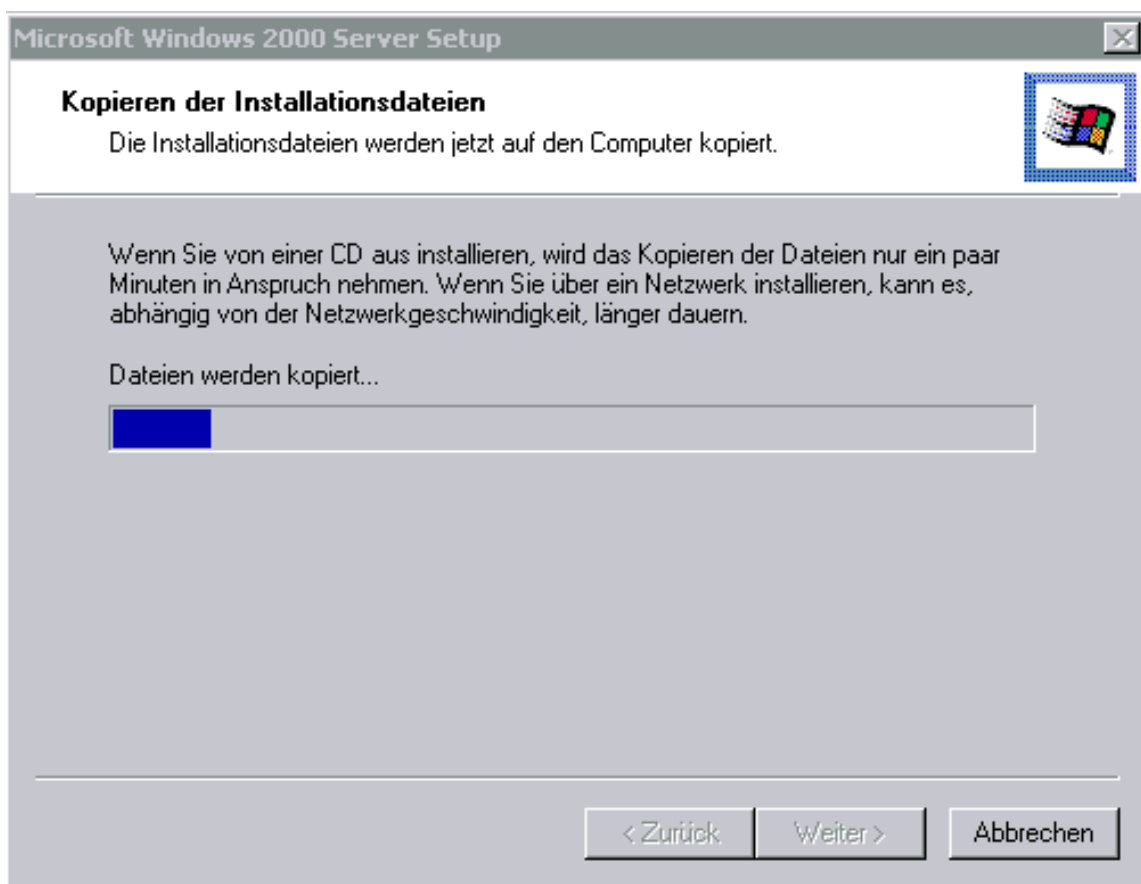


Abbildung 3.11: Wurde die Wiederherstellungskonsolle erfolgreich installiert, wird dieses Dialogfeld angezeigt.



Es gibt noch eine zweite Möglichkeit, die Wiederherstellungskonsolle zu starten. Starten Sie Ihren Computer mit einer Windows 2000-Startdiskette oder mit der Windows 2000-CD-ROM. Drücken Sie im Willkommensbildschirm die Taste (R) (für Reparieren) und dann (C), um die Wiederherstellungskonsolle zu starten.



Abbildung 3.12: Öffnen Sie die Wiederherstellungskonsolle über die entsprechende Startoption beim Booten des Systems

Über die Wiederherstellungskonsolle lassen sich SCSI- oder RAID-Geräte von Drittherstellern installieren. Drücken Sie dazu beim Start die (F6)-Taste. Sie sehen nun wie beim normalen Bootvorgang eine Punktefolge, die über den Bildschirm läuft, jedoch mit erheblich mehr Punkten. Dann werden Sie gefragt, bei welcher Windows 2000-Installation Sie sich anmelden möchten (siehe Abbildung 3.13).

Wählen Sie das zu startende Betriebssystem:

Microsoft Windows 2000 Server

Microsoft Windows 2000-Wiederherstellungskonsole

Verwenden Sie ↑ und ↓, um einen Eintrag zu markieren.
Drücken Sie anschließend die EINGABETASTE.

Problembehebung und erweiterte Windows 2000-Startoptionen: F8-TASTE drücken

Abbildung 3.13: Die Wiederherstellungskonsole fragt, bei welcher Windows 2000-Installation Sie sich anmelden möchten

Die Wiederherstellungskonsole benutzt die meisten Shellbefehle der normalen Befehlsshell. Um eine Liste aller Befehle einzusehen, geben Sie `help` ein. Um eine Liste mit bestimmten Befehlen zu sehen, geben Sie `help <befehl>` ein. Der Befehl `help fixmbr` liefert z.B. Hilfe zum Befehl `FIXMBR`.

Einige Befehle sind nicht Bestandteil der normalen Befehlsshell und bedürfen einer etwas genaueren Betrachtung.

- **LISTSVC**. Erzeugt eine Auflistung aller Dienste und zeigt deren aktuellen Startstatus an, d.h., ob der Dienst aktiviert ist oder nicht. Auf die Namen der Dienste können die Befehle `Enable` und `Disable` angewendet werden.
- **Disable** und **Enable**. Deaktivieren oder aktivieren Systemdienste. Der Befehl hat das Format `Enable <Dienstname>, [Startart]`. Der Parameter `<Dienstname>` ist der Name des Dienstes, der gestartet oder gestoppt werden soll. Der Parameter `[Starttyp]` gibt die Startart für den Dienst an.

Wenn die Startart weggelassen wird, druckt der Befehl `Enable` oder `Disable` den aktuellen Starttyp aus. Wenn ein bestimmter Dienst oder Treiber das System am Starten hindert, kann er deaktiviert und das System wieder gestartet werden. Wenn ein kritischer Dienst zufällig deaktiviert ist, kann er hier wieder aktiviert werden. Hier die zulässigen Startarten:

- `SERVICE_DISABLED`
- `SERVICE_BOOT_START`
- `SERVICE_SYSTEM_START`
- `SERVICE_AUTO_START`
- `SERVICE_DEMAND_START`
- `SERVICE_DISABLED`
- **SERVICE_DISABLED** erklärt sich selbst. Die Startart `SERVICE_BOOT_START` dient für Treiber, die Bestandteil des Bootprozesses des Systems sind, wie z.B. Gerätetreiber für bootfähige Geräte. `SERVICE_SYSTEM_START`

startet den Treiber, nachdem das Betriebssystem die Anfangsstadien des Bootprozesses beendet hat.

SERVICE_AUTO_START setzt den Dienst auf einen automatischen Start und der Dienst wird zusammen mit den anderen Diensten gestartet. **SERVICE_DEMAND_START** startet den Dienst, sobald ein Dienst startet, auf den dieser aufbaut.

- **FIXBOOT**. Dieser Befehl schreibt einen neuen Startsektor in die Systempartition. Um z.B. den Startsektor des Laufwerks C neu zu erstellen, geben Sie den Befehl **FIXBOOT C:** ein.
- **FIXMBR**. Dieser Befehl repariert den MBR (Master Boot Record) der Startpartition. Er übernimmt einen optionalen Parameter, den Gerätenamen des Geräts, das einen neuen MBR benötigt. Der MBR ist ein Datenbereich auf der Master-Festplatte des Systems, der dem Computer mitteilt, an welcher Stelle er beginnen kann die Programme zu laden, mit denen der Computer gebootet wird. **FIXMBR** prüft den MBR. Ist dieser beschädigt, werden Sie aufgefordert, ihn zu ersetzen.
- **LOGON**. Dieser Befehl wird automatisch beim Start der Wiederherstellungskonsole ausgeführt und findet die installierten Windows 2000-Systeme. Sie können dann eines auswählen, bei dem Sie sich anmelden möchten.
- **MAP**. Listet die momentan zugeordneten Laufwerke auf, d.h., er zeigt, welche Laufwerke in der Wiederherstellungskonsole verfügbar sind. Es handelt sich dabei ausschließlich um lokale Laufwerke, wie z.B. IDE-, SCSI-, CD-ROM- und Diskettenlaufwerke, nicht jedoch um Netzwerklaufwerke. Netzwerklaufwerke stehen in der Wiederherstellungskonsole nicht zur Verfügung.
- **EXIT**. Beendet die Wiederherstellungskonsole und startet das System neu.

Die Wiederherstellungskonsole hilft dabei, die meisten Probleme zu beheben, die den Start von Windows verhindern. Sie kann nicht nur Dienste aktivieren und deaktivieren, sondern auch Dateien von der Windows 2000-CD-ROM kopieren. Das Einzige, das sie nicht beheben kann, ist eine beschädigte Registrierung. Hier hilft nur die Notfalldiskette.

3.7 Die Datei Boot.ini

Die Datei *Boot.ini* teilt Windows 2000 mit, welche Betriebssysteme installiert sind, wo sie sich befinden und wie Windows 2000 ohne Benutzereingabe gestartet werden soll. Diese Datei befindet sich im Stammverzeichnis und ist normalerweise mit den Attributen Schreibgeschützt, Versteckt und System versehen. Sie können die Datei also nur sehen, wenn Sie im Windows-Explorer die Ansichtsoption Geschützte Systemdateien ausblenden (empfohlen) deaktiviert und die Option Alle Dateien und Ordner anzeigen aktiviert haben. Die Datei ist in zwei Bereiche aufgeteilt. Der *Boot Loader*-Abschnitt teilt Windows 2000 die Zeitdauer mit, die das System auf eine Benutzereingabe warten soll, bevor das Standardbetriebssystem gestartet wird. Im *Operating Systems*-Abschnitt steht, welche Betriebssysteme auf dem lokalen System installiert sind.

Der *Operating Systems*-Abschnitt enthält eine Zeile für jedes verfügbare Betriebssystem. Für diese Zeilen werden zwei Formate verwendet. Windows 2000 und Windows NT benutzen ein Format wie das folgende:

```
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Microsoft Windows 2000 Advanced Server" /fastdetect
```

Dies bedeutet, dass das Betriebssystem auf dem primären IDE-Kanal (**multi(0)** ist der primäre IDE-Kanal, **scsi(0)** wäre der erste SCSI-Kanal und **multi(1)** wäre der sekundäre IDE-Kanal) auf dem ersten Datenträger (**disk(0)**) auf der ersten primären Partition (**rdisk(0)**) und auf dem zweiten logischen Datenträger (**partition(1)**) gespeichert ist. Im Startmenü wird »Microsoft Windows 2000 Advanced Server« stehen und beim Start wird der Schalter **/fastdetect** verwendet.

Die zweite Art von Einträgen in der Datei *Boot.ini* wird für alle anderen Betriebssysteme außer Windows NT oder Windows 2000 verwendet. Sie sieht wie folgt aus:

```
C:\CMDCONS\BOOTSECT.DAT="Microsoft Windows 2000-Wiederherstellungskonsole" /cmdcons
```


Dies ist der Eintrag für die Windows 2000-Wiederherstellungskonsole, aber Einträge für Windows 98 oder sogar Linux hätten dasselbe Format. Der Teil auf der linken Seite der Gleichung ist der Pfad zur Boot-Sektor-Datei für das Betriebssystem. Bei Windows 9x ist dies normalerweise die Datei **BOOTSECT . DOS**, bei Linux der Name, den Sie für den Bootsektor vergeben haben. Der Teil auf der rechten Seite des Gleichheitszeichens ist der Text, der im Menü Startoptionen angezeigt wird. Alle Optionen, die diesem Text folgen, werden dem System beim Start übergeben.

3.8 Die Notfalldiskette

Die Notfalldiskette ist eine normale Diskette, die eine Sicherung der Systemeinstellungen enthält und dazu dient, ein Windows 2000-System wiederherzustellen, das Probleme mit der Registrierung hat. Die Notfalldiskette erstellen Sie mit dem Sicherungsprogramm, das Sie über Start/Programme/Zubehör/Systemprogramme/Sicherung öffnen. Klicken Sie im Sicherungsprogramm auf der Registerkarte Willkommen auf die Schaltfläche Notfalldiskette. Legen Sie dann eine leere 1,44-Mbyte-Diskette (3,5«) in das Diskettenlaufwerk ein und folgen Sie den Anweisungen.

Die Notfalldiskette muss jedes Mal neu erstellt werden, wenn sich die Systemeinstellungen ändern. Dies gilt insbesondere, wenn sich das Partitionierungsschema auf dem Server bei der Installation eines Service Packs ändert und bevor und nachdem Hardware zum System hinzugefügt wird.

Die Notfalldiskette setzen Sie ein, indem Sie Windows 2000 von der CD-ROM oder von der Installationsdiskette starten und dann die Option »R« wählen, wenn Sie gefragt werden, ob Sie Windows 2000 reparieren möchten. Windows 2000 fordert Sie auf, die Notfalldiskette einzulegen.

3.9 Migration von bereits bestehendem System

Häufig wird Windows 2000 Server auf einen bestehenden Windows NT-Server installiert. Bei der Planung der Migration von anderen Versionen von Windows NT oder von einer NetWare-Plattform müssen einige Dinge berücksichtigt werden.

Welche Version von Windows 2000 benötigt wird, hängt davon ab, von welchem System aus das Update erfolgt. Die folgende Tabelle erklärt, welche Version von Windows NT auf welche Version von Windows 2000 aktualisiert werden kann:

Windows 2000-Version	Update möglich von
Windows 2000 Advanced Server, Update	Windows NT 4.0 Enterprise Server Edition
Windows 2000 Advanced Server Vollprodukt	Windows NT 3.51 Server, Windows NT 4.0 Server, Windows NT 4.0 Terminal Server, Windows NT 4.0 Enterprise Edition
Windows 2000 Server Update	Windows NT 3.51 Server, Windows NT 4.0 Server
Windows 2000 Server Vollprodukt	Windows 3.51 Server, Windows 4.0 Server

Windows NT Server kann in einem Netzwerk drei verschiedene Rollen spielen. In jeder Domäne gibt es einen primären Domänencontroller und keinen oder mehrere Sicherungsdomänencontroller. Ein Server kann also auch der einzige Server sein, was besagt, dass er keine Authentifizierung der Netzwerkanmeldungen durchführt, aber vielleicht Teil der Domäne ist. Es gibt auch so genannte *Mitgliedsserver*, die Bestandteil einer Domäne, aber nicht der Domänencontroller sind.

Windows 2000 unterstützt ein Multiple-Master-Replikationsschema für Active Directory. Dies bedeutet, dass nicht unbedingt ein System, bestehend aus einem primären Domänencontroller und einem Sicherungsdomänencontroller, eingerichtet werden muss - es gibt nur Domänencontroller. Es gibt noch immer »Mitgliedsserver«, die keine Überprüfung von Anmeldungen vornehmen, aber trotzdem Bestandteil der Domäne sind.

Beim Update von Windows NT Server auf Windows 2000 Server sind folgende Optionen möglich:

Rolle in Windows NT-Domäne	Rolle in Windows 2000-Domäne
Primärer Domänencontroller	Domänencontroller
Sicherungsdomänencontroller	Domänencontroller oder Mitgliedsserver
Mitgliedsserver	Domänencontroller oder Mitgliedsserver

Bis auf die Fälle, in denen nur ein Domänencontroller existiert, kann ein Domänencontroller in einen Mitgliedsserver umgewandelt werden, ohne dass der Server neu eingerichtet werden muss. Bei einem Mitgliedsserver ist immer ein Update auf einen Domänencontroller möglich.

Die Systempartition auf einem Domänencontroller muss mit NTFS formatiert sein und der Aktualisierungsprozess erzwingt dies. Wenn die Systempartition (auf der der Order *Winnt* enthalten ist) bisher keine NTFS-Partition ist, wird sie während der Installation auf NTFS umformatiert.

Weitere Informationen zu Active Directory finden Sie in Kapitel 9.

3.10 Hinweise zur Hardware

Die Einrichtung der Hardware auf Servern ist sehr komplex. Die Konfiguration von PC-Hardware ist schwierig, aber zahlreiche neue Technologien wie PCI, USB und IEEE 1394 (FireWire) erleichtern die Installation und Konfiguration der Geräte. Dieser Abschnitt deckt verschiedene Themen ab, die Ihnen hilfreich sein könnten, wenn Sie es mit Hardwareproblemen zu tun haben.

3.10.1 Interrupts

Jedem Gerät, das mit der CPU interagiert, wird ein IRQ (Interrupt Request Line) zugewiesen. Dabei handelt es sich um eine Leitung zur Übermittlung von Signalen, über die die CPU unterbrochen wird, um ihr mitzuteilen, dass das Gerät berücksichtigt werden muss.

In einem normalen PC gibt es 16 Hardwareinterrupts, die von 0 bis 15 durchnummeriert sind. Früher benötigte jedes Gerät einen eigenen Interrupt. Seit der Einführung des PCI-Busses und von Geräten, die einen Interrupt gemeinsam nutzen können, können mehrere Geräte auf einen Interrupt zugreifen. Dadurch lassen sich die Systeme stärker erweitern. Nachfolgend sehen Sie eine Liste der Standardinterrupts und deren Verwendung:

- *Interrupt 0.* Zeitgeber. Dieser Interrupt betreibt Dinge wie die Systemuhr und den Scheduler.
- *Interrupt 1.* Tastatur. Jeder Tastendruck ruft einen Tastaturinterrupt hervor.
- *Interrupt 2.* Systemboard. Schnittstelle zu grundlegenden Systemgeräten.
- *Interrupt 3.* Die seriellen Anschlüsse COM2 und COM4 benutzen normalerweise diesen Interrupt.
- *Interrupt 4.* Die seriellen Anschlüsse COM1 und COM3 benutzen normalerweise diesen Interrupt.
- *Interrupt 5.* Paralleler Anschluss LPT1 oder nicht zugewiesen.
- *Interrupt 6.* Diskettenlaufwerk.
- *Interrupt 7.* Verfügbar.
- *Interrupt 8.* Echtzeituhr.
- *Interrupt 9.* Verfügbar (manchmal gemeinsame Benutzung mit PCI-Bus).
- *Interrupt 10.* Verfügbar.
- *Interrupt 11.* Verfügbar.
- *Interrupt 12.* Verfügbar.
- *Interrupt 13.* Numerischer Coprozessor (der Prozessor für Fließkommaberechnungen).
- *Interrupt 14.* Primärer IDE-Controller.
- *Interrupt 15.* Sekundärer IDE-Controller.

3.10.2 EIDE-Geräte

EIDE-Geräte (EIDE = Extended Integrated Drive Electronics) sind Geräte wie Festplatten-, Band- und CD-ROM-Laufwerke, die an den EIDE-Bus angeschlossen sind. In einem Computer sind normalerweise zwei EIDE-Kanäle enthalten. Der eine ist der primäre und der andere der sekundäre Kanal. An jeden Kanal können zwei Geräte angeschlossen werden. Ein Gerät wird als *Master* (Herr) und das andere als *Slave* (Sklave) bezeichnet. Wenn ein Computer nicht mehr startet, nachdem ein neues Gerät an den EIDE-Bus angeschlossen wurde, sind die Master/Slave-Jumper sehr wahrscheinlich nicht korrekt eingestellt.

3.10.3 Windows-Update

Die Windows-Update-Site (<http://windowsupdate.microsoft.com>) bietet die neuesten Hardwaretreiber und Patches und Service-Packs für Windows 2000. Windows-Update ist mit einer Funktion namens *Critical Update Notification* ausgestattet, die die Windows Update-Site überwacht und Sie darüber informiert, wenn es ein kritisches Update für das System gibt, wie z.B. einen Sicherheitspatch.

3.10.4 Busse und Geräte

Es gibt verschiedene Methoden, um Geräte an einen PC anzuschließen. Am häufigsten wird der PCI-Bus verwendet, der vollständig Plug & Play-fähig ist, Hardware eigenständig entdeckt und Windows 2000 auffordert, die Hardware zu konfigurieren. Es gibt eine neue Version des PCI-Busses. Diese bietet die Möglichkeit, Geräte zu entfernen, während der Server läuft. Studieren Sie sorgfältig die Dokumentation zu Ihrem Server, bevor Sie diese Funktion nutzen.

Der USB (*Universal Serial Bus*) ist ein 12-Mbps-Bus, der dazu dient, Geräte mit einer geringen Bandbreite an einen Computer anzuschließen, wie z.B. Zeigegeräte, Tastaturen, Modems und entfernbare Speichergeräte (beispielsweise Disketten- und ZIP-Laufwerke). Der USB ist ein Plug & Play-Bus, der die Möglichkeit bietet, Geräte hinzuzufügen und zu entfernen, ohne dass das Gerät abgeschaltet werden muss.

Apple Computer hat einen Standard veröffentlicht, der vom IEEE als »IEEE 1394«-Standard verabschiedet wurde. Dieses System, auch *FireWire* genannt, ist eine Verbindung mit einer hohen Bandbreite, die auch dazu dienen kann, alle möglichen Arten von Geräten an ein System anzuschließen. Dieses System ist ebenfalls Plug & Play-fähig. Deshalb können Sie Geräte von einem FireWire-Kanal entfernen und hinzufügen, ohne den Rechner herunterfahren zu müssen.

Für Laptops gibt es noch immer die ehrwürdigen PCMCIA-Geräte. Dies sind Slots von der Größe einer Kreditkarte, die normalerweise für Netzwerkkarten und Modems verwendet werden. Die neue PC Card-Implementierung bietet einen höheren Durchsatz für 100-Mbyte-Netzwerke.

Kapitel 4 Dateisysteme

Es gibt eine enorme Anzahl von Windows 2000 Server-Computern, die als einfache Dateiserver dienen und deren Zweck nur darin besteht, Dateien zu speichern und abzurufen. Es gibt auch eine immense Anzahl an Windows 2000 Server-Computern, die als Webserver eingesetzt werden und die für den Abruf von Dateien und deren Formatierung für die Anzeige verantwortlich sind. Zahlreiche Windows 2000 Server-Computer werden als Datenbankserver eingesetzt und haben die Aufgabe, Daten in strukturierter Form von der Festplatte zu lesen, ziemlich komplexe Aufgaben auszuführen und die Informationen wieder zurück auf die Festplatte zu schreiben. Bei den genannten Einsatzgebieten und auch bei jeder anderen Verwendung eines Windows 2000-Servers geht es um das Speichersystem in Windows 2000.

Dieses Kapitel behandelt das Speichersystem auf der Hardwareebene, der Softwareebene und der Netzwerkebene. Sie erhalten zahlreiche nützliche Informationen, die direkten Einfluss auf die Leistung und die Integrität jedes Windows 2000-Servers haben.

Und hier die Themen, die in diesem Kapitel behandelt werden:

- Betrachtungen zur Hardware
- Festplattenpartitionen
- Die Datenträgerverwaltung
- Dateisysteme
- Mit Datenträgern arbeiten
- Mit Netzlaufwerken arbeiten
- Das verteilte Dateisystem (DFS)
- Remotespeicher
- Wechselmedien

Dieses Kapitel beginnt mit einer Übersicht über Hardware, wobei die verschiedenen Festplattentechnologien behandelt und die Schnittstellen und Datentransferraten veranschaulicht werden. Außerdem wird die Partitionierung von Festplatten beschrieben und es werden die Tools erläutert, mit denen Festplattenpartitionen eingerichtet werden.

4.1 Betrachtungen zur Hardware

Es ist erstaunlich, wie weit sich die Speichertechnologie in den letzten Jahren entwickelt hat und es macht Spaß, die Entwicklung von Festplatten zu verfolgen. Dieser Abschnitt behandelt die Grundlagen der Festplattentechnologie und die Terminologie und beschreibt dann die Standardmethoden, mit denen Datenträger kontrolliert werden und wie die Kommunikation mit Datenträgern erfolgt. Anschließend wird kurz auf einige neuere Technologien eingegangen, die auf der Controllerarchitektur aufsetzen, wie RAID und Fibre Channel.

4.1.1 Festplattentechnologie

Eine Festplatte war schon zu Zeiten der IBM-Winchester-Festplattenstapel dieselbe Basiskomponente. Es gibt eine Spindel, die die Rotationsachse für eine oder mehrere flache Platten bildet. Diese Platten rotieren mit einer Geschwindigkeit zwischen 3.600 U/min. und 10.000 U/min. bei ganz modernen Festplatten. Über diesen Platten schweben die Lese-/Schreibköpfe, die die magnetischen Schwankungen auf den Platten lesen und das magnetische Feld auf der Platte ändern können, um Daten zu lesen und zu schreiben. Diese Lese-/Schreibköpfe sind auf Arme montiert, sie sich gleichzeitig über die Platten vorwärts und zurück bewegen.

Eine Festplatte wird in drei Dimensionen bemessen: *Sektoren* sind Linien, die vom Mittelpunkt der Festplatte nach außen verlaufen und die einzelnen Spuren in Abschnitte unterteilen (eine Festplatte hat eine feste Anzahl an Sektoren). *Spuren (Tracks)* sind konzentrische Ringe auf der Festplatte. Mit *Köpfen (Heads)* wird die Anzahl der durch die Schreib-/Leseköpfe nutzbaren Oberflächen der Platten bezeichnet. Denken Sie daran, dass einige Platten beidseitig genutzt werden. Daten werden auf der Basis von Sektoren pro Spur gespeichert, wobei die einzelnen Sektoren eine feste Größe in Bytes aufweisen. Die Abbildung 4.1 veranschaulicht, wie dies alles funktioniert.

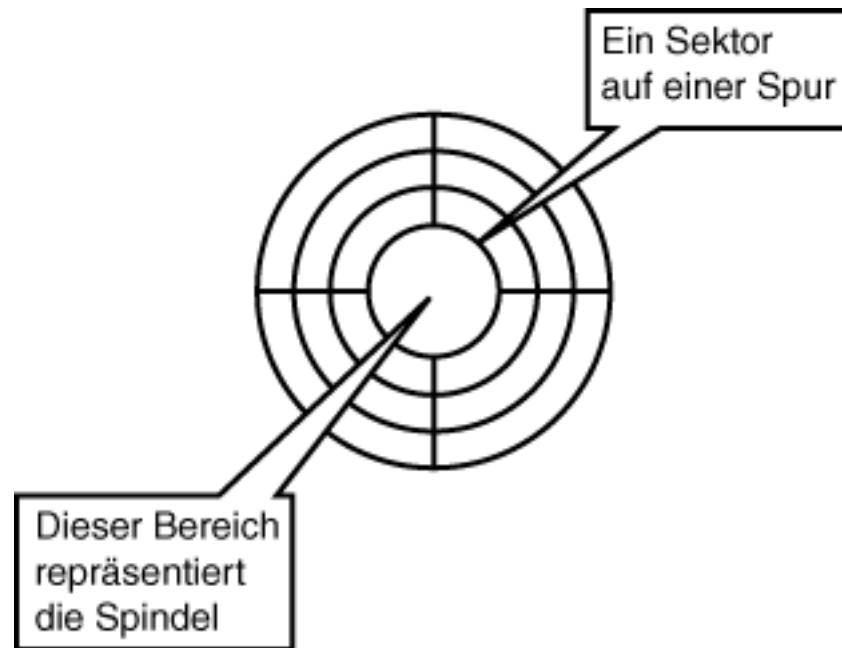


Abbildung 4.1: Dieses Diagramm zeigt die Darstellung einer Festplatte mit vier Sektoren und drei Spuren.

Mit den beiden sich bewegenden Teilen - den Lese- /Schreibköpfen und den Platten - gibt es für eine Festplatte zwei Faktoren, die die Geschwindigkeit beschränken. Ein Faktor ist die *Suchzeit* (auch *Zugriffszeit* genannt), d.h. die durchschnittliche Zeit, die benötigt wird, um den Kopf von einer Spur zu einer anderen zu bewegen. Der andere Faktor ist die *Zugriffsverzögerung durch Umdrehung* oder *Umdrehungswartezeit*, d.h. die durchschnittliche Zeit, die die Platte benötigt, um sich bis zu dem Bereich zu drehen, an dem sich die Daten befinden. Es gibt deshalb folglich zwei Möglichkeiten, um die Geschwindigkeit zu erhöhen, in der die Daten gefunden werden: dadurch, dass sich die Platten schneller drehen und die Lese-/Schreibköpfe sich schneller bewegen.

Hier einige interessante Dinge über Festplatten. Eine Festplatte benötigt eine endliche Zeitdauer von

ihrem »deaktivierten« Zustand bis zu ihrem »aktivierten« Zustand. Während dieser Zeit verbraucht die Festplatte den meisten Strom. Wenn ein System mit mehreren Festplatten ausgestattet ist, ist es für die Stromzufuhr erheblich einfacher, wenn die Festplatten nacheinander aktiviert werden. Auf diese Weise funktionieren auch die meisten Festplattenstapel. Beim Aufbau eines Servers sollte sichergestellt werden, dass die Festplatten auf diese Weise aktiviert werden, weil sich dadurch Inkonsistenzen während des Starts verhindern lassen. Ein weiterer interessanter Punkt ist der, dass die Lese-/Schreibköpfe einer Festplatte so dicht über den Platten schweben, dass kaum Platz dazwischen ist. Zwischen den Lese-/Schreibköpfen und einer Platte befindet sich nur Luft und selbst dafür ist kaum Platz. Wird eine Festplatte geöffnet, resultiert dies unweigerlich in einem Verlust sämtlicher Daten. Die Festplatte arbeitet danach außerdem nicht mehr zuverlässig, weil Staub und andere Verunreinigungen in das Laufwerk gelangen und zu einem Headcrash führen. Bei einem *Headcrash* gelangen die Lese-/Schreibköpfe in Berührung mit den Platten. Dies kann durch einen Fabrikationsfehler, Verschleiß oder Schmutzpartikel zwischen dem Lese-/Schreibkopf und der Platte bedingt sein. Dabei gehen unweigerlich Daten verloren. Festplatten sind empfindlich und sollten sehr vorsichtig behandelt werden, um ihre Lebensdauer zu erhöhen.

Jeder, der in der Computerindustrie arbeitet, weiß, dass Computer ziemlich empfindlich sind. Das gilt in erster Linie für die laufenden Festplatten. Transportieren Sie nie einen laufenden Computer. Wenn der Computer ausgeschaltet ist, sorgt ein Kondensator dafür, dass die Lese-/Schreibköpfe auf einen Bereich der Festplatte zurückgefahren werden, der keine Daten enthält. Dieser wird als *Landezone* bezeichnet. Dadurch wird die Wahrscheinlichkeit reduziert, dass die Festplatte versagt, wenn sie erschüttert wird.

Mehr müssen Sie über das Konzept der Festplatten nicht wissen. Festplatten sind Hochgeschwindigkeitsspeichermedien - nicht mehr und nicht weniger. Noch mehr gibt es eigentlich dazu nicht zu sagen.

4.1.2 Festplattencontroller

Die erheblichste Leistungsverbesserung bei Festplatten resultiert aus der Technologie, die zur Steuerung der Laufwerke in Kombination mit der Elektronik einer Festplatte verwendet wird. Deshalb ist diese Steuerungstechnologie genauso wichtig, wenn nicht sogar noch wichtiger, als die Festplatten selbst.

Es gibt mehrere Standards für Festplattencontroller, die zwei wichtigsten Standards sind jedoch IDE und SCSI. Der IDE-Standard (IDE = Integrated Device Electronics) ist preisgünstiger, aber ansonsten vergleichbar mit den meisten SCSI-Standards. SCSI (Small Computer System Interface) bezeichnet eine Hochgeschwindigkeits-Parallelschnittstelle, die durch das X3T9.2-Komitee des American National Standards Institute (ANSI) definiert wurde. An die SCSI-Schnittstellen lassen sich periphere Geräte, Scanner, CD-ROM-Brenner oder auch CD-ROM-Laufwerke anschließen.

Der IDE-Standard

Der IDE-Standard basiert auf dem ziemlich einfachen Konzept, dafür zu sorgen, dass die Festplatte läuft. Jede Festplatte verfügt über eine integrierte Controllerkarte, die alle komplexen Aufgaben wie die Zuordnung der aus Zylinder, Seite und Sektor bestehenden Adressen in die eigentlichen Adressen auf der Festplatte, den Abruf der Daten und die Zwischenspeicherung der Daten organisiert. Mit einer neueren Version von IDE namens *ATAPI* (AT Attachment Packet Interface) lässt sich eine größere Bandbreite an Geräten steuern, wie z.B. CD-ROM-Laufwerke, Bandlaufwerke und Wechselmedien (wie

ZIP-Laufwerke). Weil der größte Teil der komplexen Verarbeitung vom Laufwerk selbst verrichtet wird, sind die Controller vergleichsweise einfach aufgebaut und in die Motherboards integriert.

Die stärkste Beschränkung der ATAPI-Technologie ist die mangelnde Erweiterbarkeit. Ohne einige ziemlich technische Hürden zu überspringen, kann ein normales ATAPI-System nur zwei Geräte pro Kanal behandeln. Dies ergibt bei maximal zwei Kanälen eine Gesamtanzahl von vier Geräten. Dieser Speicherplatz reicht für einen »ernstzunehmenden« Server nicht aus. Die meisten ernstzunehmenden Server sind jedoch mit IDE-Controllern für CD-ROM-Laufwerke ausgestattet, und IDE-Controller sind auch nützlich für die Nutzung von gemeinsam genutzten ZIP-Laufwerken.

Der IDE-Standard funktioniert wie folgt: Es gibt zwei Kanäle in einem Computer: den primären und den sekundären Kanal. Jeder dieser Kanäle kann ein Master- und ein Slave-Gerät unterstützen, das Bootlaufwerk muss die primäre Partition des Master-Geräts sein. Wenn es nur ein Gerät im Kanal gibt, muss dieses das Master-Gerät sein.

Die meisten Workstations enthalten nur zwei ATAPI-Geräte: eine Festplatte und ein CD-ROM-Laufwerk. Deshalb ist das Master-Gerät des primären Kanals die Festplatte und das des sekundären Kanals das CD-ROM-Laufwerk. Ein Kanal muss nicht unbedingt ein Slave-Laufwerk enthalten. Wenn es jedoch nur ein Laufwerk gibt, ist dieses immer das Master-Laufwerk.

Controller-Kanäle

Das Konzept des Kanals gibt es sowohl bei ATAPI- als auch bei SCSI-Controllern. Ein Kanal besteht aus einer Gruppe von Geräten, die über dasselbe Kabel mit dem Controller verbunden sind. Bei einem ATAPI-Kanal gibt es zwei Geräte: den Master und den Slave. Ein SCSI-Kanal kann zwischen 7 und 16 Geräte enthalten. Ein ATAPI-Controller kann nur mit zwei Kanälen arbeiten. Ein SCSI-Controller kann dagegen normalerweise zwischen zwei und vier Kanäle bedienen.

Kopiervorgänge von einem Kanal zum anderen lassen sich normalerweise erheblich schneller durchführen als zwischen zwei Geräten innerhalb eines Kanals. Dies gilt für jedes Laufwerkteilsystem, und zwar aus folgendem Grund: Ein Kanal hat eine feste Bitrate. Wenn ein Kanal zwei Geräte enthält und Daten von einem Gerät auf das andere kopiert werden, müssen die Daten vom Quellgerät zum Controller und anschließend über denselben Kanal zum Zielgerät fließen. Wenn die Bandbreite eines Kanals z.B. 20 Mbps beträgt, steht für die Transaktion eine effektive Bandbreite von 10 Mbps zur Verfügung. Wenn zwei Kanäle in den Kopiervorgang eingebunden sind, kann der Lesevorgang mit 20 Mbps erfolgen und der Schreibvorgang ebenfalls. Die Kopie sollte deshalb doppelt so schnell fertig sein.

Betrachten Sie einen Kanal als Warteschlange. Befehle, die an die Geräte im Kanal geschickt werden müssen, werden in der Warteschlange abgelegt und vom Controller in der Reihenfolge gesendet, in der sie eingegangen sind. Wenn es zwei Kanäle gibt, gibt es auch zwei Warteschlangen. Deshalb können die Geräte die Daten rein theoretisch doppelt so schnell erhalten.

Zu Kanälen müssen Sie sich zwei Dinge merken: Erstens dürfen Sie ein RAID-Array nicht auf mehrere Kanäle verteilen. Ein RAID-Array (RAID = Redundant Array of Independent Disks) stellt ein Verfahren zur Speicherung von Daten auf mehreren Festplatten dar, um die Zuverlässigkeit und Leistung zu erhöhen. Mehr zu RAID erfahren Sie später in diesem Kapitel. Im besten Fall ändert sich durch die



Aufteilung nichts an der Geschwindigkeit; dafür sind RAID- Controller auch gar nicht gedacht. Im schlimmsten Fall aber treten Datenverluste auf. Der zweite Punkt, den Sie sich im Zusammenhang mit Kanälen merken sollten, ist, dass Sie mit Kanälen so arbeiten sollten, dass sich Geräte, die häufig miteinander kommunizieren müssen, in verschiedenen Kanälen befinden. Wenn sich z.B. ein CD-ROM-Laufwerk und eine Festplatte in unterschiedlichen Kanälen befinden, beschleunigt dies die Installation von Software, weil dabei im Wesentlichen Daten von der CD-ROM auf die Festplatte kopiert werden. Bei Datenbanken ist es oft hilfreich, die Daten und das Transaktionsprotokoll in verschiedenen Kanälen abzulegen.

Um festzulegen, ob ein Laufwerk Master oder Slave ist, muss normalerweise einfach nur ein Jumper entsprechend gesetzt werden. In der Regel lässt sich die korrekte Positionierung von der Festplatte ablesen. Manchmal ist es jedoch nötig, einen Blick ins Handbuch zu werfen oder im Internet nach einer Bedienungsanleitung zur Festplatte zu suchen.

IDE- und ATAPI-Laufwerke eignen sich hervorragend für Benutzer mit sehr kleinen Servern und Workstations, für die es keine Rolle spielt, dass sich keine weiteren Festplatten einbauen lassen, die keine außergewöhnlich schnellen Festplatten benötigen und die nicht sehr viel Geld für die neuesten, größten SCSI-Laufwerke ausgeben können. IDE-Laufwerke sind preisgünstig, zuverlässig und für die meisten Aufgaben auch schnell genug. EIDE, der Extended IDE-Standard, beinhaltet einige neue Technologien, die einen höheren Durchsatz bieten. Er benutzt jedoch dasselbe Konzept (mit den Master- und Slave-Laufwerken) wie IDE.

4.1.3 Die SCSI-Prinzipien

SCSI ist die Architektur der Wahl für umfangreiche Festplattensysteme. Jeder mittelgroße bis große Server benutzt eine Form von SCSI, um auf Festplatten- und Bandlaufwerke zuzugreifen. Es spricht vieles für SCSI: sehr viele Anbieter, eine hohe Leistung, eine geringe Belastung des Prozessors und die Möglichkeit zur Erweiterung. SCSI ist auch mindestens 15 Prozent teurer als die vergleichbare IDE-Hardware mit derselben Kapazität. Bei einem Server besteht jedoch eine große Bereitschaft, mehr Geld auszugeben, um einen geringfügigen Leistungsvorteil zu erhalten und - was noch wichtiger ist - die Möglichkeit, je nach SCSI-Standard bis zu 16 Geräte hintereinander zu hängen.

Seit der Einführung von SCSI haben sich viele verschiedene Arten entwickelt. Tabelle 4.1 zeigt die verschiedenen SCSI-Standards, die maximalen Busgeschwindigkeiten und die maximale Anzahl von Geräten, die jeweils unterstützt werden.

Name	Geschwindigkeit	Geräte	Kabellänge	Kabelpins
SCSI-1	5 Mbps	8	6 Meter	25
Fast SCSI	10 Mbps	8	3 Meter	50
Fast Wide SCSI	20 Mbps	16	3 Meter	68
Ultra SCSI	20 Mbps	8	1,5 Meter	68
Wide Ultra SCSI	40 Mbps	16	12 Meter	80
Ultra2 SCSI	40 Mbps	8	12 Meter	80

Wide Ultra2 SCSI	80 Mbps	16	12 Meter	80
Ultra3 SCSI	160 Mbps	16	12 Meter	80

Tabelle 4.1: SCSI-Standards

Ein Computer, der SCSI für die Interaktion mit Laufwerken benutzt, muss mit einem SCSI-Controller (oder *Hostadapter*) ausgestattet sein. Der Hostadapter zählt als ein Gerät des SCSI-Kanals. Wenn also in der Tabelle steht, dass 8 Geräte unterstützt werden, sind dies z.B. ein Adapter und sieben weitere Geräte. Ein SCSI-Adapter leistet wesentlich mehr als ein IDE-Controller. Er unterhält eine Warteschlange für die Befehle für verschiedene Geräte und führt diese Befehle »on the fly« aus. Dies bedeutet, dass SCSI weniger CPU-Ressourcen verbraucht, um Daten zu übertragen. Dies ist für einen stark genutzten Server ein wichtiger Punkt. Noch ein Hinweis zur Tabelle: Die meisten Hersteller verwenden den Begriff »Ultra Wide« statt »Wide Ultra«. Die Begriffe sind jedoch gleichbedeutend.

Was ist SCSI-3?



Der SCSI-3-Standard besteht eigentlich aus mehreren Standards und entspricht dem, was heute als SCSI bezeichnet wird. Fast Wide SCSI ist dasselbe wie Fast Wide SCSI-3. Eigentlich ist alles, was SCSI heißt, nun eigentlich SCSI-3. Deshalb ist ein Wide Ultra2 SCSI-Controller wesentlich schneller als ein Fast Wide SCSI-2-Controller.

Jedes Gerät in einem SCSI-Kanal muss eine SCSI-ID haben. Diese Zahl identifiziert den Kanal eindeutig. Bei den meisten Systemen gibt es drei Jumper, die die SCSI-ID festlegen, und sie sind normalerweise auf dem Laufwerk dokumentiert. Falls nicht, finden Sie die Informationen im Handbuch oder in der Website des Herstellers.

4.1.4 Fortgeschrittene Controllertechnologie

Wie bereits im Abschnitt über Festplatten erwähnt, wird die Leistung einer Festplatte durch die Zugriffsverzögerung aufgrund der Umdrehung und die durchschnittliche Zugriffszeit beschränkt. Es wurde vor nicht allzu langer Zeit herausgefunden, dass sich die Datensuche auf jedem einzelnen Laufwerk verkürzt, wenn die Daten auf mehrere Laufwerke verteilt werden. Außerdem gab es zahlreiche Initiativen, um PCs und insbesondere PC-basierte Server zuverlässiger zu machen. Der Schlüssel hierfür bestand darin, Festplatten zuverlässiger zu machen und dafür zu sorgen, dass Probleme besser behandelt werden können.

Aus diesem Grund haben sich die Wissenschaftler zusammengetan und herausgefunden, dass sich die Leistung steigern lässt, wenn mehrere preisgünstige Festplatten zusammengenommen werden. Die Wissenschaftler begannen mit zwei Festplatten, die dieselben Informationen enthielten. Es handelte sich also um exakte Duplikate. Wenn zahlreiche Anforderungen für diese Festplatten beim Controller eintrafen, leitete der Controller diese so weiter, dass beide Festplatten benutzt wurden. Dies brachte gewisse Leistungsvorteile. Wenn eine der beiden Festplatten ausfiel, konnte die andere mit einer Leistungseinbuße weiter benutzt werden, bis die zweite ersetzt werden konnte. Dieses Verfahren wird als *Festplattenspiegelung (Mirroring)* bezeichnet.

Das war alles schön und gut, es war aber Platzverschwendung. Auf zwei Festplatten steht die doppelte Speicherkapazität zur Verfügung, aber die Wissenschaftler durften nur eine Festplatte benutzen. So

fanden sie heraus, dass sie die Daten einfach auf eine größere Anzahl an Festplatten verteilen mussten, wobei sie auf jeder Festplatte nur einen kleinen Teil der Daten ablegten. Auf diese Weise ließ sich die Zugriffszeit im Vergleich zur Verwendung einer einzigen großen Festplatte derselben Kapazität stark erhöhen. Das Verfahren war nicht so schnell wie die Festplattenspiegelung, aber trotzdem noch ziemlich schnell. Bei diesem Verfahren wurde eine große Datei in Einheiten fester Größe aufgeteilt und die Einheiten wurden abwechselnd auf jede Festplatte verteilt, sodass die Datei auf alle Festplatten verteilt war. Dieses Verfahren wird als Striping-Verfahren und das Ergebnis als *Stripesetdatenträger* bezeichnet.

Anschließend wurde herausgefunden, dass dies für die Zuverlässigkeit des Systems wahrscheinlich keine gute Lösung war. Wenn eines der Laufwerke im Stripeset versagte, würden alle Daten verloren gehen. Daraufhin begannen die Wissenschaftler, *Paritätsinformationen* zu speichern. Paritätsinformationen sind redundante Daten, mit denen sich im Falle eines Festplattenversagens der Inhalt der fehlerhaften Festplatte wiederherstellen lässt.

Was ist Parität?

Parität ist eine Methode, um die Konsistenz von Daten zu überprüfen. Zumindest war dies der ursprüngliche Einsatzbereich, bevor herausgefunden wurde, dass sich mit der Parität beschädigte Daten korrigieren lassen. Das Verfahren funktioniert wie folgt. Angenommen, es gibt ein Zeichen, das acht Bit lang und z.B. wie folgt aussieht:

0010 1010

Dafür soll nun ein Paritätsbit gebildet werden. Es gibt zwei Arten von Parität: die gerade und die ungerade. Bei gerader Parität wird das Paritätsbit auf 0 gesetzt, wenn die Anzahl der Einsen gerade ist und auf 1, wenn die Anzahl der Einsen ungerade ist. Bei ungerader Parität wird das Paritätsbit auf 1 gesetzt, wenn die Anzahl der Einsen gerade ist und auf 0, wenn die Anzahl der Einsen ungerade ist. Um keine Verwirrung zu stiften, wird hier nur die gerade Parität verwendet.

Das Paritätsbit für die Binärzahl im Beispiel wäre 1, weil die 1 drei Mal vorkommt (0010 1010). Wenn die Daten übertragen oder einfach aus dem Speicher gelesen werden, ermittelt der Computer, was das Paritätsbit sein sollte und stellt dann fest, ob die Daten beschädigt sind. Der Computer weiß aber nicht, welches Bit fehlerhaft ist. Er weiß nur, dass ein fehlerhaftes Bit vorliegt.

Wie kann nun also die Parität genutzt werden um festzustellen, welche Daten beschädigt sind? Das ist eigentlich ganz einfach. Es müssen dafür Gruppen von acht Bytes gebildet werden. Berechnen Sie die Parität jeder Zahl (wie 0010 1010) und anschließend die Parität jeder Spalte wie nachfolgend gezeigt:

	Daten	Parität
Byte 1	0010 1010	1
Byte 2	1101 1010	1
Byte 3	1111 0000	0
Byte 4	0011 0011	0
Byte 5	0101 0101	0
Byte 6	0101 1010	1



Byte 7	1100 0011	0
Parität	1111 0111	

Wenn ein Bit kippt, sind zwei Paritätsbits vorhanden. Deshalb könnte der Computer herausfinden, dass sich Byte 3 geändert hat, wenn das vierte Bit in Byte 3 auf 0 kippt. Das Paritätsbit der Spalte wäre dann nämlich 0 und das System könnte ableiten, dass es eine 1 hätte sein müssen. Mit dieser Methode lassen sich auch mehrere Fehler in einem Satz von acht Bytes feststellen, wenn nicht mehr als zwei Bytes in einer Zeile oder Spalte beschädigt sind. Die Routinen für das Striping-Verfahren basieren jedoch auf einem komplexeren Verfahren, mit dem sich ganze Bytesätze wiederherstellen lassen.

Die Wissenschaftler speicherten eine externe Parität auf einem Laufwerk und stellten fest, dass das gesamte System großartig funktionierte. Dieses Verfahren hatte die gleichen Vorteile wie die Verteilung der Daten auf mehrere Laufwerke oder die Verkürzung der Verzögerungszeit durch Umdrehung, es wurde jedoch nicht so viel Platz verschwendet wie bei der Spiegelung. Dieses Verfahren wird als *Striping-Verfahren mit Parität* bezeichnet.

Dann wurde festgestellt, dass die Paritätsinformationen ebenfalls verteilt gespeichert werden konnten und dass sich dadurch die Suchzeit bei einem Laufwerksausfall beschleunigen ließ und außerdem weitere kleine Verbesserungen hinzukamen. Dieses Verfahren wird als *Striping-Verfahren mit verteilter Parität* bezeichnet.

Als Nächstes ging eine kleine Gruppe von Festplattenherstellern noch einen Schritt weiter und fand heraus, dass sich durch die Spiegelung der Stripes ein noch schnelleres und sichereres System ergab. Dieses Verfahren wird als *Gespiegeltes Striping-Verfahren mit Parität* bezeichnet.

Anschließend fand eine Gruppe von Ingenieuren heraus, dass sich sehr viel Geld damit machen ließe, wenn Festplattencontroller die Standard-SCSI-Laufwerke benutzen und diese Stripeset- und Spiegelungstechnologie implementieren könnten. Anschließend entwickelten sie Hardware mit Fehlertoleranz, sodass Festplatten hinzugefügt und entfernt werden konnten, ohne dass die anderen Festplatten offline sein mussten - und so wurde das Hot-pluggable-RAID geboren, d.h. das RAID mit der Möglichkeit des Festplatteneinbaus bei laufendem Betrieb.

RAID (*Redundant Array of Independent Disks*) wurde in einem Forschungslabor entwickelt. Die Wissenschaftler wollten sehen, ob sie einen Stapel preisgünstiger Festplattenlaufwerke nutzen konnten, anstatt neuere Laufwerke mit einer höheren Kapazität erwerben zu müssen. Dies war möglich, und nun ist jeder leistungsfähige Server mit einer Art von RAID-System ausgestattet. Hier eine Übersicht über die verschiedenen RAID-Stufen:

- *RAID Stufe 0*. Stripeset, keine Parität
- *RAID Stufe 1*. Festplattenspiegelung
- *RAID Stufe 4*. Stripeset mit Parität
- *RAID Stufe 5*. Stripeset mit verteilter Parität
- *RAID Stufe 10*. Gespiegeltes Stripeset mit verteilter Parität

Diese RAID-Systeme bieten ein hohes Maß an Verfügbarkeit und Fehlertoleranz sowie eine sehr hohe Leistung. Es wurden batteriebetriebene Zwischenspeicher verwendet, um die Schreibzugriffe zwischenspeichern zu können, ohne die Daten bei einem Stromausfall zu verlieren. Die meisten neueren

RAID-Systeme bieten die Möglichkeit, Festplatten hinzuzufügen, ohne das System herunterfahren oder bestehende Festplatten neu formatieren zu müssen. RAID ist die Technologie der Wahl für hoch verfügbare, hochleistungsfähige Server.

Eine weitere Controllertechnologie, die in letzter Zeit sehr viel Aufmerksamkeit erregt hat, ist die *Fibre Channel*-Technologie. Fibre Channel ist ein Hochgeschwindigkeitsdatenkanal, mit dem RAID-Arrays verbunden werden. Die meisten Fibre Channel-Karten verbinden einen Server mit einem externen Speicherchassis, das mit SCSI-Festplatten gefüllt ist. Der Fibre Channel-Controller adressiert diese Festplatten direkt und übernimmt alle Pflichten eines Hochleistungs-RAID-Controllers. Die Fibre Channel-Technologie bietet einen höheren Durchsatz als die bestehende SCSI-Technologie (100 Mbps). Dies gilt jedoch nicht für den SCSI Ultra3-Standard, der bisher nur als Standard existiert, ohne dass Hardware dafür verfügbar wäre.

Beide Mechanismen verwenden die Standard-SCSI-Laufwerke und setzen im Wesentlichen auf den SCSI-Laufwerken auf, wobei sie auf die Laufwerke zugreifen und die Zwischenspeicherung und die Verwaltung der Warteschlangen für jedes Laufwerk übernehmen. Windows 2000 betrachtet Stripesets, die mit diesen Controllern ausgestattet sind, als ein physisches Laufwerk und Windows 2000 weiß nicht einmal, dass es sich um besondere Festplatten handelt.

4.2 Festplattenpartitionen

Nachdem erklärt wurde, was eine Festplatte ist, soll nun beschrieben werden, wie die Daten auf der Festplatte gespeichert werden. Dieser Abschnitt behandelt die Partitionierung von Festplatten und der nächste Abschnitt die Formatierung von Datenträgern.

Die Partitionierung bietet die Möglichkeit, eine große physische Festplatte in mehrere Abschnitte zu unterteilen. Sehr häufig gibt es auf einer großen Festplatte nur eine Partition. Manchmal gibt es jedoch mehrere Partitionen und Datenträger, um die Daten besser organisieren und sichern zu können. Außerdem spielen Partitionen eine große Rolle bei der Installation, weil das »erste« Laufwerk den Master-Boot-Record (MBR) enthält, ein kleines Programm, das immer an einer bestimmten Stelle auf der Festplatte abgelegt ist und vom BIOS benutzt wird, um den Computer zu starten.

Als Erstes wird nun betrachtet, wie der Systemstart funktioniert und warum er für die Partitionierung der Festplatte relevant ist. Anschließend werden die Partitionierungsschemata von Windows 2000 genauer beleuchtet. Windows 2000 unterstützt Basisfestplatten und dynamische Festplatten. Sie erfahren außerdem, wie sich eine Basisfestplatte in eine dynamische Festplatte umwandeln lässt.

4.2.1 Der Systemstart

Haben Sie sich jemals gefragt, wie ein Computer startet? Hier ein kurzer Überblick für den Startvorgang bei Intel-Prozessoren. Wenn ein Computer angeschaltet wird, beginnt die CPU, Anweisungen im BIOS zu lesen und diese auszuführen. Das BIOS-Programm führt das System durch die POST-Routinen (POST = Power-On Self Test), die normalerweise die Grafikkarte initialisieren, den Speicher hochzählen, alle installierten PCI-Geräte und alle installierten Laufwerke auflisten. Anschließend wählt das System das Laufwerk aus, von dem gestartet wird.

Wenn das System so eingerichtet ist, dass es von einem Diskettenlaufwerk startet, wird es als Erstes

versuchen, von diesem zu starten. Wenn das System von einem CD-ROM-Laufwerk starten kann, wird es als Erstes versuchen, von diesem zu starten etc., falls sich eine bootfähige CD-ROM im Laufwerk befindet. Falls IDE-Festplatten im System vorhanden sind, versucht das System, von der aktiven Partition auf der Master-Festplatte im primären Kanal zu starten. Wenn das System mit SCSI-Festplatten ausgestattet ist, versucht es, von der aktiven Partition auf der Festplatte mit der SCSI-ID 0 im ersten SCSI-Kanal zu starten.

Wenn diese Optionen alle fehlschlagen, liefert das System eine Fehlermeldung zurück, wie z.B. »Kein Betriebssystem vorhanden«. Eine Meldung wie »Kein ROM-BIOS vorhanden« bedeutet, dass das System versucht hat, von einem ROM-Chip zu booten, was jedoch fehlschlug.

Verläuft eine der Festplattenbootoptionen erfolgreich, liest das BIOS den Master-Boot-Record der fraglichen Festplattenpartition und beginnt, das dort gefundene Programm auszuführen. Bei einem Windows 2000-System enthält der Master-Boot-Record ein kleines Programm, das den Bildschirm für die Betriebssystemauswahl öffnet. Bei einem Windows 98-System enthält der Master-Boot-Record ein Programm, das den Bildschirm »Windows 98 wird gestartet« anzeigt und dem Benutzer drei Sekunden Zeit gibt, um eine der Funktionstasten zu drücken und ein Bootmenü zu öffnen. Bei Betriebssystemen wie Linux wird im Allgemeinen ein System wie LILO benutzt, das dasselbe leistet wie der Bildschirm für die Betriebssystemauswahl in Windows 2000.

Das Programm im Master-Boot-Record dient in allen Fällen nur einem Zweck: ein Betriebssystem zu starten. Bei Windows 2000 wird über den Bildschirm zur Betriebssystemauswahl entweder Windows 2000 gestartet, indem das Programm ausgeführt wird, das in der Datei *Boot.ini* angegeben wird (siehe Kapitel 3) oder indem das gespeicherte Bild des Master-Boot-Records eines anderen Betriebssystems ausgeführt wird. Bei der Installation von Windows 2000 wird der bestehende Master-Boot-Record durch den Master-Boot-Record von Windows 2000 ersetzt. Der alte Master-Boot-Record wird in eine Datei namens *Bootsect.dos* geschrieben. Anschließend wird eine Option in die Datei *Boot.ini* eingetragen, dass das alte Betriebssystem gestartet wird, indem die Datei *Bootsect.dos* wie ein Master-Boot-Record geladen wird.

Wozu dient nun diese ganze Ausführung? Der Urlader von Windows 2000 benötigt eine aktive Partition auf der »ersten« Festplatte, die entweder die Masterfestplatte im primären IDE-Kanal ist oder die Festplatte mit der SCSI-ID 0 im ersten SCSI-Kanal. Die aktive Partition enthält einen Master-Boot-Record, der benutzt wird, um den Computer zu starten. Der Master-Boot-Record der aktiven Partition kann ein beliebiges Betriebssystem starten, das sich einer primären Partition der »ersten« Festplatte befindet. Was ist eine primäre Partition? Eine Art von Partition auf einer Basisfestplatte.

4.2.2 Basisfestplatten

Eine *Basisfestplatte* ist eine Festplatte, die das altbekannte Standardschema mit einer primären Partition, einer erweiterten Partition und logischen Laufwerken benutzt, um zu definieren, wie der Platz auf der Festplatte verwendet wird. Auf einer Basisfestplatte können bis zu vier Partitionen eingerichtet werden. Eine primäre Partition ist eine Partition, die sich nicht weiter unterteilen lässt und sehr wahrscheinlich ein Betriebssystem enthält. Eine der Partitionen auf einer Basisfestplatte kann eine erweiterte Partition sein. Deshalb könnte eine Festplatte drei primäre Partitionen und eine erweiterte Partition enthalten, eine primäre Partition und eine erweiterte Partition oder nur eine primäre Partition oder nur eine erweiterte

Partition. Eine erweiterte Partition lässt sich in logische Laufwerke aufteilen.



Wie Partitionen eingerichtet und entfernt werden, wird im Abschnitt »Die Datenträgerverwaltung« später in diesem Kapitel beschrieben.

Diese Partitionen stellen eine feste Speichermenge zur Verfügung. Das heißt, eine Partition wird durch die von ihr verwendete Speichermenge definiert und die Größe einer Partition lässt sich nur schwer verändern. Um die Größe einer Partition zu verändern, muss diese normalerweise gelöscht und neu erstellt werden. Weil eine Partition einen fortlaufenden Speicherplatz belegen muss, ist dazu jedoch in der Regel eine Löschung aller Partitionen erforderlich. Und das ist etwas schwierig. Wenn ein logisches Laufwerk zahlreiche kleinere Partitionen enthält, kann es sehr unangenehm werden, wenn eine Partition zu klein wird. Aus diesem Grund gibt es eine Datenträgerverwaltung und Kontingente als Alternative zu Partitionierungsschemata, um die Nutzung von Festplattenspeicher zu steuern. Sie sollten also davon absehen, eine große Partition aufzuteilen, um zu verhindern, dass Benutzer zu viel Festplattenspeicher verbrauchen. Stattdessen sollten Sie mit Kontingenten arbeiten. Festplattenkontingente und deren Verwaltung werden in einem eigenen Abschnitt in diesem Kapitel beschrieben.

Wozu ist die Partitionierung dann nützlich, wenn es bessere Tools gibt, um den Verbrauch von Festplattenspeicher zu kontrollieren? Die meisten Gründe für die Partitionierung von Festplatten sind auf dynamische Festplatten beschränkt, aber die Partitionierung bietet auch einige interessante Optionen für die Problembehebung und die Wiederherstellung des Betriebssystems (siehe Kapitel 3). Um verschiedene Betriebssysteme auf einem Computer zu nutzen, muss außerdem für jedes Betriebssystem eine primäre Partition eingerichtet werden. Dieses Thema wurde bereits im letzten Abschnitt zum Systemstart beschrieben.

Wie sieht es mit der Erweiterung von Partitionen und Stripesets aus? In Windows 2000 stehen diese Funktionen nur bei dynamischen Festplatten zur Verfügung.

4.2.3 Dynamische Festplatten

Alle coolen Dinge, die Sie in Windows 2000 mit der Datenträgerverwaltung machen können, beziehen sich auf dynamische Festplatten. Es lassen sich zwar alle erweiterten Partitionen, Stripesets und Spiegelungen, die mit Windows NT 4.0 erzeugt wurden, in dynamische Festplatten umwandeln, um jedoch neue erweiterte Partitionen, Stripesets und Spiegelungen einzurichten, müssen dynamische Festplatten vorhanden sein.

Auf dynamische Festplatten kann nur über Windows 2000 zugegriffen werden. Wird auf der »ersten« Festplatte eine dynamische Festplatte eingerichtet, bedeutet dies, dass auf diesem System nur Windows 2000 ausgeführt werden kann.

Wenn eine Festplatte von Windows 2000 bei der Installation erkannt oder wenn die Festplatte installiert wird, nutzt Windows 2000 diese Festplatte als Basisfestplatte. Um eine dynamische Festplatte zu erhalten, muss die Basisfestplatte aktualisiert werden. Dieser Prozess wird im nächsten Abschnitt beschrieben.

Der Hauptunterschied zwischen einer Basisfestplatte und einer dynamischen Festplatte ist der, dass eine Basisfestplatte Partitionen enthält, wohingegen eine dynamische Festplatte Datenträger beinhaltet. Dieser

Unterschied mag zwar trivial wirken, aber in Windows 2000 bezieht sich der Begriff *Datenträger* immer auf eine dynamische Festplatte und der Begriff *Partition* immer auf eine Basisfestplatte.

Die Hauptmerkmale von dynamischen Festplatten wie Spiegelsätze, Stripesets und Datenträgersätze werden in einem späteren Abschnitt beschrieben. Nun wird der Unterschied zwischen Basis- und dynamischen Festplatten erläutert und es wird gezeigt, wie eine Basisfestplatte in eine dynamische umgewandelt werden kann.

4.2.4 Basisfestplatten und normale Festplatten

Eine *Basisfestplatte* ist eine »normale« Festplattenpartition, auf die durch ein beliebiges Betriebssystem einschließlich Windows 2000 zugegriffen werden kann. Wenn auf einem System mehrere Betriebssysteme installiert werden, wie z.B. Windows 2000 und Windows 98, kann Windows 98 nur auf Basisfestplatten zugreifen. Basisfestplatten benutzen das Standardschema der primären und erweiterten Partitionen mit logischen Laufwerken. Immer, wenn Änderungen an einer Basisfestplatte vorgenommen werden, muss das System neu gestartet werden, bevor die Änderungen wirksam werden. Auf Basisfestplatten besteht ein Zugriff über mehrere Betriebssysteme, wie z.B. Windows 98, wenn auf dem System mehrere Betriebssysteme installiert sind.



Nur weil eine Partition von verschiedenen Betriebssystemen genutzt werden kann, heißt das noch lange nicht, dass dies auch für das Dateisystemformat gilt. Partitionen, die mit NTFS formatiert wurden, stehen für Windows 98 nicht zur Verfügung, auch wenn die NTFS-Partition sich auf einem Systemdatenträger befindet. FAT32-Partitionen sind Basislaufwerke, die sowohl unter Windows 98 als auch unter Windows 2000 verfügbar sind.

Bei einem *dynamisches Laufwerk* lassen sich Änderungen der Aufteilung »on the fly« vornehmen, ohne dass das System neu gebootet werden muss. Dies bedeutet, dass dynamische Festplatten die Erweiterung eines Datenträgers und die Arbeit mit Spiegelsätzen unterstützen.

Die Eigenschaften von dynamischen Festplatten und Basisfestplatten gelten für alles, was Windows 2000 als physisches Laufwerk interpretiert - egal, ob es sich um eine Festplatte oder einen Festplattenstapel mit einem Hardware-RAID-Controller handelt. Windows 2000 betrachtet alle Speicherräume als eine Festplatte. Es muss die gesamte Festplatte aktualisiert werden. Dynamische Laufwerke stehen auf einem Notebook nicht zur Verfügung.

Die Aktualisierung einer Basisfestplatte in eine dynamische Festplatte ist ein einmaliger Prozess. Nachdem eine Basisfestplatte aktualisiert wurde, lässt sie sich nicht zurückverwandeln, ohne dass alle Festplattenpartitionen entfernt werden und die Daten auf den Festplattenpartitionen verloren gehen. Es ist deswegen zwar möglich, von einer dynamischen Festplatte zu einer Basisfestplatte zurückzukehren. Dieser Prozess ist jedoch mit einem großen Aufwand verbunden.

Gehen Sie wie folgt vor, um eine dynamische Festplatte aus einer Basisfestplatte zu erzeugen:

1. Stellen Sie sicher, dass diese Aktualisierung tatsächlich erforderlich ist.
2. Prüfen Sie noch einmal, ob die Aktualisierung tatsächlich vorgenommen werden soll, da es ziemlich aufwändig ist, aus einer dynamischen Partition wieder eine Basisfestplatte zu machen.
3. Entfernen Sie alle anderen Betriebssysteme von der Festplatte, die aktualisiert werden soll. Nach der

Aktualisierung kann auf diese Betriebssysteme nicht mehr zugegriffen werden.

4. Erstellen Sie eine Sicherung des gesamten Systems.

5. Öffnen Sie die Datenträgerverwaltung, indem Sie in der Systemsteuerung doppelt auf **Verwaltung** und im Ordner **Verwaltung** doppelt auf **Computerverwaltung** klicken. Klicken Sie in der Computerverwaltung dann auf **Datenspeicher** und **Datenträgerverwaltung** (siehe Abbildung 4.2). Weitere Informationen zur Datenträgerverwaltung finden Sie im Abschnitt »Die Datenträgerverwaltung« in diesem Kapitel.

6. Klicken Sie mit der rechten Maustaste auf die zu konvertierende Festplatte und wählen Sie im Kontextmenü den Befehl **In dynamische Festplatte umwandeln**. Wenn dies nicht funktioniert, können Sie versuchen, auf die Festplatte (z.B. Festplatte 0) statt auf die Partition zu klicken (z.B. C:). Wenn eine Festplatte mehrere Partitionen enthält, müssen Sie mit der rechten Maustaste auf die Festplatte klicken. Ansonsten können Sie auf den Partitionsbereich klicken.

7. Wählen Sie im Dialogfeld **Aktualisierung auf dynamische Festplatte** die Festplatten, die aktualisiert werden sollen (siehe Abbildung 4.3) und klicken Sie anschließend auf OK.

Nach der Aktualisierung gibt es keine offensichtlichen Veränderungen, außer, dass nur noch über Windows 2000 auf die dynamischen Festplatten zugegriffen werden kann.

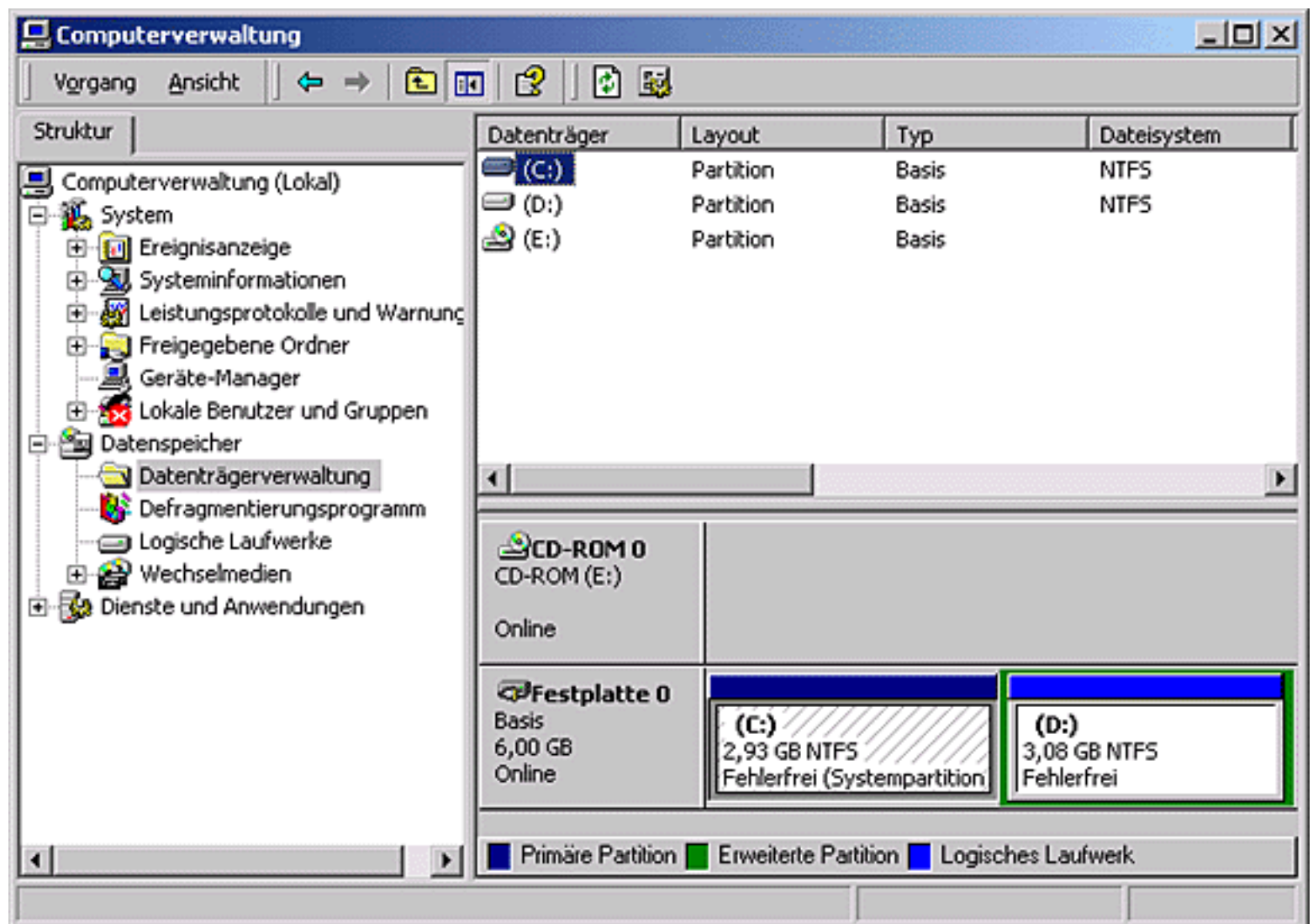


Abbildung 4.2: Die Datenträgerverwaltung im Snap-In Computerverwaltung.

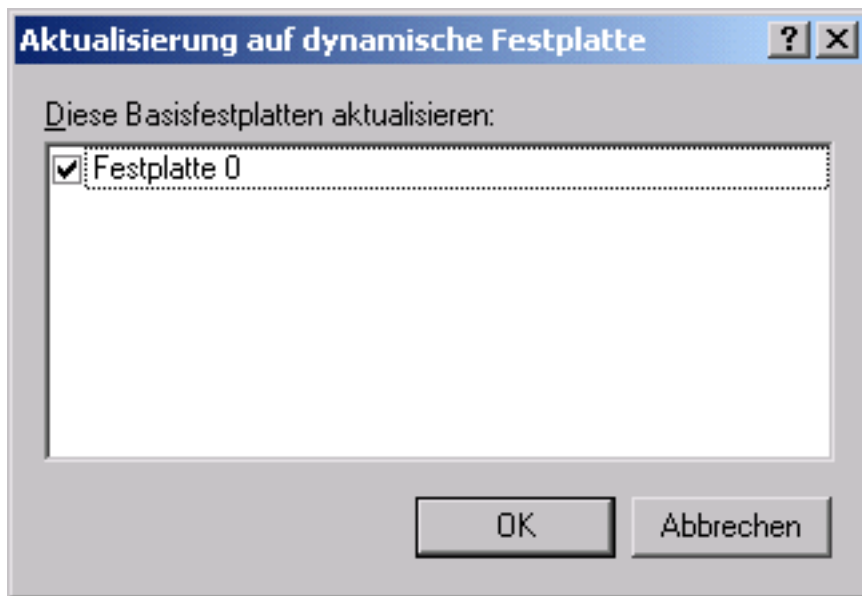


Abbildung 4.3: Um Festplatte 0 in eine dynamische Festplatte umzuwandeln, muss nur das Kontrollkästchen aktiviert werden.

4.3 Die Datenträgerverwaltung

Die Datenträgerverwaltung ersetzt die Festplattenverwaltung von Windows NT 4.0. Mit der Datenträgerverwaltung lassen sich Festplatten, Partitionen und Datenträger verwalten. Das ist eine ganze Menge. Hier ein Überblick über die Themen, die zur Datenträgerverwaltung beschrieben werden:

- Die Datenträgerverwaltung starten
- Partitionen erstellen und löschen
- Datenträger erweitern
- Laufwerksbuchstaben ändern
- Laufwerke ohne Laufwerksbuchstaben ändern

Mit der Datenträgerverwaltung lassen sich auch Stripesets erstellen. Dies wird jedoch im Abschnitt zu Stripesets behandelt. Werfen Sie nun einen Blick darauf, wie die Datenträgerverwaltung gestartet wird.

4.3.1 Die Datenträgerverwaltung starten

Die Datenträgerverwaltung ist ein Snap-In der Microsoft Management Console (MMC). Deshalb ist die Anwendung in der Datei *diskmgmt.msc* enthalten, die sich im Verzeichnis *%SYSTEMROOT%\system32* befindet. Diese Anwendung lässt sich auf verschiedene Arten starten. Eine Möglichkeit besteht darin, die Computerverwaltung zu öffnen und dann den Ordner **Datenspeicher** und anschließend den Ordner **Datenträgerverwaltung** zu wählen. Um die Computerverwaltung zu öffnen, klicken Sie in der Systemsteuerung doppelt auf **Verwaltung** und anschließend doppelt auf das Symbol **Computerverwaltung**.

Schneller geht es, wenn Sie **Start/Ausführen** wählen und dann *Diskmgmt.msc* eingeben. Dadurch wird die Datenträgerverwaltung ohne die Computerverwaltung gestartet. Auf diese Weise lässt sich jede

beliebige Snap-In-Datei direkt starten.

Die Datenträgerverwaltung wird in Abbildung 4.2 gezeigt. Nehmen Sie sich einen Augenblick Zeit, um die Benutzeroberfläche zu betrachten. Im oberen Teil des Fensters werden die Laufwerksbuchstaben, die Partitionen und Datenträger gezeigt, die im lokalen System zur Verfügung stehen. Beachten Sie, dass auch das CD-ROM-Laufwerk in der Liste enthalten ist. Dies dient dazu, den Wechsel des Laufwerksbuchstaben des CD-ROM-Laufwerks zu ermöglichen und alle Laufwerksbuchstaben anzuzeigen, die momentan in Benutzung sind.

In der unteren Hälfte des Fensters werden die Partitionen angezeigt, die in der oberen Hälfte definiert werden. Sie werden jedoch den physischen Festplatten zugeordnet, auf denen sie eingerichtet sind. Die Festplatten in einem System sind fortlaufend durchnummeriert. Die Nummerierung beginnt bei der Festplatte 0. Für jede Festplatte werden die eingerichteten Partitionen, deren Größe und das Dateisystem angezeigt, mit dem jede Partition formatiert wurde.

4.3.2 Die Eigenschaften der Festplatte

Um die Eigenschaften einer Festplatte zu prüfen, klicken Sie mit der rechten Maustaste darauf und wählen im Kontextmenü den Befehl **Eigenschaften**. Es öffnet sich das Dialogfeld **Eigenschaften von [Festplatte]** (siehe Abbildung 4.4), das alle Informationen zu einer Festplatte enthält:

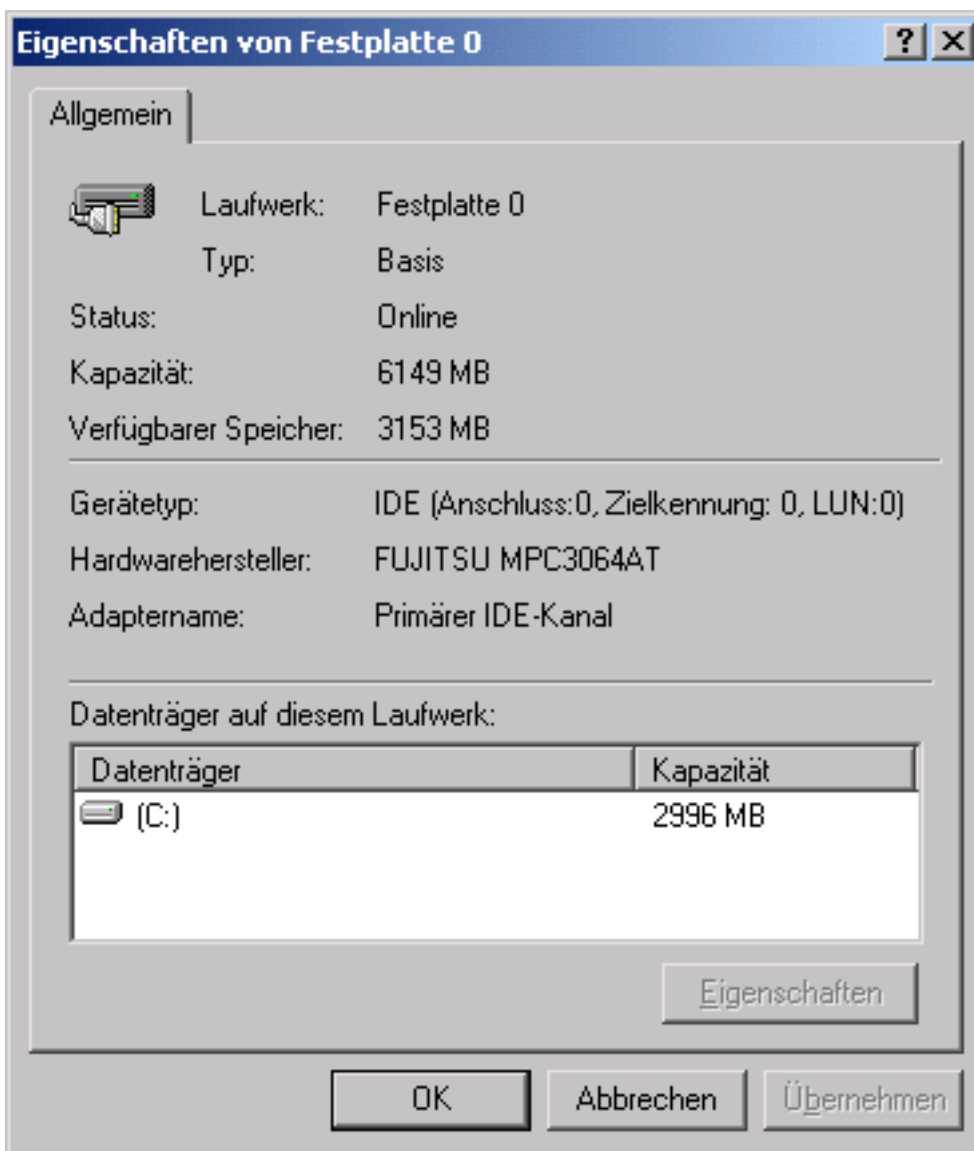


Abbildung 4.4: Eigenschaften einer Festplatte.

- *Typ.* Basis- oder dynamische Festplatte.
- *Status.* Online oder offline. Diese Angabe wird für Wechselmedien wie Iomega-Jaz-Laufwerke verwendet.
- *Kapazität.* Die Festplattenkapazität einschließlich dem partitionierten und nicht partitionierten Speicherplatz.
- *Verfügbarer Speicher.* Anteil des Speichers, der nicht Bestandteil einer Partition ist. Diese Angabe sollte nicht mit »freiem Speicher« verwechselt werden, d.h. dem bisher ungenutzten Speicherplatz einer Partition.
- *Gerätetyp.* Diese Eigenschaft definiert den Adaptertyp (z.B. SCSI oder IDE), der für den Zugriff auf die Festplatte verwendet wird. Es wird die SCSI-ID oder der Master/Slave-Status angegeben. Die Angabe **Anschluss: 0** definiert den verwendeten Kanal.
0 ist der primäre Kanal. Die Angabe **Lun:0** repräsentiert die LUN (Logical Unit Number). Bei einem SCSI-Laufwerk ist dies die SCSI-ID, bei IDE-Laufwerken steht die Angabe 1 für das Slave-Laufwerk in einem IDE-Kanal.
- *Hardwarehersteller.* Der Hardwarehersteller und normalerweise auch die Modellnummer. Dies ist

sehr hilfreich bei der Bestellung von Ersatzteilen und der Erweiterung der Kapazität.

- *Adaptername*. Der Name des Adapters, der für den Zugriff auf die Festplatte benutzt wird. Diese Angabe kann bei der Problembehebung nützlich sein.
- *Datenträger*. Eine Liste aller Datenträger oder Partitionen, die auf der Festplatte enthalten sind.

4.3.3 Eigenschaften von Datenträgern oder Partitionen

Neben den Eigenschaften einer Festplatte kann die Datenträgerverwaltung auch die Eigenschaften eines Datenträgers oder einer Partition anzeigen. Dasselbe Dialogfeld lässt sich auch über den Windows-Explorer öffnen. Klicken Sie dazu mit der rechten Maustaste im Explorer auf den Laufwerksbuchstaben und wählen Sie im Kontextmenü den Befehl **Eigenschaften**. Das Dialogfeld **Eigenschaften** für ein Laufwerk enthält zahlreiche Optionen, die auf verschiedene Registerkarten verteilt sind (siehe Abbildung 4.5).

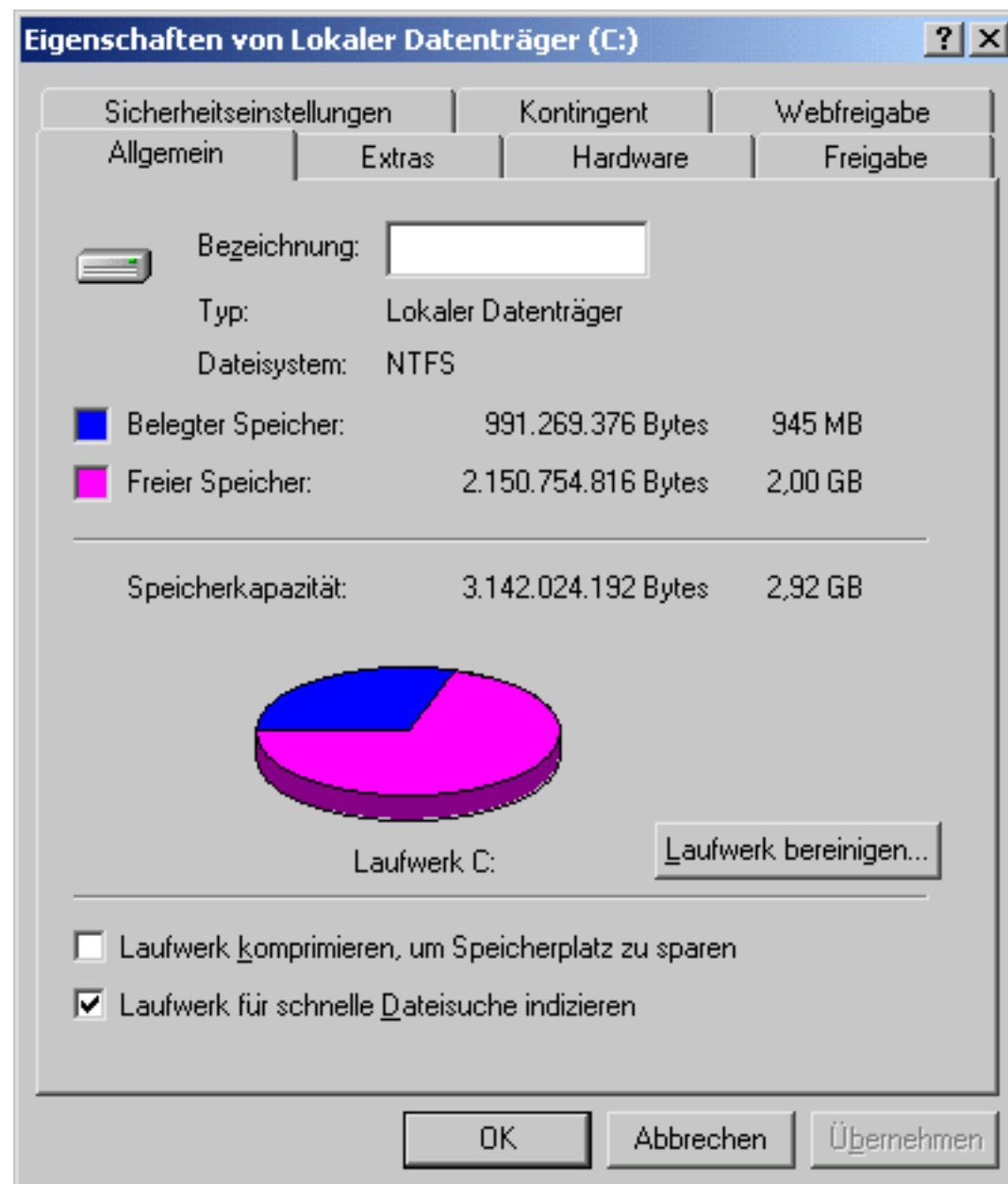


Abbildung 4.5: Die Eigenschaften einer Partition. Beachten Sie die Anzahl der Registerkarten.

Diese Abbildung zeigt die Registerkarte Allgemein.

Die Registerkarte Allgemein

Wie in Abbildung 4.5 gezeigt, enthält die Registerkarte **Allgemein** allgemeine Informationen über den Datenträger, wie z.B. die Gesamtkapazität, den belegten Speicher und den freien Speicher. Ein Kreisdiagramm veranschaulicht die Prozentwerte für den freien und den belegten Speicher.

Auf dieser Registerkarte kann auch eine Datenträgerbezeichnung festgelegt werden. Die *Datenträgerbezeichnung* bietet eine Möglichkeit, den Inhalt einer Festplatte zu definieren, indem ihr eine frei wählbare Textbezeichnung zugewiesen wird. Es handelt sich in erster Linie um ein Kommentarfeld, mit dem die Festplatte beschrieben wird. Eine aussagekräftige Bezeichnung der Festplatten erleichtert die Administration.

Über die Schaltfläche **Laufwerk bereinigen** wird die Anwendung **Bereinigen des Datenträgers** gestartet, mit der Speicherplatz auf einem Laufwerk freigegeben werden kann. Die Anwendung **Bereinigen des Datenträgers** erfüllt einige nützliche Aufgaben (siehe Abbildung 4.6). Sie bietet die Möglichkeit, alle übertragenen Programmdateien zu löschen, die ActiveX-Steuerelemente und Java-Applets enthalten. Über sie lassen sich auch vom Internet Explorer angelegte temporäre Internet-Dateien und der Papierkorb löschen, Dateien komprimieren, die schon länger nicht mehr benutzt wurden und Dateien bereinigen, die von den Katalogdateien für den Inhaltsindex benutzt werden. Standardmäßig sind nur die Kontrollkästchen **Übertragene Programmdateien** und **Temporary Internet Files** aktiviert. Für jede Option lassen sich über die Schaltfläche **Dateien anzeigen** die betroffenen Dateien anzeigen.



Abbildung 4.6: Die Anwendung Bereinigen des Datenträgers dient dazu, nicht benutzte und temporäre Dateien vom Laufwerk zu löschen.

Das Kontrollkästchen **Laufwerk komprimieren, um Speicherplatz zu sparen** steht nur bei NTFS-Laufwerken zur Verfügung. Mit dieser Option wird eine NTFS-Komprimierung auf das gesamte Laufwerk angewendet und neue Dateien werden ebenfalls komprimiert. Dies ist nützlich, wenn ein Dateiserver sehr viel Verarbeitungszeit zur Verfügung hat und zahlreiche Dokumente enthält, die sich gut komprimieren lassen, wie z.B. Microsoft Word- oder PowerPoint-Dateien.

Mit dem Kontrollkästchen **Laufwerk für schnelle Dateisuche indizieren** wird festgelegt, dass der Microsoft-Indexdienst in regelmäßigen Abständen ausgeführt wird und Indizes erzeugt, die später für die Suche nach Dateien auf dem Laufwerk benutzt werden können. Bei großen Datenträgern kann dies nützlich sein, weil alle Header-Informationen in Microsoft Office-Dokumenten indiziert werden und sich Dokumente zu einem Thema dadurch leichter finden lassen.

Die Registerkarte Extras

Die Registerkarte **Extras** (siehe Abbildung 4.7) enthält Verknüpfungen zu häufig benutzten Tools für

Datenträger. Die **Fehlerüberprüfung** stellt fest, ob Fehler auf dem Datenträger enthalten sind, und kann zahlreiche Fehler in Laufwerksstrukturen beheben. Die Option **Sicherung** startet das Sicherungssystem, das in Kapitel 25 ausführlich beschrieben wird. Das Tool **Defragmentierung** startet das Programm **Defragmentierung**, mit dem sich die Fragmentierung der Festplatte reduzieren lässt.



Abbildung 4.7: Über die Registerkarte Extras lassen sich die Fehlerüberprüfung, die Sicherung und die Defragmentierung leicht starten.

Die Defragmentierung tritt auf einem Datenträger immer auf, wenn Lese- und Schreiboperationen durchgeführt werden. Das Betriebssystem teilt den verfügbaren Speicher auf einem Datenträger in Cluster auf. Wenn eine Datei auf den Datenträger geschrieben wird, schreibt das Betriebssystem immer in Clustern auf den Datenträger. Manchmal lassen sich die einzelnen Cluster einer Datei nicht direkt nebeneinander speichern, sodass die Datei fragmentiert wird und auf dem ganzen Datenträger verteilt ist. Die Dateien lassen sich dadurch schneller speichern. Im Laufe der Zeit kann eine exzessive Fragmentierung jedoch Probleme verursachen, weil das Betriebssystem, um eine Datei zu laden, den gesamten Datenträger nach den Einzelteilen durchsuchen muss. Der Defragmentierungsprozess schreibt

im Wesentlichen alle fragmentierten Dateien erneut auf den Datenträger, sodass sie hintereinander liegen.

Die Registerkarte Hardware

Die Registerkarte **Hardware** listet alle Laufwerke auf, die im System enthalten sind und zeigt die Laufwerksbezeichnung, die Modellnummer und den Status an. Über die Registerkarte **Hardware** lässt sich das Dialogfeld **Eigenschaften** für jedes Laufwerk per Mausklick auf die gleichnamige Schaltfläche öffnen, in dem die Treiber aktualisiert und Probleme behandelt werden können.

Die Registerkarte Freigabe

Wenn das gesamte Laufwerk freigegeben werden soll, muss ein Eintrag auf der Registerkarte **Freigabe** enthalten sein. Über diese Registerkarte kann Benutzern der Zugriff auf ganze Laufwerke über eine Netzwerkfreigabe gewährt werden. Alle Laufwerke (ausgenommen von CD-ROM-Laufwerken) werden mit einer versteckten Freigabe mit dem Laufwerksbuchstaben, gefolgt von einem Dollarzeichen, freigegeben (z.B. C\$ für Laufwerk C:). Über diese Standardfreigaben können Administratoren direkt auf ein Laufwerk zugreifen; und sie lassen sich nicht entfernen.

Selbstverständlich kann das Laufwerk unter einem neuen Namen in sichtbarer Form freigegeben werden. Klicken Sie dazu auf die Schaltfläche **Neue Freigabe** und füllen Sie das in Abbildung 4.8 gezeigte Dialogfeld aus.

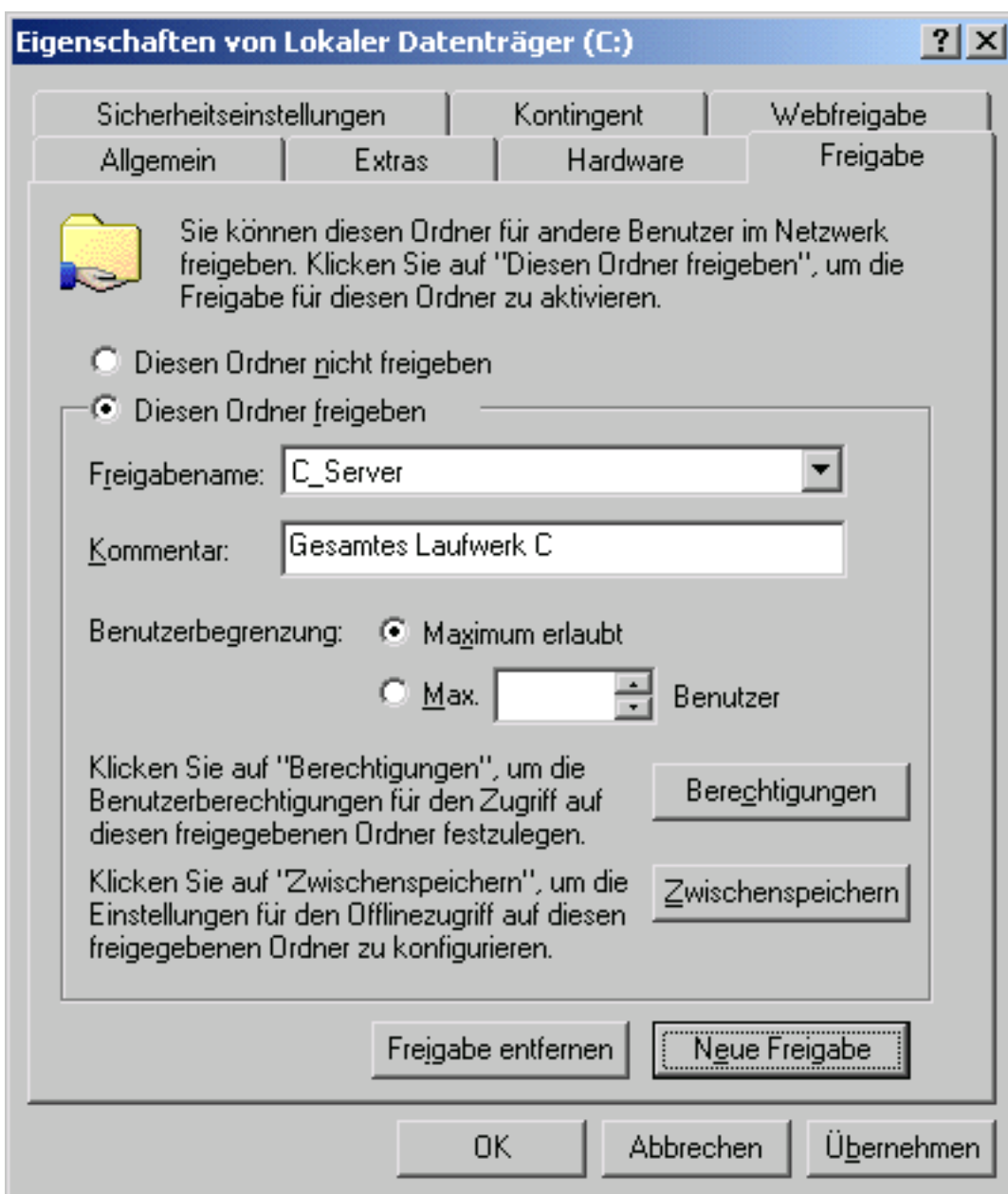


Abbildung 4.8: Über die Registerkarte Freigabe lassen sich Laufwerke oder Ordner für Benutzer im Netzwerk freigeben.

Um die Eigenschaften einer bestehenden Freigabe zu ändern, wählen Sie diese im Listenfeld **Freigabename** aus. Anschließend können Sie den Kommentar, die Benutzerbegrenzung, die Berechtigungen und den Zwischenspeicher ändern. Der Kommentar für einen Ordner ist eine einfache Erläuterung, die neben dem Ordnernamen angezeigt wird, wenn der Benutzer den Server durchsucht. Die Benutzerbegrenzung legt die maximale Anzahl von Benutzern fest, die gleichzeitig auf die Freigabe zugreifen können. Dies ist nützlich, wenn nur eine begrenzte Bandbreite zur Verfügung steht.

Um die Berechtigungen für eine Freigabe zu ändern, klicken Sie auf die Schaltfläche **Berechtigungen**. Die Berechtigungen für administrative Freigaben wie C\$ lassen sich nicht ändern. Die Berechtigungen für neu eingerichtete Freigaben jedoch schon. Bei administrativen Freigaben gelten die Berechtigungen für die lokale Gruppe der Administratoren, die nicht geändert werden können. Wird eine neue Freigabe erstellt, ist standardmäßig ein Vollzugriff für die Gruppe **Jeder** aktiviert. Um diese Berechtigungen zu ändern, können Sie über die Schaltflächen **Hinzufügen** und **Entfernen** Benutzer hinzufügen, die einen

Zugriff haben sollten. Anschließend können Sie für jede Gruppe im unteren Bereich des Dialogfelds die Berechtigungen festlegen (siehe Abbildung 4.9).

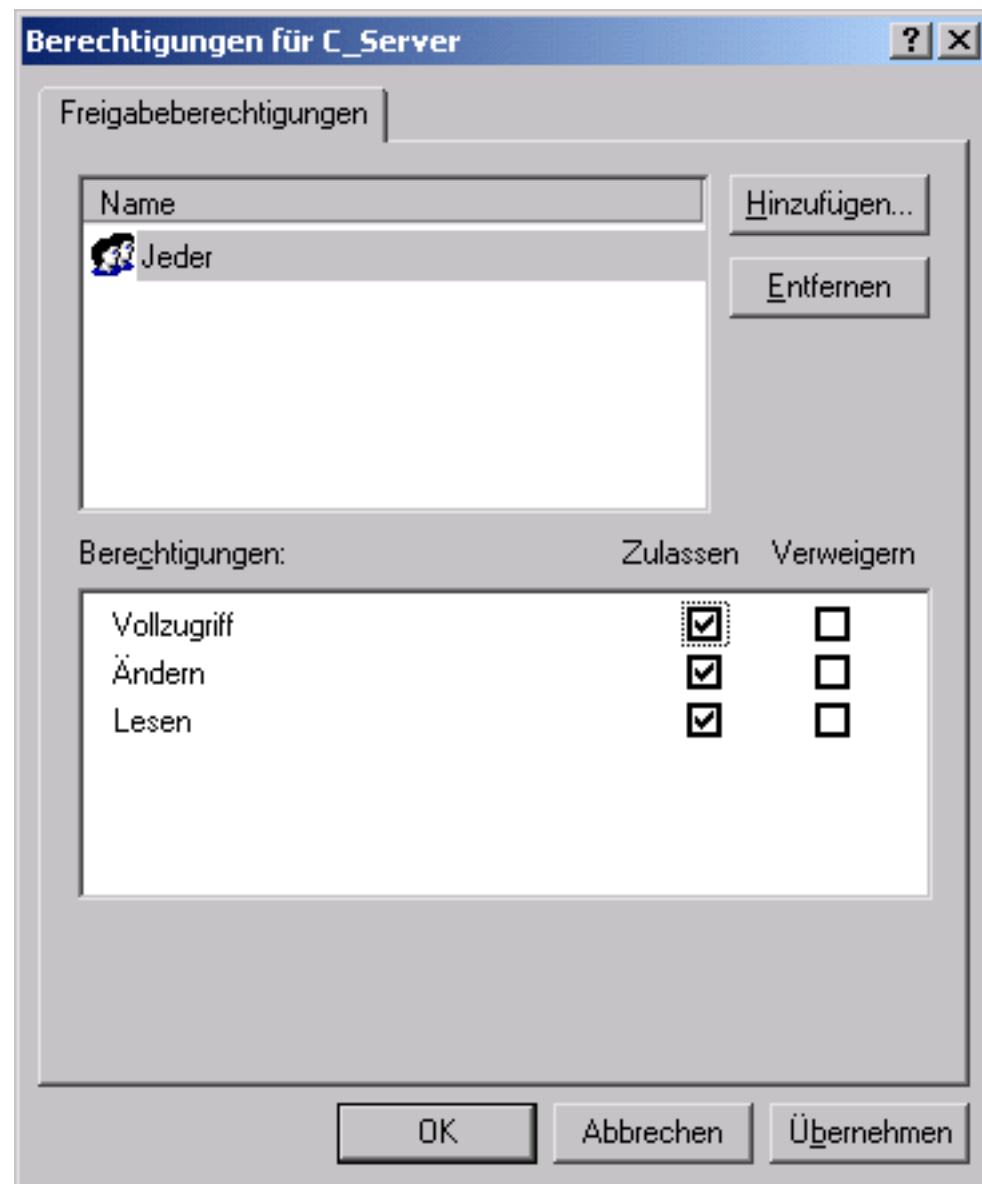


Abbildung 4.9: Im Dialogfeld **Berechtigungen** wird festgelegt, welche Benutzer Zugriff auf eine Freigabe haben. Bei der gezeigten Einstellung haben alle Benutzer einen Vollzugriff.

Weitere Informationen finden Sie im Abschnitt »Netzwerkfreigaben« später in diesem Kapitel.

Die Registerkarte Sicherheitseinstellungen

Die Registerkarte **Sicherheitseinstellungen** wird nur bei Laufwerken angezeigt, die mit NTFS formatiert sind. Auch hier lässt sich festlegen, welche Berechtigungen für einen Benutzer oder eine Benutzergruppe gelten. Im Abschnitt zu den Dateisystemen finden Sie mehr zum Thema Sicherheitseinstellungen.

Die Registerkarte Kontingent

Auf dieser Registerkarte kann der Administrator die Menge des Festplattenspeicherns festlegen, die Benutzer oder Benutzergruppen verwenden dürfen. Diesem Thema ist später in diesem Kapitel ein

ganzer Abschnitt gewidmet.

Die Registerkarte Webfreigabe

Obwohl dies vielleicht zunächst nicht sehr sinnvoll erscheint, lässt sich hier ein gesamtes Laufwerk für den Zugriff über das Internet freigeben. Diese Registerkarte ist nur vorhanden, wenn der Internet Information Server installiert ist. Mehr zu diesem Thema finden Sie in Kapitel 20.

Nachdem die grundlegende Benutzeroberfläche beschrieben wurde, soll nun gezeigt werden, wie Festplattenpartitionen und Datenträger erstellt, verändert und entfernt werden.

4.3.4 Die Verwaltung von Partitionen und Datenträgern

In der Datenträgerverwaltung werden nicht nur nette Bilder zum Laufwerkstatus angezeigt und Veränderungen zur Freigabe von Laufwerken vorgenommen, sondern es lassen sich auch Partitionen hinzufügen, ändern und entfernen.

»Eine Partition entfernen« mag zwar ganz nett und unschuldig klingen, die Daten werden dabei jedoch komplett gelöscht. Mit den Partitionierungswerkzeugen sollten Sie nur experimentieren, wenn eine gute Sicherung für das gesamte System existiert. Es können schlimme Dinge passieren und wenn bei der Partitionierung etwas durcheinander gerät, schreit dies förmlich nach Problemen.

Eine neue Partition erstellen

Um eine neue Partition erstellen zu können, muss in der Datenträgerverwaltung Speicherplatz mit dem Status **Freier Speicherplatz** oder **Nicht zugeordnet** vorhanden sein. Nicht zugeordneter Speicherplatz auf einem Datenträger ist Speicherplatz, der noch nicht Bestandteil einer anderen Partition ist, wohingegen freier Speicherplatz Bestandteil einer erweiterten Partition ist, die noch nicht in ein logisches Laufwerk umgewandelt wurde. Um eine Partition zu erstellen, klicken Sie mit der rechten Maustaste auf den Bereich **Nicht zugeordnet** oder **Freier Speicherplatz** und wählen im Kontextmenü den Eintrag **Partition erstellen**. Der **Assistent zum Erstellen von Partitionen** wird nun geöffnet (siehe Abbildung 4.10) und Sie werden gefragt, welche Art von Partition Sie erstellen möchten. Zur Auswahl stehen die primäre Partition, die erweiterte Partition und das logische Laufwerk. Wenn die Partition in einem Bereich mit der Bezeichnung **Nicht zugeordnet** erstellt wird, steht die Option **Logisches Laufwerk** nicht zur Verfügung. Wird die Partition dagegen in einem Bereich mit der Bezeichnung **Freier Speicherplatz** erstellt, ist die Option **Logisches Laufwerk** die einzig verfügbare Option.

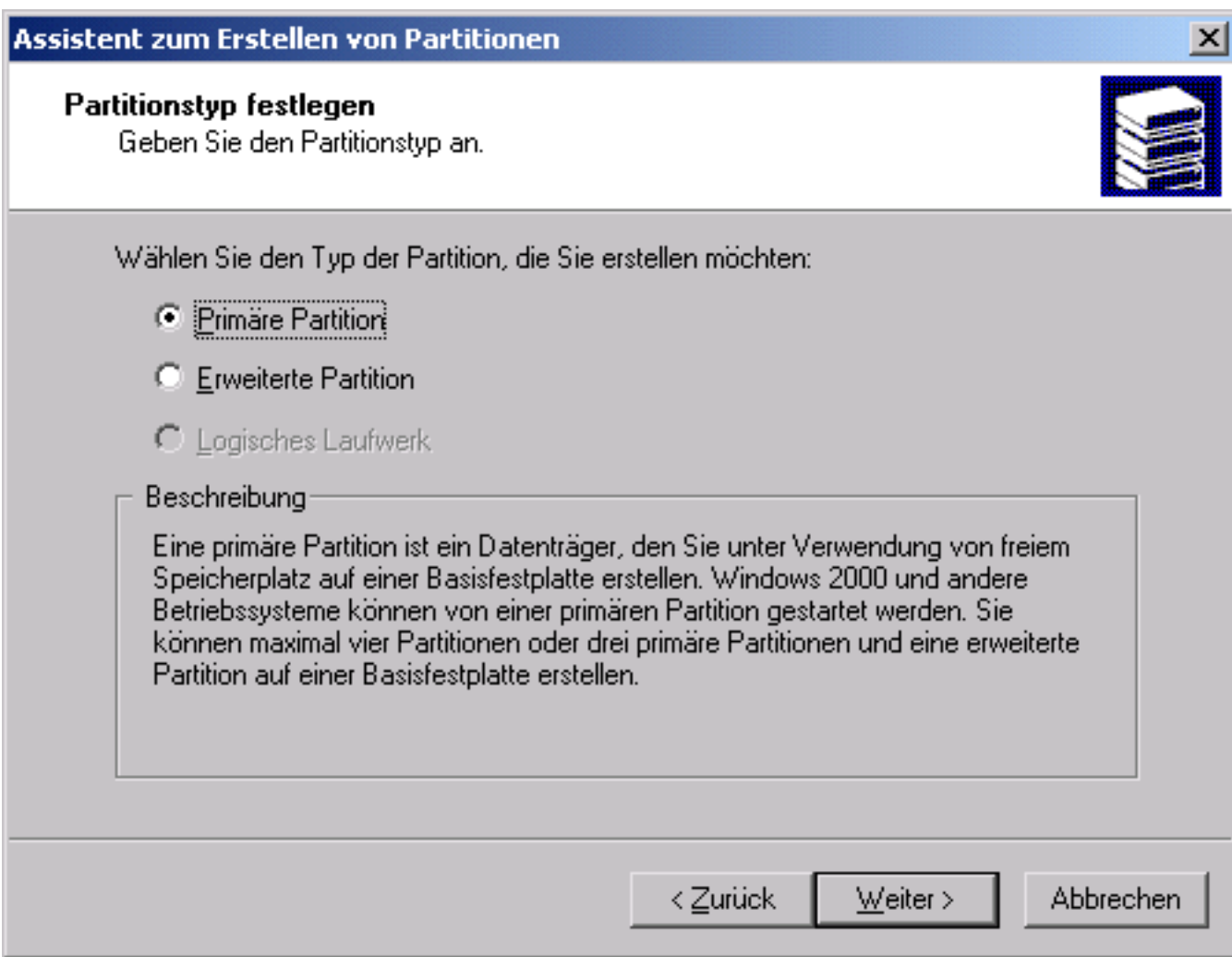


Abbildung 4.10: Der Assistent zum Erstellen von Partitionen fragt, welche Art von Partition erstellt werden soll. Im Beispiel wurde die primäre Partition gewählt.

Geben Sie als Nächstes an, wie viel Speicherplatz für diese neue Partition zur Verfügung stehen soll. Es wird sowohl die minimale als auch die maximale Größe angezeigt. Die Größe hängt von der Größe der Festplatte und anderen Faktoren ab. Bei der Standardeinstellung wird der gesamte nicht zugeordnete Speicherplatz verwendet.

Im letzten Schritt des Assistenten finden Sie eine Zusammenfassung der Einstellungen, die Sie im Assistenten vorgenommen haben (siehe Abbildung 4.11). Über die Schaltfläche **Zurück** können Sie Änderungen vornehmen. Klicken Sie auf die Schaltfläche **Fertig stellen**, um die Einstellungen zu übernehmen und die Partitionierung durchzuführen.

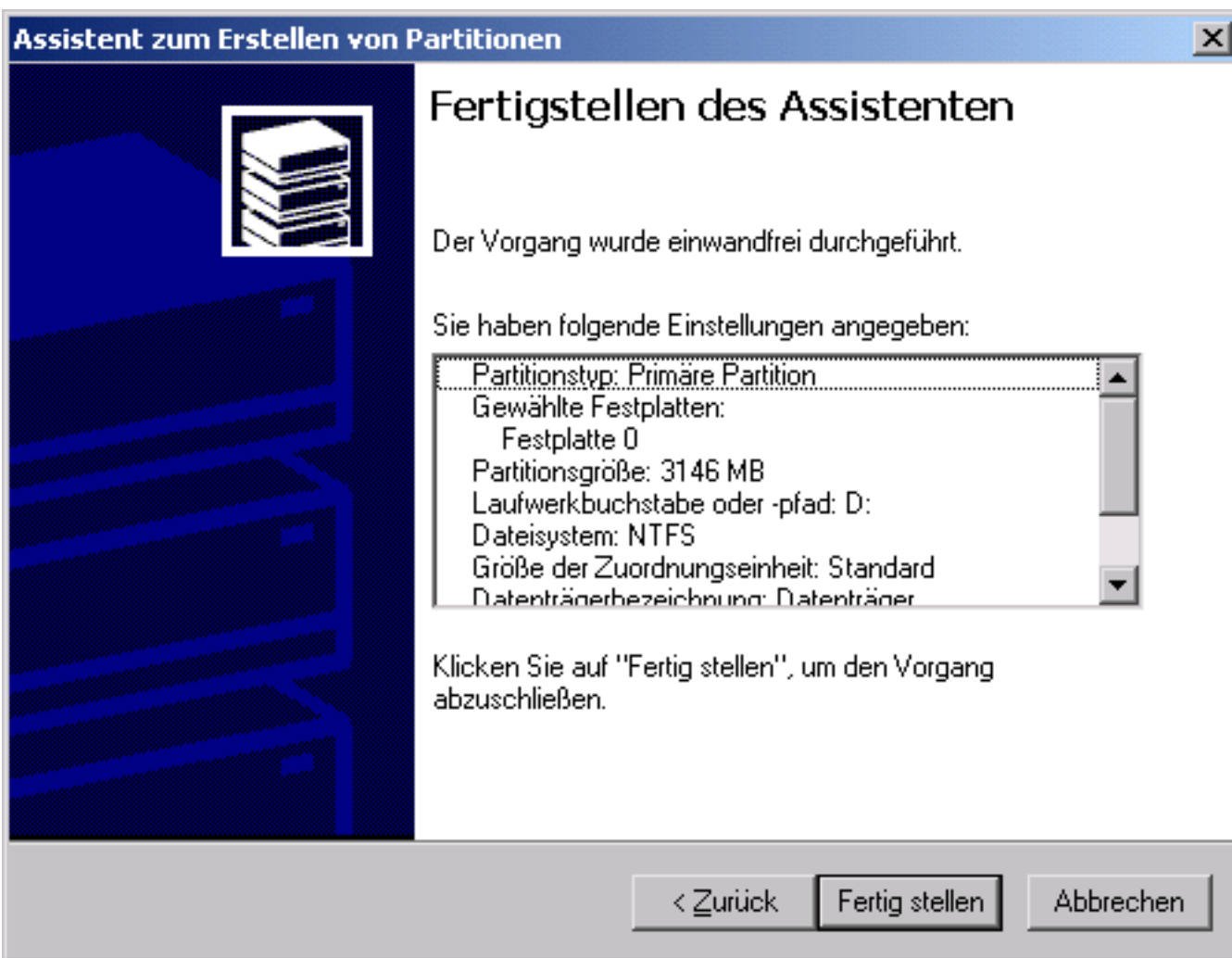


Abbildung 4.11: Diese Seite bietet einen letzten Überblick über die gewählten Einstellungen. Klicken Sie auf **Fertig stellen**, um die Änderungen zu übernehmen.

Die neue Partition ist nun direkt eingerichtet und kann formatiert werden.

Eine Partition verändern

Es gibt zwei Arten von Änderungen, die an einer Partition vorgenommen werden können. Die Partition kann aktiviert und der Laufwerksbuchstabe verändert werden.

Wird eine Partition aktiviert, betrachtet das BIOS diese Partition als Startpartition. Ein System kann nur eine aktive Partition enthalten und diese muss sich auf der Festplatte 0 befinden, der ersten Festplatte im System. Wenn die gewählte Partition nicht bootfähig ist, kann das System erst dann wieder booten, wenn eine sinnvolle aktive Partition gewählt wird. Um eine Partition zu aktivieren, klicken Sie mit der rechten Maustaste darauf, und wählen Sie im Kontextmenü den Befehl **Partition als aktiv markieren**. Handelt es sich bereits um die aktive Partition, ist diese Option deaktiviert. Nur primäre Partitionen lassen sich als aktiv markieren. Deshalb steht diese Option bei erweiterten Partitionen im Kontextmenü gar nicht zur Verfügung.

Die Veränderung des Laufwerksbuchstabens ist weit weniger dramatisch. Klicken Sie dazu mit der rechten Maustaste auf die Partition, deren Laufwerksbuchstaben Sie ändern möchten, und wählen Sie im Kontextmenü den Befehl **Laufwerksbuchstaben und -pfad ändern**. Es öffnet sich das Dialogfeld

Laufwerksbuchstabe und -pfad für Datenträger ändern. Markieren Sie das Laufwerk und klicken Sie auf die Schaltfläche **Ändern**, um das Dialogfeld **Laufwerksbuchstaben oder -pfad bearbeiten** zu öffnen (siehe Abbildung 4.12). In diesem Dialogfeld können Sie den Laufwerksbuchstaben ändern und auch angeben, dass das Laufwerk wie ein Verzeichnis in einem anderen Pfad bereitgestellt wird. Dies entspricht dem »Mount«-Befehl bei UNIX. Das Laufwerk kann tatsächlich an verschiedenen Orten in unterschiedlichen Dateisystemen gemountet werden.

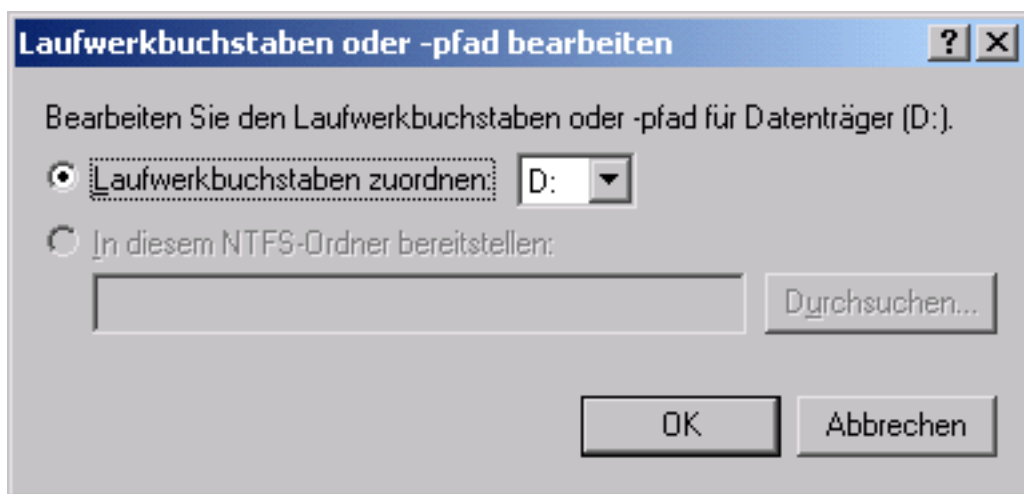


Abbildung 4.12: Hier können Sie den Laufwerksbuchstaben ändern. Denken Sie daran, dass dies bei manchen Anwendungen Probleme verursachen könnte!



Bevor Sie glauben, dass die Idee, »ein Laufwerk in ein Verzeichnis zu mounten«, eine Innovation von Microsoft sei, sollten Sie wissen, dass UNIX dies seit Anfang der siebziger Jahre anbietet und Microsoft dieses Konzept nun aufgreift. Das ganze Konzept ist fast so innovativ wie weiße Socken.

Unter folgenden Umständen sollten Sie den Laufwerksbuchstaben nicht ändern:

- Falls eine Anwendung in dem Laufwerk installiert ist, sollten Sie den Laufwerksbuchstaben auf keinen Fall ändern. Die meisten Anwendungen speichern den Pfad zu den ausführbaren Dateien und den Modulen in der Registrierung und eine Änderung des Laufwerksbuchstaben würde nicht in der Registrierung berücksichtigt werden.
- Der Laufwerksbuchstabe sollte nicht geändert werden, wenn Dienste auf dem Computer installiert sind, die auf Daten basieren, die in dem Laufwerk abgelegt sind. Wenn das Laufwerk D: z.B. eine SQL Server-Datenbank enthält und der Laufwerksbuchstabe auf E: geändert wird, wird die Datenbank als beschädigt gekennzeichnet, wenn SQL Server neu gestartet wird.
- Der Laufwerksbuchstabe sollte nicht geändert werden, wenn es keinen besseren Grund gibt, als aufeinander folgende Laufwerksbuchstaben zu erhalten.

Wenn sich der Laufwerksbuchstabe ändert, werden freigegebene Verzeichnisse weiterhin korrekt freigegeben und alle Benutzerrechte/Berechtigungen werden korrekt angewandt.

Eine Partition löschen

Eine Partition zu löschen ist genau so gefährlich, wie es klingt. Wird eine Partition gelöscht, ist sie weg. Die Daten, die auf der Partition enthalten waren, ebenfalls. Diese Daten sind verloren und lassen sich

nicht wiederherstellen.

Um eine logische Partition zu löschen, müssen Sie zunächst alle logischen Laufwerke von der Partition und anschließend die erweiterte Partition entfernen. Dies ist eine Sicherheitsfunktion, die sicherstellt, dass der Benutzer genau weiß, was passiert, bevor die Daten entfernt werden.

Um eine Partition zu löschen, klicken Sie mit der rechten Maustaste darauf und wählen im Kontextmenü entweder den Befehl **Partition löschen** oder **Logisches Laufwerk löschen**. Es öffnet sich ein Hinweisfenster, das Sie bestätigen müssen. Anschließend wird die Partition entfernt.

4.3.5 Dynamische Festplatten

Dynamische Festplatten bieten einige zusätzliche Optionen, die ebenfalls behandelt werden müssen, für die jedoch auch zusätzliches Hintergrundwissen erforderlich ist. In den folgenden Abschnitten in diesem Kapitel werden einige dieser Features ausführlicher beschrieben. Der Abschnitt »Erweiterte Datenträger« beschreibt, wie Datenträger erweitert werden und die Abschnitte »Stripesetdatenträger« und »RAID-5-Datenträger« behandeln den Einsatz von Stripesets und RAID 5 in Windows 2000.

4.3.6 Kontingente einrichten

Lange Zeit hat Microsoft Sicherheitshooks in die Betriebssysteme eingebaut, um Festplattenkontingente zu unterstützen. Es gibt einige Anwendungen von Drittanbietern, die diese Hooks implementieren, um Festplattenkontingente zu erzwingen. Mit Windows 2000 hat Microsoft schließlich Festplattenkontingente im Betriebssystem implementiert. Das wurde auch Zeit.

Festplattenkontingente bieten dem Administrator die Möglichkeit, den Speicherplatz zu beschränken, der einem Benutzer zur Verfügung steht, um Dateien zu speichern. Für die Benutzer wird kein Speicherplatz reserviert. Somit bieten Kontingente eine flexible Möglichkeit, Speicher zu verwalten.

Festplattenkontingente gibt es in anderen Betriebssystemen bereits seit langem. Nun sind sie aber auch vollständig in Windows 2000 implementiert.

Kontingente werden auf der Basis von Partitionen (oder logischen Laufwerken) eingerichtet. Dies ist ein weiteres Argument für große Partitionen und Laufwerke. Weil Partitionen keine Reservierungen für einen Benutzer darstellen, ist es üblich, den Speicherplatz auf dem Server zu überbuchen, weil (hoffentlich) nicht alle Benutzer den Speicherplatz vollständig ausnutzen, der ihnen zur Verfügung steht.

Kontingente werden auf der Registerkarte **Kontingent** des Dialogfelds **Eigenschaften von Datenträger** eingerichtet (siehe Abbildung 4.13). Um dieses Dialogfeld zu öffnen, klicken Sie mit der rechten Maustaste auf die gewünschte Partition und wählen im Kontextmenü den Befehl **Eigenschaften**. Aktivieren Sie anschließend im **Eigenschaften**-Dialogfeld die Registerkarte **Kontingent**. Dieses Dialogfeld steuert alle Optionen für Festplattenkontingente in der ausgewählten Partition. Kontingente stehen nur für das Dateisystem NTFS zur Verfügung. Wurde eine Festplatte oder Partition mit einem anderen Dateisystem formatiert, lassen sich keine Kontingente einrichten. Der nächste Abschnitt beschreibt die verschiedenen Arten von Dateisystemen.

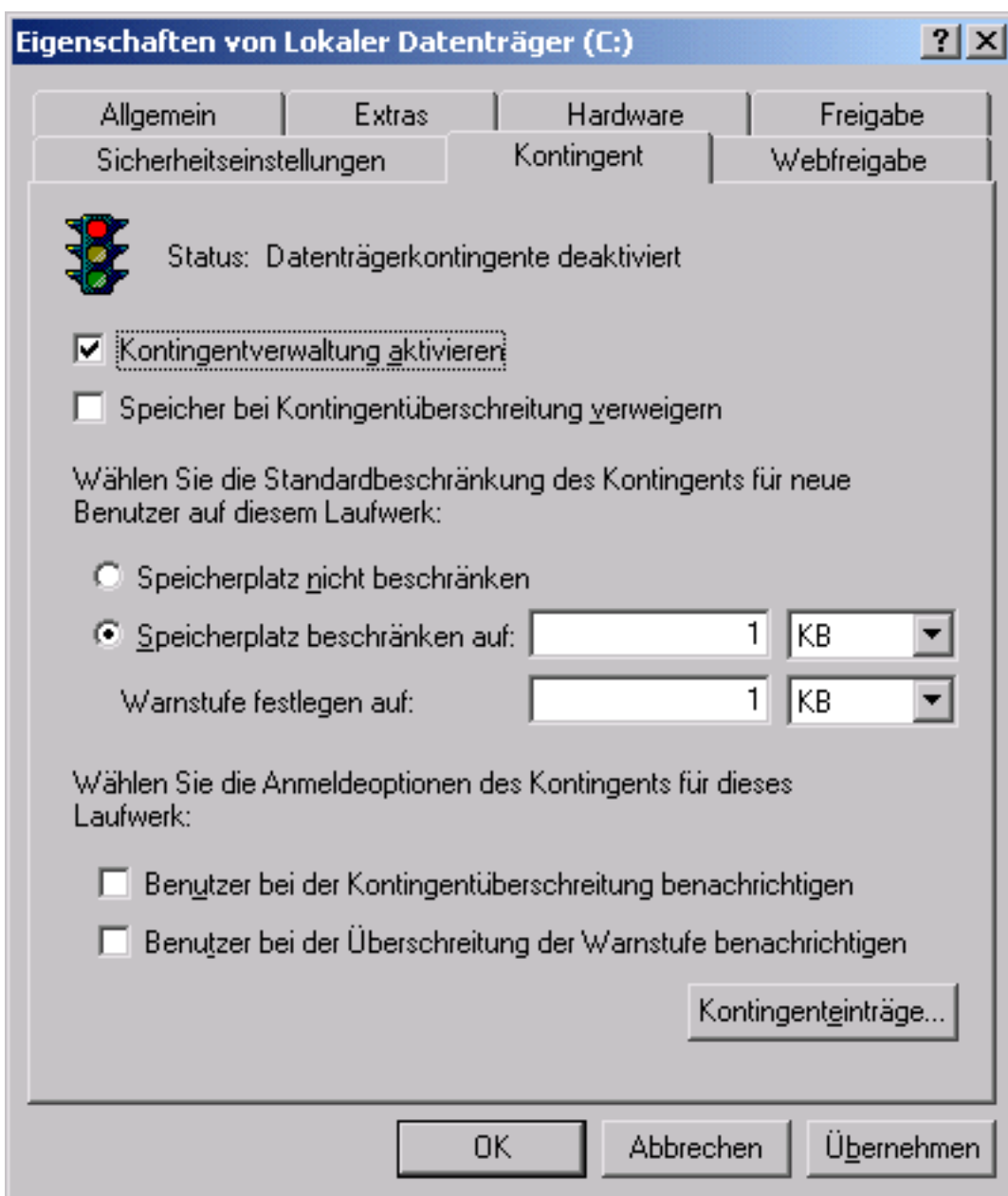


Abbildung 4.13: Über die Registerkarte Kontingent werden Kontingente für den Datenträger eingerichtet.

Um Kontingente zu aktivieren, klicken Sie auf das Kontrollkästchen **Kontingentverwaltung aktivieren**. Dadurch werden die restlichen Optionen im Dialogfeld aktiviert. Um den Festplattenspeicher streng zu beschränken, aktivieren Sie das Kontrollkästchen **Speicher bei Kontingentüberschreitung verweigern**. Wählen Sie die Speicherplatzbeschränkung, indem Sie auf die Option **Speicherplatz beschränken auf** klicken und dann einen Wert für die Kontingentgrenze und die Warnstufe wählen. Wird die Warnstufe überschritten, erhält der Benutzer eine entsprechende Benachrichtigung. Überschreitet der Benutzer die Kontingentgrenze, wird ein schärferer Warnhinweis eingeblendet oder der Benutzer wird daran gehindert, die Grenze zu überschreiten. Wenn das Kontrollkästchen **Speicher bei Kontingentüberschreitung verweigern** nicht aktiviert ist, können Benutzer den ihnen zugewiesenen Festplattenspeicher ungehindert überschreiten.

Die beiden Kontrollkästchen **Benutzer bei der Kontingentüberschreitung benachrichtigen** und **Benutzer bei der Überschreitung der Warnstufe benachrichtigen** legen fest, wann Einträge von

Windows 2000 im Ereignisprotokoll vorgenommen werden. Wenn das erste Kontrollkästchen aktiviert wird, werden die Warnungen nur protokolliert, sobald der Benutzer seine Kontingentgrenze überschreitet. Wenn das zweite Kontrollkästchen aktiviert ist, wird im Ereignisprotokoll aufgezeichnet, wenn der Benutzer die Warnstufe überschreitet. Normalerweise wird entweder nur das erste Kontrollkästchen aktiviert oder beide.

Festplattenkontingente

Es gibt im Wesentlichen zwei Ansätze für Festplattenkontingente: Kontingente mit weichen Beschränkungen und Kontingente mit harten Beschränkungen. Die Kontingentverwaltung kann so eingerichtet werden, dass ein Benutzer sein Kontingent überschreiten kann und diese Information dem Administrator dann einfach zur Verfügung steht. Der andere Ansatz besteht darin, Kontingente so einzurichten, dass ein Benutzer sein Kontingent nicht überschreiten und Daten erst dann wieder speichern kann, wenn er Daten vom Datenträger entfernt hat.

Bei »harten« Beschränkungen besteht die Wahrscheinlichkeit, dass Anwendungen nicht feststellen, dass der Speicherplatz nicht ausreicht oder dass der Benutzer dies in seiner Eile nicht bemerkt, wenn er den Computer herunterfährt. Der Benutzer ignoriert dann möglicherweise die Warnhinweise, fährt den Computer herunter und geht nach Hause. Am nächsten Morgen kann sich der Administrator auf einen verärgerten Anruf gefasst machen.



Beim Ansatz der »weichen« Beschränkung erhält der Benutzer möglicherweise keinerlei Warnhinweise und hat deshalb vielleicht keinen echten Anreiz, nicht benötigte Daten von der Festplatte zu löschen. Dieser Ansatz ist wesentlich sicherer, ihn durchzusetzen jedoch erheblich schwieriger.

Wenn Sie nun die beiden Ansätze gegenüberstellen, gehen beim Ansatz der harten Beschränkung möglicherweise mehr Anrufe beim Helpdesk ein und einige Benutzer sind verärgert. Beim Ansatz der weichen Beschränkung müssen die Benutzer vom Helpdesk aufgefordert werden, Festplattenspeicher freizumachen, weil die Wahrscheinlichkeit hoch ist, dass sie dies von sich aus nicht tun.

Ein weiterer Punkt, der berücksichtigt werden muss, ist folgender: Sind Festplattenkontingente wirklich eine gute Idee? Wägen Sie die Vor- und Nachteile gegeneinander ab. Festplattenspeicher wird immer preisgünstiger, wohingegen die Kosten für Supportpersonal immer weiter steigen. Bedenken Sie auch die Verärgerung der Benutzer, wenn diese ihre Kontingentgrenze erreichen, und werten Sie all diese Faktoren in Ihrer Situation und Umgebung aus. Es gibt hier keine einfachen Antworten.

Kontingenteinträge einrichten

Gehen Sie wie folgt vor, um Kontingenteinträge für verschiedene Benutzer einzurichten:

1. Klicken Sie auf der Registerkarte **Kontingent** auf die Schaltfläche **Kontingenteinträge**. Es öffnet sich das Dialogfeld **Kontingenteinträge für Datenträger** (siehe Abbildung 4.14).

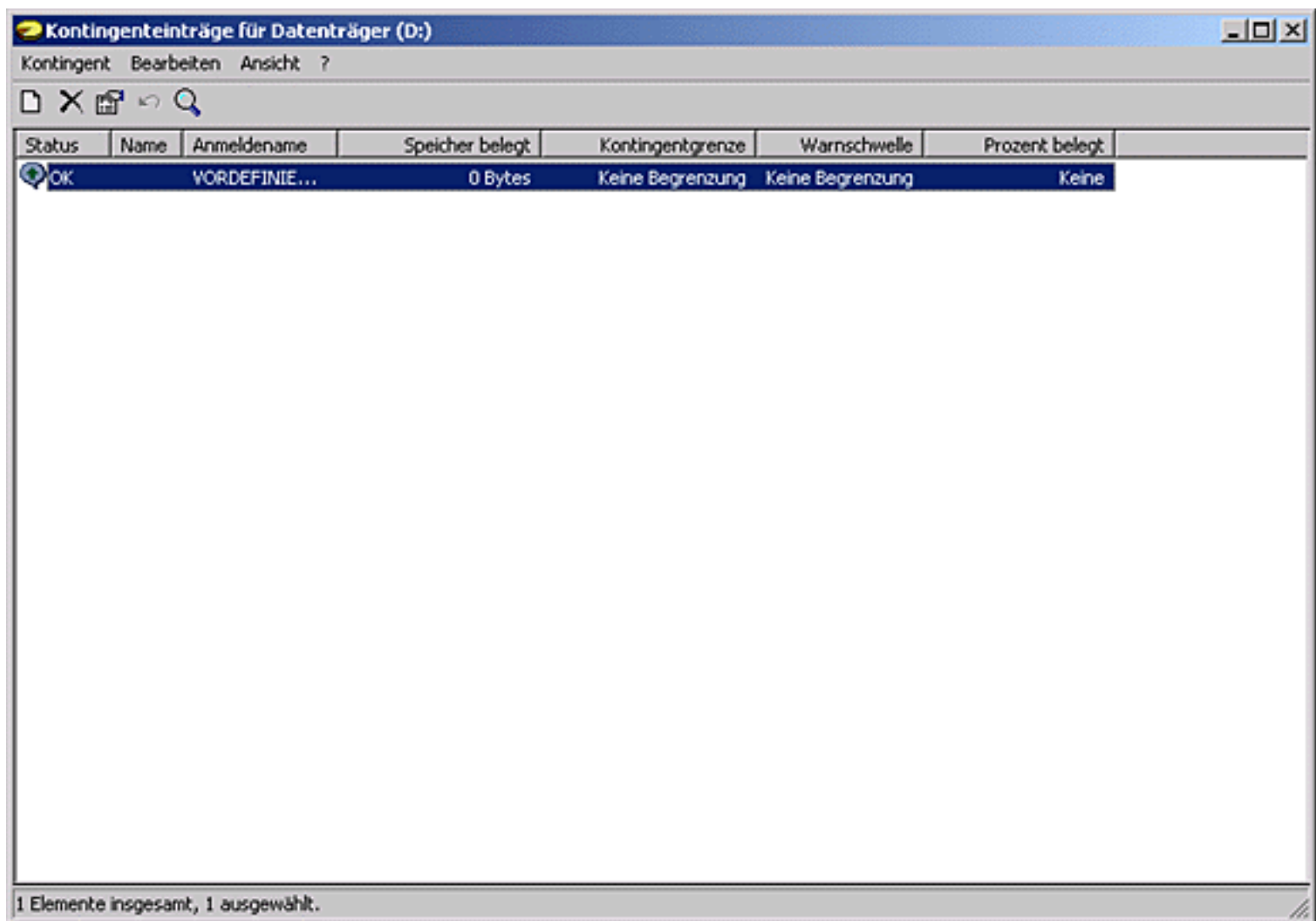


Abbildung 4.14: Das Dialogfeld **Kontingenteinträge für Datenträger** zeigt die Kontingente für alle Benutzer, die für diese Partition eingerichtet wurden.

2. Wählen Sie im Menü **Kontingent** den Befehl **Neuer Kontingenteintrag**. Es öffnet sich das Dialogfeld **Benutzer auswählen**. Wählen Sie aus der Liste der Benutzer und Gruppen den Benutzer aus, für den Sie das Kontingent einrichten möchten, und klicken Sie auf die Schaltfläche **Hinzufügen**. Wollen Sie das Kontingent für mehrere Benutzer einrichten, wählen Sie diese zusätzlich aus. Klicken Sie anschließend auf OK.
3. Wählen Sie im Dialogfeld **Neuen Kontingenteintrag hinzufügen** die Option **Speicherplatz beschränken auf** und legen Sie den Wert für die Kontingentgrenze fest. Im Listenfeld dieser Zeile können Sie die Einheit auswählen. Voreingestellt ist die Einheit KB.
4. Legen Sie in der Zeile **Warnstufe festlegen auf** fest, ab welchem Wert der Benutzer einen Warnhinweis erhalten soll. Auch hier können Sie einen Wert und eine Einheit angeben.
5. Klicken Sie anschließend auf OK. Der neue Eintrag ist nun im Dialogfeld **Kontingenteinträge für Datenträger** zu sehen.

Wenn Sie Nachhilfe in den metrischen Präfixen benötigen, finden Sie in Tabelle 4.2 eine Übersicht, was die Einheiten in den Listenfeldern bedeuten.

Abkürzung	Einheiten	Größe (Bytes)

KB	Kilobyte	1.024
MB	Megabyte	1.048.576
GB	Gigabyte	1.073.741.824
TB	Terabyte	1.099.511.627.776
PB	Petabyte	1.125.899.906.842.624
EB	Exabyte	1.152.921.504.606.846.976

Tabelle 4.2: Metrik

Sehr wahrscheinlich kennen Sie die ersten drei oder vier Einträge. Aber kannten Sie auch die letzten beiden? Dies ist Microsofts Art, die Zukunft für neue Speichermedien zu planen.



Kontingente können nicht für Mitglieder der Gruppe **Administratoren** eingerichtet werden. Mitglieder dieser Gruppe können so viel Speicherplatz verbrauchen, wie sie möchten.

Kontingente löschen

Um das Kontingent für einen bestimmten Benutzer zu löschen, klicken Sie im Dialogfeld **Kontingenteinträge für Datenträger** doppelt auf den Eintrag für den Benutzer, klicken im Dialogfeld **Kontingenteinstellungen für Benutzer** auf die Option **Speicherplatz nicht beschränken** und bestätigen mit OK.

Um die Dateien zu löschen, die zu einem Benutzer gehören, markieren Sie den Eintrag für den Benutzer im Dialogfeld **Kontingenteinträge für Datenträger** und wählen im Menü **Kontingent** den Befehl **Kontingenteintrag löschen**.

Kontingenteinstellungen im- und exportieren

Weil die Kontingenteinstellungen für jede Partition gespeichert werden müssen und weil dies sehr mühselig ist, wenn mehrere Server verwaltet werden müssen, lassen sich Kontingenteinträge auch im- und exportieren. Gehen Sie dazu wie folgt vor:

1. Richten Sie die Kontingenteinträge für eine Partition ein.
2. Wählen Sie im Dialogfeld **Kontingenteinträge für Datenträger** im Menü **Kontingent** den Eintrag **Exportieren**.
3. Geben Sie im Dialogfeld **Exportiert Kontingenteinstellungen** einen Namen und einen Dateityp für die exportierten Kontingenteinstellungen ein und klicken Sie auf **Speichern**.

Gespeicherte Kontingenteinstellungen lassen sich im Dialogfeld **Kontingenteinträge für Datenträger** über den Befehl **Kontingent/Importieren** importieren.

4.4 Dateisysteme

Nachdem die Partitionen eingerichtet sind, müssen sie formatiert werden, um Daten speichern zu können. Der Hauptzweck eines Dateisystems besteht darin, dem Betriebssystem eine Struktur zur Organisation und Verwaltung von Dateien zu bieten. Ein Dateisystem muss wissen, wo die Dateien auf dem Datenträger abgelegt und welche Teile des Datenträgers in Benutzung sind. Außerdem muss das Dateisystem wissen, wie die einzelnen Teile einer Datei auf dem Datenträger miteinander verbunden sind, um die gesamte Datei abrufen zu können.

Es gibt drei Arten von Dateisystemen, mit denen jeder Administrator konfrontiert wird. Das Rohdateisystem ist ein vollkommen unformatiertes Dateisystem und entspricht einfach dem unformatierten Speicherplatz auf dem Datenträger. Diese Art von Dateisystem wird nicht sehr häufig verwendet. Es gibt aber einige Versionen von Microsoft SQL Server, die Daten in die unformatierten Partitionen eines Datenträgers schreiben können. Der einzige echte Verwendungszweck von unformatiertem Speicherplatz ist der, ihn mit einem anderen Dateisystem zu formatieren.

Die beiden für Windows 2000 relevanten Dateisysteme sind FAT und NTFS. Das FAT-Dateisystem ist ziemlich alt und bietet nicht sehr viel mehr als die Möglichkeit, Dateien zu speichern. Mit einer verbesserten Version von FAT namens FAT32 lässt sich mehr Festplattenspeicher adressieren. Sonstige Verbesserungen gegenüber FAT gibt es nicht. NTFS ist ein transaktionsbasiertes Dateisystem mit integrierter Sicherheit und Komprimierung. Es ist technologisch sehr weit entwickelt, aber auch in sich stimmig und zuverlässig.

Dieser Abschnitt beschreibt, wie die beiden Dateisysteme funktionieren und wie sie verwaltet werden.

4.4.1 FAT

Das FAT-Dateisystem (FAT = File Allocation Table, Dateizuordnungstabelle) ist das Dateisystem, das von MS-DOS verwendet wurde. Es verwendet eine Tabelle, die auf dem Datenträger gespeichert ist, um aufzuzeichnen, wo die Dateien und Verzeichnisse auf dem Datenträger abgelegt sind. Es entspricht also einer Karte für die verfügbaren Speicherstellen auf dem Datenträger. Das FAT-Dateisystem speichert zwei Kopien dieser »Karten« ganz am Anfang des Datenträgers. Rein theoretisch werden diese beiden Kopien permanent synchron gehalten. Manchmal geht diese Synchronität jedoch verloren und sie müssen geprüft und erneut synchronisiert werden.

Um Daten effizient zu speichern, bildet ein Dateisystem Dateneinheiten, die als *Cluster* bezeichnet werden. Beim FAT-Dateisystem besteht ein Cluster immer aus 2.048 Byte oder 2 Kbyte. Ein Cluster repräsentiert die kleinste Speichereinheit, die das Dateisystem zuordnen kann. Das heißt, eine Datei, die 500 Byte umfasst, beansprucht 2 Kbyte Speicherplatz und eine Datei, die 2.047 Byte umfasst, ebenfalls. Eine Datei, die 2.049 Byte umfasst, beansprucht dagegen 4 Kbyte Speicherplatz.



Dieser Hinweis gilt eher für Workstations als für Server, er eignet sich jedoch, um die Auswirkungen der Clustergröße zu veranschaulichen. Die Clustergröße von 2 Kbyte ist normalerweise im Durchschnitt nicht so verschwenderisch, falls nicht eine Anwendung installiert ist, die Hunderte von kleinen Dateien speichert. Ein Beispiel für eine solche Anwendung ist eine C++-Entwicklungsumgebung, die buchstäblich Hunderte kleiner Dateien anlegt und bedeutend mehr Speicherplatz belegen kann, als sich aus der Summe der Dateigrößen ergibt.

Wenn eine Datei auf den Datenträger geschrieben wird, werden die nächsten beiden verfügbaren Stellen verwendet, die nicht unbedingt nebeneinander liegen müssen. Wenn ein Programm z.B. auf eine Datendatei zugreift, die in zwei Clustern gespeichert ist, und das Programm dann einen dritten Cluster hinzufügt, weil weitere Daten gespeichert werden müssen, weist das Dateisystem dafür möglicherweise einen Cluster zu, der nicht in der Nähe des vorhandenen Clusters liegt. Es geht schneller, einen Cluster zuzuordnen und die Daten dann in diesen zu schreiben, als drei neue Cluster zuzuweisen und die bestehenden Cluster dann zu kopieren, damit die Cluster auf dem Datenträger nebeneinander liegen.

Wie verfolgt das Dateisystem diese Transaktionen? Sie werden in der Dateizuordnungstabelle, d.h. der FAT (File Allocation Table), gespeichert. Die FAT enthält alle Cluster, egal, ob benutzt oder unbenutzt. Wenn die Cluster benutzt werden, wird aufgezeichnet, wo der nächste Cluster für jede Datei liegt. In anderen Worten ist das ganze eine große verkettete Liste (Linked List). Wenn ein Programm auf einen bestimmten Teil einer Datei zugreifen muss, sendet es eine Anforderung an das Betriebssystem und das Betriebssystem berechnet dann, in welchem Cluster die entsprechenden Teile enthalten sind und folgt der verketteten Liste bis zu diesem Cluster und liest dann die Daten ein und liefert diese an das Programm zurück.

Dies klingt ziemlich aufwändig. Es ist jedoch nicht so schlimm, wie es aussieht. Die Algorithmen sind ziemlich standardisiert und wurden unglaublich gut optimiert, weil sie sehr wichtig sind. Wenn eine Änderung vorgenommen werden muss, wird der neue Cluster zugeordnet und beide Kopien der FAT werden aktualisiert. Wenn eine Datei gelöscht wird, wird die gesamte Clusterkette als verfügbar markiert.

Diese Technologie hat gewisse Beschränkungen. Sie ist z.B. sehr anfällig für Stromausfälle oder ähnliche Probleme, weil sie von der Aktualisierung der FAT abhängig ist. Dies ist ein weiterer Grund, warum Computer immer heruntergefahren und nicht direkt ausgeschaltet werden sollten, weil bei einem ordnungsgemäßen Herunterfahren sichergestellt wird, dass alle Daten auf den Datenträger geschrieben werden, bevor das Gerät abgeschaltet wird.

Was die Speichermenge betrifft, ist das FAT-Dateisystem sehr beschränkt, weil es nur Partitionen bis zu 4 Gbyte verwalten kann. Dateien dürfen außerdem nicht größer als 2 Gbyte sein. Das FAT-Dateisystem arbeitet mit einer Clustergröße von 2 Kbyte, sodass selbst die kleinste Datei mindestens 2 Kbyte Speicherplatz auf dem Datenträger beansprucht. Das FAT32-Dateisystem unterstützt Datenträger zwischen 512 Mbyte und 2 Tbyte (Terabyte), aber Windows 2000 formatiert nur FAT32-Partitionen bis zu 32 Gbyte.

Auf das FAT- und das FAT32-Dateisystem kann von Windows 95, Windows 98 und Windows 2000 aus zugegriffen werden, so lange sich die Partitionen auf einer Basisfestplatte befinden. Denken Sie daran, dass Windows 2000 das einzige Betriebssystem ist, das auf dynamische Festplatten zugreifen kann. Dies gilt auch für Dual-Boot-Systeme, die entweder mit Windows 2000 oder einem anderen Betriebssystem

gestartet werden können. Über das Netzwerk kann auf jede dieser Partitionstypen von jeder beliebigen Clientsoftware zugegriffen werden, egal, unter welcher Betriebssystemversion diese läuft.

Warum wird das FAT-Dateisystem dann überhaupt noch verwendet? Ein Hauptgrund ist, dass Windows 95-Versionen vor dem so genannten »OSR-2-Release« nicht auf das FAT32-Dateisystem zugreifen können. Der zweite Grund ist, dass FAT32 nicht auf eine Diskette passt. Deshalb werden alle Disketten mit dem FAT-Dateisystem formatiert. Dies gilt auch für die meisten »erweiterten« Disketten wie LS120 SuperDrive und ZIP-Laufwerke. Diese sind ebenfalls mit dem FAT-Dateisystem formatiert.

Ein weiterer erheblicher Vorteil des FAT32-Dateisystems gegenüber FAT ist die kleinere Clustergröße. FAT32 benutzt standardmäßig Cluster mit einer Größe von 512 Byte. Deshalb kann dieses Dateisystem kleinere Dateien wesentlich effizienter speichern.

Trotz der Vorzüge von FAT32 beim Umgang mit großen Datenträgern hat es noch immer den wesentlichen Nachteil, dass die Verwaltung über eine Dateizuordnungstabelle erfolgt und nicht transaktionsbasiert ist. Außerdem wird keine Sicherheit auf Dateiebene unterstützt. Was ist ein transaktionsbasiertes Dateisystem und wie funktioniert Sicherheit auf Dateiebene? Werfen wir nun einen Blick auf das NTFS-Dateisystem.

4.4.2 NTFS

NTFS (NT File System) ist das Dateisystem, das Sie unter Windows 2000 verwenden sollten. NTFS bietet einige große Vorteile, aber auch gewisse Nachteile. Die großen Vorteile von NTFS bestehen darin, dass NTFS ein transaktionsbasiertes Dateisystem verwendet und dass es Sicherheit auf Dateiebene unterstützt. Zu den Nachteilen gehört die Tatsache, dass nur Windows 2000 NTFS lesen kann und dass NTFS mehr Speicherplatz und Prozessorleistung beansprucht als FAT. Zunächst wird ausgeführt, was unter einem »transaktionalen Dateisystem« zu verstehen ist. Anschließend wird die Sicherheit auf Dateiebene genauer betrachtet, die Windows 2000 bietet.

Transaktionale Dateisysteme

Ein transaktionales Dateisystem verfolgt Änderungen des Dateisystems in besonderer Weise, um Daten auf dem Datenträger zu speichern. Ein nicht transaktionales Dateisystem wie das FAT-Dateisystem schreibt die Daten wie folgt auf den Datenträger:

- Es sucht leere Cluster.
- Es schreibt Daten in leere Cluster.
- Es schreibt zwei Kopien der Änderungen in die Dateizuordnungstabellen.

Was geschieht, wenn der Strom zwischen dem zweiten und dem dritten Schritt ausfällt? Die Information wird zwar auf den Datenträger geschrieben. Weil die Änderungen jedoch nicht in der Dateizuordnungstabelle eingetragen wurden, besteht kein Zugriff auf die Informationen auf dem Datenträger. Wenn das System während des dritten Schrittes ausfällt, wurde vielleicht eine Dateizuordnungstabelle bereits aktualisiert, die andere aber noch nicht. Noch schlimmer wäre, wenn eine der Dateizuordnungstabellen in einem inkonsistenten Zustand verbleiben würde, indem ein Teil der Informationen bereits eingetragen wurde, ein anderer Teil jedoch noch nicht.

Um dies zu verhindern, geht ein transaktionales Dateisystem wie folgt vor:

- Es sucht leere Cluster.
- Es trägt im Journal die Absicht ein, die leeren Cluster zu verwenden, um dort Daten zu speichern.
- Es schreibt die Daten in die Cluster.
- Es aktualisiert das Journal, um deutlich zu machen, dass die Daten komplett in die Cluster geschrieben wurden.

Wenn der Strom bei einem dieser Schritte ausfällt, kann das Dateisystem vollständig wiederhergestellt werden, wenn das System wieder gestartet wird, indem das Journal gelesen wird und alle Änderungen rückgängig gemacht werden, die vom letzten Schritt nicht als vollständig gekennzeichnet wurden. Das heißt, das System geht davon aus, dass jede Transaktion, die im letzten Schritt nicht fertiggestellt wurde, durch den Stromausfall unterbrochen wurde. Die Zuordnung der Cluster wird rückgängig gemacht und die Datei wird in den Zustand zurückversetzt, in dem sie sich vor der Transaktion befand.

Dies klingt zwar ziemlich kompliziert, es sprechen jedoch zwei Dinge für diesen Ansatz. Erstens ist dieses System ziemlich fehlertolerant. Auf diese Weise werden Transaktionen auch von Datenbankverwaltungssystemen behandelt. Das Modell ist geprüft und es hält sich schon seit langer Zeit. Der Vorteil dieses komplexeren Systems ist, dass es, weil es auch von Datenbanken verwendet wird, sorgfältig geprüft und optimiert wurde, um eine optimale Leistung zu bieten. Der Performanceunterschied lässt sich fast vernachlässigen.

Das Konzept eines transaktionsbasierten (oder journalbasierten) Dateisystems ist überhaupt nicht einzigartig für NTFS. Bei High-End-UNIX-Systemen gibt es dieses Konzept bereits seit langem und es gibt neue journalbasierte Dateisysteme, die für Linux und andere freie Betriebssysteme getestet werden.

Das Journal, das von NTFS verwendet wird, verwaltet sich selbst. Es entfernt komplette Transaktionen aus dem Protokoll, sodass das Protokoll nicht sehr viel Festplattenspeicher beansprucht. Es gibt kein echtes Konzept für eine Transaktionsprotokollsicherung wie bei einem Datenbanksystem, aber jede Datei wird mit einem veränderten Datum gespeichert. Deshalb lassen sich die Dateien, die sich seit der letzten Sicherung geändert haben, leichter herausfiltern. Transaktionsprotokollsicherungen werden von vielen Datenbanksystemen verwendet, um eine Wiederherstellung zu einem bestimmten Zeitpunkt zu ermöglichen.

Sicherheit auf Dateiebene

Bei einem Dateisystem auf einem Netzwerkcomputer ist es nützlich, den Zugriff auf bestimmte Dateien auf gewisse Benutzer beschränken zu können. Windows 2000 gestattet diese Art von Verwaltung nur bei NTFS-Partitionen. Bei der Sicherheit auf Dateiebene spielen zwei Konzepte eine Rolle: Berechtigungen und Benutzer. Mit Berechtigungen wird festgelegt, wie Benutzer mit den Dateien interagieren können. Benutzer sind Einheiten, die mit Dateien interagieren müssen.

NTFS unterstützt verschiedene Berechtigungen und gruppiert diese in einer Weise, die ihren Einsatz erleichtert. Nachfolgend sehen Sie eine Liste der Arten von Interaktionen, die NTFS entweder erlauben oder unterbinden kann:

- *Ordner durchsuchen/Datei ausführen.* Wenn diese Berechtigung für einen Ordner aktiviert wird, kann der Benutzer auf den Ordner zugreifen, um zu einem Unterordner zu gelangen. Weitere Informationen zum Durchsuchen von Ordnern finden Sie in Kapitel 2 im Abschnitt zum POSIX-Teilsystem. Wenn die Berechtigung auf eine Datei angewendet wird, kann der Benutzer

die Datei ausführen. Der Benutzer muss die Datei dazu nicht lesen können.

- *Ordner auflisten/Daten lesen.* Wird diese Berechtigung einem Ordner zugewiesen, darf der Benutzer eine Liste aller Dateien und Unterordner lesen, die in dem Ordner enthalten sind. Wird die Berechtigung auf eine Datei angewendet, darf der Benutzer die Datei lesen.
- *Ordner erstellen/Daten anhängen.* Wird diese Berechtigung auf einen Ordner angewendet, dürfen Unterordner in dem Ordner angelegt werden. Wird die Berechtigung auf eine Datei angewendet, kann der Benutzer Daten an die Datei anhängen.
- *Löschen.* Der Benutzer darf das Objekt löschen, dem diese Berechtigung zugewiesen wurde. Handelt es sich um eine Datei, darf der Benutzer diese löschen. Handelt es sich um einen Unterordner, kann der Benutzer diesen nur löschen, wenn er leer ist.
- *Unterordner und Dateien löschen.* Der Benutzer darf alle Dateien und Unterordner in einem Ordner löschen, ohne dass er Lese- und Schreibzugriff auf die Dateien hat und weiß, was im Unterordner enthalten ist, der gelöscht wird.
- *Dateien erstellen/Daten schreiben.* Wird diese Berechtigung auf einen Ordner angewendet, darf der Benutzer Dateien in diesem Ordner erstellen. Wird die Berechtigung auf eine Datei angewendet, darf der Benutzer den Dateiinhalt verändern.
- *Berechtigungen lesen.* Der Benutzer darf die Berechtigungen lesen, die dem Objekt zugewiesen wurden, unabhängig davon, ob es sich um eine Datei oder einen Ordner handelt.
- *Berechtigungen ändern.* Der Benutzer darf die Berechtigungen für die Datei oder den Ordner ändern.
- *Attribute lesen.* Der Benutzer kann sehen, mit welchen Attributen die Datei versehen ist (z.B. schreibgeschützt oder versteckt). Dies gilt für die Standarddateiattribute von NTFS.
- *Attribute schreiben.* Der Benutzer darf die Attribute einer Datei ändern (z.B. schreibgeschützt oder versteckt). Dies gilt für die Standarddateiattribute von NTFS.
- *Erweiterte Attribute lesen.* Der Benutzer darf die erweiterten Attribute einer Datei lesen (Archiv- und Indexattribute oder Komprimierungs- und Verschlüsselungsattribute).
- *Erweiterte Attribute schreiben.* Der Benutzer darf die erweiterten Attribute von Dateien verändern.
- *Besitzrechte übernehmen.* Der Benutzer darf den Besitz einer Datei übernehmen.
- *Synchronisieren.* Der Benutzer kann die Datei oder den Ordner mit seiner Arbeitsstation synchronisieren.

Dies ist ein ziemlich komplexes Berechtigungssystem. Es ist sogar wesentlich komplexer, als den meisten Administratoren lieb ist. Diese Berechtigungen werden als erweiterte Berechtigungen bezeichnet. Es gibt auch eine Gruppe mit einfachen Berechtigungen, die in aller Regel verwendet werden (siehe Tabelle 4.3).

Erweiterte Berechtigungen	Voll-zugriff	Ändern	Lesen, Ausführen	Lesen	Schreiben
Ordner durch-suchen/Datei ausführen	X	X	X		
Ordner auflis-ten/Daten lesen	X	X	X	X	

Attribute lesen	X	X			
Erweiterte Attribute lesen	X	X	X	X	
Dateien erstellen/Daten schreiben	X	X			X
Ordner erstellen/Daten anhängen	X	X			X
Attribute schreiben	X	X			X
Erweiterte Attribute schreiben	X	X			X
Unterordner und Dateien löschen	X				
Löschen	X	X			
Berechtigungen lesen	X	X	X	X	X
Berechtigungen ändern	X				
Besitzrechte übernehmen	X				
Synchronisieren	X	X	X	X	X

Tabelle 4.3: Erweiterte und Standardberechtigungen

Die meiste Zeit werden nur zwei Arten von Berechtigungen verwendet: der *Vollzugriff* und die Berechtigungen *Lesen* und *Ausführen*. Entweder muss ein Benutzer in der Lage sein, eine Datei vollständig zu kontrollieren oder er muss die Datei einfach nur lesen können. Die restlichen Berechtigungen sind restriktiver, werden aber nicht so häufig benutzt.

Nachdem Sie wissen, was Berechtigungen sind, muss noch das Thema Benutzer behandelt werden. In diesem Zusammenhang sind drei Arten von Benutzern wichtig. Der *spezielle Benutzer (Creator Owner)*, der *individuelle Benutzer* und die *Gruppe*. Dieser Benutzer ist Besitzer eines Objekts, wobei das Objekt entweder eine Datei oder ein Verzeichnis sein kann. Der Creator Owner hat Vollzugriff auf das Objekt und kann nur Vollzugriff für das Objekt erhalten. Bei NTFS ist der Besitz einer Datei ein wichtiges Konzept. Der Besitzer einer Datei kann immer alles mit der Datei machen und sie z.B. an einen anderen Benutzer weitergeben. Um den Besitz zu übertragen, muss der Ersteller-Besitzer dem Benutzer die Berechtigung **Besitzrechte übernehmen** zuweisen. Anschließend kann die Person, die die Datei haben möchte, tatsächlich den Besitz der Datei übernehmen.



Windows 2000 verleiht dem Administrator, anders als die meisten anderen Betriebssysteme, nicht automatisch Vollzugriff auf alle Dateien. Dies ist eigentlich eine ganz nützliche Sicherheitsfunktion. Der Administrator erhält jedoch Zugriff auf jede Datei, indem er deren Besitzrechte übernimmt. Weil die Besitzrechte nicht zurückgegeben werden können, besitzt der Administrator die Datei so lange, bis ein Benutzer kommt und die Besitzrechte vom Administrator übernimmt.

Drei Dinge beeinflussen die Möglichkeiten eines Benutzers, auf ein Objekt zuzugreifen: die

Zugriffsberechtigungen des Benutzers, die Zugriffsberechtigungen der Gruppe und die nicht gewährten Rechte des Benutzers oder der Gruppe. Wenn ein Benutzerkonto Zugriff auf eine Datei hat, werden die Berechtigungen des Benutzerkontos verwendet. Wenn ein Benutzer keine Zugriffsberechtigung für eine Datei hat (entweder nicht erlaubt oder verweigert), kann der Benutzer trotzdem auf die Datei zugreifen, wenn er Mitglied einer Gruppe ist, die Zugriff auf die Datei hat. Wenn entweder für den Benutzer oder die Gruppe eine bestimmte Berechtigung verweigert wird, wird dem Benutzer diese Berechtigung für die Datei verweigert.

Wenn der Benutzer Mitglied von zwei Gruppen ist und selbst keine Zugriffsrechte hat, werden ihm die am wenigsten restriktiven Berechtigungen für die Datei gewährt. Das heißt, wenn *Mmueller* Mitglied der Gruppe *DatabaseAdmins* ist, die Lese- und Schreibzugriff auf eine Datei hat und er außerdem Mitglied der Gruppe *ExchangeAdmins* ist, die nur Lesezugriff auf die Datei hat, hat der Benutzer *Mmueller* Lese- und Schreibzugriff auf die Datei.

Bei Berechtigungen kommt folgendes Schema zum Einsatz:

Aktuelle Berechtigung	Vorgehensweise von Windows 2000
Dem Benutzer oder der Gruppe wird der Zugriff verweigert.	Dem Benutzer wird der Zugriff verweigert.
Der Benutzer hat bestimmte Berechtigungen.	Die Berechtigungen des Benutzers werden verwendet.
Die Gruppe hat bestimmte Berechtigungen, der Benutzer nicht.	Die Berechtigungen der Gruppe werden verwendet.

Vererbung von Berechtigungen

Bei Berechtigungen kommt das Prinzip der *Vererbung* zum Einsatz. Damit übernimmt ein Unterordner die Eigenschaften seines übergeordneten Ordners und jede Datei übernimmt die Eigenschaften des Ordners, in dem sie erstellt wurde. Dies ist sehr nützlich, weil damit Berechtigungen ganz oben in der Verzeichnisstruktur zugewiesen werden können, die dann auf neue Objekte übertragen werden, ohne dass der Administrator die Berechtigungen für jedes neue Objekt manuell ändern muss. Wenn also eine neue Datei in einem Ordner erstellt wird, auf den jedes Mitglied der Gruppe *Rechnungswesen* Zugriff hat, kann auch jedes Mitglied dieser Gruppe die neue Datei benutzen. Für die Datei gelten außerdem dieselben Berechtigungen wie für den Ordner, in dem sie sich befindet. Bei Bedarf kann die Vererbung für bestimmte Verzeichnisse deaktiviert werden.

Die Vererbung beeinflusst nur Dateien, die erstellt werden, nachdem die Berechtigungen festgelegt wurden. Um die Berechtigungen für alle Objekte zu ändern, die einem bestimmten Ordner untergeordnet sind, müssen die Berechtigungen in der gesamten untergeordneten Verzeichnisstruktur geändert werden.

Dateiberechtigungen zuweisen

Dateiberechtigungen lassen sich ziemlich leicht zuweisen. Es gibt dafür eine ganz nette Oberfläche. Klicken Sie z.B. im Windows-Explorer mit der rechten Maustaste auf das Objekt und wählen Sie im Kontextmenü den Befehl **Eigenschaften**. Klicken Sie im **Eigenschaften**-Dialogfeld auf die Registerkarte

Sicherheitseinstellungen (siehe Abbildung 4.15). Im oberen Teil dieser Registerkarte wird eine Namensliste angezeigt und im unteren Teil die Berechtigungen, die der Datei zugewiesen wurden. Auf der Registerkarte **Sicherheitseinstellungen** sind die Berechtigungen der einzelnen Benutzer aufgeführt. Wählen Sie einen Benutzer aus der Liste im oberen Teil aus, ändert sich der untere Bereich der Registerkarte und zeigt die Berechtigungen an, die der gewählte Benutzer hat. Die Kontrollkästchen können sich in drei Zuständen befinden: Aktiviert, deaktiviert und grau unterlegt. Ein aktiviertes Kontrollkästchen in der Spalte **Zulassen** kennzeichnet, dass der ausgewählte Benutzer diese bestimmte Berechtigung für das Objekt hat. Ein aktiviertes Kontrollkästchen in der Spalte **Verweigern** gibt an, dass dem Benutzer diese Berechtigung für die Datei verweigert wird.

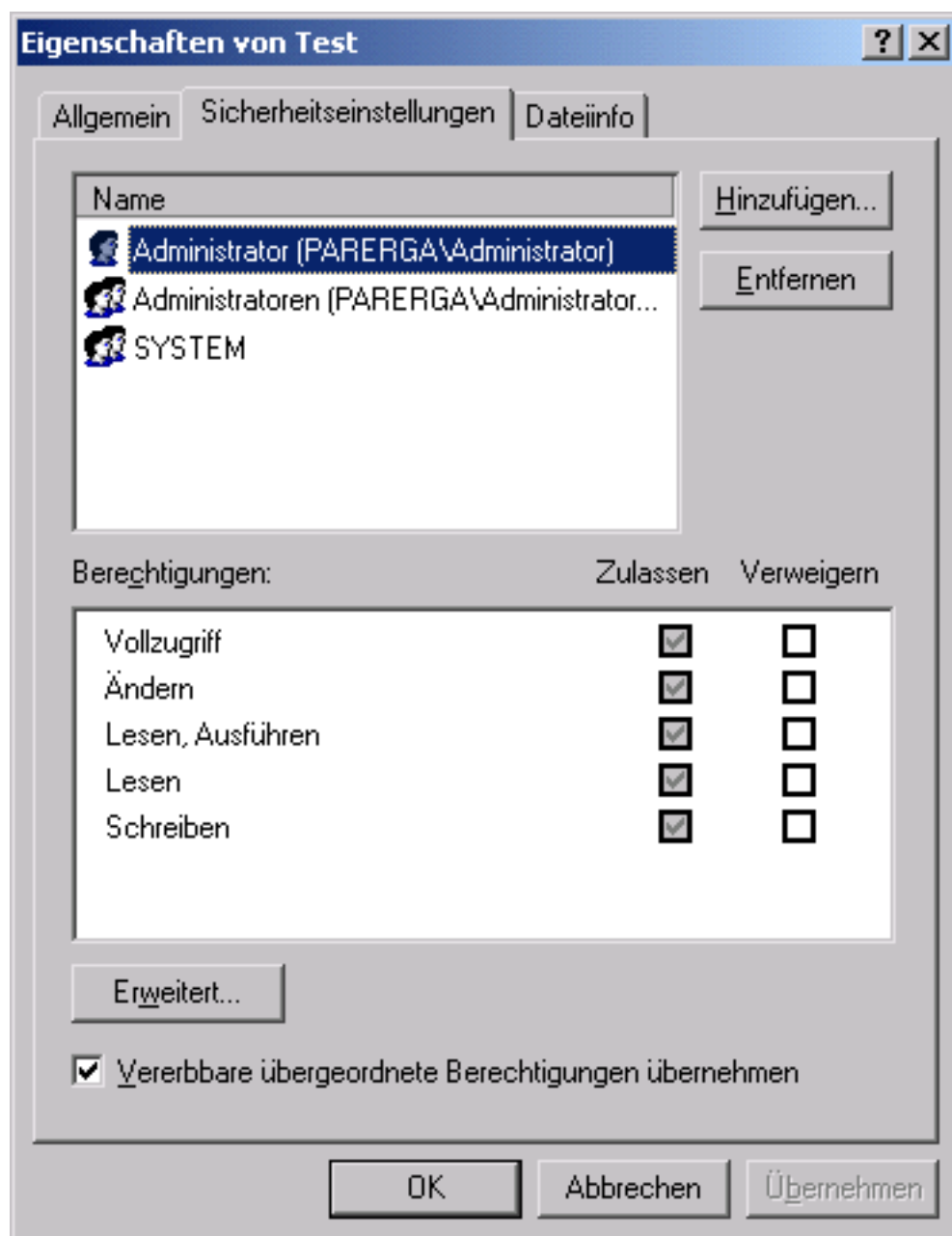


Abbildung 4.15: Auf der Registerkarte Sicherheitseinstellungen werden die Berechtigungen für einzelne Benutzer eingerichtet.

Wenn ein Kontrollkästchen grau unterlegt ist, wurden die Berechtigungen vom übergeordneten Objekt übernommen. Um Berechtigungen zu ändern, die grau unterlegt sind, müssen Sie entweder das Kontrollkästchen **Vererbte übergeordnete Berechtigungen übernehmen** am unteren Rand der

Registerkarte deaktivieren oder die Berechtigungen für das übergeordnete Objekt ändern. Wenn sich das grau unterlegte Kontrollkästchen in der Spalte **Zulassen** befindet, wird, wenn das Kontrollkästchen **Verweigern** für die Berechtigung aktiviert wird, die Berechtigung auch dann verweigert, wenn das Kontrollkästchen **Zulassen** für die Berechtigung aktiviert und grau unterlegt ist.

Wenn Sie Berechtigungen für einen Ordner einrichten, müssen Sie manchmal alle Berechtigungen für alle existierenden untergeordneten Objekte zurücksetzen. Denken Sie daran, dass die Vererbung, die über das Kontrollkästchen **Vererbbare übergeordnete Berechtigungen übernehmen** aktiviert wird, nur die neu erstellten Dateien beeinflusst und nicht die bereits bestehenden Dateien.

Um die Unterordner und andere Dateien in einem Verzeichnis einzurichten, müssen Sie auf der Registerkarte **Sicherheitseinstellungen** auf die Schaltfläche **Erweitert** klicken, um das Dialogfeld **Zugriffseinstellungen** zu öffnen (siehe Abbildung 4.16). Hier werden alle Zugriffsberechtigungen angezeigt, die für das Objekt eingerichtet wurden; die Zugriffsberechtigungen lassen sich hier bearbeiten. Klicken Sie auf die Schaltfläche **Anzeigen/Bearbeiten**, um spezielle Eigenschaften für den Ordner oder die Datei einzurichten. Wird das Kontrollkästchen **Berechtigungen in allen untergeordneten Objekten zurücksetzen und die Verbreitung vererbbarer Berechtigungen aktivieren** aktiviert, werden die Berechtigungen auf alle Unterordner und Dateien im aktuellen Ordner vererbt, die im Feld **Berechtigungseinträge** angezeigt werden.

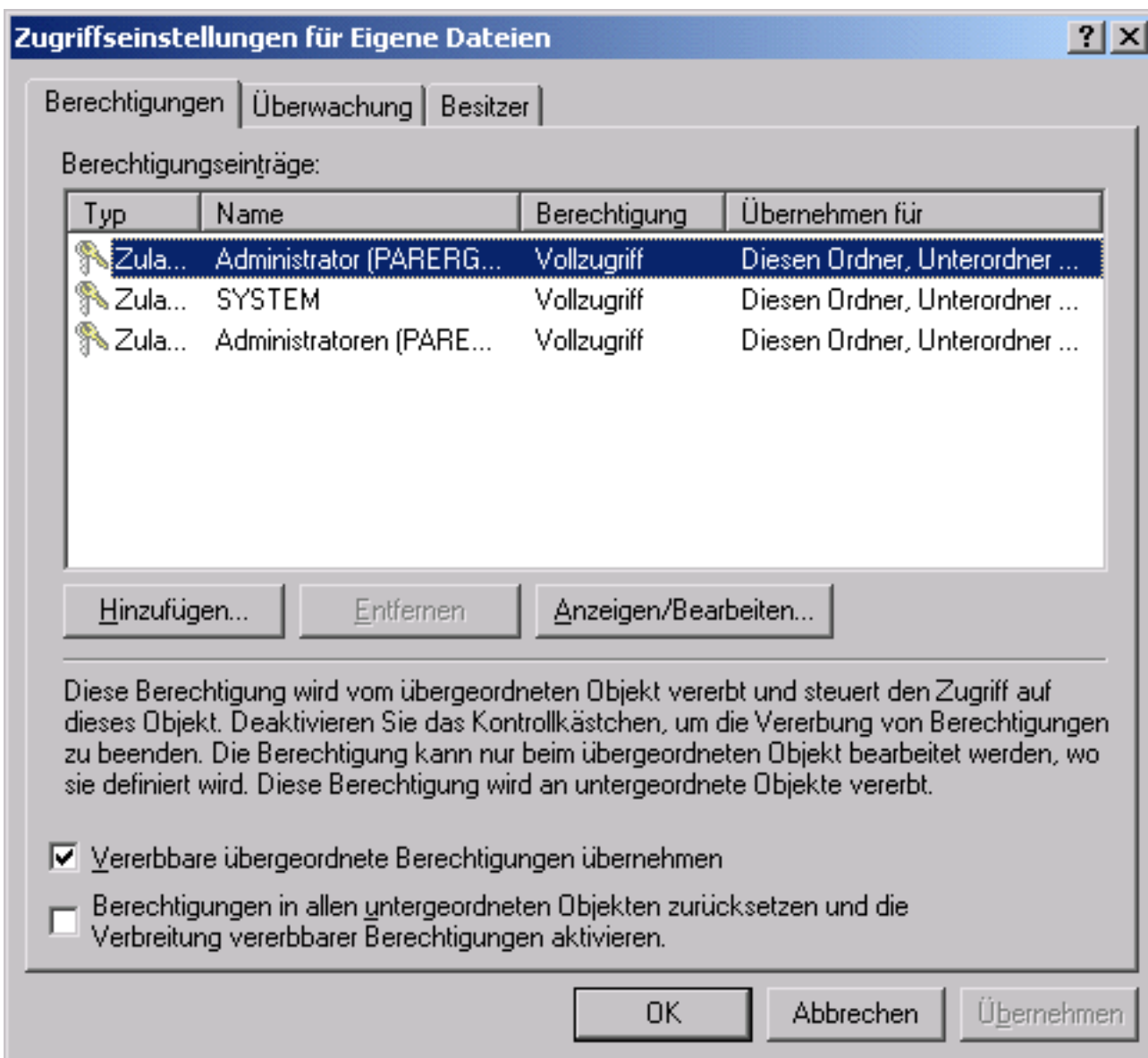


Abbildung 4.16: Über die erweiterten Berechtigungen lassen sich Unterordner und Dateien in einem Ordner auf die aktuellen Einstellungen zurücksetzen.



Wenn die Berechtigungen für ein Verzeichnis zurückgesetzt werden, das Tausende von Dateien enthält, kann dies einige Zeit in Anspruch nehmen. Das sollte die Benutzer bis auf die erhöhte Festplatten- und Prozessoraktivität nicht beeinträchtigen.

Auf der Registerkarte **Besitzer** im Dialogfeld **Zugriffseinstellungen** lässt sich der Besitzer einer Datei ändern. Besitzerrechte können nur übernommen und niemals weitergegeben werden. Um jemanden Besitzerrechte für eine Datei zu vergeben, muss das Kontrollkästchen **Zulassen** für die Berechtigung **Besitzerrechte übernehmen** aktiviert werden. Anschließend muss das Besitzerrecht noch über die Schaltfläche **Übernehmen** auf der Registerkarte **Besitzer** im Dialogfeld **Zugriffseinstellungen** zugewiesen werden.

Das ist doch alles Unsinn! Wie werden Berechtigungen in der realen Welt angewendet?

Die Zuweisung von Dateiberechtigungen ist ein komplexes Thema und Sie müssen sich etwas damit befassen, um zu verstehen, wie sie funktioniert. Dieser Abschnitt beschreibt, wie Dateiberechtigungen funktionieren und wie sie benutzt werden.

In den meisten Netzwerken gibt es drei Situationen für die Sicherheit von Dateien: die Benutzerverzeichnisse, die Gruppenverzeichnisse und der öffentlich zugängliche Raum. Bei Benutzerverzeichnissen hat der Benutzer immer Vollzugriff und alle Objekte erben die Berechtigungen vom Stammordner. Der Benutzer ist automatisch Besitzer aller Objekte im Ordner, weil er diese in erster Linie anlegen wird.

Gruppenverzeichnisse ähneln Benutzerverzeichnissen. Sie enthalten alle Dateien, die von bestimmten Gruppen innerhalb des Unternehmens verwendet werden, wie z.B. ein Ordner *Rechnungswesen*, der alle Informationen zum Inventar enthält. Alle Mitglieder der Gruppe *Rechnungswesen* sollten Vollzugriff auf diesen Ordner haben und allen weiteren Benutzern sollte der Zugriff verweigert werden. So lassen sich die Daten des Rechnungswesens sichern.

In einigen Netzwerken gibt es ein Verzeichnis, das für jeden zugänglich ist und über das Benutzer Dateien austauschen können. Auf diese Art von Verzeichnis sollte die Gruppe **Jeder** Vollzugriff haben. Es gibt natürlich bestimmte Richtlinien und andere Beschränkungen, die für den Ordner eingerichtet werden sollten, damit er nicht unkontrolliert wächst. Hier wäre z.B. der Einsatz eines Kontingents sinnvoll.



Die Sicherheit von Dateien ist ein sehr wichtiges Thema und der erste Schritt, um die Dateien zu sichern, besteht darin, eine Partition im NTFS-Format zu erstellen. Erstellen Sie anschließend Ordner in der Partition und experimentieren Sie mit diesen Ordnern, in dem Sie z.B. das Kontrollkästchen **Vererbbare übergeordnete Berechtigungen übernehmen** deaktivieren, anschließend Dateien ändern und sich unter anderen Benutzernamen anmelden. Probieren Sie als Nächstes aus, wie die verschiedenen Dateiberechtigungen funktionieren.

4.4.3 Konvertierung von Formaten

Die Formate FAT und FAT32 lassen sich auf NTFS aktualisieren. Nachdem ein Datenträger in das NTFS-Format konvertiert wurde, lässt sich dies jedoch nicht mehr rückgängig machen. NTFS benötigt mindestens 5 Mbyte Festplattenspeicher für den Overhead, der genutzt wird, um das Journal und Sicherheitsinformationen zu speichern.

Um eine Partition zu formatieren, öffnen Sie die Datenträgerverwaltung. Klicken Sie mit der rechten Maustaste auf die Partition und wählen Sie im Kontextmenü den Befehl **Formatieren**. Es öffnet sich das Dialogfeld **Formatieren** (siehe Abbildung 4.17). Geben Sie eine Datenträgerbezeichnung ein, wählen Sie das Dateisystem aus, mit dem der Datenträger formatiert werden soll, und legen Sie im Listefeld **Größe der Zuordnungseinheit** den gewünschten Wert fest. Die Größe der Zuordnungseinheit ist die kleinste Menge an Festplattenspeicher, die zugeordnet werden kann. Bei größeren Festplatten benötigen Sie größere Zuordnungseinheiten. Normalerweise ist es am besten, die Standardeinstellung beizubehalten, weil das System die kleinste Größe der Zuordnungseinheit wählt, mit der sich der Datenträger formatieren lässt. Eine Formatierung im QuickFormat löscht alle Zuordnungsinformationen vom Datenträger, ohne jedoch den gesamten Datenträger zu initialisieren. Diese Formatierung lässt sich

bei großen Datenträgern wesentlich schneller durchführen.

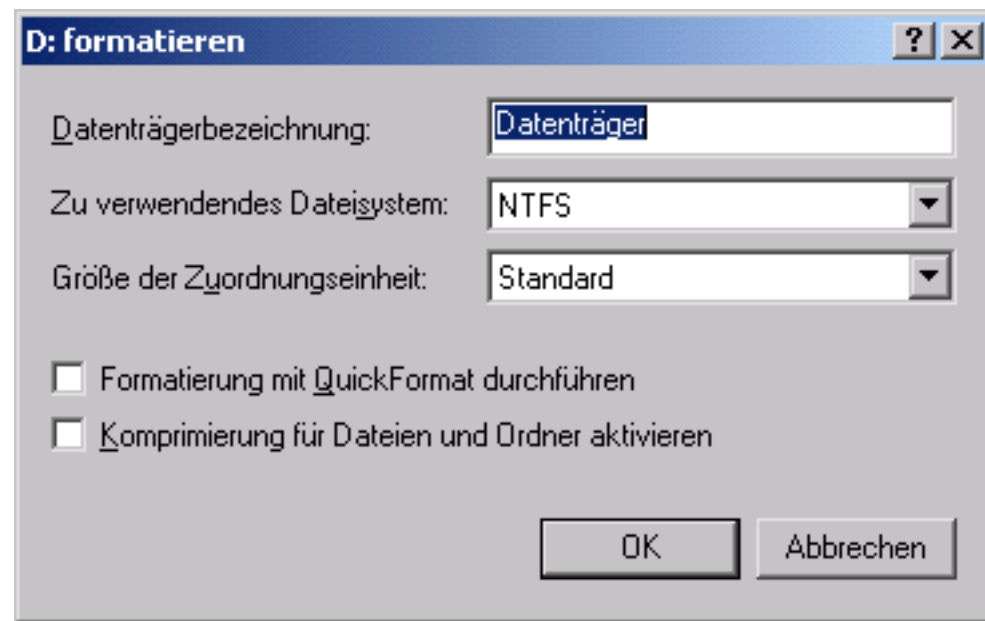


Abbildung 4.17: Wählen Sie das Dateisystem aus, mit dem der Datenträger formatiert werden soll, und klicken Sie anschließend auf OK.

Um eine Partition von FAT oder FAT32 in NTFS zu konvertieren, öffnen Sie eine Eingabeaufforderung, indem Sie **Start/Ausführen** wählen und in das Dialogfeld **Ausführen** den Befehl `cmd` eingeben, um die Eingabeaufforderung zu öffnen. Benutzen Sie anschließend den Konvertierbefehl. Um z.B. den Datenträger C: in NTFS zu konvertieren, verwenden Sie folgenden Befehl:

```
convert c: /fs:ntfs
```

Wenn das Laufwerk benutzt wird, das Laufwerk das Systemlaufwerk ist oder das Laufwerk die Auslagerungsdatei enthält, erfolgt die Konvertierung erst, wenn das System neu gebootet wird. Ansonsten beginnt die Konvertierung sofort.

Datenträger lassen sich auch mit dem Format-Befehl von der Eingabeaufforderung formatieren. Für das FAT32-System sieht der Befehl z.B. wie folgt aus:

```
Format d: /fs:fat32
```

4.4.4 Empfehlungen

Es gibt heftige Diskussionen darüber, wie Festplatten für den Einsatz im Server am besten partitioniert und formatiert werden sollen. Dieser Abschnitt enthält Empfehlungen des Autors.

Ich formatiere die Bootpartitionen und die Systempartition immer mit dem FAT-Dateisystem. Die Bootpartition ist bei mir immer ungefähr 2 Gbyte groß. Dafür gibt es verschiedene Gründe, die sich alle

auf eine einfache Tatsache zurückführen lassen: Auf jede FAT-Partition besteht ein Zugriff über eine MS-DOS-Startdiskette. Wenn es Probleme in der primären Partition gibt, kann ich ein Dienstprogramm von Microsoft (ScanDisk) oder Norton Disk Doctor einsetzen, um den Schaden zu finden und möglicherweise zu beheben. Wenn ich DLLs manuell installieren muss und Windows 2000 dies nicht zulässt, kann ich den Server außerdem mit einer Startdiskette booten und die Installation vornehmen.

Der Nachteil ist, dass, wenn ich den Server mit einer Startdiskette booten kann, dies auch jeder andere tun kann. Der Server ist dann nicht mehr sicher. Mein Gegenargument ist jedoch, dass, wenn ein Eindringling bis zu meinem Server gelangen und ihn mit einer Startdiskette starten kann, dieser sowieso nicht korrekt gesichert war. Außerdem gibt es zahlreiche Dienstprogramme, mit denen sich NTFS-Datenträger von einer Startdiskette lesen lassen.

Wenn der Server korrekt konfiguriert ist, gibt es keinen signifikanten Datenverkehr, der auf den Bootdatenträger geschrieben wird, weil keine Auslagerung stattfindet und keine Benutzerdaten auf dem Datenträger gespeichert werden. Deshalb ist es kein Problem, die Dateizuordnungstabelle unberührt und synchron zu halten, weil sich sowieso nur sehr selten etwas ändert.

Die Datenträger, auf denen Daten gespeichert werden, sollten immer mit NTFS formatiert werden. Durch die höhere Zuverlässigkeit von NTFS aufgrund der Verwendung eines Journals, die Sicherheit und die kleineren Clustergrößen (selbst bei großen Datenträgern) eignet sich NTFS hervorragend für große Datenträger. Das Sicherheitssystem von NTFS bietet eine hohe Flexibilität bei der Sicherung von Dateien, ist jedoch gleichzeitig für die richtigen Personen auch leicht zugänglich.

Die Festplatte meiner Dual-Boot-Workstation habe ich mit FAT32 formatiert, weil sowohl Linux als auch Windows 2000 darauf zugreifen können.

Dies sind nur Vorschläge. Das Wichtigste ist, ein Schema zu entwickeln, mit dem sich Reparaturen leicht durchführen lassen und das eine hohe Systemleistung gewährleistet.

4.5 Datenträger

Der Begriff *Datenträger* wird für die Partitionen auf einer dynamischen Festplatte verwendet. Dieser Abschnitt beschreibt, wie Datenträger benutzt, wie Stripesets eingerichtet und wie die speziellen Features von dynamischen Festplatten genutzt werden. Windows 2000 unterstützt folgende Arten von Datenträgern:

- *Einfache Datenträger*. Entsprechen der primären Partition auf einer Basisfestplatte.
- *Übergreifende Datenträger*. Datenträger, die mehr als eine Festplatte umfassen.
- *Gespiegelte Datenträger*. Zwei Festplatten, die genau dieselben Informationen enthalten, um Fehlertoleranz zu bieten.
- *Stripesetdatenträger*. Drei oder mehr Festplatten, die als ein Datenträger behandelt werden können, wobei die Daten gleichmäßig auf die Festplatten verteilt sind.
- *RAID-5-Datenträger*. Drei oder mehr Festplatten, wobei die Daten und die Paritätsinformationen gleichmäßig über die Festplatten verteilt sind.

4.5.1 Einfache Datenträger

Ein einfacher Datenträger ist ein Datenträger auf einer dynamischen Festplatte. Er kann die gesamte Festplatte umfassen oder nur einen Teil davon. Die Abbildung 4.18 zeigt einfache Datenträger auf einer dynamischen Festplatte in der Datenträgerverwaltung.

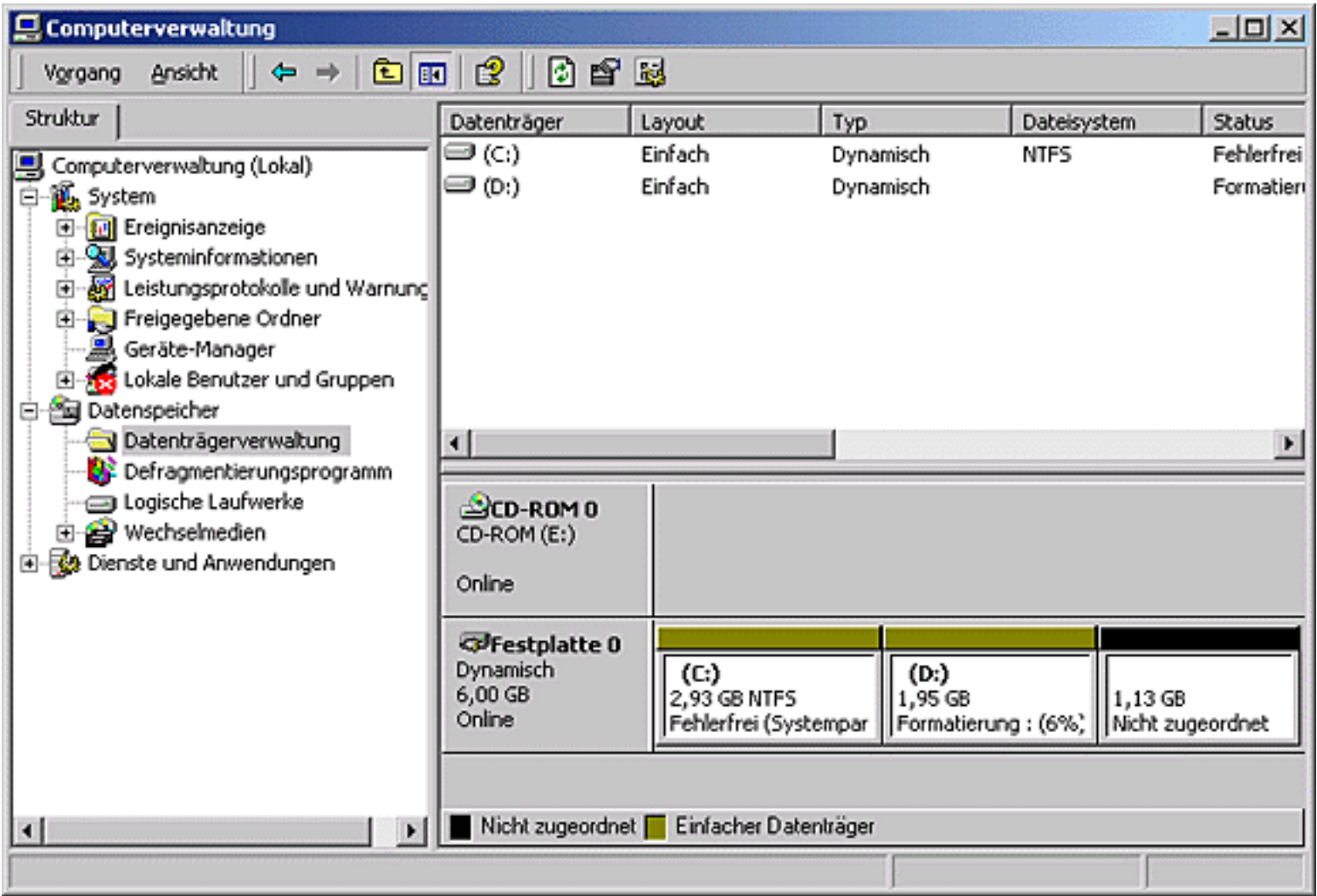


Abbildung 4.18: In der Datenträgerverwaltung zeigt sich, wie einfach einfache Datenträger am Bild schirm repräsentiert werden.

Um einfache Datenträger zu erzeugen, klicken Sie mit der rechten Maustaste auf den noch nicht zugeordneten Bereich auf einer dynamischen Festplatte und wählen im Kontextmenü den Befehl **Datenträger erstellen**.

Es öffnet sich der **Assistent zum Erstellen von Datenträgern** und fragt, welche Art von Datenträger Sie erstellen möchten, auf welchen Festplatten Sie ihn erstellen möchten und wie der neue Datenträger formatiert werden soll.

Klicken Sie mit der rechten Maustaste auf den Datenträger und wählen Sie im Kontextmenü den Befehl **Datenträger löschen**, um einen einfachen Datenträger zu löschen. Dabei gehen alle Daten verloren, die sich auf dem Datenträger befinden. Sie sollten also sehr vorsichtig sein. Über das Kontextmenü, das Sie durch Anklicken eines Datenträgers mit der rechten Maustaste öffnen, können Sie auch den Laufwerksbuchstaben oder Pfad ändern und den Datenträger neu formatieren.

4.5.2 Übergreifende Datenträger

Wenn ein kleiner Server zu wenig Festplattenspeicher hat, lässt sich leicht eine neue Festplatte hinzufügen. Etwas schwieriger könnte es schon werden, diese Festplatte zu nutzen. Es wäre praktisch, wenn der Datenträger, der alle Benutzerdateien enthält, einfach auf die neue Festplatte erweitert werden könnte. Genau diese Möglichkeit bieten übergreifende Datenträger. Sie erweitern im Wesentlichen einen Datenträger von einer Festplatte auf eine neue, ohne dass ein neuer Laufwerksbuchstabe zugeordnet wird. Sie fügen den neuen Speicherplatz einfach zum bestehenden Datenträger hinzu. Dies ist bei kleinen Servern sehr nützlich, bei denen zunächst nur ein gewisser Speicherplatz zur Verfügung steht, der dann mit den wachsenden Bedürfnissen der Benutzer angepasst werden muss. Bei der Erweiterung des Datenträgers wird einfach Festplattenspeicher zum Datenträger hinzugefügt, was wesentlich einfacher ist als der Versuch, die Daten auf separate Laufwerksbuchstaben aufzuteilen.



Ein kleiner Hinweis zu übergreifenden Datenträgern: Wenn ein Datenträger zwei Festplatten umfasst und eine dieser Festplatten defekt ist, steht der gesamte Datenträger nicht mehr zur Verfügung und muss von einer Sicherung wiederhergestellt werden. Sind zwei Festplatten in einem Datenträger enthalten, verdoppelt sich die Wahrscheinlichkeit, bei einem Hardwarefehler Daten zu verlieren. Enthält ein Server wichtige Daten, sollten Sie deshalb lieber gespiegelte Datenträger oder RAID-5-Datenträger verwenden.

Um einen Datenträger erweitern zu können, benötigen Sie eine NTFS-Partition, die Sie erweitern können und nicht belegten Speicherplatz, mit dem Sie die Partition erweitern können. Klicken Sie dann in der Datenträgerverwaltung mit der rechten Maustaste auf die NTFS-Partition und wählen Sie im Kontextmenü den Befehl **Datenträger erweitern**. Der **Assistent zum Erweitern von Datenträgern** startet nun. Klicken Sie auf **Weiter** und wählen Sie dann die Festplatte oder den Datenträger, auf die der Datenträger erweitert werden soll (siehe Abbildung 4.19). Um einzelne Festplatten hinzuzufügen, wählen Sie diese im Listefeld auf der linken Seite aus und klicken auf die Schaltfläche **Hinzufügen**. Klicken Sie anschließend die einzelnen Festplatten im rechten Listefeld an, können Sie die Größe der ausgewählten Festplatte verändern, indem Sie einen neuen Wert in das Feld **Größe** eingeben.

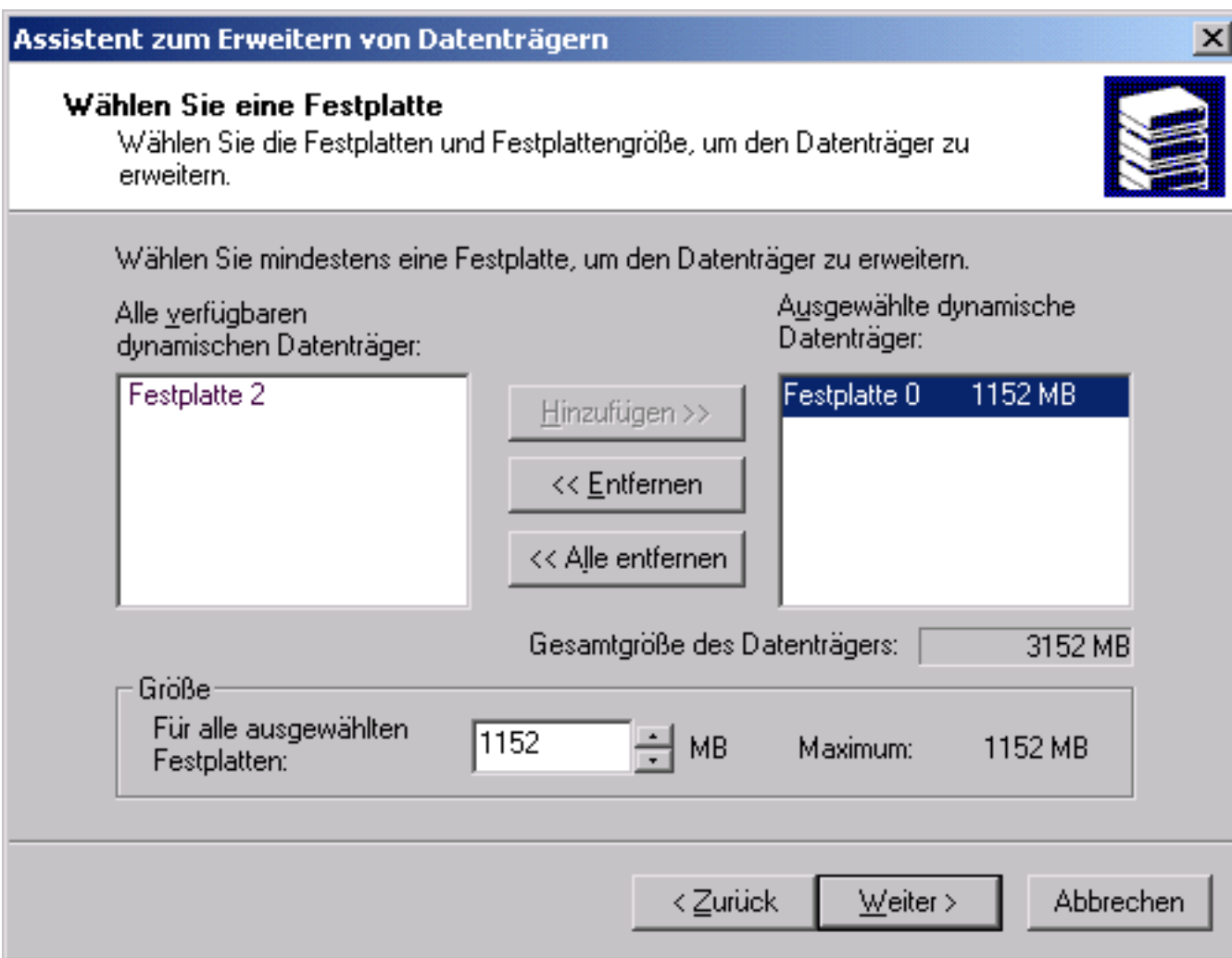


Abbildung 4.19: Hier wird ein Datenträger um nicht belegten Speicherplatz erweitert.

4.5.3 Gespiegelte Datenträger

Ein gespiegelter Datenträger ist ein Datenträger, der auf beiden Datenträgern duplizierte Daten enthält. Beide Datenträger enthalten genau dieselben Daten. Wenn Daten auf einen Datenträger geschrieben werden, werden sie automatisch auf den anderen Datenträger gespiegelt.

Gespiegelte Datenträger bieten eine hohe Lese-, aber eine geringe Schreibleistung. Lesen geht schneller, weil jede Festplatte gleichzeitig etwas anderes lesen kann. Der Schreibvorgang dauert länger, weil er auf beiden Datenträgern gleichzeitig erfolgen muss.

Um einen gespiegelten Datenträger zu erstellen, erstellen Sie zunächst einen einfachen Datenträger, klicken dann mit der rechten Maustaste auf diesen und wählen im Kontextmenü den Befehl **Spiegelung hinzufügen**. Es öffnet sich ein Dialogfeld, in dem Sie die Festplatte angeben müssen, auf die der Datenträger gespiegelt werden soll. Wählen Sie eine Festplatte aus und klicken Sie auf die Schaltfläche **Spiegelung hinzufügen**. Der Spiegelungsvorgang startet nun.

Nachdem die Spiegelung erstellt wurde, kann auf den Datenträger mit einem Laufwerksbuchstaben zugegriffen werden oder über einen Pfad, falls die Laufwerke auf eine NTFS-Partition gemountet wurden.

Wenn eine der Festplatten bei einem gespiegelten Datenträger versagt, ist einiges an Aufwand nötig, um die Fehlertoleranz des gespiegelten Datenträgers wiederherzustellen. Als Erstes sollte versucht werden, die Festplatte zu reaktivieren, indem das System herunter- und wieder hochgefahren wird. Wenn die Fehler nicht konsistent auftreten, liegt vielleicht ein Fehler in der Laufwerklogik vor, der sich durch einen Neustart beheben lässt. Nehmen Sie sich einen Augenblick Zeit, um die Verkabelung der Festplatten zu überprüfen und sich zu vergewissern, dass weder die Datenkabel noch die Stromzufuhr lose sind. Bei hintereinander geschalteten SCSI-Geräten sollten Sie prüfen, ob alle Geräte korrekt terminiert sind. Schalten Sie den Computer wieder ein und öffnen Sie die Datenträgerverwaltung. Klicken Sie anschließend mit der rechten Maustaste auf die Festplatte, die versagt hat, und wählen Sie im Kontextmenü den Befehl **Datenträger erneut aktivieren**. Der Status der Festplatte ändert sich nun. Es wird zunächst **Regenerieren** und anschließend der Status **Fehlerfrei** angezeigt, wenn die Festplatte erfolgreich reaktiviert werden konnte.

Wenn sich die Festplatte nicht mehr aktivieren lässt, müssen Sie eine neue installieren und die Spiegelung neu einrichten. Entfernen Sie dazu die alte Spiegelung zwischen den beiden Datenträgern, indem Sie mit der rechten Maustaste auf den fehlerfreien alten Datenträger klicken und im Kontextmenü den Befehl **Spiegelung entfernen** wählen. Klicken Sie anschließend noch einmal mit der rechten Maustaste auf den fehlerfreien alten Datenträger und wählen Sie im Kontextmenü den Befehl **Spiegelung hinzufügen**. Die Spiegelung wird auf die gleiche Weise wie beim ersten Mal eingerichtet.

Um einen Datenträger aus einem gespiegelten Datenträger zu entfernen, klicken Sie zunächst mit der rechten Maustaste auf einen der Datenträger, und wählen Sie im Kontextmenü den Befehl **Spiegelung entfernen**. Der Datenträger wird nun in nicht zugeordneten Speicherplatz umgewandelt, der dann als einfacher Datenträger weiter genutzt werden kann.

4.5.4 Stripesetdatenträger

Ein Stripesetdatenträger ist ein Datenträger, dessen Daten auf 2 bis 32 Festplatten verteilt sind. Die Festplatten sind in Blöcke unterteilt und diese Blöcke sind über die Festplatten verteilt. Bei einem Stripesetdatenträger mit drei Festplatten wird der erste Block z.B. auf der ersten Festplatte, der zweite auf der zweiten Festplatte und der dritte auf der dritten Festplatte gespeichert. Der vierte Block wird dann wieder auf der ersten Festplatte gespeichert etc. Auf diese Weise werden die Daten über alle Festplatten verteilt.

Der Stripesetdatenträger ist der Datenträger mit der höchsten Leistung, den Windows 2000 anbietet. Wenn eine Datei z.B. auf drei Festplatten verteilt gespeichert wird, muss das System die einzelnen Teile von den drei Festplatten lesen können, um die gesamte Datei zu lesen. Und alle Festplatten können gleichzeitig nach ihrem Informationsblock suchen. Im Idealfall erfolgt der Lesevorgang drei Mal so schnell, als wenn das Dokument nur auf einer Festplatte gespeichert wird.

Stripesetdatenträger bieten überhaupt keine Fehlertoleranz. Wenn eine Festplatte beschädigt ist, ist der gesamte Datenträger unbrauchbar. Das Striping-Verfahren sollte deshalb nur bei Daten verwendet werden, die im Wesentlichen statisch sind und regelmäßig gesichert werden.

Um einen Stripesetdatenträger einzurichten, klicken Sie mit der rechten Maustaste auf nicht benutzten Speicherplatz einer der Festplatten, die in den Stripesetdatenträger aufgenommen werden soll, und wählen Sie im Kontextmenü den Befehl **Datenträger erstellen**. Klicken Sie im **Assistent zum Erstellen**

von **Datenträgern** auf **Weiter** und anschließend auf die Option **Stripesetdatenträger**. Im nächsten Dialogfeld (siehe Abbildung 4.20) wählen Sie die Festplatten aus, die im Stripesetdatenträger enthalten sein sollen. Klicken Sie im linken Feld auf alle Laufwerke, die Sie in den Stripesetdatenträger aufnehmen möchten, und klicken Sie dann auf die Schaltfläche **Hinzufügen**. Klicken Sie auf **Weiter**, nachdem alle Festplatten hinzugefügt wurden. Im nächsten Schritt müssen Sie wie beim Erstellen eines einfachen Datenträgers einen Laufwerksbuchstaben und einen Pfad angeben. Klicken Sie auf **Weiter**, um zur Zusammenfassung zu gelangen, und auf **Fertig stellen**, um den Stripesetdatenträger einzurichten.

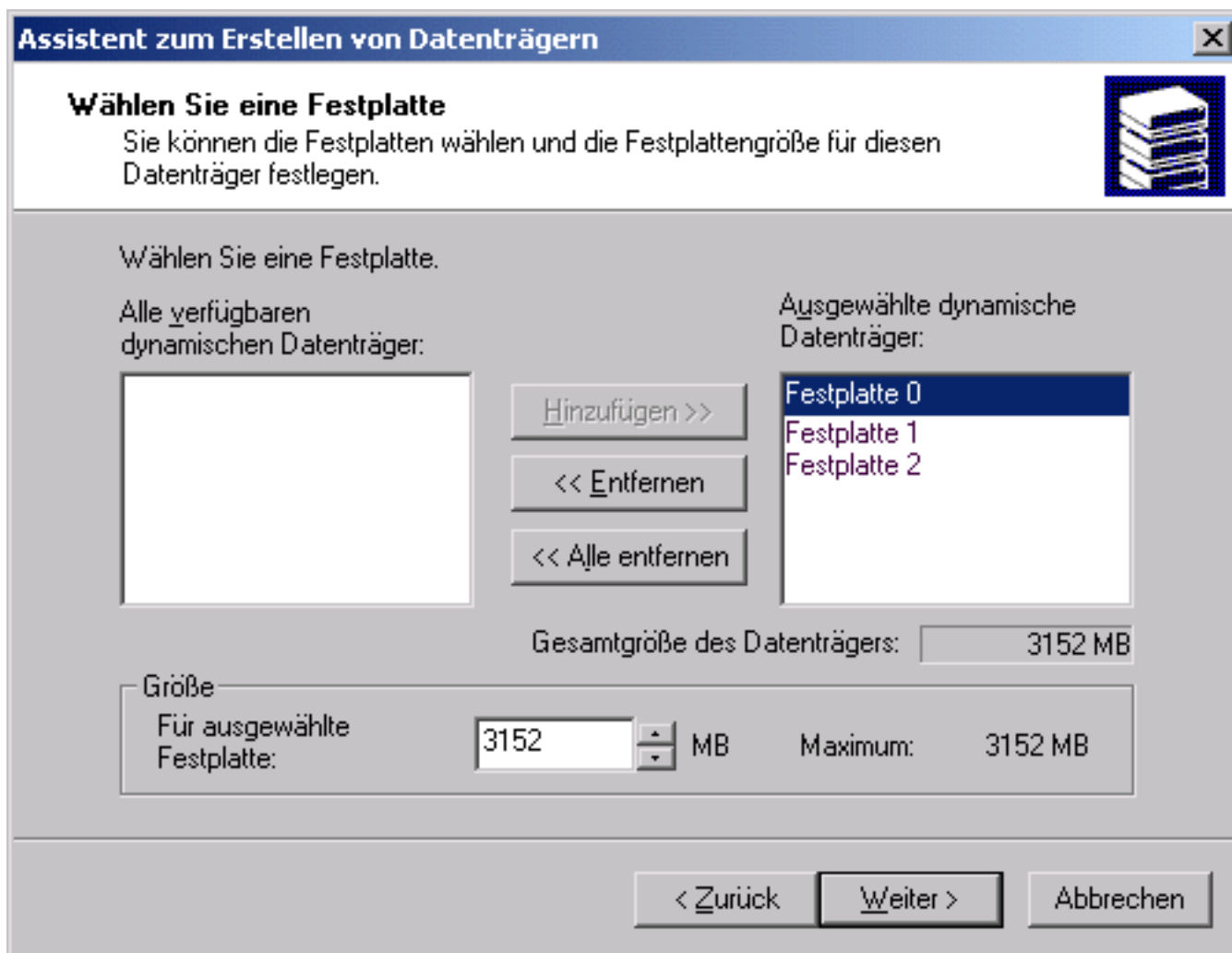


Abbildung 4.20: In diesem Dialogfeld legen Sie fest, welche Festplatten im Stripesetdatenträger enthalten sein sollen. Wählen Sie mindestens 2 und höchstens 32 Festplatten aus.

4.5.5 RAID-5-Datenträger

RAID-5-Datenträger führen das Konzept der Stripesetdatenträger noch einen Schritt weiter. Anstatt nur die Daten zu speichern, verteilen sie auch die Paritätsinformationen beim Speichern über alle Festplatten. Die Paritätsinformationen werden dabei in Blöcken direkt neben den eigentlichen Daten gespeichert.

RAID-5-Datenträger werden auf die gleiche Weise eingerichtet wie Stripesetdatenträger. Im ersten Schritt des Assistenten müssen Sie jedoch die Option **RAID-5-Datenträger** statt **Stripesetdatenträger** auswählen.

4.5.6 Einige Hinweise zu Windows 2000-Datenträgern

Gespiegelte Datenträger, Stripesetdatenträger und RAID-5-Datenträger sind großartige Features von Windows 2000 und je nachdem, welche Auswahl Sie getroffen haben, bieten sie auch ein hohes Maß an Fehlertoleranz. Sie bieten jedoch nicht dieselbe Leistung wie ein gutes hardwarebasiertes RAID-System.

Die Spiegelung und das Striping-Verfahren beinhalten sehr viel Overhead. Der Prozessor muss berechnen, wo die verschiedenen Blöcke gespeichert werden können und außerdem muss die Parität berechnet werden. Der Prozessor hat dabei eine ganze Reihe von E/A-Funktionen zu verrichten, die er leicht behandeln kann. Es gibt jedoch verschiedene hardwarebasierte RAID-Systeme, die dieselben Funktionen bieten und der CPU die gesamte Arbeit abnehmen, sodass sie wichtigere Tasks durchführen kann.

Hardware-RAID-Systeme bieten außerdem einige nützliche Funktionen, wie z.B. die Möglichkeit, Speicherplatz zum laufenden System hinzuzufügen oder eine fehlerhafte Festplatte bei laufendem System auszutauschen. Bevor Sie diese Funktionen nutzen, sollten Sie jedoch das Handbuch des RAID-Herstellers ausführlich lesen. Im Allgemeinen sind die Systeme aber sicher und leicht zu handhaben und produzieren keine Ausfallzeiten.

Außerdem bieten viele Hardware-RAID-Systeme Funktionen wie die Möglichkeit, eine Festplatte bereitzuhalten, die die Funktion einer anderen übernimmt, sobald diese fehlerhaft arbeitet.

Das Software-RAID-System von Windows 2000 ist sehr interessant und bietet für Unternehmen, die keinen Hardware-RAID kaufen möchten, sehr viele Funktionen. Hardware-RAIDs sind jedoch erheblich effizienter und bieten eine höhere Fehlertoleranz als Software-RAIDs.

4.6 Netzwerkfreigaben

Viele Windows 2000-Server werden als Dateiserver eingesetzt. Ein Dateiserver ist ein Computer im Netzwerk, der einen zentralen, sicheren und zuverlässigen Zugriff auf die Dateien im Netzwerk bietet. Windows 2000 Server benutzt das CIFS-Protokoll (CIFS = Common Internet File System) für die Freigabe von Dateien. Bevor Microsoft sich aufs Internet stürzte und alles so umbenannte, dass der Begriff »Internet« enthalten ist, hieß das CIFS-Protokoll »SMB« (Server Message Block).

Windows 2000 verwendet die Architektur der Netzwerkfreigaben, um die Dateien für die Clients über das Netzwerk verfügbar zu machen. Jeder Ordner auf einem Windows 2000-Computer lässt sich über das Netzwerk freigeben und über Berechtigungen kann festgelegt werden, welche Benutzer Zugriff auf die Freigabe haben und wie viele Benutzer gleichzeitig auf eine Freigabe zugreifen können.

Zur Nutzung von Freigaben gehören zwei Dinge: Der Administrator muss ein Verzeichnis auf dem Server freigeben und der Benutzer muss über eine Clientworkstation auf das freigegebene Verzeichnis zugreifen.

4.6.1 Verzeichnisse freigeben

Um ein Verzeichnis freizugeben, öffnen Sie den Windows-Explorer und wechseln zum übergeordneten Ordner jenes Ordners, der freigegeben werden soll. Um z.B. den Ordner *D:\Benutzerdateien* freizugeben, wechseln Sie zum Laufwerk D:, klicken mit der rechten Maustaste auf den Ordner *Benutzerdateien* und wählen im Kontextmenü den Befehl **Freigabe**. Um einen Ordner freizugeben, klicken Sie auf die Option **Diesen Ordner freigeben** (siehe Abbildung 4.21). Dadurch werden die restlichen Optionen im Dialogfeld verfügbar. Geben Sie nun den Freigabenamen ein. Dieser muss nicht mit dem Ordnernamen übereinstimmen. Dies ist jedoch der Standardwert. Das Feld **Kommentar** ist optional. Sie können es nutzen, um die Art von Informationen zu beschreiben, die freigegeben werden. Im Bereich **Benutzerbegrenzung** wird die Anzahl der gleichzeitigen Zugriffe für die Freigabe festgelegt. Der Standardwert ist **Maximum erlaubt**. Das heißt, es sind so viele Verbindungen zulässig, wie es Lizenzen gibt.

Über die Schaltfläche **Zwischenspeichern** wird der Standardzwischenspeicher für den Ordner eingerichtet. Wenn der Benutzer beschließt, diese spezielle Freigabe zwischenspeichern, werden die Dateien bei Lese- und Schreibzugriffen zwischen der Workstation des Benutzers und dem Server kopiert und synchronisiert. Dadurch reduziert sich der Netzwerkverkehr, aber der Benutzer kann auch Dateien entfernen und auf einem Laptop oder mit einem anderen Medium bearbeiten.

Bei den Einstellungen für **Zwischenspeichern** wird z.B. festgelegt, wie Benutzer lokale Kopien von Dokumenten oder Programmen zwischenspeichern. Für das Zwischenspeichern gibt es drei Einstellungen. Bei der Einstellung **Manuelles Zwischenspeichern für Dokumente** muss der Benutzer angeben, welche Dokumente gespeichert werden sollen. Bei der Einstellung **Automatisches Zwischenspeichern für Dokumente** wird jedes Dokument automatisch lokal zwischengespeichert, auf das zugegriffen wird. Bei der Einstellung **Automatisches Zwischenspeichern für Programme** werden lokale Kopien von Programmen auf dem Computer des Benutzers angefertigt. In allen Fällen überwacht Windows 2000 den lokalen Computer des Benutzers und kopiert die Daten so, dass ältere Kopien der Programme oder Dokumente überschrieben werden.

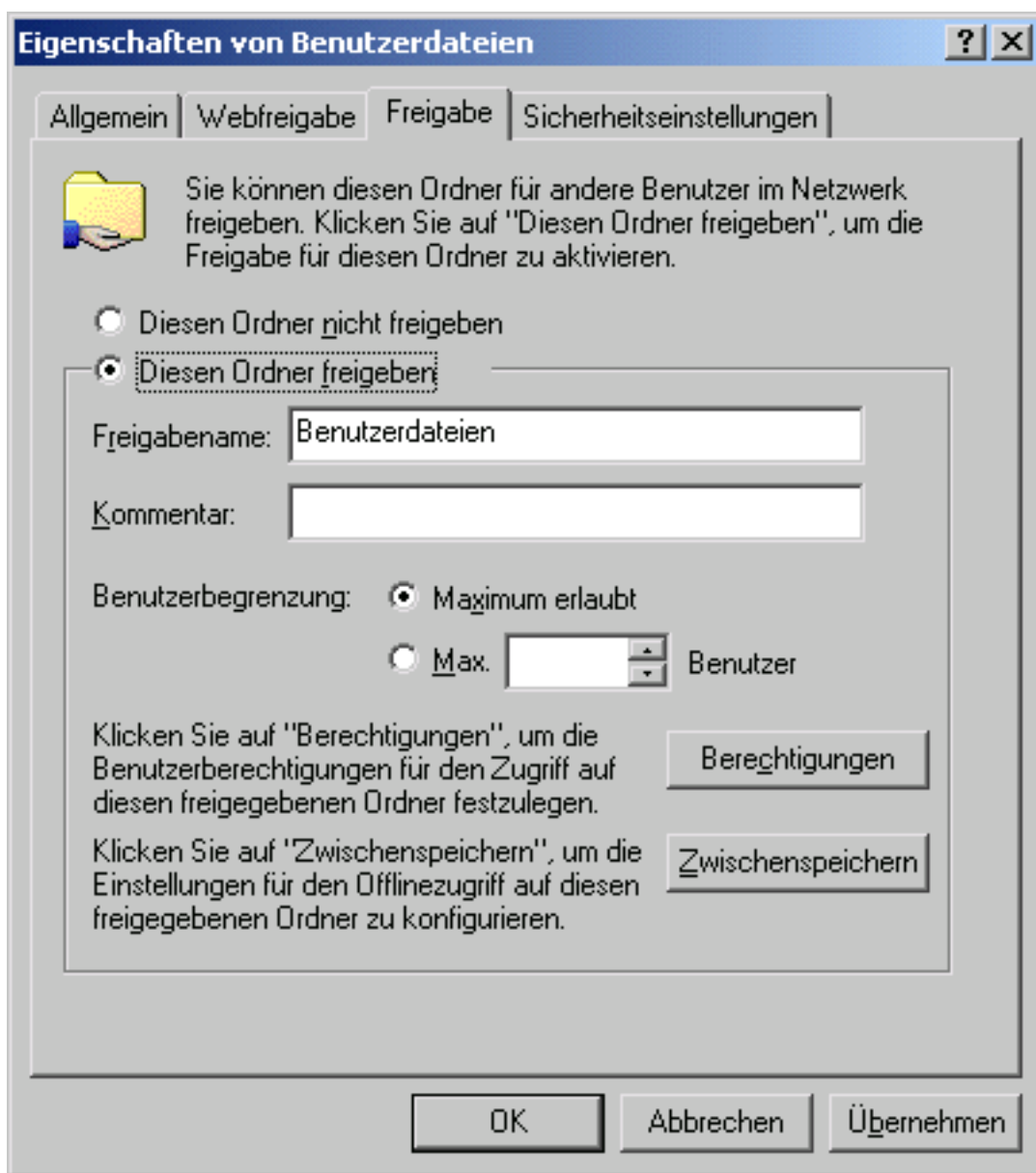


Abbildung 4.21: Auf der Registerkarte Freigabe werden Ordner für die Freigabe an Benutzer im Netzwerk eingerichtet.

Die Schaltfläche **Berechtigungen** öffnet das gleichnamige Dialogfeld (siehe Abbildung 4.22), in dem Berechtigungen für die Freigabe zugewiesen werden können. Wenn es sich um einen NTFS-Datenträger handelt, stehen alle Berechtigungen zur Verfügung. Legen Sie fest, wer auf alle Dateien und Unterordner im freigegebenen Ordner Zugriff haben sollte und welche Art von Zugriff bestehen sollte. Es gibt drei Zugriffsebenen: den **Vollzugriff**, bei dem Dateien gelesen, geschrieben und Unterordner angelegt werden dürfen. Mit der Berechtigung **Ändern** dürfen nur bestehende Dateien geändert und mit der Berechtigung **Lesen** dürfen die Dateien nur gelesen werden. Die Berechtigungen können für einzelne Benutzer oder Benutzergruppen vergeben werden.

Für alle drei Berechtigungsebenen (**Vollzugriff**, **Ändern** und **Lesen**) gibt es drei verschiedene Optionen (**Zulassen**, **Verweigern** und keines von beidem). Wird das Kontrollkästchen **Verweigern** aktiviert, wird die entsprechende Aktion unabhängig davon verweigert, welche anderen Optionen gewählt werden. Wird z.B. die Berechtigung **Ändern** auf **Zulassen** gesetzt und **Lesen** auf **Verweigern**, sind die Dateien in der Freigabe schreibgeschützt. Wenn die Berechtigung **Vollzugriff** auf **Verweigern** gesetzt wird, ist für die

Berechtigungen **Lesen** und **Ändern** ebenfalls das Kontrollkästchen **Verweigern** aktiviert, weil bei einem verweigerten Vollzugriff auch keine Lese- und Schreibvorgänge zulässig sind. Um einen Schreibschutz korrekt einzurichten, sollte die Berechtigung **Lesen** auf **Zulassen** und die Berechtigung **Ändern** auf **Verweigern** gesetzt sein. Der Benutzer kann den Inhalt des Ordners dann nur lesen. Wenn eine Gruppe, bei der der Benutzer Mitglied ist, die Berechtigung **Ändern** hat, kann der Benutzer den Ordnerinhalt trotzdem nur lesen.

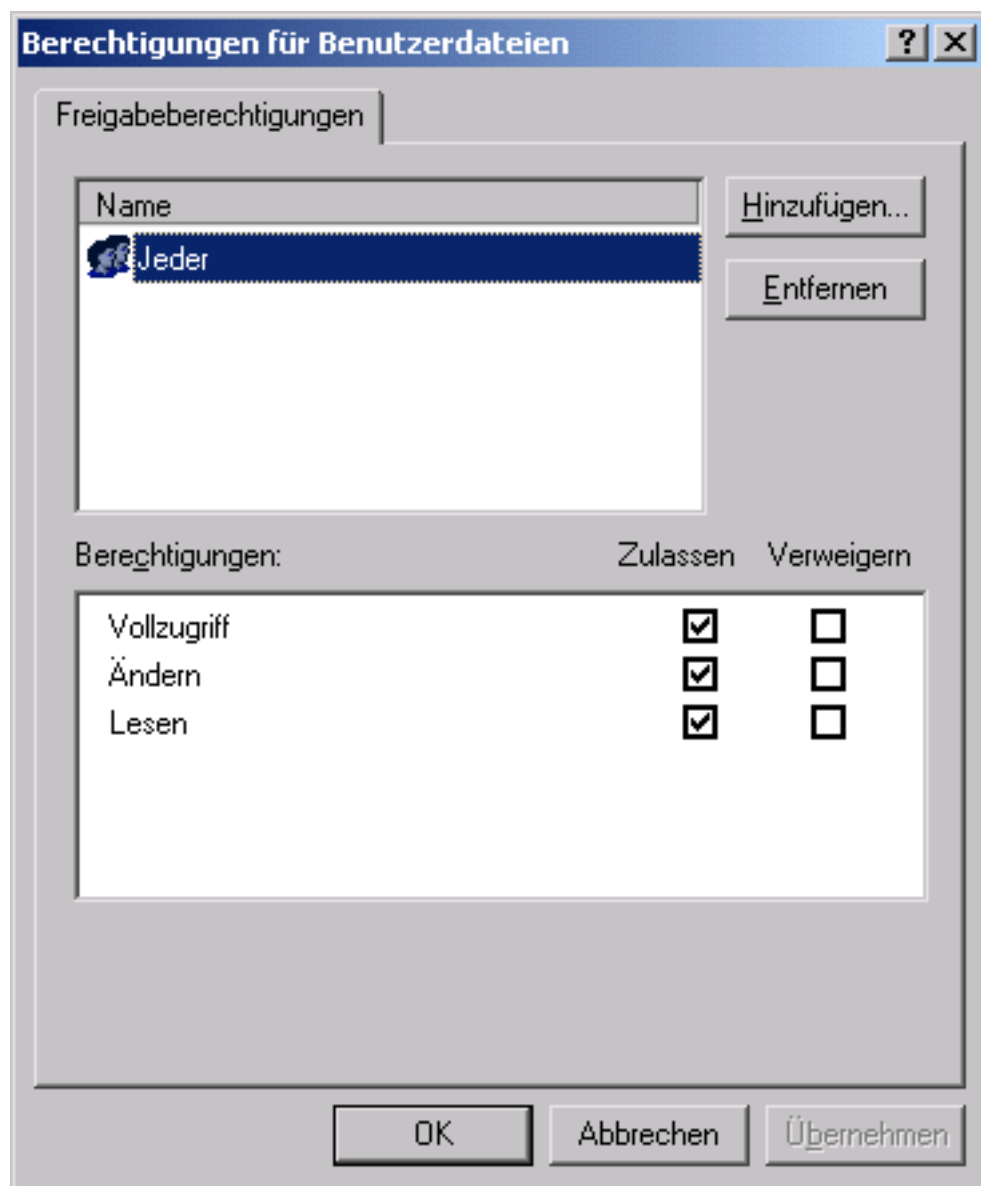


Abbildung 4.22: Die Liste der Benutzer, die Zugriff auf die Freigabe haben und die Art des Zugriffs, der ihnen gewährt wird.

Wenn sich der freigegebene Ordner in einer NTFS-Partition befindet, ist die Situation etwas komplexer. Um auf eine Datei zugreifen zu können, die auf einer NTFS-Partition freigegeben wird, muss der Benutzer auf die Freigabe zugreifen dürfen und Zugriff auf die Datei haben. Um die Dinge einfach zu halten, können Sie die Kombination aus Freigabeberechtigungen und NTFS-Berechtigungen als restriktivste Kombination der Berechtigungen betrachten. Wenn ein Benutzer die Berechtigung **Lesen** für eine Freigabe hat, jedoch **Vollzugriff** für alle Dateien und Ordner, kann der Benutzer die Dateien von der Freigabe trotzdem nur lesen.

Der Zugriff auf eine Freigabe kann Benutzern und Gruppen wie der auf eine Datei zugewiesen werden. Klicken Sie auf die Schaltfläche **Hinzufügen** und wählen Sie dann die Benutzer im Dialogfeld **Benutzer, Computer oder Gruppen auswählen** aus. Bestätigen Sie mit OK, wenn Sie alle Benutzer und Gruppen ausgewählt haben. Die Benutzer und Gruppen werden nun im Dialogfeld **Berechtigungen** angezeigt.

Nachdem ein Ordner freigegeben wurde, steht er den Benutzern sofort zur Verfügung. Um die Freigabe eines Ordners aufzuheben, öffnen Sie das **Eigenschaften**-Dialogfeld für den Ordner und aktivieren auf der Registerkarte **Freigabe** die Option **Diesen Ordner nicht freigeben**. Die Benutzer können dann zwar die momentan geöffneten Dateien aus der Freigabe weiterhin benutzen, nicht aber neue Dateien aus der Freigabe öffnen. Nachdem sie die geöffneten Dateien geschlossen haben, können sie auch darauf nicht mehr zugreifen.

Um den aktuellen Status der Freigaben zu prüfen, öffnen Sie die Computerverwaltung und klicken auf **Freigegebene Ordner**. Dieser Ordner enthält die drei Elemente **Freigaben**, **Sitzungen** und **Geöffnete Dateien**. Im Ordner **Freigaben** sind alle aktuellen Freigaben auf dem lokalen Computer enthalten. Darunter befinden sich viele Freigaben mit einem Dollarzeichen (\$) am Ende. Dies sind versteckte Freigaben, die in einem Dateiverwaltungsprogramm nicht angezeigt werden. Freigaben wie C\$ sind administrative Freigaben, die nur Administratoren zur Verfügung stehen und Netzwerkclients nicht in der Liste der Freigaben angezeigt werden.

Der Ordner **Sitzungen** enthält alle Benutzer, die momentan auf die einzelnen Freigaben zugreifen. Es wird angezeigt, wer mit einer Freigabe verbunden ist, wie viele Dateien geöffnet sind und wie lange die Verbindung bereits besteht. Um die Verbindung eines Benutzers zu beenden, klicken Sie mit der rechten Maustaste auf die Sitzung und wählen Sie im Kontextmenü den Befehl **Sitzung schliessen**. Der Benutzer hat nun keine Verbindung mehr zum Server und verliert möglicherweise Daten. Sie sollten dieses Verfahren also nur anwenden, wenn es absolut nötig ist. Im Ordner **Geöffnete Dateien** sind alle Dateien enthalten, die von einem Netzwerkbenutzer geöffnet wurden und es wird angezeigt, ob der Benutzer die Datei liest, Daten in die Datei schreibt oder beides. Klicken Sie mit der rechten Maustaste auf eine Datei in diesem Ordner und wählen Sie im Kontextmenü den Befehl **Datei schliessen**, um den Zugriff des Benutzers auf diese Datei zu beenden.

Freigaben über die Eingabeaufforderung einrichten

Es ist immer sinnvoll zu wissen, wie Operationen von der Eingabeaufforderung und über die grafische Benutzeroberfläche ausgeführt werden. Dafür gibt es zwei Gründe: Erstens gilt, dass eine Operation, die sich über die Eingabeaufforderung ausführen lässt, auch als Skript in eine Batchdatei geschrieben werden kann. Zweitens lassen sich Dienstprogramme wie Telnet und Rconsole (Remote Console) nutzen, die nur wenig Bandbreite verbrauchen und mit denen sich eine reine textorientierte Verbindung zu einem Server herstellen lässt. Telnet wird in Kapitel 19 ausführlicher beschrieben. Telnet und Rconsole bieten nur eine Befehlszeilenoberfläche und funktionieren großartig bei langsamen DFÜ-Netzwerk-Verbindungen.

Um ein Verzeichnis über die Eingabeaufforderung freizugeben, verwenden Sie den Befehl `net share`. Der Befehl `net share` hat fünf Modi, die davon abhängen, welche Argumente übergeben werden.

Geben Sie den Befehl `net share` an der Eingabeaufforderung ein, werden alle



nicht versteckten Freigaben auf dem lokalen Server aufgelistet.

Geben Sie `net share Freigabename` ein, werden alle Freigabeeigenschaften für die angegebene Freigabe aufgelistet. Zu den Eigenschaften gehören der Freigabename, der lokale Pfad zum Ordner, der freigegeben wird, der Kommentar, die maximale Anzahl der Benutzer und die aktuellen Benutzer der Freigabe.

Die dritte Option ist `net share Freigabename=Laufwerk:Pfad`. Dadurch wird der Ordner im angegebenen Laufwerk:Pfad unter dem angegebenen Namen ohne Beschränkung der Verbindungen an die Gruppe Jeder freigegeben. Um die Anzahl der Benutzer zu beschränken, fügen Sie den Schalter `/users:Anzahl` hinzu. Mit der Angabe `/users:50` wird die Anzahl der Benutzer auf 50 beschränkt.

Die vierte Option ist ähnlich wie die dritte, es wird jedoch kein Laufwerk und kein Pfad angegeben (`/users`). Diese Option dient dazu, die Eigenschaften des Pfads zurückzusetzen.

Die fünfte Option ist der Befehl `net share Freigabename /delete`. Damit wird eine Freigabe gelöscht.

4.6.2 Auf freigegebene Verzeichnisse zugreifen

Nachdem die Verzeichnisse nun freigegeben sind, werden Benutzer darauf zugreifen wollen. Dieser Abschnitt bietet einen kurzen Überblick darüber, wie Clients auf Freigaben zugreifen. Die Vorgehensweise ist dabei abhängig von der verwendeten Clientsoftware.

Um auf eine Freigabe zugreifen zu können, muss der Benutzer den Namen des Servers und den der Freigabe kennen, die zusammen den UNC-Namen der Freigabe bilden (UNC = Universal Naming Convention). UNC-Namen haben das Format `\\Server\Freigabe`. Wenn ein Server z.B. »Einstein« heißt und die Freigabe »Relativität«, würde der UNC-Pfad so aussehen: `\\Einstein\Relativität`. Denken Sie daran, dass weder beim Server- noch beim Freigabennamen die Groß-/Kleinschreibung berücksichtigt wird.

Um die Daten in einer Freigabe zu betrachten, haben die Benutzer zwei Möglichkeiten. Sie können der Freigabe einen Laufwerksbuchstaben zuweisen. Dann steht die Freigabe wie ein lokales Laufwerk zur Verfügung. Benutzer können aber auch einfach den UNC-Pfad zur Freigabe angeben.

Die einfachste Möglichkeit, ein Netzlaufwerk zu verbinden, besteht darin, mit der rechten Maustaste auf das Symbol **Arbeitsplatz** zu klicken und im Kontextmenü den Befehl **Netzlaufwerk verbinden** zu wählen. Es öffnet sich das Dialogfeld **Netzlaufwerk verbinden** (siehe Abbildung 4.23), in das Sie den UNC-Namen der Freigabe eingeben oder, je nach Betriebssystem, über die Schaltfläche **Durchsuchen** nach dem Ordner suchen können. Die einzige wichtige Option auf dieser Seite, die von Clientsystem zu Clientsystem besteht, ist das Kontrollkästchen **Verbindung bei Anmeldung wiederherstellen**. Wenn der Benutzer wünscht, dass die Verbindung zum Netzlaufwerk auch das nächste Mal besteht, wenn er sich anmeldet, muss er dieses Kontrollkästchen aktivieren.

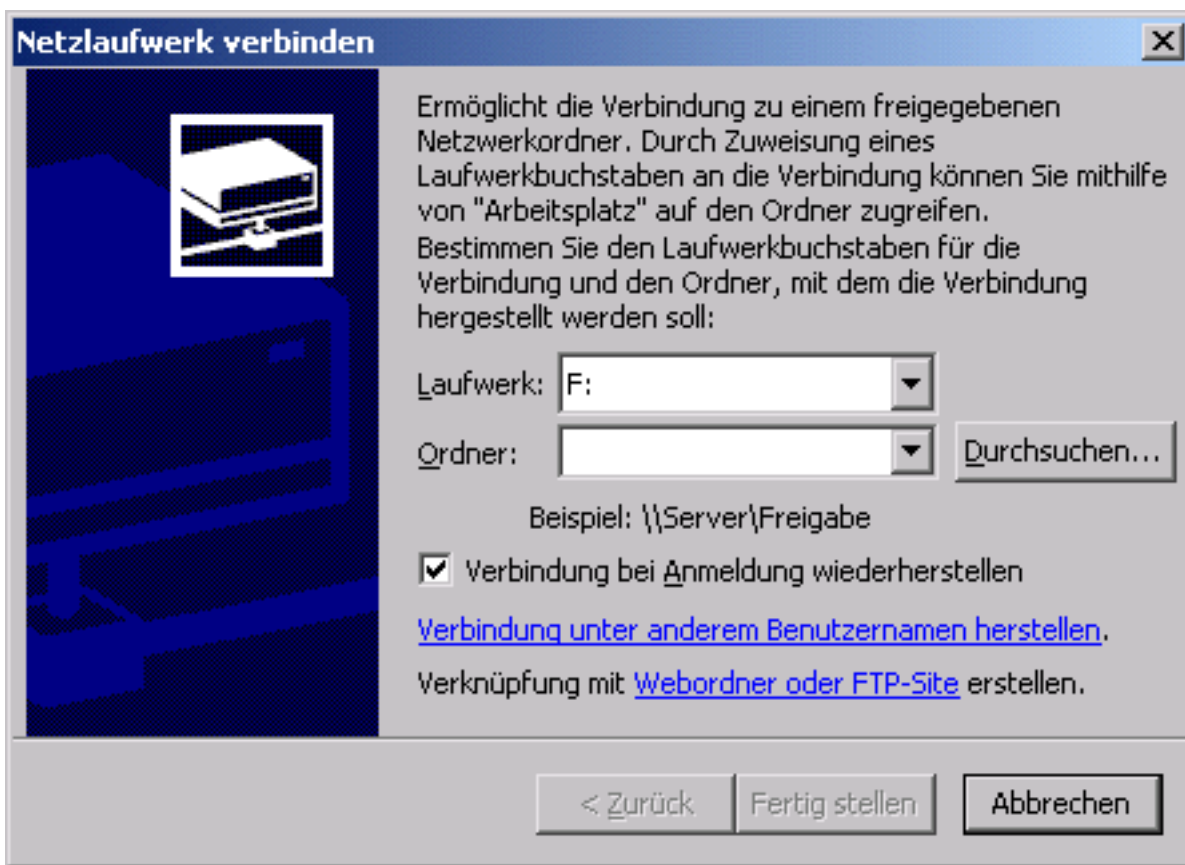


Abbildung 4.23: Um ein Netzlaufwerk zu verbinden, geben Sie entweder den UNC-Pfad zur Freigabe ein oder wählen diesen über die Schaltfläche Durchsuchen aus.

Was passiert, wenn der Benutzer versucht, eine Verbindung zu einer Freigabe herzustellen? Als Erstes sendet der Client das Sicherheitstoken, das er bei der Anmeldung beim Server erhalten hat. Der Server prüft dann, ob der Client auf die Freigabe zugreifen darf. Ist dies der Fall, kann er auf die Freigabe zugreifen.

Wenn die Identifizierung des Tokens fehlschlägt, benutzt das System eine Kombination aus dem Benutzernamen und dem Kennwort. Wenn auch dies fehlschlägt, kann keine Verbindung hergestellt werden. Die nächste Aktion hängt vom Betriebssystem ab. Bei Windows 95 oder Windows 98 wird dem Benutzer der Zugriff verweigert. Bei Windows NT oder Windows 2000 öffnet sich ein Dialogfeld **Verbinden als**. Der Benutzer kann die Authentifizierung nun erneut mit einem anderen Benutzerkonto probieren, indem er einen Benutzernamen und ein Kennwort eingibt.



Eine Verbindung über die Eingabeaufforderung herstellen

Über die Eingabeaufforderung können Sie mit dem Befehl `net use` eine Verbindung zu einer Freigabe herstellen. Dieser Befehl hat vier Operationsmodi. Im ersten Modus, bei dem nur der Befehl `net use` ohne Schalter eingegeben wird, werden alle Verbindungen angezeigt, die der Computer momentan unterhält. Beim zweiten Modus hat der Befehl die Syntax `net use <Laufwerk> <UNC-Pfad>` und verbindet ein Laufwerk mit einem UNC-Pfad. Die dritte Methode dient dazu, eine Verbindung zum Home-Laufwerk des Benutzers herzustellen: `net use <Laufwerk> /HOME`. Der vierte Modus hat die Syntax `net use /persistent:[yes/no]`. Damit wird festgelegt, ob bei der nächsten Anmeldung wieder eine Verbindung zum Laufwerk hergestellt werden soll. Um einfach ein Verzeichnis in einer Freigabe zu betrachten, benutzen Sie den `Dir`-Befehl mit dem vollständigen Pfad, wie z.B. `dir \\intrepid\c$\winnt`.

4.7 Verteiltes Dateisystem (DFS)

Wäre es nicht praktisch, ein großes Dateisystem zu haben, das mehrere Server übergreift? Es wäre auch großartig, wenn dieses Dateisystem die Daten automatisch über das Netzwerk replizieren könnte, sodass Benutzer die Datei von einem Server herunterladen können, der sich in ihrer Nähe befindet.

Das verteilte Dateisystem (DFS = Distributed File System) ist ein neues Merkmal von Windows 2000, mit dem sich ein serverübergreifendes Dateisystem mit automatischer Replikation und Sperrung einrichten lässt, um die Beschädigung von Daten zu verhindern. Das verteilte Dateisystem kann Daten auf Computer verteilen, die weit verstreut sind. Dadurch lässt sich die Fehlertoleranz erhöhen.

Das verteilte Dateisystem hatte eine lange Anlaufzeit. Es gibt schon seit Jahren Betaversionen, aber bisher war es noch nie auf dieser Stufe in das Betriebssystem integriert. Das verteilte Dateisystem bietet einen verteilten und konsistenten Zugriff auf Dateien, sodass Benutzer immer auf dieselbe Weise auf eine Datei zugreifen können. Die Benutzer erhalten dabei immer die aktuelle Datei.

Dieser Abschnitt beschreibt das verteilte Dateisystem. Dabei werden zunächst die allgemeinen Konzepte erklärt, auf denen das verteilte Dateisystem aufbaut. Anschließend wird erläutert, wie das verteilte Dateisystem verwaltet wird. Zum Schluss wird beschrieben, wie Clients über das verteilte Dateisystem auf Dateien zugreifen können.

4.7.1 Konzepte des verteilten Dateisystems

Ein verteiltes Dateisystem beginnt mit einem DFS-Stamm. Dies ist die Spitze einer hierarchischen Struktur, die dem normalen Verzeichnissystem mit Ordnern und Dateien sehr stark ähnelt. Eine DFS-Verknüpfung ist eine Verbindung zwischen einem DFS-Stamm und einem freigegebenen DFS-Ordner. Eine DFS-Verknüpfung verbirgt den tatsächlichen Speicherort der DFS-Freigabe vor dem Benutzer, sodass die Daten von einer beliebigen Anzahl an Standorten innerhalb eines Freigabesatzes abgerufen werden können. Freigegebene DFS-Ordner können bis zu 32 Replikate eines freigegebenen Ordners enthalten.

Freigegebene DFS-Ordner enthalten die normalen freigegebenen Ordner, die nach einer

Replikationsrichtlinie repliziert werden, die von einem Administrator eingerichtet wird. Es stehen folgende Replikationsrichtlinien zur Verfügung:

- *Automatische Replikation.* Bei der automatischen Replikation werden die freigegebenen Ordner nach einem festgelegten Zeitplan repliziert. Der Standardzyklus liegt bei 15 Minuten. Der Dateireplikationsdienst prüft somit alle 15 Minuten, ob alle Replikate synchronisiert sind. Die automatische Replikation kann nur bei NTFS-Partitionen eingesetzt werden.
- *Manuelle Replikation.* Bei der manuellen Replikation muss ein Administrator den Replikationsprozess starten. Wenn große Dateien in einem DFS gespeichert sind oder die Dateien sich nur selten ändern, ist eine manuelle Replikation sinnvoll.

Der DFS-Stamm lässt sich ebenfalls replizieren. Ist der Computer, der den DFS-Stamm enthält, ausgeschaltet, kann das Replikat Anforderungen behandeln.

Es gibt zwei Arten von DFS-Stammverzeichnissen. Wenn ein DFS-Stamm auf einem Domänenserver eingerichtet wird, der in Active Directory teilnimmt, wird der DFS-Stamm als domänenbasiert bezeichnet. Ein domänenbasierter DFS-Stamm ist nicht beschränkt und der DFS-Stamm fungiert als freigegebener DFS-Ordner und kann Dateien enthalten. Außerdem wird ein domänenbasierter DFS-Stamm in Active Directory veröffentlicht, sodass darauf leichter zugegriffen werden kann.

Ein eigenständiger DFS-Stamm kann nur eine Ebene beinhalten (d.h. ein DFS-Stamm verweist nur auf einen Satz freigegebener DFS-Ordner). Außerdem kann der DFS-Stamm keine freigegebenen Ordner enthalten. Deshalb müssen sich alle Daten auf der anderen Seite einer DFS-Verknüpfung befinden.

Dateien, die in DFS gespeichert werden, werden lokal von jedem Client zwischengespeichert, der auf die DFS-Struktur zugreift. Es lässt sich ein Intervall festlegen, nach dem der Client prüft, ob eine neuere Version einer Datei im Zwischenspeicher repliziert wurde.

4.7.2 Das verteilte Dateisystem einrichten

Öffnen Sie über die Systemsteuerung die **Verwaltung** und klicken Sie doppelt auf das Objekt **Verteiltes Dateisystem (DFS)**. Um ein verteiltes Dateisystem einzurichten, wählen Sie im Menü **Vorgang** den Befehl **Neuen DFS-Stamm**. Der **Assistent zum Erstellen eines neuen DFS-Stamms** wird nun gestartet und stellt Ihnen verschiedene Fragen, um den DFS-Stamm einzurichten. Wählen Sie, ob Sie einen Domänen-DFS-Stamm oder einen eigenständigen DFS-Stamm einrichten möchten (siehe Abbildung 4.24). Klicken Sie dann auf **Weiter**. Geben Sie im nächsten Schritt den Namen des Servers ein, der als Host für den DFS-Stamm verwendet werden soll, und klicken Sie auf **Weiter**. Geben Sie im nächsten Schritt den Namen der Freigabe und des Servers ein, der den DFS-Stamm beherbergt, und klicken Sie auf **Weiter**. Zum Schluss wird die Zusammenfassung angezeigt. Klicken Sie auf **Fertig stellen**, um den DFS-Stamm einzurichten.

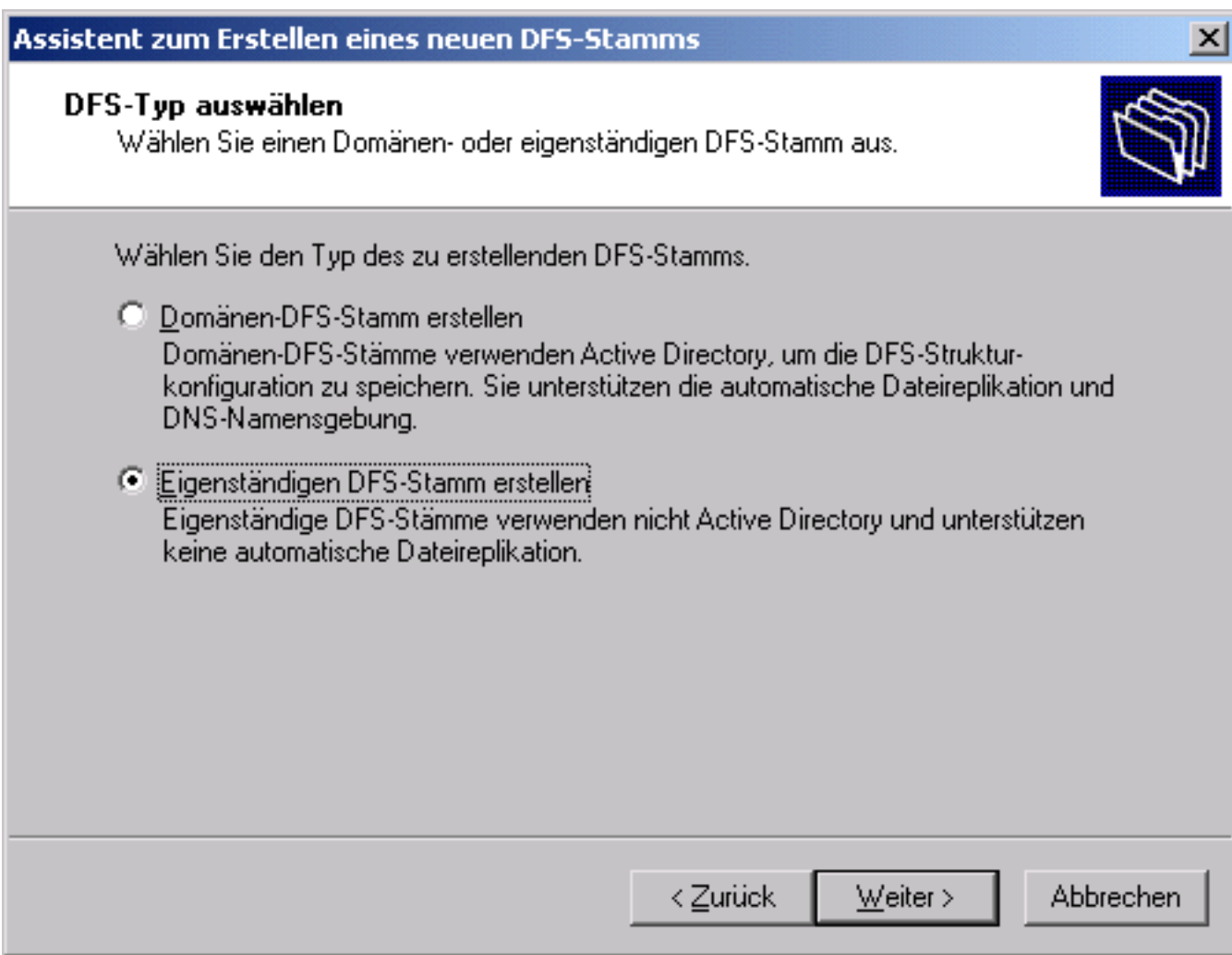


Abbildung 4.24: Der neue Assistent zum Erstellen eines neuen DFS-Stamms führt Sie durch die Implementierung des verteilten Dateisystems

4.7.3 Das verteilte Dateisystem nutzen

Um von einem DFS-Client eine Verbindung zu einem DFS-Stamm herzustellen, öffnen Sie in der Systemsteuerung die **Verwaltung** und klicken in dieser doppelt auf das Element **Verteiltes Dateisystem (DFS)**. Wählen Sie dann im Menü **Vorgang** den Befehl **Einen vorhandenen DFS-Stamm anzeigen**. Sie werden aufgefordert, den Namen des DFS-Stamms einzugeben. Der Name eines DFS-Stamms kann auf drei Arten angegeben werden. Bei Domänen-DFS-Stämmen kann die Angabe `\\<Domäne>\<Stamm>` benutzt werden, wobei `<Domäne>` der voll qualifizierte Domänenname für die Domäne ist (z.B. `\\intrepid.com\dfsroot`). Bei eigenständigen DFS-Stämmen sind die Angaben `\\<Server>\<Stamm>` und `\\<Server>\<freigegebener Ordner>` gültig. Der DFS-Stamm kann über die DFS-Anwendung durchsucht werden.

4.8 Remotespeicher

Der Remotespeicher ist ein System, mit dem sich Wechselmedien wie Bandlaufwerke, CD-ROM-Laufwerke oder optische Laufwerke wie normale Laufwerke über das Netzwerk verwenden lassen. Der Remotespeicher unterhält einen Katalog aller Dateien, die auf den Medien enthalten sind, und

verwendet die Wechselmedienverwaltung um festzustellen, wo sich die verschiedenen Medien befinden, und um die Dateien zu laden. Die Wechselmedienverwaltung wird im nächsten Abschnitt beschrieben.

Um was geht es also? Um ein System, über das sich Dateien automatisch von einem Bandlaufwerk abrufen lassen, sofern dieses online ist (entweder in einem Bandlaufwerk oder einem Laufwerkswechsler). Die Anforderungen können auch in eine Warteschlange gesetzt werden.

Dieses System erlaubt es, alte oder selten benutzte Dateien auf Band zu archivieren und ohne die Intervention des Administrators wieder zu benutzen. Dieses Konzept ist schon alt. Bei Mainframe-Computern besteht die Möglichkeit, Daten automatisch von Bandlaufwerken abzurufen, schon seit langem und selbst automatische Bandwechsler gibt es schon seit langem. Dieses System bietet die Möglichkeit, in kurzer Zeit auf die immensen Bandlaufwerksspeicher zuzugreifen. Bandlaufwerke sind erheblich preisgünstiger und lassen sich leichter erweitern und verwalten als Festplattenspeicher. Um Dateien zu archivieren, bietet der Remotespeicher den Benutzern viele Vorteile.

4.8.1 Das Konzept des Remotespeichers

Der Remotespeicher verwendet einen Datenträger auf einer Festplatte als Schnittstelle zwischen dem Benutzer und den Dateien auf dem Bandlaufwerk. Die Dateien werden auf den Datenträger kopiert und dann überwacht der Remotespeicher die Verwendung des Datenträgers und entfernt Dateien aus dem Dateisystem, die nur selten benutzt werden. Die Dateien werden so entfernt, dass die Dateinamen an Ort und Stelle bleiben und nur die eigentlichen Daten entfernt werden.

Wenn ein Benutzer eine Datei anfordert, findet der Remotespeicher automatisch heraus, auf welchem Band die Datei gespeichert ist und ruft sie vom Band ab. Dies kann eine Weile dauern. Deshalb ist es wichtig, die Benutzer entsprechend zu informieren.

4.8.2 Remotespeicher einrichten

Wenn Sie den Remotespeicher nicht bereits bei der Installation von Windows 2000 installiert haben, können Sie dies nun nachholen. Klicken Sie in der Systemsteuerung doppelt auf **Software** und wählen Sie im Ordner **Software** die Schaltfläche **Windows-Komponenten hinzufügen/entfernen**. Aktivieren Sie im **Assistent für Windows-Komponenten** den **Remotespeicher** und überlassen Sie dann dem Assistenten die Installation. Warten Sie nach der Installation, bis die Empfehlung eingeblendet wird, das System neu zu starten.

Öffnen Sie nach dem Neustart die Computerverwaltung, klicken Sie auf **Datenspeicher** und öffnen Sie den Ordner **Remotespeicher**.

4.9 Die Wechselmedienverwaltung

Die Wechselmedienverwaltung ist ein System, um Medienbibliotheken zu verwalten, wie z.B. Bibliotheken von Bandlaufwerken oder optischen Datenträgern. Über die Wechselmedienverwaltung können Sie anders als beim Remotespeicher keine Datenträger erweitern, sondern es werden Anwendungen wie der **Sicherung** und dem **Remotespeicher** Informationen zur Verfügung gestellt, wo welche Daten abgelegt sind.

Die Wechselmedienverwaltung verwendet zwei Arten von Gruppierungen: Eine Bibliothek Hardware, die Wechselmedien lesen kann. Eine Jukebox für optische Datenträger ist ein Beispiel für eine solche Bibliothek oder auch ein Laufwerkwechsler. Es gibt zwei Arten von Bibliotheken. Eine Roboterbibliothek wechselt die Medien automatisch und eine eigenständige Datenträgerbibliothek ist ein Wechselmedium, bei dem der Benutzer oder Administrator die Medien wechseln muss.

Ein *Medienpool* ist eine logische Gruppe von Medien, mit der Band- oder andere Laufwerke gruppiert werden. Ein Medienpool kann nur Medien (wie einzelne Bandlaufwerke) oder andere Medienpools beinhalten. Er enthält folgende Kategorien: **Freie Medien**, **Importmedien**, **Nicht erkannte Medien** und **Anwendungsmedien**.

Ein nicht erkannter Medienpool enthält Bandlaufwerke, die noch nicht initialisiert wurden. Nicht erkannte Medien können dem Medienpool **Freie Medien** zugewiesen werden. Dabei werden die Medien initialisiert und stehen zur Benutzung zur Verfügung.

Der Medienpool **Importmedien** besteht aus einem Satz von Medien, die nicht von der Wechselmedienverwaltung auf diesem Computer erkannt wurden, aber von einer anderen Wechselmedienverwaltung. Normalerweise kommt dies vor, wenn Wechselmedien, die bisher an einem Computer angeschlossen waren, an einem anderen Computer angeschlossen werden. Oder auch, wenn Wechselmedien von einem Büro in ein anderes gebracht werden. Medien in diesem Medienpool können entweder in den Medienpool **Freie Medien** verschoben werden, wo sie überschrieben werden, oder in den Medienpool **Anwendungsmedien**, wo sie benutzt werden.

Der Medienpool **Freie Medien** enthält Medien, die bisher noch keiner Anwendung zugewiesen wurden. Das heißt, die Medien lassen sich noch frei nutzen.

Der Medienpool **Anwendungsmedien** enthält Medien, die momentan von einer Anwendung genutzt werden, wie z.B. der **Sicherung**. Eine Anwendung kann mehrere Medienpools steuern. Die Anwendung **Sicherung** kann z.B. einen Medienpool für vollständige Sicherungen und einen für inkrementelle Sicherungen enthalten.

Medienpools werden über die Computerverwaltung verwaltet. Öffnen Sie dazu in der Computerverwaltung den Ordner **Datenspeicher** und in diesem den Ordner **Wechselmedien**. Dieser enthält vier Elemente: **Medienpools**, **Ressourcen**, **Warteschlange** und **Operatoranforderungen**.

Der Ordner **Medienpool** dient dazu, Medienpools zu erstellen und zu verwalten. Um einen neuen Medienpool zu erstellen, markieren Sie den Ordner **Medienpools** und klicken auf die Schaltfläche **Neuer Medienpool**. Es öffnet sich das Dialogfeld **Eigenschaften von Neuem Medienpool erstellen** (siehe Abbildung 4.25). Geben Sie den Namen und eine Beschreibung für den Medienpool ein und definieren Sie dann, was der Medienpool enthalten wird. Ein Medienpool kann vom Diskettenlaufwerk bis zu DLT-Bändern alles enthalten. Die Medien in einem Medienpool müssen jedoch gleich sein. Wählen Sie im Bereich **Richtlinien für Zuordnungen**, wie die neuen Medien erstellt und aus dem Pool entfernt werden. Medien lassen sich manuell per Drag & Drop zu einem Pool hinzufügen, nachdem dieser eingerichtet wird. Sie lassen sich aber auch automatisch neu zuordnen, wenn der Pool Speicherplatz benötigt. Wenn ein Medium nicht mehr benötigt wird, kann die Zuordnung aufgehoben werden und es kann in den Medienpool **Freie Medien** zurückgenommen werden.

Eigenschaften von Neuen Medienpool erstellen [?] [X]

Allgemein | Sicherheitseinstellungen

Name:

Beschreibung:

Typ: Anwendungsspezifische Medien

Medieninformationen

☐ Enthält andere Medienpools

☒ Enthält Medien des Typs:

CD-R

Richtlinien für Zuordnungen

☐ Medien aus dem Pool freier Medien nehmen

☐ Medien in den Pool freier Medien zurückgeben

☐ Limit für Neuzuordnungen: 100

OK Abbrechen

Abbildung 4.25: Im Dialogfeld **Eigenschaften von neuen Medienpool erstellen** wird der neue Medienpool definiert.

Der Ordner **Ressourcen** enthält alle physischen Geräte, die mit dem Computer verbunden sind. Hier können Sie einrichten, welche Geräte der Wechselmedienverwaltung zur Verfügung stehen sollen.

Das Element **Warteschlange** enthält die Anforderungen, die momentan von der Wechselmedienverwaltung verarbeitet werden sowie deren Status. Wenn z.B. eine Sicherung durchgeführt wird, enthält die Warteschlange den Status des Jobs und es wird aufgeführt, welche Bandlaufwerke benutzt werden.

Das Element **Operatoranforderungen** enthält die noch nicht bearbeiteten Operatoranforderungen. Eine Operatoranforderung ist eine Anforderung an den Operator, Medien im Laufwerk zu wechseln, indem entweder ein neues Band oder das bereits bestehende Band wieder eingelegt wird.

Kapitel 5 Netzwerke

5.1 Microsofts Netzwerkkonzepte

Wenn Sie in diesem Kapitel Anleitungen suchen, um Benutzer oder ein Active Directory einzurichten, sind Sie an der falschen Stelle. Mehr hierzu finden Sie in Teil III des Buches. Wenn Sie jedoch kurz Luft holen und Informationen über die Netzwerk- und Sicherheitskonzepte von Microsoft erhalten möchten, sind Sie hier richtig.

Dieses Kapitel führt Sie in die Grundkonzepte von Microsoft-Netzwerken ein. Ein Grundverständnis der Netzwerkkonzepte hilft Ihnen, wenn Sie Entscheidungen zur Infrastruktur der Computer in einem Netzwerk treffen müssen. Im Verlauf des Buches werden verschiedene Hardwarekomponenten und Verwaltungsprogramme beschrieben. Dieses Kapitel legt den Grundstein, um diese Systeme zu verstehen.

Um ein Windows 2000-Netzwerk verwalten zu können, sollten Sie die Grundkonzepte der Netzwerktechnologie von Microsoft kennen. Dies bedeutet nicht, dass Microsoft PCs mit Angelschnüren und -haken miteinander verbindet, oder dass die Dinge sich so grundsätzlich unterscheiden, dass ein erfahrener Netzwerkingenieur sie nicht wiedererkennen kann. Microsoft hat jedoch eigene Nuancen und diese zu kennen, kann sehr nützlich sein.

Die meisten Besonderheiten von Microsoft-Netzwerken sind nicht neu. Es gibt sie schon seit der Einführung der Microsoft-NetBIOS-Netzwerke Anfang und Mitte der achtziger Jahre. Wenn Sie jedoch bisher noch nichts mit Windows NT, LAN Manager oder sogar LANtastic zu tun hatten, erhalten Sie hier die so sehr benötigten Grundlagen.

Ein Hauptmerkmal von Microsoft Windows-Netzwerken ist die Art und Weise, wie Windows die Berechtigungen für Ressourcen verwaltet. Ein Microsoft-Netzwerk ist zunächst ein offenes System. Wenn eine Ressource wie beispielsweise ein Netzwerkdrucker oder ein Ordner freigegeben wird, haben zunächst alle Benutzer einen Vollzugriff darauf. Um den Zugriff auf die freigegebene Ressource zu steuern, muss der Administrator aktiv die Berechtigungen für die Ressourcen ändern.

Im Gegensatz dazu sind die meisten anderen Netzwerkbetriebssysteme zunächst geschlossen. Wenn Ressourcen eingerichtet werden, werden dafür normalerweise zunächst keine Berechtigungen vergeben. Standardmäßig hat also ausschließlich der Administrator Zugriff auf die Ressourcen und er kann dann festlegen, wer welche Zugriffsberechtigungen hat.

Es ist schwer zu sagen, was besser ist. Aber ohne sich dieses Unterschieds bewusst zu sein, könnte es einem NetWare-Administrator z.B. leicht passieren, dass er das Burgtor weit offen stehen lässt (ganz zu schweigen von der Datei mit den Gehaltsdaten).

5.1.1 Arbeitsgruppen und Domänen

In Windows 2000 haben sich viele Features geändert. Arbeitsgruppen und Domänen bleiben aber die Säulen der Benutzerkontenverwaltung. Workstation-Computer, Benutzer und Gruppen werden in diesen beiden Formen organisiert, aktiviert und verwaltet. Um die Verwaltung von Active Directory zu

verstehen, müssen Sie sich zuerst mit diesen beiden Formen der Verwaltung auseinandersetzen.

Arbeitsgruppen

Das Arbeitsgruppen-Modell kommt in Peer-to-Peer-Netzwerken mit fünf bis zehn Benutzern zum Einsatz. Dies liegt an der Art und Weise, in der Arbeitsgruppen Benutzer und Gruppen verwalten.



Der Begriff Peer-to-Peer entspringt der Tatsache, dass es in einem solchen Netzwerk keinen Computer gibt, der als »Server« oder als »Client« betrachtet wird. Alle Computer dienen sowohl als Server als auch als Clients. Deshalb sind sie Gleichgestellte (engl. *Peers*).

Arbeitsgruppen setzen sich aus Windows 2000-, Windows 95/98-, Windows NT- und Windows für Workgroups-Computern zusammen. Die Computer werden in derselben Gruppe in der Netzwerkumgebung angezeigt. Wenn Benutzer aus einer Arbeitsgruppe versuchen, auf freigegebene Ressourcen zuzugreifen, können sie alle Ressourcen auf Computern benutzen, die in der Arbeitsgruppe enthalten sind. Aus diesem Grund wäre es exakter, Arbeitsgruppen als Zusammenschluss von Computern und nicht von Benutzern zu beschreiben. Dass Sie eine Ressource sehen können, heißt nicht, dass Sie Zugriff darauf haben oder dass für Sie ein Benutzername auf dem Server eingerichtet ist.

In einer Arbeitsgruppe muss jeder Server Benutzer und Gruppen verwalten (siehe Abbildung 5.1). Diese Benutzer- und Gruppenlisten werden nicht freigegeben und Benutzer von einer fremden Liste können nicht auf die Ressourcen eines Computers zugreifen. Wenn ein Benutzer z.B. bei Server A in der Arbeitsgruppe 1 authentifiziert wurde, hat er keinen Zugriff auf die Ressourcen auf Server B, obwohl sich Server B in derselben Arbeitsgruppe befindet. Möglicherweise existiert auf Server B nicht einmal ein Benutzerkonto für ihn.

Wird ein Benutzername nebst Kennwort auf allen Servern in der Arbeitsgruppe manuell eingerichtet - was häufig geschieht -, kann der Benutzer auf alle Server zugreifen. Der Benutzer würde dann einmal seinen Namen und das Kennwort eingeben. Wenn er versucht, auf einen anderen Server zuzugreifen, behält er einfach den bereits eingegebenen Benutzernamen und das Kennwort bei. Dies ist für den Benutzer komfortabel. Der Administrator muss jedoch auf allen Computern dieselbe Benutzerliste warten.

In einem Peer-to-Peer-Netzwerk werden die Benutzer sehr wahrscheinlich nur sehr wenige Ressourcen freigeben. Peer-to-Peer-Netzwerke haben ihren Ursprung darin, dass sich kleine Unternehmen sehr teure Ressourcen wie den ursprünglichen Hewlett-Packard LaserJet-Drucker nicht für jeden Arbeitsplatz leisten konnten. Die Lösung bestand darin, die PCs miteinander zu verbinden und den Drucker freizugeben. Wenn nur eine kleine Anzahl an PC-Dateien, Freigaben oder Druckern freigegeben wird, ist es für die einzelnen Benutzer kein so großer Aufwand, eine Benutzerliste zu pflegen.

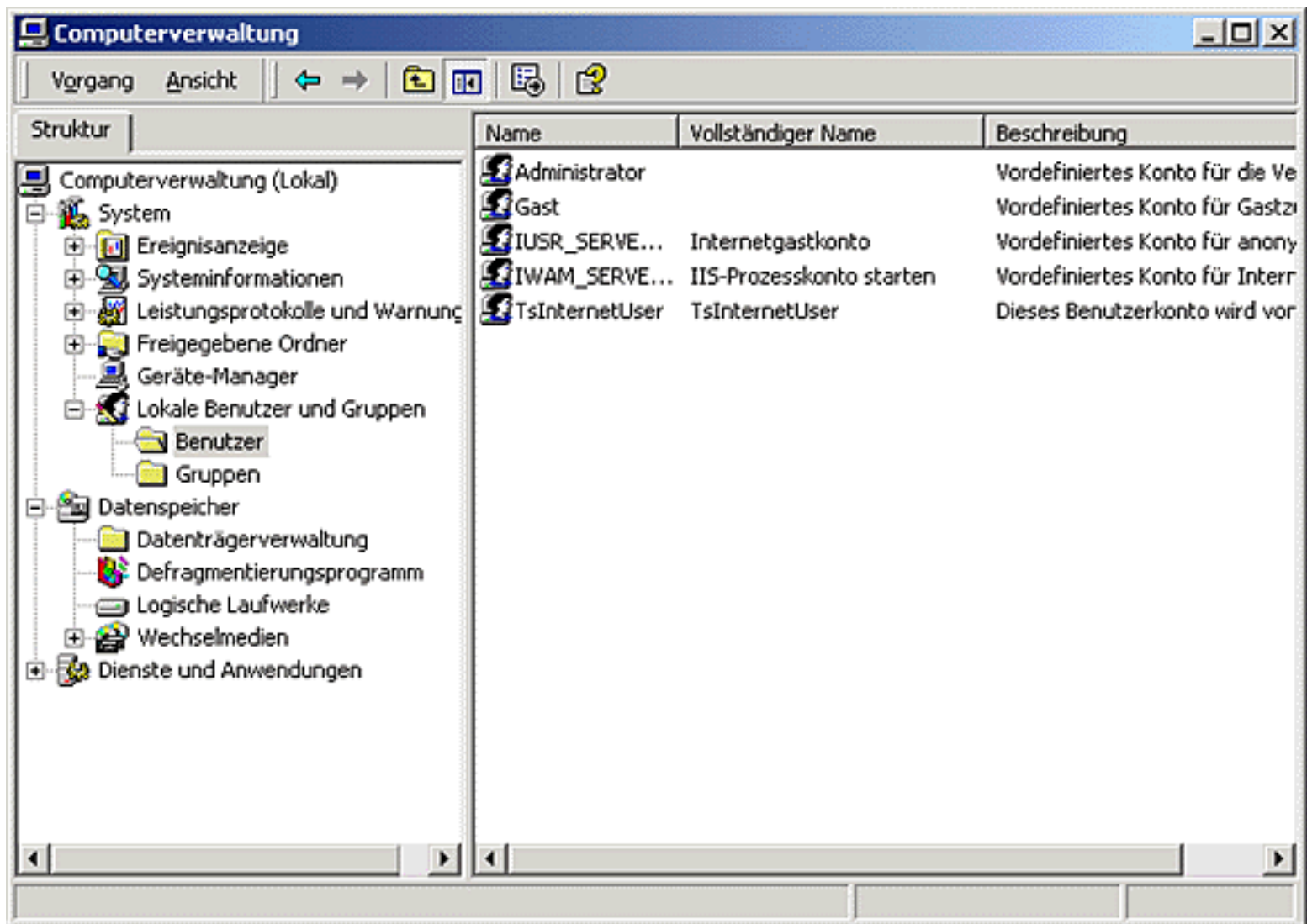


Abbildung 5.1: Der Benutzermanager in einer Arbeitsgruppe.

Wenn ein Benutzer in einem kleinen Unternehmen einen neuen Drucker an seinen Computer anschließt, kann er diesen einfach installieren und freigeben (siehe Abbildung 5.2). Nachdem der Benutzer den Drucker freigegeben hat, können alle Computer in der Arbeitsgruppe den Computer und die Ressourcen in der *Netzwerkumgebung* sehen (siehe Abbildung 5.3). Der Benutzer kann dann Berechtigungen für die Ressource in seiner Benutzerliste einrichten.

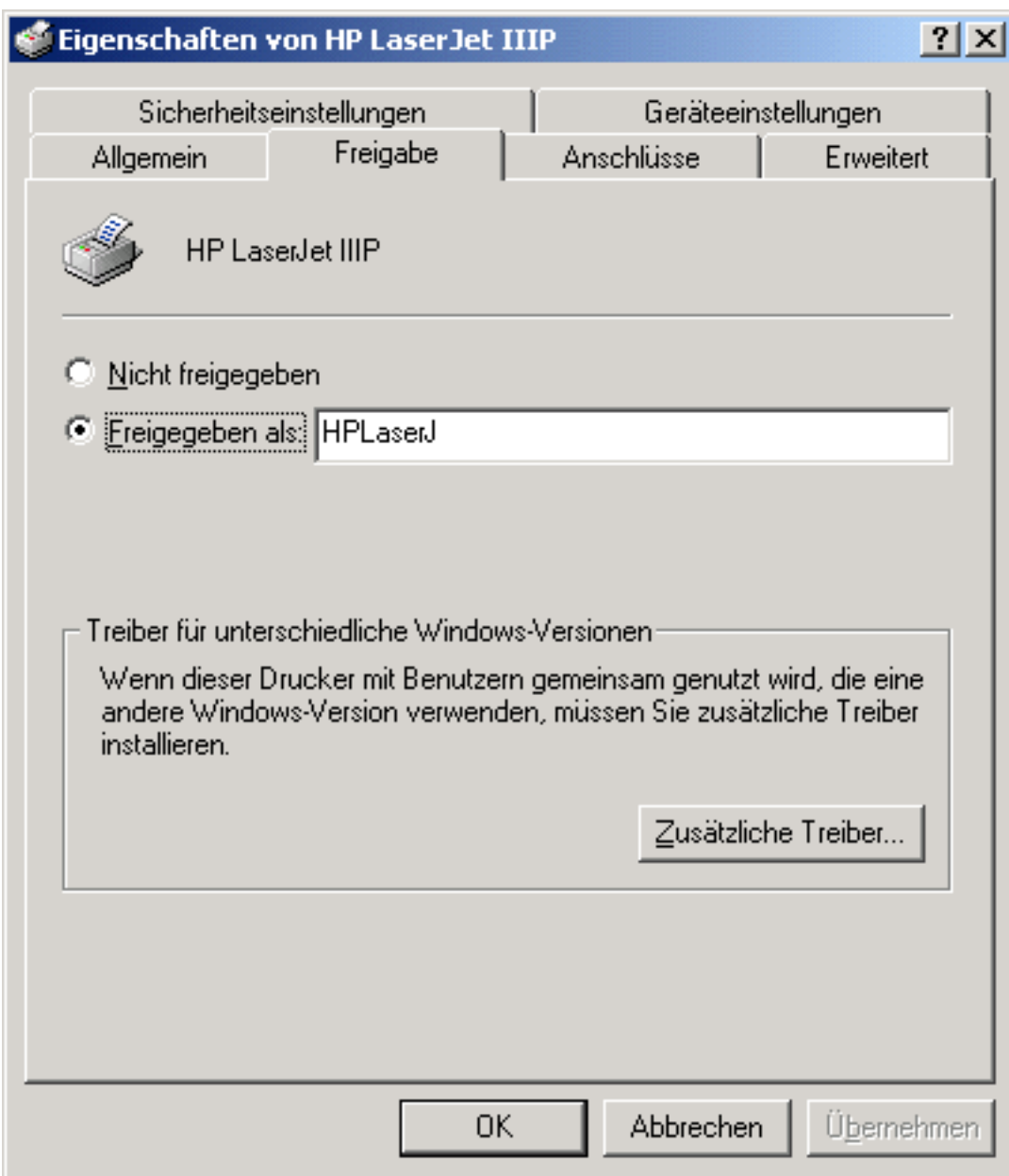


Abbildung 5.2: Die Registerkarte Freigabe.

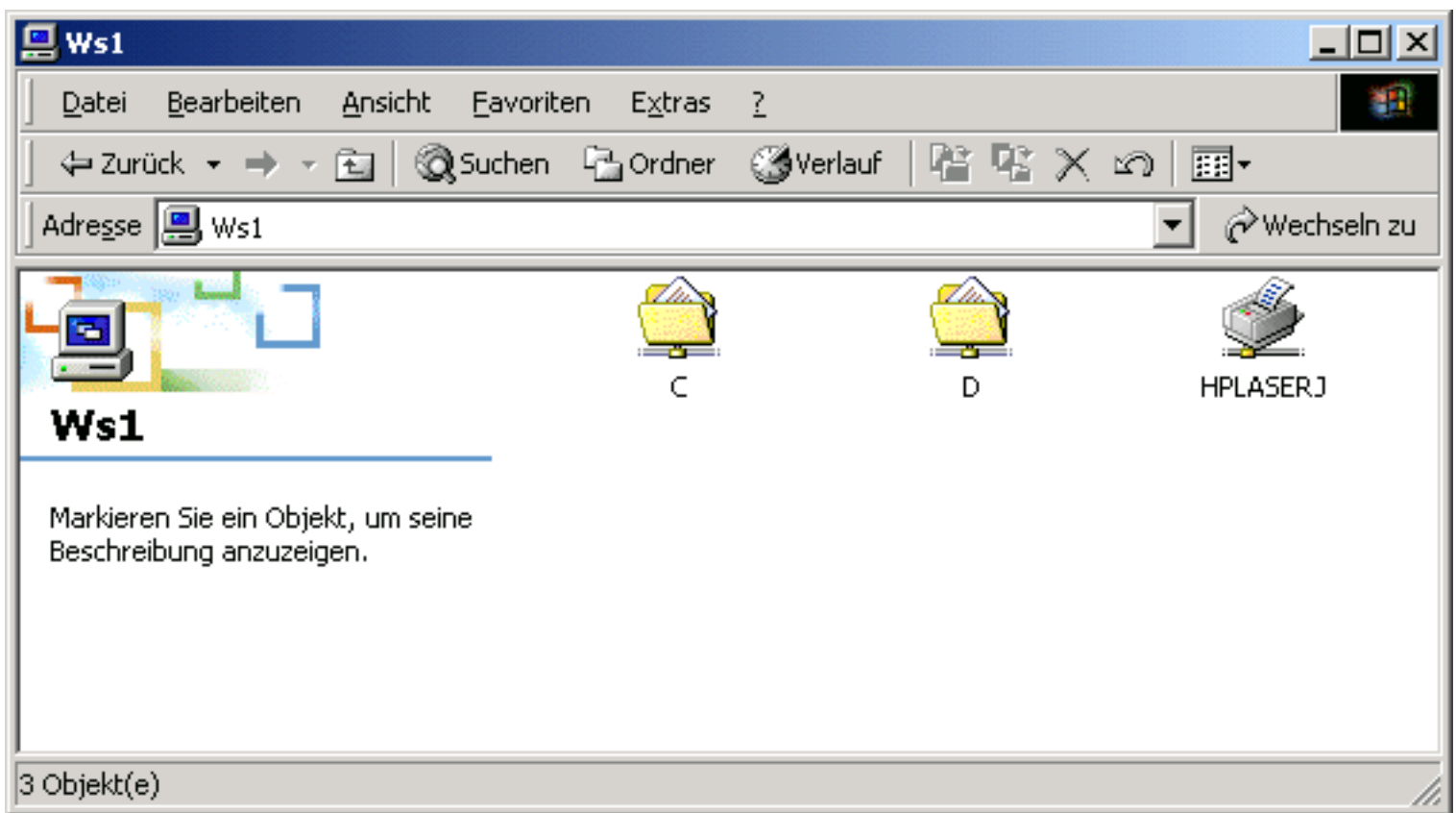


Abbildung 5.3: Die Netzwerkumgebung mit freigegebenen Ordnern und Druckern.

Wenn das Netzwerk jedoch mehr als fünf bis zehn Benutzer oder Freigaben enthält, stürzt das gesamte Modell in sich zusammen. Wichtig ist hier, dass der Administrator die Benutzer, Gruppen und Berechtigungen für jede Freigabe auf dem Server verwalten muss, der die freigegebenen Ressourcen bereitstellt. Der Administrator eines Peer-to-Peer-Netzwerks mit 100 PCs müsste z.B. 100 separate Benutzerlisten, 100 verschiedene Gruppenkonfigurationen und 100 verschiedene Ressourcensammlungen verwalten. Dazu müsste er alle 100 Server manuell einrichten.

In einer solchen Umgebung ist der Einsatz des Domänenmodells sinnvoll.

Domänen

In Windows 2000 ist das Domänenmodell zum Bestandteil eines wesentlich umfassenderen Schemas namens Active Directory geworden und Domänen sind Bestandteil der Active Directory-Installation. In diesem Abschnitt soll jedoch nur das Domänenmodell beschrieben werden. Active Directory ist ein eigenes Kapitel gewidmet.

Wenn ein Netzwerk sehr viele Benutzer und Ressourcen enthält, eignet sich das Domänenmodell besser als das Arbeitsgruppenmodell zur Verwaltung des Netzwerks. Eine Domäne ist eine Sammlung von Benutzerkonten und Gruppen von Benutzerkonten, die von mehreren Servern gemeinsam genutzt werden (siehe Abbildung 5.4). Im Domänenmodell lassen sich alle Computer, Benutzer und Gruppen zentral verwalten. Für große Organisationen ist dies wesentlich attraktiver als das Arbeitsgruppenmodell.

Das Benennungsschema von Domänen sollte Internetnutzern bekannt sein. Die Benennungskonventionen in Windows 2000 folgen dem Domain Name System (DNS), das im Internet verwendet wird.

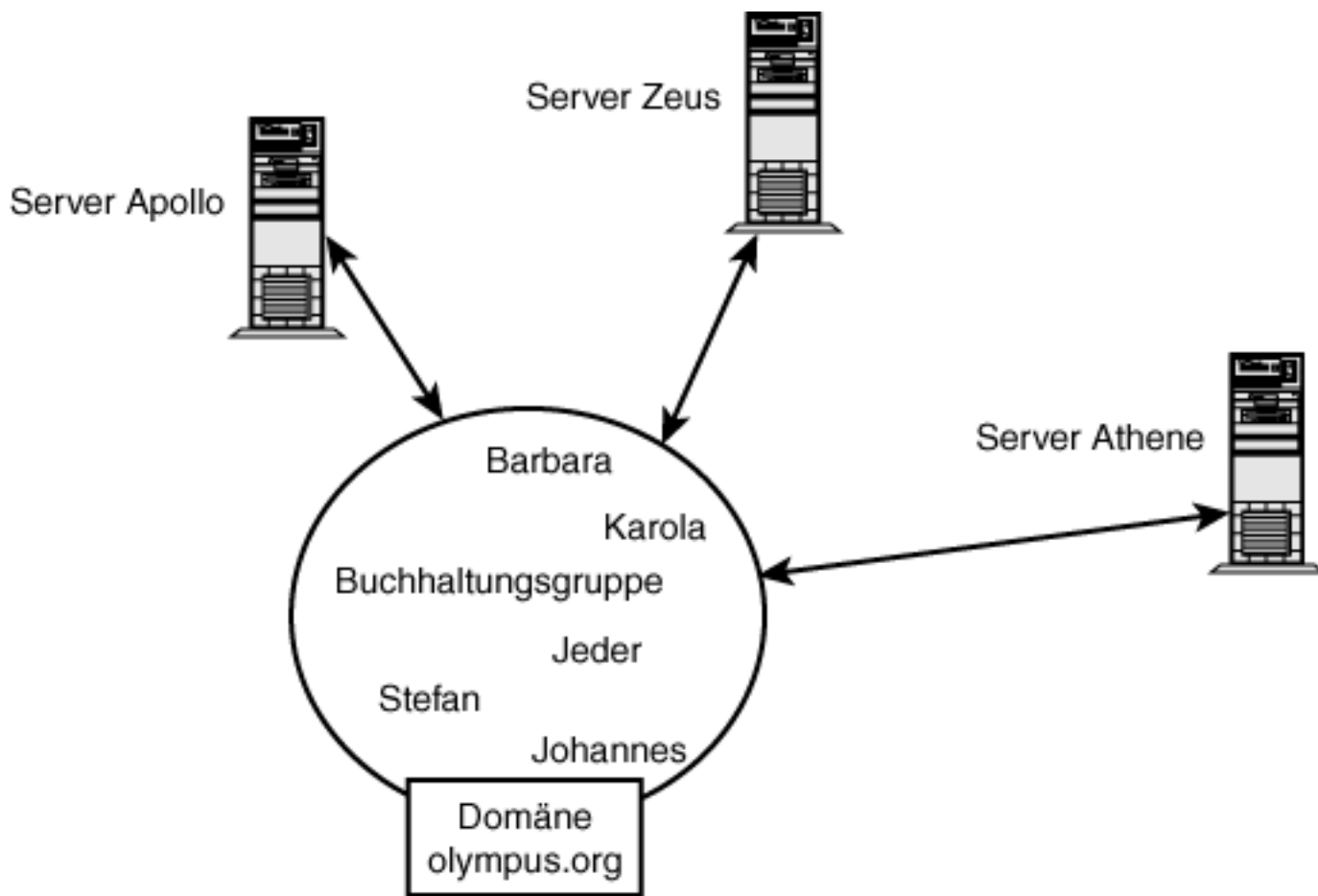


Abbildung 5.4: Das Konzept einer Domäne.

Beim DNS gibt es sechs Topleveldomänen, d.h. übergreifende Namenskategorien, für Domänen in den USA sowie Länderkürzel für Domänen in allen übrigen Ländern, wie z.B. *.de* für Deutschland oder *.fr* für Frankreich, denen alle weiteren Domänen untergeordnet sind. Diese Topleveldomänen und Länderkürzel sind den Domännennamen als Suffixe angehängt. Aus diesem Schema resultieren Domännennamen wie *microsoft.com* oder *yahoo.de*. Es gibt die folgenden Topleveldomänen:

- *.com* für kommerzielle Unternehmen
- *.edu* für Bildungsinstitutionen in den USA
- *.gov* für Regierungsbehörden in den USA
- *.mil* für militärische Organisationen in den USA
- *.net* für Netzerkanbieter
- *.org* für gemeinnützige Organisationen

Dadurch, dass in Windows 2000 nun das DNS-Benennungssystem zur Benennung von Domänen verwendet wird, steht ein globales Standardbenennungsschema zur Verfügung. Windows 2000-Server lassen sich damit global an jedem beliebigen Standort einsetzen, wenn der DNS-Server registriert und mit dem Internet verbunden ist. Einzelheiten zur Registrierung des Domännennamens bei InterNic finden Sie in Kapitel 8. In diesem Kapitel brauchen Sie nur zu wissen, woher die Benennungskonvention stammt.

Das Konzept der Domänen wurde erweitert, sodass Domänen nun über so genannte Domänenstrukturen miteinander verbunden werden können.

Domänenstrukturen

Eine Domänenstruktur ist eine Sammlung von Domänen, die weitere Domänen und Subdomänen in einer DNS-Hierarchie enthält. Die Stammdomäne in einer Domänenstruktur kann einen DNS-Namen wie z.B. `yahoo.de`, `indiana.edu` oder `mcp.com` tragen). Der Name der untergeordneten Domänen wird auf der Basis der Domänenstruktur gebildet. Das heißt, der Name der Unterdomäne wird dem der Stammdomäne vorangestellt, wie z.B. bei den Domänen `sams.mcp.com` und `architecture.indiana.edu`.

Die einzelnen Domänenstrukturen lassen sich zu übergeordneten Strukturen, so genannten Gesamtstrukturen, zusammenfassen, die keinen gemeinsamen Domänennamen benutzen müssen. Die Domäne `mcp.com` kann z.B. mit der Domäne `indiana.edu` zur einer Gesamtstruktur verknüpft werden. Die Stammdomäne kann dann z.B. `bellind.com` heißen. Der Name der Stammdomäne muss also nichts mit den Namen der einzelnen Domänenstämme zu tun haben.

Die meisten Unternehmen werden niemals eine Größe erreichen, bei der es nötig wäre, solche Gesamtstrukturen mit Stammdomänen einzurichten. Bei dem momentanen Trend zur Globalisierung von Unternehmen wird dies jedoch zukünftig öfter erforderlich sein. Dank des neuen Domänenmodells und Benennungsschemas ist dies auch problemlos möglich.

Organisationseinheiten

Die Domänen sind größer geworden und sie lassen sich außerdem in kleinere Einheiten aufteilen. Diese Einheiten heißen Organisationseinheiten (OU = Organizational Unit). Wenn Sie mit der Welt von NetWare NDS vertraut sind, werden Sie hier etwas Altbekanntes wiedererkennen, das bereits seit Jahren existiert. Falls Sie dieses Konzept noch nicht kennen, finden Sie nachfolgend eine Beschreibung.

Es ist noch immer so, dass die Überwachung innerhalb der Grenzen der Domäne erfolgt. Aus diesem Grund wurde das Domänenmodell häufig kritisiert. Ein Domänenadministrator hat alle Macht und es gibt wenig Möglichkeiten, das Modell feinkörniger zu machen.

Der Administrator einer Domäne kann nun aber Container (Organisationseinheiten) einrichten, Objekte in diesen Containern erstellen und verschiedenen Administratoren die Verantwortung für diese Container übertragen (siehe Abbildung 5.5). Der Administrator kann jedoch weiterhin den Domänenstamm überwachen. Dies verleiht dem Domänenmodell erheblich mehr Flexibilität als bisher und lässt auch ein Wachstum zu.

Durch die Aufteilung der Verwaltung kann die Arbeitslast von einem einzelnen Administrator genommen werden. Die Flexibilität der Informationsnetzwerke innerhalb von Unternehmen lässt sich so erhöhen.

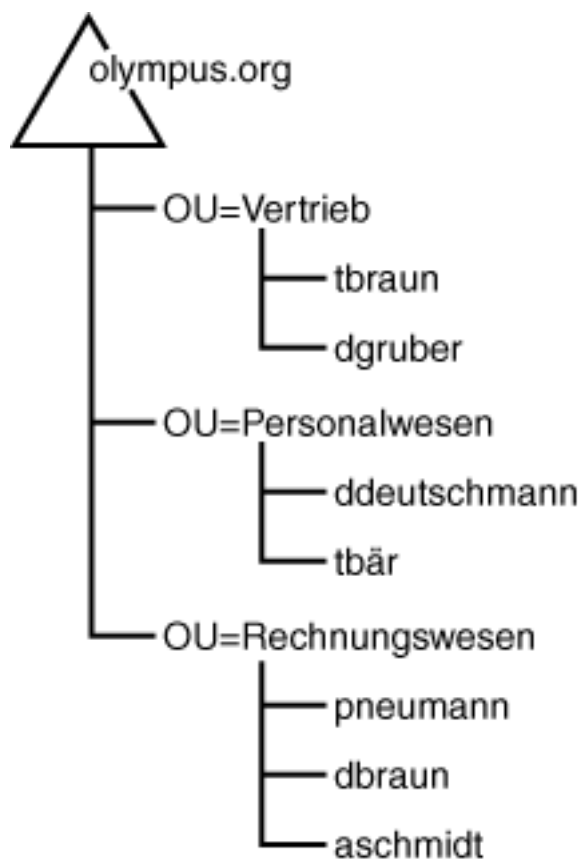


Abbildung 5.5: Die Organisationseinheiten in einer Domäne.

Domänenkontrolle

An dieser Stelle werden die Änderungen in Windows 2000 ganz offensichtlich und sie entsprechen auch dem, was schon lange erwünscht war. Domänen sind nun, was die Anpassung der Größe und die sonstigen Möglichkeiten betrifft, erheblich flexibler.

Die Domänenkontrolle beinhaltet die Verwaltung und die Verteilung von Domäneninformationen auf den Servern im Netzwerk. Wenn an der Definition eines Benutzers oder einer Gruppe eine Veränderung vorgenommen werden muss, muss eine Autorität eingerichtet werden, damit dieses System funktioniert. Um Wachstum zuzulassen, muss ein Weg gefunden werden, die Veränderungen auf mehr als einem Computer zu speichern und den Zugriff auf diese Informationen zu erleichtern. Dies ist mit der Domänenkontrolle möglich.

DNS-Master

Eine Domäne wird auf dem ersten Server in der Domäne erstellt und dieser Server ist für einen Augenblick der DNS-Master. Diese Tatsache ist sehr wichtig, weil Sie wissen müssen, dass Domänen Informationssammlungen sind, die zentral gesteuert werden müssen. Diese Ebene der Kontrolle kann später auf einen anderen Server übertragen werden, aber während der Lebensdauer einer Domäne ist in einer strikten Domänenumgebung ein Computer für die Aufzeichnung verschiedener Änderungen in der Domäne verantwortlich.

Bei Windows NT Server wurden alle Änderungen in einer Domäne von einem Computer überwacht. Bei Windows 2000 ist die Kontrolle in einzelne Funktionen unterteilt. Es gibt Funktionen, die in jeder

Gesamtstruktur einmal enthalten sein müssen, und Funktionen, die in jeder Domänenstruktur einer Gesamtstruktur enthalten sein müssen.

Hier nun die Funktionen, die in jeder Gesamtstruktur genau einmal enthalten sein müssen:

- *Schemamaster*. Der Schemamaster überwacht alle Änderungen von Informationen, die einer Domäne zugrunde liegen (das so genannte *Schema*).
- *DNS-Master*. Steuert das Hinzufügen und Entfernen von Domänen in der Gesamtstruktur.

Hier die Funktionen, die in jeder Domänenstruktur enthalten sein müssen:

- *RID-Master*. Jede Domäne enthält einen RID-Master (RID = Relative ID Master). Dieser Controller hat die Aufgabe, jedem Domänencontroller relative Bezeichner zuzuordnen.
- Um die Objekte in einer Domäne unterscheiden zu können, wird jedem Objekt eine eindeutige Sicherheitskennung zugewiesen. Eine Sicherheitskennung (SID = Security ID) besteht aus einer Domänensicherheitskennung und einem eindeutigen relativen Bezeichner. Die Sicherheitskennung besteht also wie die Telefonnummer aus einem Bereichscode (Domänensicherheitskennung) und einer individuellen Nummer (relativer Bezeichner).
- *PDC-Emulation*. Damit auch Windows NT-Domänencontroller an der Authentifizierung teilnehmen können, benötigen Domänen eine PDC-Emulation. Ein Sicherungsdomänencontroller kann damit Aktualisierungen empfangen und durch eine Migration weiter arbeiten.
- *Infrastrukturmaster*. Jede Domäne muss einen Infrastrukturmaster enthalten, damit die Zuordnung von Benutzern zu Gruppen über die Domänen einer Gesamtstruktur hinweg synchronisiert bleiben. Wenn ein Mitglied einer Gruppe umbenannt, entfernt oder verschoben wird, versendet der Infrastrukturmaster die Änderung.

Nachdem ein Betriebsmaster eingerichtet wurde, muss sich jeder Computer, der in der Domäne enthalten sein soll, bei der Domäne registrieren. Durch die Registrierung wird der Computer Bestandteil der Ressourcen, die von der Domäne angeboten werden. Alle freigegebenen Ressourcen dieses Computers werden von der Domänensicherheit überwacht. Beschränkungen, die für Domänenbenutzer und Gruppen eingerichtet wurden, werden auf Computern angewendet, die Bestandteil der Domäne sind.



Windows 95/98-Computer können nicht in eine Windows 2000- oder Windows NT-Domäne aufgenommen werden. Benutzer können jedoch über Windows 95/98-Computer auf die Domäne zugreifen. Dies beinhaltet jedoch nur die Überwachungsebene, die auf diesen Computern unterstützt wird.

Domänencontroller

Domänencontroller werden wie Betriebsmaster eingerichtet, wenn der erste Server in der Domäne installiert wird. Zu den Funktionen von Domänencontrollern gehören die Verwaltung der Benutzer- und Gruppenkonten sowie die Verwaltung des Zugriffs auf Verzeichnisse und auf freigegebene Ressourcen. Um die Fehlertoleranz zu erhöhen, sollte ein Verzeichnis mindestens zwei Domänencontroller enthalten (siehe Abbildung 5.6).

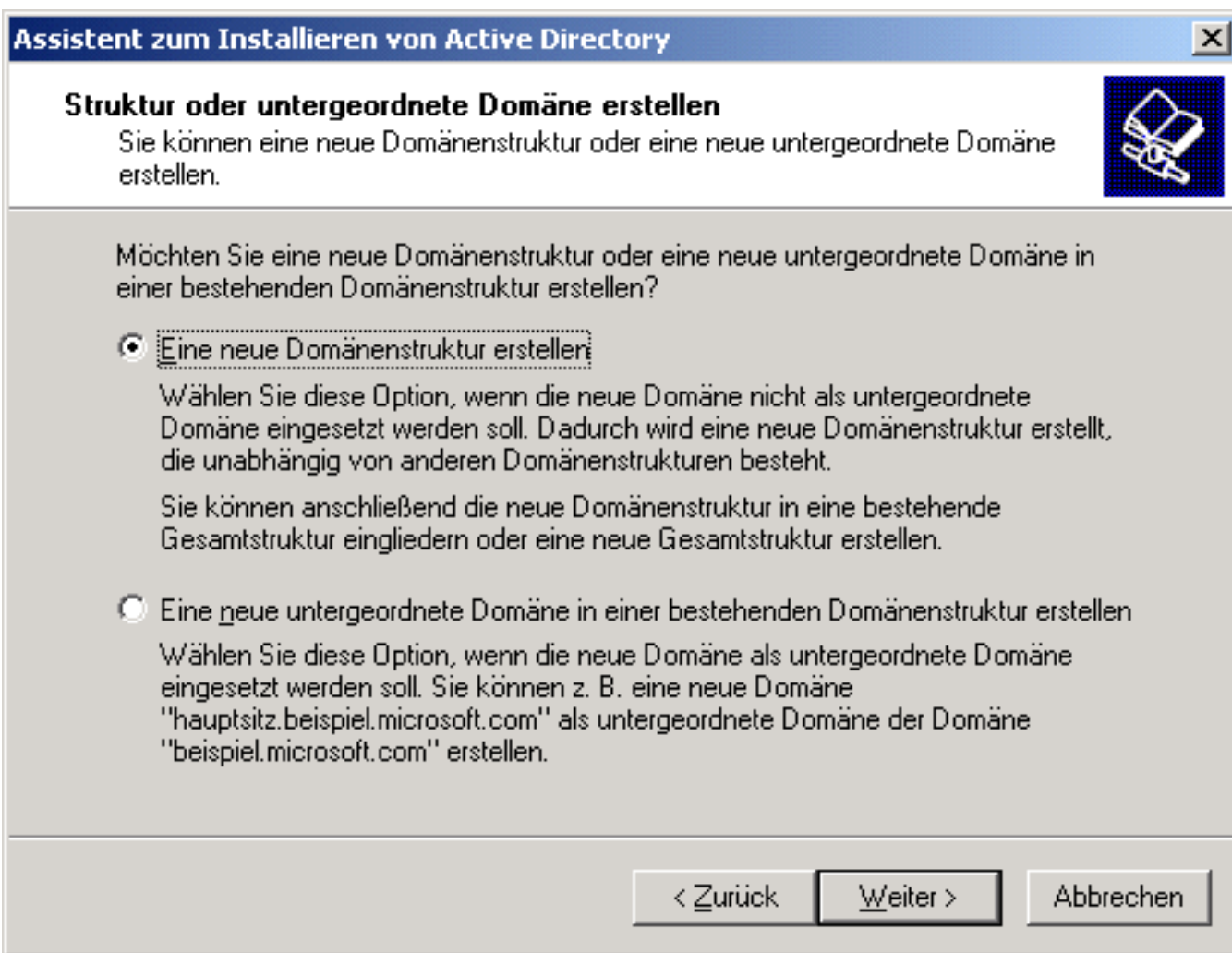


Abbildung 5.6: Einen Domänencontroller installieren.

Nachdem der erste Server installiert wurde, können andere Server in der Domäne installiert werden und an der Domänenkontrolle teilnehmen. Der Computer ist dann Bestandteil einer Multimaster-Systemdomäne. Dies stellt eine starke Veränderung gegenüber dem NT-Modell des allein stehenden Servers oder des primären Domänencontrollers dar.

Wenn der primäre Domänencontroller unter Windows NT heruntergefahren war, konnte kein Benutzer sein Kennwort ändern. Bei einem Multimastermodell kann ein Domänencontroller die Änderungen annehmen und Replikate an die anderen Domänencontroller in der Domäne verschicken.

Vertrauensstellungen

Eine Vertrauensstellung wird zwischen Domänen eingerichtet, damit die Benutzer und Gruppen aus einer Domäne auf Ressourcen einer anderen Domäne zugreifen können. In Windows 2000 gibt es zwei neue Formen von Vertrauensstellungen und das Konzept der Vertrauensstellungen wurde sehr stark verbessert.

Explizite Vertrauensstellungen (Klassische Vertrauensstellungen)

Domänen wurden bisher über so genannte Vertrauensstellungen miteinander verbunden. Diese werden nun als *explizite Vertrauensstellungen* bezeichnet. Eine explizite Vertrauensstellung ist eine einseitige Beziehung, mit der eine Verbindung zwischen den Ressourcen einer Domäne und den Benutzern und

Gruppen einer anderen Domäne hergestellt wird. Die Bezeichnung »explizite Vertrauensstellung« stammt daher, dass die Vertrauensstellung von den Administratoren der teilnehmenden Domänen explizit eingerichtet werden muss.

Wenn z.B. der Administrator von Domäne A eine Vertrauensstellung für Domäne B einrichtet, erhalten die Benutzer und Gruppen aus Domäne B Zugriff auf die Ressourcen in Domäne A (siehe Abbildung 5.7). Es handelt sich um eine unidirektionale Vertrauensbeziehung, die explizit eingerichtet wurde.

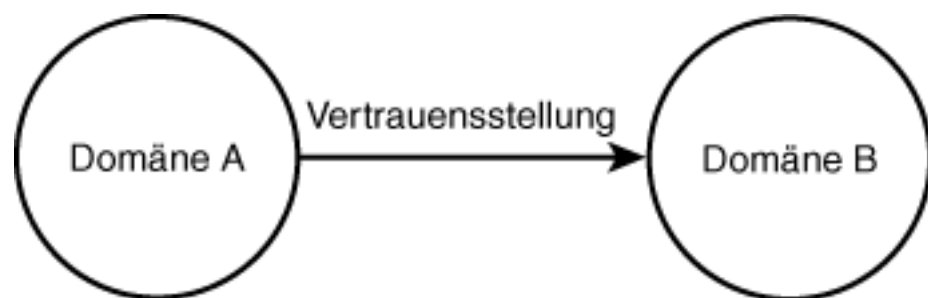


Abbildung 5.7: Eine klassische unidirektionale Vertrauensstellung.

Damit die Benutzer und Gruppen aus Domäne A auf Ressourcen in Domäne B zugreifen können, muss eine separate Vertrauensstellung eingerichtet werden. Dadurch würde Domäne B Domäne A vertrauen. Wurden zwei Vertrauensstellungen eingerichtet, gibt es vollständiges Vertrauen. Jede Vertrauensstellung muss separat eingerichtet werden und die Administratoren in jeder Domäne müssen sich darum kümmern.

In dieses Schema muss nur eine weitere Domäne integriert werden und schon wird es ziemlich problematisch, die Vertrauensstellungen aufrecht zu erhalten (siehe Abbildung 5.8). Wenn ein Unternehmen mit zwei Domänen ein anderes Unternehmen mit einer Domäne kauft und diese Domäne in einer vollständigen Vertrauensstellung mit allen aktuellen Domänen verbinden möchte, wird für jede Domäne eine bidirektionale Vertrauensstellung benötigt:

- Zwischen Domäne A und Domäne B muss eine Vertrauensstellung bestehen.
- Zwischen Domäne A und Domäne C muss eine Vertrauensstellung bestehen.
- Zwischen Domäne B und Domäne A muss eine Vertrauensstellung bestehen.
- Zwischen Domäne B und Domäne C muss eine Vertrauensstellung bestehen.
- Zwischen Domäne C und Domäne A muss eine Vertrauensstellung bestehen.
- Zwischen Domäne C und Domäne B muss eine Vertrauensstellung bestehen.

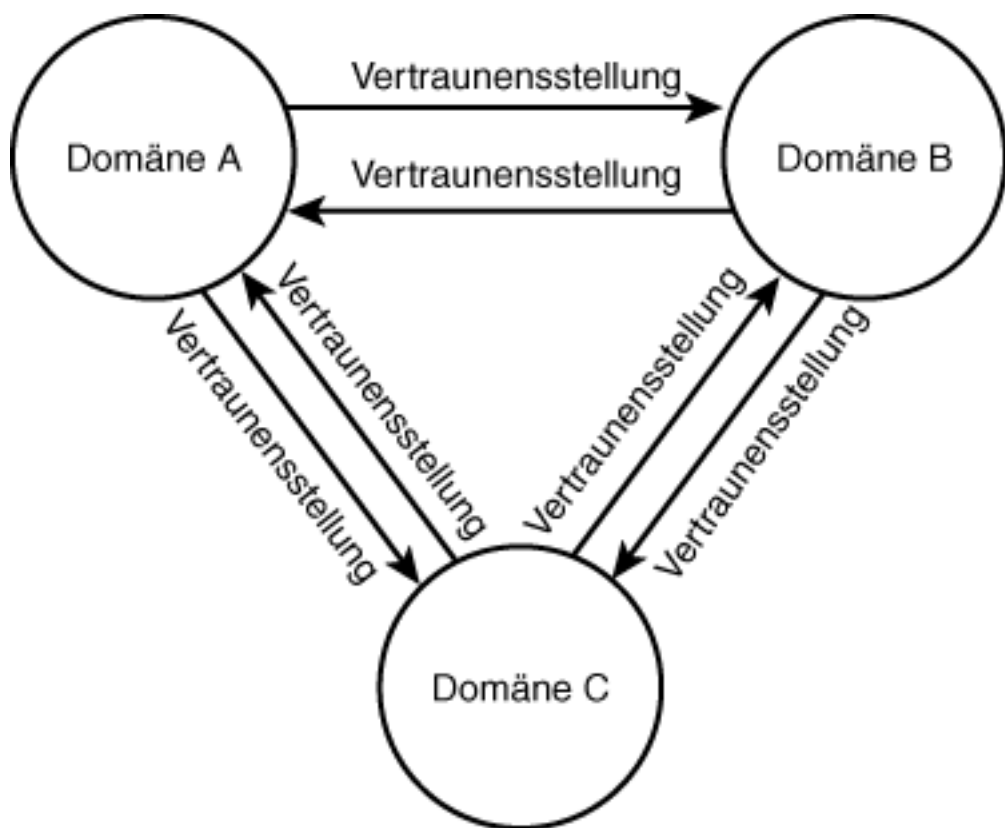


Abbildung 5.8: Der Anfang einer umfangreichen kompletten Vertrauensstellung.

Wird eine Vertrauensstellung von Domäne A nach Domäne B und von Domäne B nach Domäne C eingerichtet, heißt dies jedoch nicht, dass eine Vertrauensstellung von Domäne A nach Domäne C besteht. Diese klassischen Beziehungen sind nicht transitiv, sie stehen jedoch in einem Active Directory-Modell zur Verfügung.

Um zu verstehen, warum das Betriebssystem Windows 2000 mit einem solchen Enthusiasmus erwartet wurde, müssen Sie wissen, dass die explizite Vertrauensstellung nicht mehr die bevorzugte Methode ist, um mehrere Domänen miteinander zu verbinden. Stellen Sie sich vor, Sie müssten verschiedene Domänen miteinander verbinden und dafür Vertrauensstellungen einrichten.

Nichttransitive Vertrauensstellungen

Eine nichttransitive Vertrauensstellung ist eine Vertrauensstellung zwischen zwei Domänen, die nicht in derselben Domänenstruktur enthalten sind oder bei denen eine teilnehmende Domäne keine Windows 2000-Domäne ist. Diese Vertrauensstellungen können unidirektional und bidirektional, nicht aber transitiv sein (siehe hierzu den nächsten Abschnitt). Hier einige Beispiele für nichttransitive Vertrauensstellungen:

- zwischen Windows 2000-Domänen und Windows NT-Domänen
- zwischen zwei Windows 2000-Domänen, die sich in unterschiedlichen Gesamtstrukturen befinden

Transitive Vertrauensstellungen

Eine transitive Vertrauensstellung ist eine Vertrauensstellung zwischen zwei Domänen innerhalb einer Domänenstruktur oder einer Gesamtstruktur. Wenn untergeordnete Domänen in einer Domänenstruktur erstellt werden, besteht zwischen der untergeordneten und der übergeordneten Domäne automatisch eine

transitive Vertrauensstellung. Diese ist immer bidirektional und wird automatisch eingerichtet.

Es lassen sich auch so genannte *verknüpfte Vertrauensstellungen* einrichten. Mehr hierzu erfahren Sie in Kapitel 9.

5.1.2 Active Directory

Die größte Nachfrage bestand nach einem System, das eine hierarchische Verwaltung von Benutzern und Ressourcen ähnlich wie bei der Verwaltung von Dateien in einem Verzeichnis oder von Datensätzen in einer Datenbank erlaubt. Mit Active Directory wird diese Struktur nun eingeführt.

Wie Sie bei der Bildung von expliziten Vertrauensstellungen sehen können, wird in den heutigen großen unternehmensweiten PC-Netzwerken eine Möglichkeit benötigt, Benutzer und Ressourcen zuzuordnen. Diese Methode muss flexibel genug sein, um eine lokale Verwaltung zu ermöglichen. Sie muss aber auch transitive Beziehungen zulassen, die zu mobilen Mitarbeitern oder Ressourcen bestehen. Die lokalen Manager müssen ihre Mitarbeiter und Mitarbeiterinformationen überprüfen können und die EDV-Abteilung muss die Systeme und Richtlinien auf diesen Systemen überwachen können.

Active Directory bietet all diese Dinge. Mit Active Directory wird eine mehrschichtige Struktur eingerichtet, bei der Beziehungen über die Grenzen eines bestimmten Containers oder einer Domäne hinweg eingerichtet werden können (siehe Abbildung 5.9).

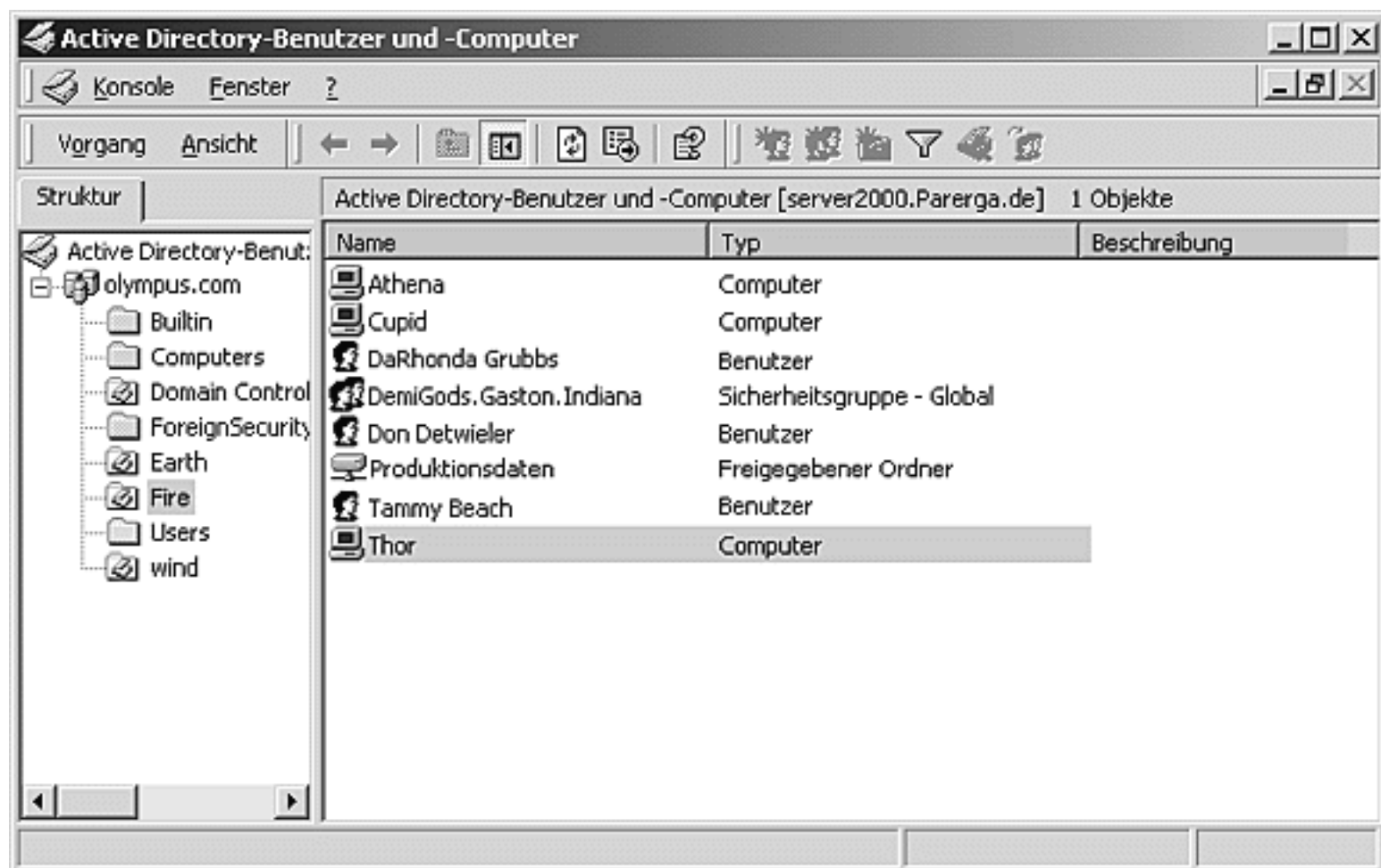


Abbildung 5.9: Eine Hierarchie aus Domänen, Benutzern und Computern

Die Struktur

In Active Directory sind Domänen Bestandteil einer so genannten Struktur. Innerhalb der Struktur ist jedes Element wie beim Dateisystem über eine baumartige Struktur mit anderen Objekten verbunden. Eine Struktur besteht aus Container- und Blattobjekten. Ein Blatt ist einfach ein Benutzer oder eine Ressource, die im Container enthalten ist und in diesem überwacht wird.

Containerobjekte wurden bereits in diesem Kapitel beschrieben, jedoch unter einer anderen Bezeichnung. Domänen und Organisationseinheiten sind Beispiele für Containerobjekte.

Benutzer- und Ressourcenobjekte sind leistungsfähiger als einfache Benutzerkonten, denen nur Zugriffsberechtigungen für Freigaben zugeordnet werden können. Ein Blattobjekt kann nun mehrere Elemente enthalten, die zuvor getrennt verwaltet werden mussten. Blattobjekte enthalten Informations- und Kontrollfelder und werden so zu Kontrollcentern für die Benutzeraktivität und -kontrolle.

Ein Benutzerobjekt kann den vollständigen Namen, die E-Mail-Adresse und die Telefonnummer eines Individuums enthalten. Es kann auch Informationen darüber enthalten, wie die Windows-Umgebung des Benutzers aussehen soll, wenn er sich von einem beliebigen Standort innerhalb des Unternehmens anmeldet. Bei den Dienstprogrammen, die in Windows NT enthalten waren, musste der Administrator die Informationen an mehreren Stellen speichern und verschiedene Dienstprogramme verwalten, um dasselbe zu erreichen.

Kein Master

Im klassischen Domänenmodell ist das Konzept eines einzelnen Masters nie ganz verschwunden. Bei einem Systemversagen musste der Administrator intervenieren, um alles wiederherzustellen. Active Directory ist ein Multimaster-System.

In dieser Konfiguration werden mehrere Exemplare des Verzeichnisses auf verschiedene Server im Netzwerk verteilt. Wenn eine Veränderung vorgenommen wird, repliziert das System, das die Änderung bemerkt, diese über das Verzeichnis. Änderungen werden bei jedem Kontrollpunkt nach Zeit und Wichtigkeit aufgezeichnet. Dies ermöglicht einen effizienten Informationstransfer.

Es resultiert eine bessere Leistung und Fehlertoleranz, genau wie beim Sicherheitsdomänencontroller im klassischen Domänenmodell. Es können jedoch von jeder Stelle aus Änderungen am Verzeichnis vorgenommen werden und diese Änderungen werden unabhängig von einem System wirksam.

Die verzeichnisbasierte Netzwerksicherheit und -verwaltung ist nicht neu. Novell NetWare benutzt sie bereits seit fast zehn Jahren. Sie ist jedoch neu für den Microsoft-Administrator.

5.1.3 Netzwerkdienste

Windows 2000 enthält viele Schichten, die an der Oberfläche nicht sichtbar sind. Dazu gehören die Dienste, die die Dienstprogramme steuern, die der Server anbietet. Diese Dienste sind nicht mehr im Dialogfeld **Netzwerk** enthalten (falls Sie ein alter Windows NT-Veteran sind). Sie befinden sich an einem Ort, der Windows 95/98-Nutzern bekannter sein dürfte. Bei Windows 2000 sind sämtliche Dienste, Protokolle und Adapter unter den Eigenschaften einer bestimmten Verbindung aufgeführt. Die Verbindungen sind im Ordner *Netzwerk- und DFÜ-Verbindungen* enthalten. Die Eigenschaften einer

Verbindung können Sie einsehen, indem Sie doppelt darauf klicken und dann die Schaltfläche **Eigenschaften** wählen.

Die Netzwerkdienste sorgen dafür, dass Benutzer sich anmelden können, Computer eine IP-Adresse erhalten und vieles mehr.

5.2 Netzwerke (Ihr LAN oder WAN) und Netzwerke (Segmentierung)

Um zu verstehen, wie Windows 2000 und Active Directory verteilt werden müssen, müssen Sie das Netzwerk kennen, über das Sie die Ressourcen verteilen. Sie werden z.B. feststellen, dass Sie das Netzwerk lahm legen, wenn Sie keine Domänen und Strukturen einrichten. Die Netzwerkinfrastruktur sollte im Idealfall auf eine maximale Bandbreite ausgelegt sein. Es ist jedoch Ihre Aufgabe als Windows 2000-Administrator, so viel wie möglich über die Systeme und darüber, wie Ihr System mit ihnen interagiert, in Erfahrung zu bringen.

Die Replikation von Domäneninformationen über kostspielige WAN-Leitungen (WAN = Wide Area Network) kann dazu führen, dass Benutzeranforderungen langsamer beantwortet werden. Deshalb sollten Sie wissen, was ein WAN ist. Wenn Sie mit einem LAN arbeiten (LAN = Local Area Network), brauchen Sie vielleicht nicht unbedingt eine Struktur einzurichten. Zu den Begriffen LAN und WAN kommen nun noch die Begriffe SAN (System Area Network) und MAN (Metropolitan Area Network) hinzu. Hier die Definitionen für die vielen Abkürzungen:

- *LAN (Local Area Network)*. Ein Netzwerk, das sich nur auf ein Gebäude erstreckt. Zu LANs gehören auch Hochgeschwindigkeits-Campusnetzwerke mit einer Übertragungsrate von 2 Kbps oder höher.
- *WAN (Wide Area Network)*. Netzwerke, die sich über einen Bereich erstrecken, für den spezielle Vermittlungsvorrichtungen (Router) und eine Standleitung erforderlich sind.
- *SAN (System Area Network)*. Ein Segment des Netzwerks, das für die Kommunikation zwischen Servern und/oder Serverkomponenten reserviert ist. Ein Netzwerk, das nur für die Sicherung des Dateiservers eingerichtet wurde, wäre ein Beispiel für ein SAN.
- *MAN (Metropolitan Area Network)*. Eine Sonderform des WANs, die nur Computer innerhalb einer Stadt enthält. MANs können Daten bis zu einer Entfernung von ca. 75 km übertragen.
- *Netzwerksegment*. Systeme werden im Netzwerk über ihre Computer- und die Netzwerkadresse identifiziert. Ein Netzwerksegment ist ein Teil des Netzwerks, der alle Computer mit derselben Netzwerkadresse enthält.

Bei Netzwerken ist ein möglichst hoher Durchsatz wünschenswert. Die Datenmenge, die das Netzwerk durchlaufen kann, d.h. die Datenübertragungskapazität, wird als *Bandbreite* bezeichnet. Das Ziel ist es, jedem Computer eine möglichst hohe Bandbreite zu bieten, egal, ob dieser in ein LAN oder WAN integriert ist.

Eine Möglichkeit, eine hohe Bandbreite zu gewährleisten, besteht darin, die Bandbreite auf der Basis des Bedarfs in Bereiche aufzuteilen und den Datenfluss entsprechend zu steuern. Das Ethernet ist die vorherrschende Topologie, mit der PCs in einem Netzwerk verbunden werden. Um eine Überlastung zu

vermeiden, können die Computer aufgeteilt werden. Dieser Vorgang wird als *Segmentierung* bezeichnet. Zur Veranschaulichung nun ein paar Beispiele. Die Benutzer in der Grafikabteilung eines Unternehmens versenden z.B. große Bilddateien über das Netzwerk, was zu Spitzenzeiten zu einer Verringerung der Netzwerkleistung führt. Das Problem lässt sich dadurch lösen, dass die Grafikabteilung in ein separates Netzwerksegment verlegt wird.

Wenn ein Netzwerk auf mehrere Standorte verteilt ist, greifen die Benutzer eines Standorts möglicherweise nicht auf den anderen Standort zu. Hier wäre es sinnvoll, dafür zu sorgen, dass der Netzwerkverkehr der beiden Standorte nicht vermischt wird. Wenn Sie eine passende Domänenstruktur einrichten, können Sie derartige Probleme mit dem Netzwerkverkehr vollständig vermeiden.

Netzwerke lassen sich auf zwei Arten segmentieren, die nachfolgend beschrieben werden.

5.2.1 Switched Ethernet

Die erste Möglichkeit, ein Netzwerk zu segmentieren, besteht darin, es in verschiedene Domänen aufzuteilen, die miteinander kollidieren könnten. Bei einem Ethernet sind die einzelnen Computer über eine Bus- oder eine Sterntopologie miteinander verbunden (siehe Abbildung 5.10).

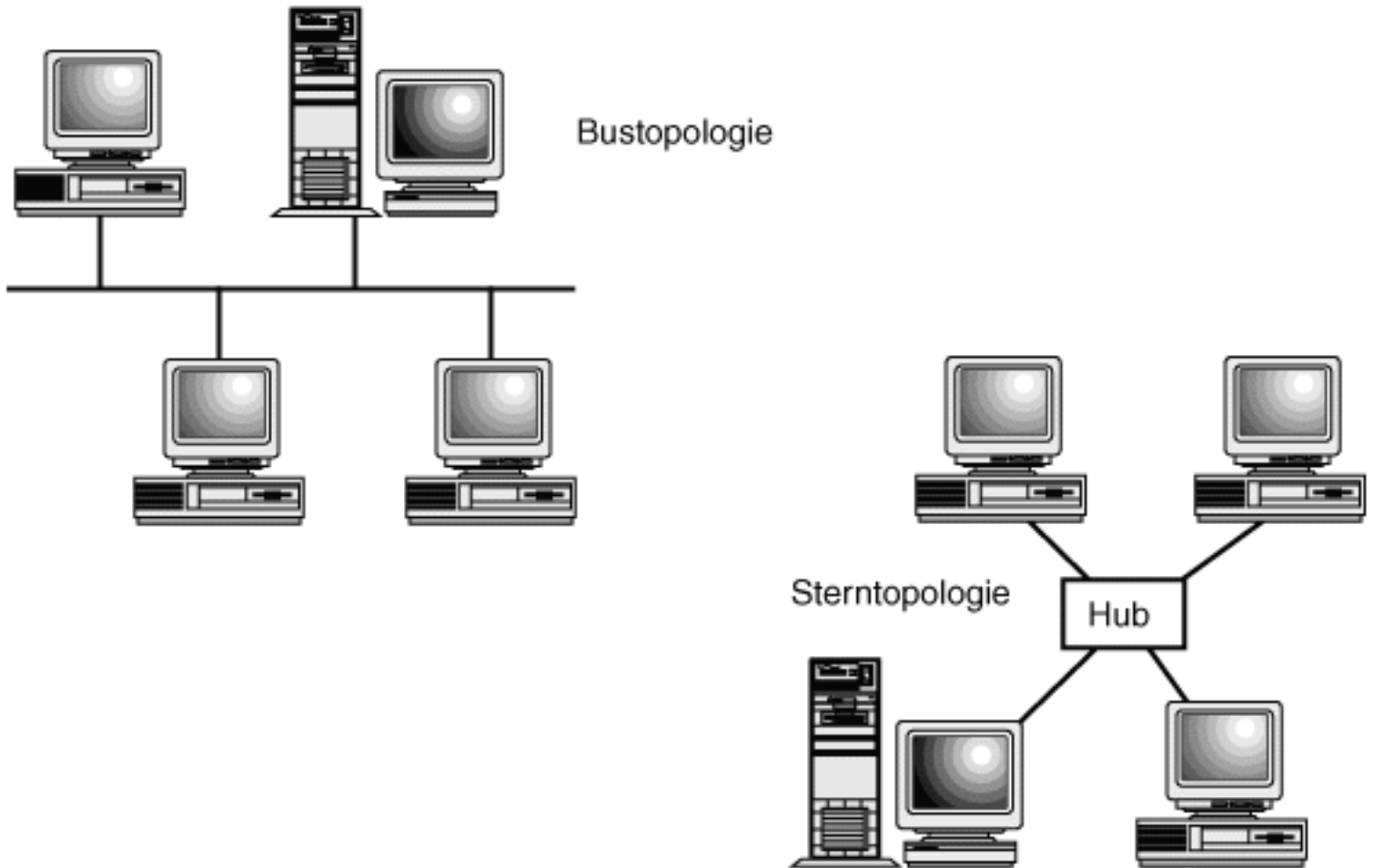


Abbildung 5.10: Ethernet-Topologien

Wenn ein System versucht, über eine Leitung zu kommunizieren, horcht es zunächst an dieser um festzustellen, ob die Leitung bereits von einem anderen System benutzt wird. Dies liegt daran, dass

immer nur ein System die Leitung benutzen kann. Wenn die Leitung frei ist, beginnt das System, ein Signal zu senden. Wenn gleichzeitig ein anderes System beginnt, Daten zu senden, führt dies zu einer Kollision. Nun warten die beiden Systeme eine zufällige Zeitspanne und versuchen dann noch einmal zu senden. Wegen dieses Verhaltens werden die Systeme in einem Segment eines Ethernets auch als Mitglieder einer Kollisionsdomäne bezeichnet.

Kollisionen sind in Ethernets nichts Ungewöhnliches und werden sogar erwartet. Treten sie jedoch zu häufig auf, verbringen die Computer im Ethernet die meiste Zeit damit, auf eine freie Leitung zu warten und nicht damit, zu kommunizieren. Dieses Problem lässt sich dadurch lösen, dass die Computer entweder dedizierte Leitungen erhalten oder dass zumindest die Anzahl der Teilnehmer verringert wird. Dazu werden einzelne Segmente eingerichtet, die über Vermittlungseinrichtungen oder Brücken miteinander verbunden sind.



Switches (Vermittlungseinrichtungen) sind die Nachfolger der so genannten Brücken, d.h. der Geräte, die zwei lokale Netzwerke miteinander verbinden. Switches teilen nicht nur ein Signal auf der Basis der MAC-Adressen auf, sondern sie übernehmen auch Routingfunktionen, d.h., sie suchen die beste Route für die Daten.

Die Geräte, die diese Aufgaben erfüllen, werden als Switches bezeichnet. Wenn ein PC versucht, mit einem anderen zu kommunizieren und die Kontrolle über die Leitung erhält, sendet er zunächst einen Rundspruch und wartet auf eine Antwort, die ihm die Hardwareadresse des PCs mitteilt, an den er die Daten senden möchte. Er sendet dann die Signale an diese spezielle MAC-Adresse (MAC = Media Access Control). Bei diesem Verfahren müssen alle Computer die Leitung abhören um festzustellen, ob die Signale für sie bestimmt sind. Das kostet Zeit.

Wenn sich die Computer in einem Netzwerk so aufteilen ließen, dass nicht so viele Signale gesendet werden müssten, ließe sich das ganze Durcheinander verhindern. Werden die Computer so aufgeteilt, dass sie nur die Elemente abhören, die auf ihren Leitungen gesendet werden, entstehen separate Kollisionsdomänen. Die getrennten Kommunikationsleitungen der einzelnen Kollisionsdomänen werden über einen Switch miteinander verbunden.

Ein Switch ist ein Hochgeschwindigkeitsschalter, über den entweder die einzelnen Computer oder Gruppen von Computern auf einem Hub miteinander verbunden sind. Jede Kommunikationsleitung ist eine separate Kollisionsdomäne. Diese separaten, aber trotzdem miteinander verbundenen Abschnitte des Netzwerks werden als Segmente bezeichnet. Der Switch horcht die Leitungen ab, mit denen er verbunden ist und notiert die MAC-Adressen der verbundenen Computer (siehe Abbildung 5.11). Wenn ein Computer Daten senden möchte, registriert der Switch die MAC-Adresse des Zielcomputers und leitet die Daten an das passende Segment weiter.

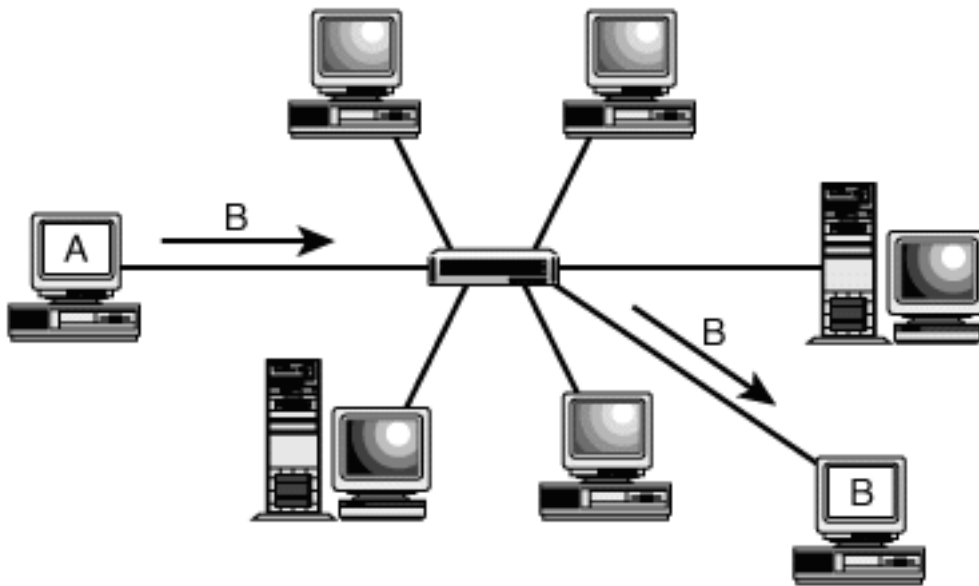


Abbildung 5.11: Das Switched Ethernet gewährleistet eine hohe Bandbreite durch eine spezifische Kommunikation.

Eine Kollisionsdomäne im Ethernet (10 oder 100 MB) sollte maximal 35 aktive Benutzer enthalten. Sie sollten nun keine Panik bekommen, wenn Sie daran denken, dass mehrere Hundert Benutzer mit dem Hub in Ihrem Unternehmen verbunden sind. Der Begriff *aktiver Benutzer* bezeichnet einen Computer, der Signale versendet. Wenn fünfzig Benutzer an ihrem Schreibtisch sitzen, während nur der Bildschirmschoner läuft, zählen sie nicht als aktive Benutzer. Nur Sie können feststellen, wie viele Benutzer jeweils aktiv sind. Um jedoch Probleme mit der Bandbreite zu vermeiden, sollten Sie darauf achten, dass maximal 35 aktive Benutzer in einer Gruppe enthalten sind.

Denken Sie auch an Gruppen wie die erwähnte Grafikabteilung. Bei solchen Gruppen sollten Sie in Erwägung ziehen, diese allein an einen Switch oder Switch-Port zu hängen.

Serververbindungen mit diesen Gruppen sollten über den Switch laufen. Optimal wäre ein direkter Pfad zwischen Benutzern und den Serverressourcen. Dahinter steckt das Konzept zu verhindern, dass der Server mit Workstations von Benutzern um die Kollisionsdomäne konkurrieren muss. Es wäre katastrophal, wenn ein Server eine geringe Leistung aufweisen würde, weil ein Benutzer die neueste Version eines Action Games herunter lädt.

5.2.2 Mit Routern verbundene Segmente

Die Netzwerkkommunikation erfolgt in vielen verschiedenen Schichten. Diese Schichten werden im OSI-Modell (OSI = Open Systems Interconnection) zusammengefasst. Dieses Modell hilft zu verstehen, warum ein Segment in diesem Zusammenhang sich von einer Kollisionsdomäne unterscheidet. Abbildung 5.12 zeigt das OSI-Modell.

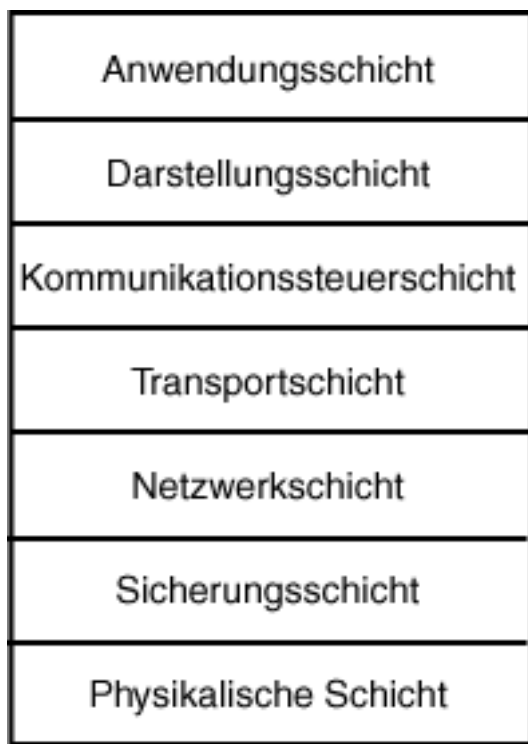


Abbildung 5.12: Das OSI-Modell

Es soll nun nicht das OSI-Modell beschrieben werden, sondern Sie sollen einfach nur sehen, dass es in den Kommunikationsschichten verschiedene Punkte gibt, an denen Entscheidungen getroffen werden und der Datenfluss geändert werden kann. Dies sind die Netzwerk- und die Sicherungsschicht. Diese beiden Schichten sind für die Kommunikation zuständig, nachdem eine physische Verbindung hergestellt wurde.

Die Sicherungsschicht wird in einem Switched Ethernet verwendet. Sie hat unter anderem die Aufgabe, die MAC-Adresse des Computers zu ermitteln.

Die Netzwerkschicht ermittelt dann die Netzwerkadresse des Signals und stellt fest, ob sie zu dem Computer gehört, der das Signal empfangen hat.

Router sind Vermittlungsvorrichtungen, die ähnlich wie Switches den Datenfluss weiterleiten. Statt den Datenfluss jedoch auf der Basis von MAC-Adressen zu verteilen, kennen Router jedoch nur das Netzwerk, in dem sich das Zielsystem befindet und leiten die Daten an dieses weiter (siehe hierzu die Definition von Netzwerksegmenten am Anfang des Netzwerkabschnitts in diesem Kapitel).

Router werden häufig eingesetzt, um den Datenfluss in einem WAN zu steuern, weil der Datenfluss von Router zu Router spezifischer ist. Router kennen die Pfade zu bestimmten Netzwerken oder lernen diese. Es ist also keine Rundsendung einer MAC-Adresse erforderlich, sondern ein System landet zunächst im korrekten Netzwerk und sendet dann die Anforderung.

5.3 RRAS

RRAS (Routing and Remote Access Services) fasst Dienste zusammen, die den Fernzugriff auf Systeme erlauben. Ursprünglich hieß dieser Dienst RAS (Remote Access Services) und wurde eingesetzt, um Benutzern den Zugriff auf den Server über ein Modem zu ermöglichen. Der Routingbestandteil des

Dienstes macht den Dienst zu einem robusteren System für die Kommunikation über Standardtelefonleitungen und das Internet.

5.3.1 Der Remote-Zugriff

Remote-Benutzer können über RRAS auf ihren Computer im Büro zugreifen und die anderen Computer im Netzwerk so benutzen, als säßen sie vor ihrem Computer im Büro. RRAS erlaubt den Zugriff auf einen Server über eine DFÜ-Netzwerkverbindung. Das Modem oder die ISDN-Karte des Benutzers erfüllt dann die Funktion einer Netzwerkkarte, die mit dem Netzwerk im Büro verbunden ist. Der Hauptunterschied zwischen einer normalen Netzwerkverbindung und einer Verbindung über die Telefonleitung ist die Geschwindigkeit, da eine Standardtelefonleitung erheblich langsamer arbeitet als die Netzwerkverbindung im Büro (57,6 Kbps im Gegensatz zu 10.000 Kbps). Aus diesem Grund werden die Benutzer, die auf diese Weise auf das Netzwerk zugreifen, nur Daten abrufen und die Anwendungen dann auf ihren lokalen Workstations ausführen.

Einen guten Vergleich für diese Art der Kommunikation bieten das Internet und das World Wide Web. Um auf das Web zuzugreifen, stellen Sie eine Verbindung zum Internet her und starten dann den Webbrowser auf Ihrem Computer. Der Browser überträgt Daten von verschiedenen Hosts und zeigt sie an.

5.3.2 Multiprotokollrouting

Für kleine Unternehmen und in vielen kleinen Routinganwendungen kann es unerschwinglich sein, einen separaten Router zu erwerben, der den Datenfluss an eine Remote-Site oder ein anderes Segment im Haus leitet. Es wäre gut, wenn sich einfach eine andere Netzwerkschnittstelle auf dem Server einrichten ließe, die den Datenfluss mittels des Netzwerkbetriebssystems und des Routers lenkt.

Um Computer mit Windows als Router miteinander verbinden zu können, mussten viele Änderungen vorgenommen werden. Windows 2000 bietet diese Möglichkeit nun.

RRAS kann den Datenfluss in IP- und IPX-Netzwerken über den Server routen. Es ist auch möglich, Protokolle von Drittanbietern einzubinden, aber IP (das Protokoll, das im Internet verwendet wird) und IPC (das Protokoll, das von vielen NetWare-Netzwerken verwendet wird) sind integriert.

Routing on demand

Wenn Sie Netzwerke über Standardtelefonleitungen miteinander verbinden, kann es unerschwinglich teuer sein, diese Verbindung 24 Stunden am Tag verfügbar zu halten. Aus diesem Grund kann RRAS so konfiguriert werden, dass die Verbindung nur dann hergestellt wird, wenn ein Bedarf vorhanden ist. Wenn ein Benutzer beispielsweise versucht, auf eine Ressource im Netzwerk zuzugreifen, die sich auf der anderen Seite eines DFÜ-Netzwerk-WANs befindet, würde die Leitung aktiviert werden. Nach einer bestimmten Zeitspanne, in der keine Aktivität verzeichnet wird, würde die Verbindung wieder getrennt werden.

Virtuelles privates Netzwerk (VPN)

Wegen der Kosten, die bei der Installation von Standleitungen zwischen verschiedenen Standorten

entstehen, verwenden viele Unternehmen das Internet und andere öffentliche Netzwerke für ihre WAN-Verbindungen. Dadurch entsteht ein kostengünstigeres Kommunikationssystem, es birgt aber zahlreiche neue Probleme in sich. Das Internet ist weit von einem sicheren Netzwerk entfernt und Eindringlinge könnten leicht feststellen, was ein Unternehmen produziert.

Eine Lösung für dieses Problem besteht darin, die Informationen vor dem Versand in ein sicheres Paket zu packen. Genau das macht ein VPN (Virtual Private Network). VPNs nehmen die Pakete, die versendet werden sollen, und packen sie in ein privates (verschlüsseltes) Paket um, das nur vom passenden System auf der anderen Seite des öffentlichen Netzwerks gelesen werden kann. Der Versand erfolgt über ein Protokoll namens PPTP (Point-to-Point Tunneling Protocol). Um eine solche Verbindung herzustellen, müssen die beiden Parteien mit dem öffentlichen Netzwerk verbunden sein. Ein Vorteil dieser Technik ist auch, dass Clients über eine Einwahlverbindung von jeder Stelle aus auf das Netzwerk zugreifen können, von der auch ein Zugriff auf das Internet besteht.

Kapitel 6 Drucken

Ein altes Sprichwort besagt ungefähr folgendes: »Computer sind im Vergleich zu Druckern einfach, zuverlässig und bedienungsfreundlich«. Zu den unangenehmsten Aufgaben eines Systemadministrators gehört die Druckerverwaltung und es spielt keine Rolle, ob es sich um Windows 2000, UNIX oder ein anderes Betriebssystem handelt. Die Schnittstelle zwischen Computern und Druckern war schon immer ziemlich jämmerlich und Drucker sind mit so vielen beweglichen Teilen ausgestattet, dass sie sogar noch unzuverlässiger sind als die billigste Workstation. Das Ziel dieses Kapitels ist es, Ihnen ein Verständnis für das Drucksystem von Windows 2000 zu vermitteln, sodass Sie die Drucker in Ihrem Netzwerk leichter installieren und verwalten sowie Probleme behandeln können. Hier ein kurzer Überblick über das, was Sie in diesem Kapitel erwartet:

- Druckkonzepte
- Druckwarteschlangen einrichten
- Druckerverwaltung
- Druckwarteschlangen verwalten
- Problembehandlung

Je schneller Sie anfangen, desto schneller ist dieses unangenehme Thema vom Tisch. Werfen wir nun also zuerst einen kurzen Blick auf die Druckkonzepte.

6.1 Druckkonzepte

Windows 2000 verwendet dasselbe Druckertreiber-Setup wie Windows NT 4.0 und integriert Windows 95 und Windows 98 sehr gut. Beim Druckkonzept von Windows 2000 arbeitet eine Anwendung im Wesentlichen mit den Druckertreibern zusammen, um einen Strom von Druckbefehlen zu erzeugen, die an den Drucker gesendet werden. Anschließend muss der Drucker diese Befehle entschlüsseln und zu Papier bringen. Um besser zu verstehen, wie dies alles funktioniert, wird nun kurz die Arbeitsweise von Druckern beschrieben. Als Nächstes wird die Welt der Schriftarten kurz erläutert. Anschließend wird die Funktionsweise von Druckertreibern dargestellt und zum Schluss die Kommunikation mit Druckern. Außerdem wird ein Druckauftrag vom Anfang bis zum Ende verfolgt um festzustellen, wie die einzelnen Teile ineinander greifen.

6.1.1 Drucker

Es gibt drei Arten von Druckern. Die *Zeilendrucker* sind heutzutage sehr selten. Sie drucken eine komplette Zeile auf einmal. Sie werden insbesondere im Großrechner- und Minicomputerbereich eingesetzt. Beim zweiten Druckertyp, dem *Zeichendrucker*, erfolgt der Ausdruck Zeichen für Zeichen, wie z.B. bei manchen Matrixdruckern oder Typenraddruckern. Der Ausdruck ist sehr langsam. Die Druckqualität ist gemessen an modernen Standards ziemlich dürftig. Sowohl Zeilen- als auch Zeichendrucker sind fast vollständig auf den Ausdruck von Text beschränkt und die Qualität des Ausdrucks von Grafiken ist sogar noch schlechter als die von Text.

Seitendrucker wie Laserdrucker, manche Matrixdrucker, LED-Drucker und viele Tintenstrahldrucker

benutzen eine ganz andere Technik. Sie legen eine gesamte Seite im Druckerspeicher ab und drucken diese auf einmal. Seitendrucker zeichnen sich beim Ausdruck von Grafiken und Text aus und beherrschen sogar den Vierfarbdruck. Seitendrucker sind momentan der Standard beim Drucken. Viele der preisgünstigeren Tintenstrahldrucker sind zwar eigentlich Zeilendrucker, sie benutzen jedoch aufwändige Treiber, durch die sie sich wie ein Seitendrucker verhalten. Diese Tintenstrahldrucker bieten scharfe Farben und einen qualitativ hochwertigen Ausdruck, sind aber in der Regel langsamer als Laserdrucker.

Seitendrucker sind insofern eingeschränkt, als sie nur eine feste Seitengröße bedrucken können. Die Drucker eignen sich zwar hervorragend für den Ausdruck auf DIN A4-Seiten. Um jedoch größere Formate zu bedrucken, wird ein *Plotter* benötigt. Plotter werden normalerweise bei Ingenieurs- und Marketinganwendungen eingesetzt. Ingenieure drucken häufig großformatige Zeichnungen aus und im Marketing werden Plotter eingesetzt, um größere Schilder oder Plakate auszudrucken.

Es gibt zahlreiche Druckersprachen. Sie beschreiben, wie Text und Grafik auf einer Seite positioniert werden. Am häufigsten werden die Sprachen HPGL (Hewlett-Packard Graphics Language) und PostScript von Adobe eingesetzt. Die Treiber erstellen eigentlich kleine Druckersteuerungsprogramme, die an den Drucker gesendet und von ihm ausgeführt werden. PostScript ist von diesen beiden Sprachen die umfangreichere und zeichnet sich bei der Behandlung von geometrischen Formen und beim Vierfarbdruck mit hoher Genauigkeit aus. Die meisten High-End-Drucker sind PostScript-Drucker und PostScript ist auch die bevorzugte Druckersprache für den Apple Macintosh. Deshalb sehen Ausdrücke über den Mac in der Regel am besten auf PostScript-Druckern aus. Seitendrucker und Plotter benutzen dieselbe Druckersprache für das Seitenlayout.

Weil Seitendrucker und Plotter kleine Programme ausführen, benötigen sie einen Hauptspeicher. Die Größe des Speichers, mit dem ein Drucker ausgestattet ist, beeinflusst die Menge der Grafiken und die Anzahl der Schriftarten, die ein Drucker behandeln kann. Ältere Drucker sind in der Regel mit 1 bis 2 Mbyte RAM ausgestattet, neuere Drucker mit erheblich mehr.

Hier noch ein paar logistische Hinweise zum Thema Drucken, die für Neulinge hilfreich sein könnten. Drucker benötigen Tintenpatronen oder Tonerkassetten und Papier. Sie sollten mindestens zwei Ersatzpatronensätze oder -kassetten auf Lager haben, um die alten ersetzen zu können, wenn sie nicht mehr funktionieren oder leer sind. Der Grund dafür ist offensichtlich: der Toner ist in der Regel genau dann leer, wenn etwas sehr Wichtiges ausgedruckt werden muss. Wenn nur eine Ersatztonerkassette vorhanden ist, ist diese bestimmt defekt. Sie sollten auch ausprobieren, was passiert, wenn der Drucker plötzlich ausgeschaltet wird. Dies kommt häufig vor, wenn ein Benutzer versehentlich etwas ausdruckt und glaubt, dass er das Problem lösen kann, indem er den Drucker ausschaltet. Es kann Ihnen sehr viel Zeit sparen zu wissen, wo das Papier stecken bleibt, wenn der Drucker einfach ausgeschaltet wird.

6.1.2 Schriftarten

Schriftarten legen fest, wie der Text auf der Seite aussieht. Eine Schriftart kann entweder als Druckerschriftart im Drucker vorhanden sein, oder sie wird in den Drucker geladen. Druckerschriftarten können entweder in den Drucker integriert oder über eine Schriftartkassette geladen werden. Wenn Windows 2000 einen Druckauftrag sendet, muss Windows wissen, über welche Schriftarten der Drucker bereits verfügt und welche erst an den Drucker gesendet werden müssen.

Schriftarten gibt es in zwei Ausführungen: mit fester und mit variabler Breite. Bei einer Schriftart mit fester Breite haben alle Buchstaben dieselbe Breite. Der Buchstabe »l« beansprucht also genau gleich viel Platz wie der Buchstabe »W«. Schriftarten mit fester Breite werden in Anwendungen verwendet, in denen die Zeichen innerhalb einer Spalte genau untereinander stehen müssen. Ein Beispiel für eine Schriftart mit fester Breite ist Courier. Schriftarten mit variabler Breite sehen besser und natürlicher aus und sind im normalen Text auch leichter lesbar. Bei diesen Schriftarten beansprucht das Zeichen »W« mehr Platz als das Zeichen »l«.

Schriftarten haben auch verschiedene Attribute wie die Strichstärke, die Schriftneigung und das Attribut »unterstrichen«. Die Strichstärke kann normal, halbfett oder fett sein und die Schriftneigung ist entweder normal oder kursiv. Das Attribut »unterstrichen« kann entweder aktiviert oder deaktiviert sein.

Es gibt zwei Möglichkeiten, um Schriftarten zu speichern. Bei *Rasterschriftarten* werden Bilder der einzelnen Buchstaben gespeichert - in der Regel gibt es mehrere Bilder jedes Buchstabens in unterschiedlichen Größen, Schriftneigungen und Strichstärken. Rasterschriftarten haben normalerweise die Erweiterung *.fon* und beanspruchen mehr Speicherplatz als Vektorschriftarten. Bei Vektorschriftarten wird jedes Zeichen nur einmal gespeichert und zwar so, dass sich das Zeichen von einer sehr kleinen bis zu einer sehr großen Größe leicht skalieren lässt. Die Buchstaben werden nicht als Bilder gespeichert, sondern als Vektorbeschreibungen. Um einen Buchstaben zu vergrößern, muss er nur auf die passende Größe skaliert werden. Vektorschriftarten lassen sich leichter skalieren und sehen in großen Schriftgrößen besser aus als Rasterschriftarten. Die Anzeige und der Ausdruck beanspruchen jedoch eine höhere Verarbeitungsleistung als bei Rasterschriftarten. Bei einer Vektorschriftart wird für den Buchstaben »I« z.B. die Information gespeichert, dass er aus zwei horizontalen Strichen der Länge 2 und einem vertikal zentrierten Strich der Länge 4 besteht. Um diesen Buchstaben zu vergrößern, müssen die Schriftinformationen einfach nur mit einem bestimmten Faktor multipliziert werden. Deshalb bleiben auch die Proportionen erhalten und der Buchstabe sieht immer korrekt aus.

Wenn Schriftarten in den Drucker geladen werden, stammen sie von dem Computer, auf dem gedruckt wird, und nicht vom Server. Aus diesem Grund nützt es nicht viel, auf dem Server zusätzliche Schriftarten zu installieren. Dadurch wird nur das Server-Setup komplexer.

6.1.3 Druckertreiber

Windows 2000 und auch alle anderen Windows-Betriebssysteme benutzen das Konzept der »Minitreiber«, um Gerätetreiber einzurichten. Das Betriebssystem stellt dabei Anwendungen zur Verfügung, die über die grundlegenden Informationen zur Kommunikation mit verschiedenen Arten von Geräten verfügen. Sie benötigen einen Druckertreiber, um spezielle Funktionen implementieren und die gewünschten Operationen ausführen zu können. Es handelt sich also um ein Schichtenmodell. Eine Anwendung muss nur wissen, wie Daten an den Standarddrucker eines Betriebssystems gesendet werden. Der Gerätetreiber ist dann dafür zuständig, die Daten und Anweisungen des Betriebssystems für den Ausdruck vorzubereiten. Der Gerätetreiber muss nichts über die verwendete Anwendung wissen und das Betriebssystem muss nicht viel darüber wissen, wie der Drucker funktioniert.

Schriftarten lassen sich bei diesem System z.B. sehr leicht in den Drucker laden. Der Druckertreiber muss das System darüber informieren, welche Schriftarten im Drucker installiert sind und legt dann fest, ob die Schriftarten in den Drucker geladen werden müssen. Entweder ist der Drucker in der Lage, das Betriebssystem darüber zu informieren, wenn neue Schriftarten installiert werden, wenn z.B. eine

Schriftartkassette hinzugefügt wird, oder der Administrator muss den Treiber so konfigurieren, dass dieser weiß, über welche Schriftarten der Drucker verfügt. Ob ein Drucker dem System mitteilen kann, welche Schriftarten installiert sind, hängt davon ab, wie alt er ist.

Wenn Windows 2000 Server einen Drucker im Netzwerk freigibt, können die Druckertreiber für andere Benutzer auch auf dem Server gespeichert werden. Wenn z.B. Windows 2000 Professional- und Windows 95-Clients einen Windows 2000 Server-Computer benutzen, kann der Administrator die Treiber für die Windows 95-Clients auf dem Server installieren, die dann übertragen werden, wenn der Windows 95-Client auf den Netzwerkdrucker zugreift. Das heißt, dass der Windows 95-Benutzer nicht aufgefordert wird, Treiberdisketten für den Drucker einzulegen, sondern dass die Treiber automatisch installiert werden. Mehr hierzu finden Sie im Abschnitt »Druckwarteschlangen einrichten« später in diesem Kapitel. Jedes Mal, wenn eine Clientworkstation etwas ausdruckt, wird die Version des Druckertreibers geprüft. Durch die Aktualisierung des Druckertreibers auf dem Server erhöht sich zwar der Datenverkehr auf dem Server, dies kommt jedoch im Laufe eines Tages nicht allzu häufig vor.

6.1.4 Kommunikation mit Druckern

Unabhängig davon, welche Art von Drucker in einem Unternehmen verwendet werden, müssen die Computer mit den Druckern kommunizieren können, damit der Ausdruck erfolgen kann. Es gibt verschiedene Methoden, um mit Druckern zu kommunizieren, wie z.B. über parallele Schnittstellen, serielle Schnittstellen, USB-Anschlüsse, direkte Datenein- und -ausgabe, Windows 2000-Netzwerkverbindungen, TCP/IP-Druckeranschlüsse und LPR-Anschlüsse.

Erst gab es nur parallele Anschlüsse. Der parallele Anschluss eines Computers sendet Daten über ein 25-poliges paralleles Kabel an den Drucker. Dieses Kabel überträgt alle Datenbits parallel und beinhaltet ein Synchronisierungssignal, die Erdung und einen Kanal, über den der Drucker mit dem Computer kommunizieren kann. Parallele Schnittstellen sind gemessen an heutigen Standards nicht sehr schnell. Die Daten werden mit 115 Kbps übertragen. In den meisten Fällen reicht diese Geschwindigkeit jedoch aus. Parallele Schnittstellen sind der Standard und es ist schwierig, einen Drucker zu finden, der nicht mit einer parallelen Schnittstelle ausgestattet ist. Die Anschlüsse bei Paralleldruckern tragen die Bezeichnung LPTn (d.h. LPT1, LPT2 etc.).

Serielle Drucker sind über die serielle Schnittstelle mit dem Computer verbunden. Die Kommunikation erfolgt seriell mit bis zu 56 oder sogar 115 Kbps. Ein serieller Anschluss muss alle Datenbits nacheinander senden. Es gibt 9- und 25-polige serielle Kabel, es werden aber nur drei oder vier Pins verwendet. Serielle Drucker können bidirektional kommunizieren und somit auch Informationen an den Computer übermitteln. Serielle Anschlüsse haben normalerweise die Bezeichnung COMn (d.h. COM1, COM2 etc.).

USB (Universal Serial Bus) ist eine ziemlich neue Technologie und bietet viele Vorteile. Die Kommunikation erfolgt bidirektional mit einer Geschwindigkeit von bis zu 12 Mbps. Das ist mehr als schnell genug für die Kommunikation mit dem Drucker. USB ist außerdem eine Plug & Play-Technologie. Wenn der Drucker an einen USB-Port angeschlossen wird, informiert er das Betriebssystem darüber und das Betriebssystem richtet dann die Treiber ein und bereitet diese für die Nutzung vor.

Die Ein-/Ausgabe über eine Datei wird nur sehr selten benutzt und dient meistens dazu, die

verschiedenen Druckoperationen zu testen. Die Druckausgabe kann dabei in eine Datei umgelenkt werden. Die Daten können anschließend manuell auf einen Druckeranschluss kopiert werden. Dies kann nützlich sein, um die Druckerausgabe zu testen und in Fällen, in denen Benutzer eine Datei auf einem Computer ausdrucken müssen, an den kein Drucker angeschlossen und der auch nicht in ein Netzwerk integriert ist. Der Benutzer kann in eine Datei drucken, die Datei auf eine Diskette kopieren, zu einem anderen Computer gehen und die Datei auf den Drucker »kopieren«. Um eine Datei auf den Drucker zu kopieren, muss folgender Befehl an der Eingabeaufforderung eingegeben werden:

```
Copy a:\Datei.prn lpt1:
```

Dieser Befehl kopiert die Datei *Datei.prn* auf den Drucker, der mit dem Anschluss LPT1 verbunden ist. Der Vorteil dieser Vorgehensweise liegt darin, dass die Anwendung, mit der die Datei erstellt wurde, nicht auf dem Computer installiert sein muss, der mit dem Drucker verbunden ist. Der Computer muss nur Zugriff auf den fraglichen Drucker haben.

Windows 2000, Windows NT und Windows 95/98 verfügen über eine Druckerfreigabe, die dieselbe Semantik verwendet wie bei der Freigabe von Dateien. Auf einen freigegebenen Drucker kann über einen UNC-Namen zugegriffen werden. Um z.B. auf einen Drucker namens »lp« zuzugreifen, der auf dem Computer namens »Kermit« freigegeben wurde, muss die Angabe `\\kermit\lp` verwendet werden. Der Drucker könnte mit der folgenden Befehlszeile auch einem lokalen Anschluss zugeordnet werden:

```
Net use lpt1: \\kermit\lp
```

Dadurch wird der Drucker `\\kermit\lp` dem lokalen Gerät namens LPT1 zugeordnet. Der Copy-Befehl für den manuellen Ausdruck einer Datei würde dann wie folgt lauten:

```
Copy a:\Datei.prn \\kermit\lp
```

Damit würde die Datei *Datei.prn* von Laufwerk A: auf den Drucker *lp* kopiert werden, der an den Computer *Kermit* angeschlossen ist.

Bei Druckservern können zwei oder mehr Drucker an parallele Anschlüsse angeschlossen und über eine Netzwerkverbindung im LAN verfügbar gemacht werden. Sie benutzen normalerweise das TCP/IP-Druckprotokoll, um mit dem Druckserver zu kommunizieren, der die eingehenden Daten dann an den korrekten Drucker leitet. Neuere Drucker haben diese Funktionalität bereits integriert, was einen höheren Durchsatz von der einzelnen Workstation zum Drucker ermöglicht (oder bei der Umleitung über einen Server).

Windows 2000 bietet auch die LPR-Portüberwachung, um eine Kommunikation mit Druckern zu ermöglichen, die an UNIX-Computer angeschlossen sind.

6.1.5 Der Ablauf eines Druckauftrags

Ein Druckauftrag wird erzeugt, wenn ein Benutzer in einer Anwendung den Befehl **Datei/Drucken** wählt. Die Anwendung, z.B. Microsoft Word, findet dann heraus, was gedruckt werden muss, und sendet den Druckauftrag an das Betriebssystem. Das Betriebssystem bestimmt, wo der Ausdruck erfolgen soll und prüft mit dem Druckertreiber, was gedruckt werden muss. Der Druckertreiber sammelt dann die gesamten Informationen und erzeugt den Datenstrom, der an den Drucker gesendet wird.

Der Druckertreiber sendet den Datenstrom an eine Warteschlange. Die Warteschlange übergibt dann den ersten Auftrag an den Spooler. Der Spooler empfängt die Druckaufträge, speichert sie und sendet die Daten dann in einer Geschwindigkeit an den Drucker, die dieser verarbeiten kann. Während der Spooler Daten an den Drucker sendet, kann der Benutzer weiterarbeiten. Dies ist möglich, weil die ganze »harte« Arbeit (beispielsweise die Grafik für den Ausdruck zu erzeugen) bereits erledigt wurde. Der Spooler muss nur noch mit dem Drucker kommunizieren. Nachdem der Spooler den Auftrag an den Drucker gesendet hat, löscht er den Druckauftrag und fährt herunter. Er speichert so lange eine vollständige Kopie des Druckauftrags, bis der Drucker den Auftrag erledigt hat. Dies dient zur Absicherung, falls im Drucker ein Papierstau entsteht, der Drucker ausgeschaltet wird oder ähnliches. In einem solchen Fall weiß der Spooler, inwieweit der Ausdruck bereits erfolgt ist und kann an dieser Stelle fortfahren.

Während des gesamten Druckprozesses benachrichtigt der Spooler die Druckerverwaltung über den Status des Druckauftrags. D.h. die Druckerverwaltung erfährt, wie viele Bytes an den Drucker gesendet wurden und wie viele Bytes noch gedruckt werden müssen. Während der Spooler diese Daten aktualisiert, prüft er auch, ob der Druckauftrag gelöscht oder angehalten wurde, und reagiert entsprechend, wenn diese Ereignisse aufgetreten sind.

6.2 Druckwarteschlangen einrichten

Damit Windows 2000 einen Drucker nutzen kann, muss eine Druckwarteschlange eingerichtet werden. Eine Druckwarteschlange ist eine Struktur, in der die Druckaufträge in der korrekten Reihenfolge gespeichert werden, bevor sie an den Drucker gesendet werden.

Eine Druckwarteschlange kann Druckaufträge an einen oder mehrere Drucker senden. Diese Drucker müssen aber entweder identisch sein oder denselben Treiber verwenden. Werden mehrere Drucker benutzt, lassen sich die Druckaufträge schneller erledigen und umfangreiche Druckaufträge behindern nicht den Ausdruck einzelner Seiten. Es ist sinnvoll, die Drucker, die über eine Druckwarteschlange gesteuert werden, an einem Standort aufzustellen, damit die Benutzer wissen, wo sie ihre Ausdrücke abholen können. An diesem Ort sollten auch die Ersatzteile gelagert werden. Wenn sehr viel ausgedruckt wird, wird auch viel Toner verbraucht.

In dem Abschnitt »Der Ablauf eines Druckauftrags« wird nicht unterschieden, welche Teile des Systems auf welchem Computer existieren. Das liegt daran, dass alle Druckaufträge gleich behandelt werden. Der einzige Unterschied besteht im Standort der Druckwarteschlange. Bei lokalen Druckern sind die Druckwarteschlangen lokal. Bei Netzwerkdruckern wird die Druckwarteschlange auf dem Server erzeugt und die Druckaufträge werden über das Netzwerk gesendet. Ein Druckauftrag wird an eine Druckwarteschlange und anschließend an den Spooler gesendet.

Um eine Druckwarteschlange einzurichten, öffnen Sie die Systemsteuerung und klicken doppelt auf

Drucker oder wählen im Menü **Start** den Befehl **Einstellungen/Drucker** (es gibt wahrscheinlich auch noch ein Dutzend anderer Möglichkeiten, das Druckerfenster zu öffnen). Klicken Sie doppelt auf das Symbol **Neuer Drucker**, um den **Druckerinstallations-Assistent** zu öffnen (siehe Abbildung 6.1). Klicken Sie auf die Schaltfläche **Weiter** um fortzufahren.

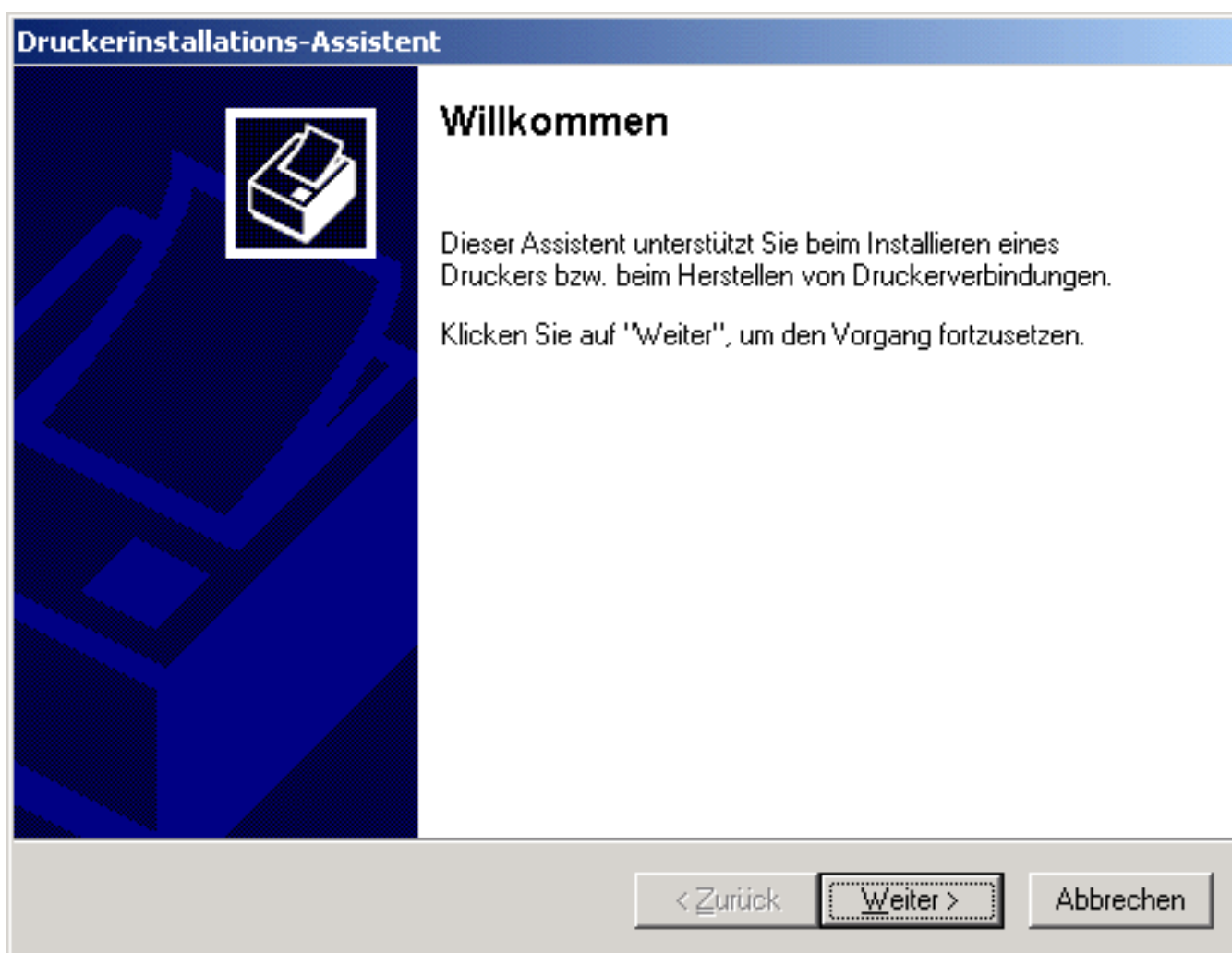


Abbildung 6.1: Dies ist der Begrüßungsbildschirm des Druckerinstallations-Assistenten, mit dem Sie einen neuen Drucker einrichten.

Im nächsten Schritt werden Sie gefragt, ob Sie einen lokalen Drucker oder einen Netzwerkdrucker installieren möchten. Dies ist irreführend. Über einen Netzwerkdrucker können Sie auf die Warteschlange auf einem anderen Windows 2000-Computer zugreifen, mit einem lokalen Drucker auf den Drucker, der am Computer angeschlossen ist. Der Netzwerkdrucker ist in diesem Zusammenhang also eine bestehende Windows-Druckwarteschlange und der lokale Drucker ist alles, was noch nicht als Windows-Druckwarteschlange existiert.

Wenn Sie die Option **Netzwerkdrucker** wählen, stehen zwei Optionen zur Auswahl. Um auf eine Standard-Windows 2000-Druckwarteschlange zu drucken, müssen Sie entweder den Namen des Druckers eingeben oder auf die Schaltfläche **Weiter** klicken, um den Drucker zu suchen. Die zweite Option besteht darin, über das HTTP-Protokoll zu drucken. Dazu muss ein Computer, auf dem IIS oder Peer Web Services laufen, so konfiguriert sein, dass Druckanforderungen über HTTP zulässig sind. Dies ist nützlich, wenn sich Firewalls oder Proxyserver zwischen dem lokalen Computer und dem Drucker befinden. Dieser Mechanismus arbeitet über den Standardport 80 von HTTP, der von den meisten

Firewalls durchgelassen wird.

Wenn Sie die Option **Lokaler Drucker** wählen und der Drucker tatsächlich ein lokaler Drucker ist, der über die parallele, die serielle oder eine USB-Schnittstelle mit dem Computer verbunden ist, können Sie das Kontrollkästchen **Automatische Druckererkennung und Installation von Plug & Play Druckern** aktiviert lassen. Wenn der Drucker über einen anderen Anschluss mit dem Computer verbunden ist, wie z.B. LPR oder TCP/IP, sollten Sie das Kontrollkästchen deaktivieren.

Wenn der Drucker über Plug & Play automatisch erkannt wird, wird die Druckwarteschlange erzeugt und die Treiber werden installiert. Wenn der Drucker nicht erkannt wird, müssen Sie den Anschluss wählen, über den der Drucker mit dem Computer verbunden ist oder einen neuen Anschluss erstellen. Die bestehenden Anschlüsse sind die normalen parallelen und seriellen Anschlüsse sowie der Anschluss FILE, bei dem beim Ausdruck ein Dateiname angegeben werden muss und die Daten dann an diese Datei gesendet werden.

Um einen neuen Anschluss zu erstellen, wählen Sie die gleichnamige Option und anschließend im Listenfeld die Art des Anschlusses. Üblicherweise stehen die folgenden Optionen zur Verfügung. Die Liste basiert aber auf den Optionen, die auf dem lokalen Computer installiert sind:

- *Local Port.* Diese Option dient dazu, einen neuen lokalen Anschluss einzurichten. Sie werden aufgefordert, einen Namen für den Anschluss einzugeben.
- *Standard TCP/IP Port.* Mit dieser Option wird eine Verbindung zu Printserver-Geräten wie HP JetDirect-Anschlüssen hergestellt. Diese Option startet einen anderen Assistenten (**Assistent zum Hinzufügen eines Standard-TCP/IP-Druckerports**), der Sie auffordert, die IP-Adresse und den Portnamen des Druckers einzugeben.
- *LPR Port.* Mit dieser Option lässt sich eine Verbindung zu UNIX-Servern herstellen, um die an diese angeschlossenen Drucker zu nutzen. Sie werden aufgefordert, den Namen des UNIX-Servers und den des Druckers einzugeben.

Nachdem Sie den Anschluss erstellt haben, müssen Sie den Druckertyp wählen, der mit dem Anschluss verbunden ist. Wenn der Drucker nicht in der Liste enthalten ist oder wenn Sie einen neueren Treiber auf Diskette oder CD-ROM haben, klicken Sie auf die Schaltfläche **Datenträger** und installieren den Treiber von Diskette oder CD-ROM.

Nachdem der Treiber installiert wurde, müssen Sie den Namen für den Drucker eingeben. Dieser Name dient dazu, den Drucker zu identifizieren. Wenn mehrere Drucker derselben Marke und desselben Modells vorhanden sind, sollten Sie bei der Benennung nicht nur den Namen und das Modell berücksichtigen.

Im nächsten Schritt müssen Sie entscheiden, ob der Drucker freigegeben werden soll. Wählen Sie einen Freigabenamen für den Drucker, der auf dem Server eindeutig sein muss. Im nächsten Schritt können Sie den Druckerstandort und einen Kommentar eingeben. Der Kommentar kann z.B. die verfügbaren Papiergrößen angeben oder ob der Drucker den Vierfarbausdruck unterstützt.

Wählen Sie als Nächstes, ob eine Testseite gedruckt werden soll. Bei der Serverinstallation ist es normalerweise sinnvoll sicherzustellen, dass der Drucker funktioniert, bevor die Benutzer darauf zugreifen. Zum Schluss wird eine Zusammenfassungsseite eingeblendet, die ähnlich aussieht wie in Abbildung 6.2. Diese Seite zeigt den Freigabenamen, den Druckernamen, den Druckertreiber und alle

anderen Details zum Drucker.

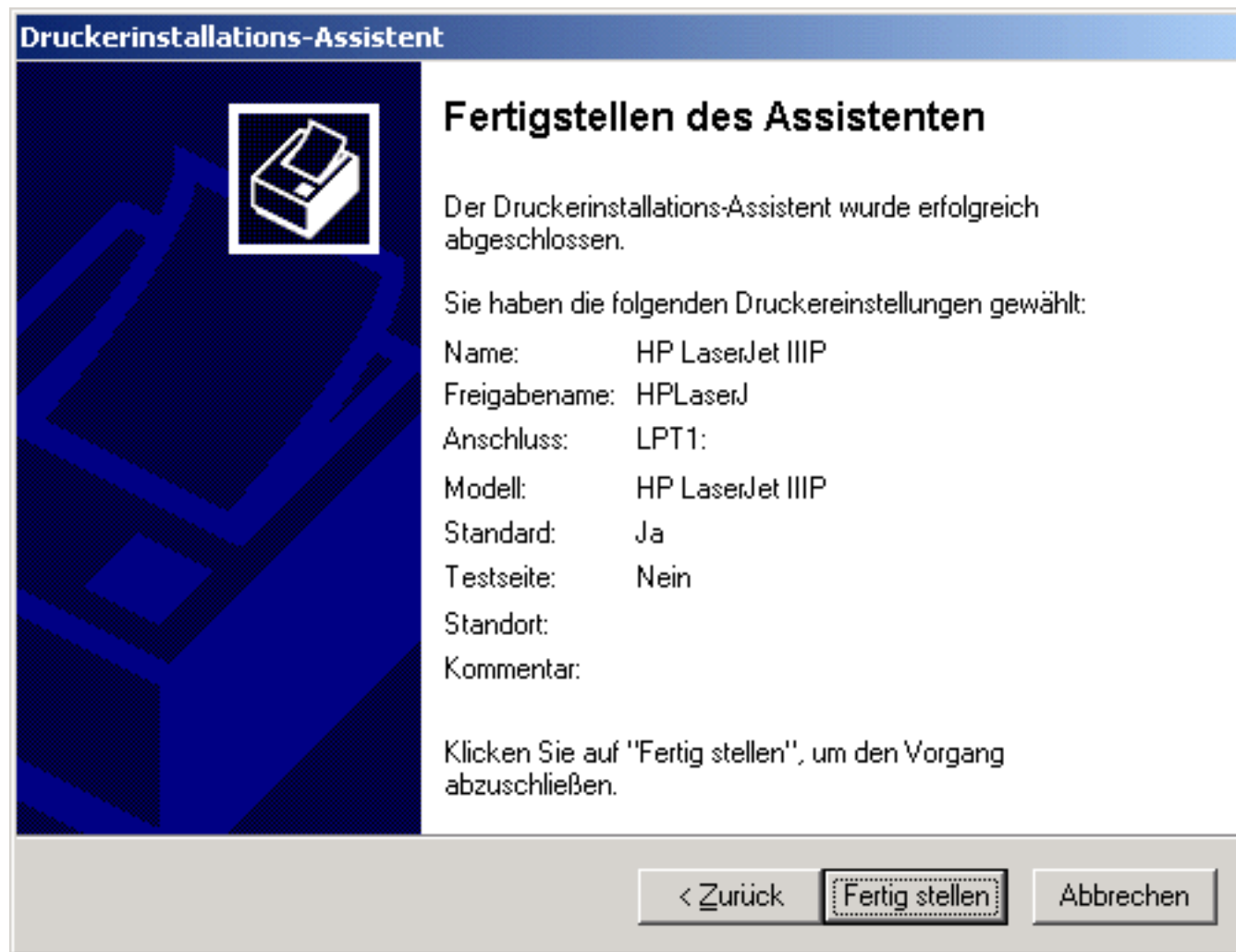
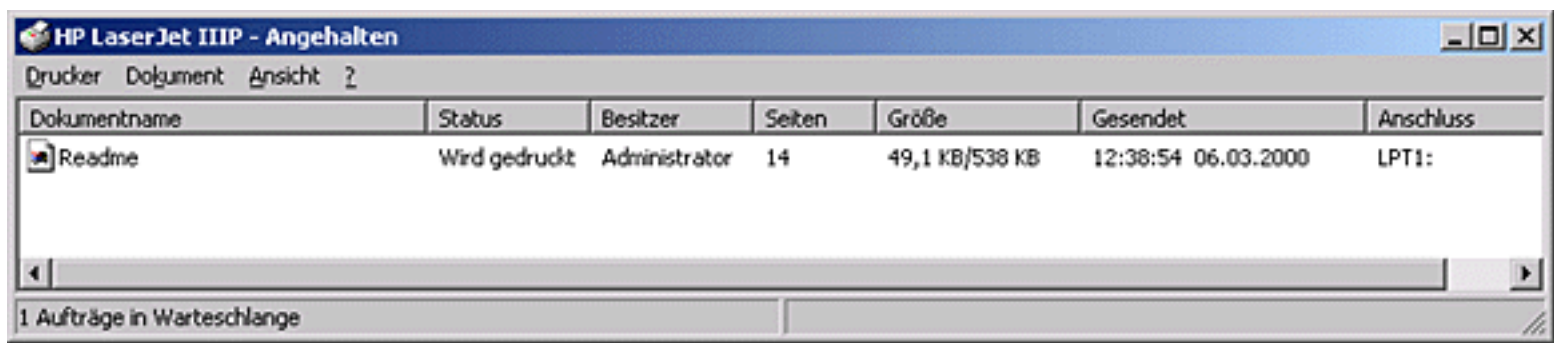


Abbildung 6.2: Diese Statusseite wird vom Druckerinstallations-Assistenten angezeigt und fasst die gewählten Einstellungen zusammen.

6.3 Die Druckerverwaltung

Mit der Druckerverwaltung werden Dokumente in einer Druckwarteschlange verwaltet. Dies bedeutet, dass Sie in der Druckerverwaltung die Druckwarteschlange und den Status der Druckaufträge in der Druckwarteschlange betrachten können. Es wird außerdem angezeigt, ob der Benutzer die benötigten Berechtigungen hat. Die Reihenfolge der Objekte in der Druckwarteschlange lässt sich verändern und Druckaufträge können aus der Druckwarteschlange gelöscht werden.

Denken Sie daran, dass eine Druckwarteschlange einfach nur eine Liste von Druckaufträgen ist, die darauf warten, bearbeitet zu werden. Jeder dieser Druckaufträge hat bestimmte Eigenschaften, die Sie sehen können, wie z.B. die Anwendung, mit der er erstellt wurde und die Länge des Druckauftrags in Seiten. Ein Beispiel für eine Druckwarteschlange sehen Sie in Abbildung 6.3. Beachten Sie, dass die Warteschlange angehalten ist und keine Druckaufträge die Warteschlange verlassen.



The screenshot shows a window titled "HP LaserJet IIIIP - Angehalten". Below the title bar is a menu bar with "Drucker", "Dokument", and "Ansicht". The main area is a table with the following columns: "Dokumentname", "Status", "Besitzer", "Seiten", "Größe", "Gesendet", and "Anschluss". There is one row with the document "Readme", status "Wird gedruckt", owner "Administrator", 14 pages, size "49,1 KB/538 KB", sent at "12:38:54 06.03.2000", and connected to "LPT1:". At the bottom, a status bar indicates "1 Aufträge in Warteschlange".

Dokumentname	Status	Besitzer	Seiten	Größe	Gesendet	Anschluss
Readme	Wird gedruckt	Administrator	14	49,1 KB/538 KB	12:38:54 06.03.2000	LPT1:

1 Aufträge in Warteschlange

Abbildung 6.3: Ein Beispiel für eine angehaltene Druckwarteschlange auf dem Server mit einem Dokument.

Ein Merkmal der Druckerverwaltung ist es, dass Sie auf die Spaltenköpfe klicken können, um die Druckaufträge nach diesem Kriterium in aufsteigender oder absteigender Reihenfolge zu sortieren. Um z.B. alle Druckaufträge auf einen Blick zu sehen, die von einem bestimmten Benutzer stammen, klicken Sie auf die Spalte **Besitzer** und gehen dann zu diesem Benutzer. Per Drag & Drop lässt sich außerdem die Anordnung der Spalten verändern.

6.3.1 Die Befehle des Menüs Drucker

Im Menü **Drucker** der Druckerverwaltung kann der Benutzer Änderungen am Drucker und der Warteschlange vornehmen. Über die Option **Als Standarddrucker verwenden** wird ein Drucker als Standarddrucker ausgewählt. Dies bedeutet, dass alle Anwendungen diesen Drucker als ersten in der Druckerliste anzeigen und dass beim Klick auf die Schaltfläche **Drucken** automatisch dieser Drucker gewählt wird. Über den Befehl **Druckeinstellungen** im Menü **Drucker** lassen sich verschiedene druckerspezifische Einstellungen vornehmen, wie z.B. die Orientierung der Seite, die Reihenfolge, in der die Seiten gedruckt werden, der Papierschacht und die Papiergröße. Diese Optionen sind bei jedem Drucker unterschiedlich und hängen von den Funktionen des Druckers ab.

Mit dem nächsten Befehl, **Drucker anhalten**, werden alle Druckaufträge in der Warteschlange gestoppt. Die Druckaufträge bleiben jedoch weiterhin in der Warteschlange. Dies ist nützlich, wenn der Drucker ausgetauscht wird oder wenn der Drucker an eine Workstation angeschlossen ist und die Workstation Prozessorzeit für einen lokalen Benutzer benötigt. Mit der Option **Alle Druckaufträge abbrechen** werden alle aktuellen Druckaufträge gestoppt und die restlichen Aufträge in der Warteschlange werden gelöscht.

Die Option **Freigabe** ist identisch mit derjenigen bei der Einrichtung des Druckers. Der Drucker kann von anderen Computern im Netzwerk benutzt werden. Dieser Befehl ist eine Abkürzung für den Befehl **Eigenschaften**. Bei beiden Befehlen öffnet sich dasselbe Dialogfeld, beim Befehl **Freigabe** ist jedoch die Registerkarte **Freigabe** aktiviert (siehe Abbildung 6.4).

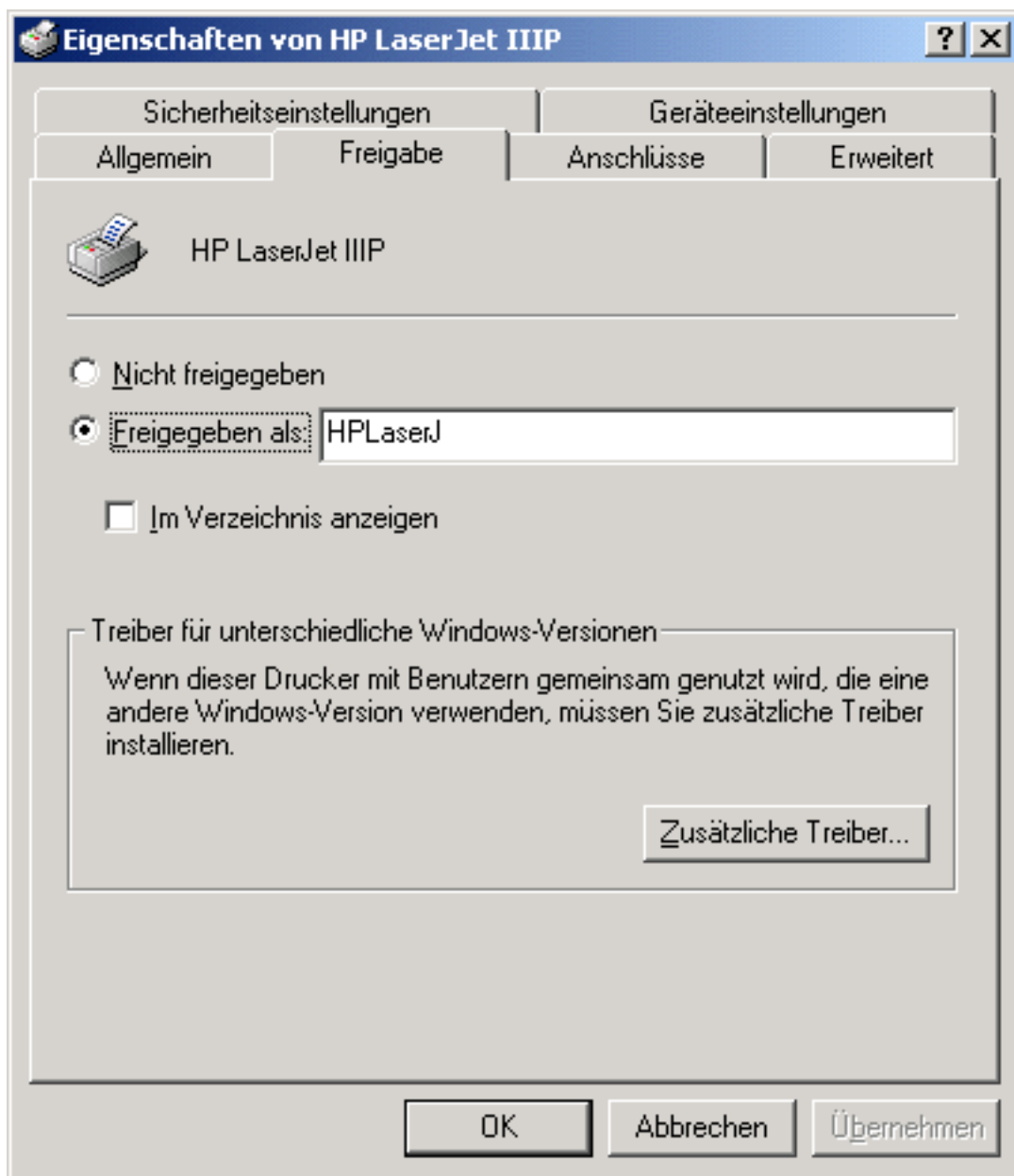


Abbildung 6.4: Die Registerkarte Freigabe im Eigenschaften-Dialogfeld des Druckers.

Wird der Befehl **Drucker offline verwenden** gewählt, werden die Druckaufträge in die Druckwarteschlange gesetzt und erst dann ausgeführt, wenn der lokale Computer wieder online ist. Diese Option ist nützlich für Benutzer, die am Laptop arbeiten und den Auftrag ausdrucken wollen, wenn sie den Laptop das nächste Mal an den Drucker anschließen.

6.3.2 Die Eigenschaften des Druckers

Über den Befehl **Eigenschaften** öffnet sich das **Eigenschaften**-Dialogfeld, in dem Sie fast alle Funktionen eines Druckers variieren können. Auf der Registerkarte **Allgemein** können der Druckername, der Standort und der Kommentar geändert werden und es lässt sich wie bei der Einrichtung eines neuen Druckers eine Testseite ausdrucken.

Die Registerkarte Erweitert

Die Registerkarte **Erweitert** bietet zahlreiche interessante Optionen (siehe Abbildung 6.5). Beispielsweise kann hier festgelegt werden, zu welchen Tageszeiten der Drucker verfügbar sein soll. Standardmäßig ist der Drucker immer verfügbar. Sie können jedoch auch festlegen, dass er nur zu bestimmten Zeiten benutzt werden kann. Hier können auch Prioritäten für Druckaufträge vergeben werden. Druckaufträge mit einer höheren Priorität werden zuerst gedruckt, egal, an welcher Stelle sie in der Warteschlange stehen. Druckaufträge mit einer geringen Priorität werden erst gedruckt, nachdem die Aufträge mit der hohen Priorität beendet wurden.

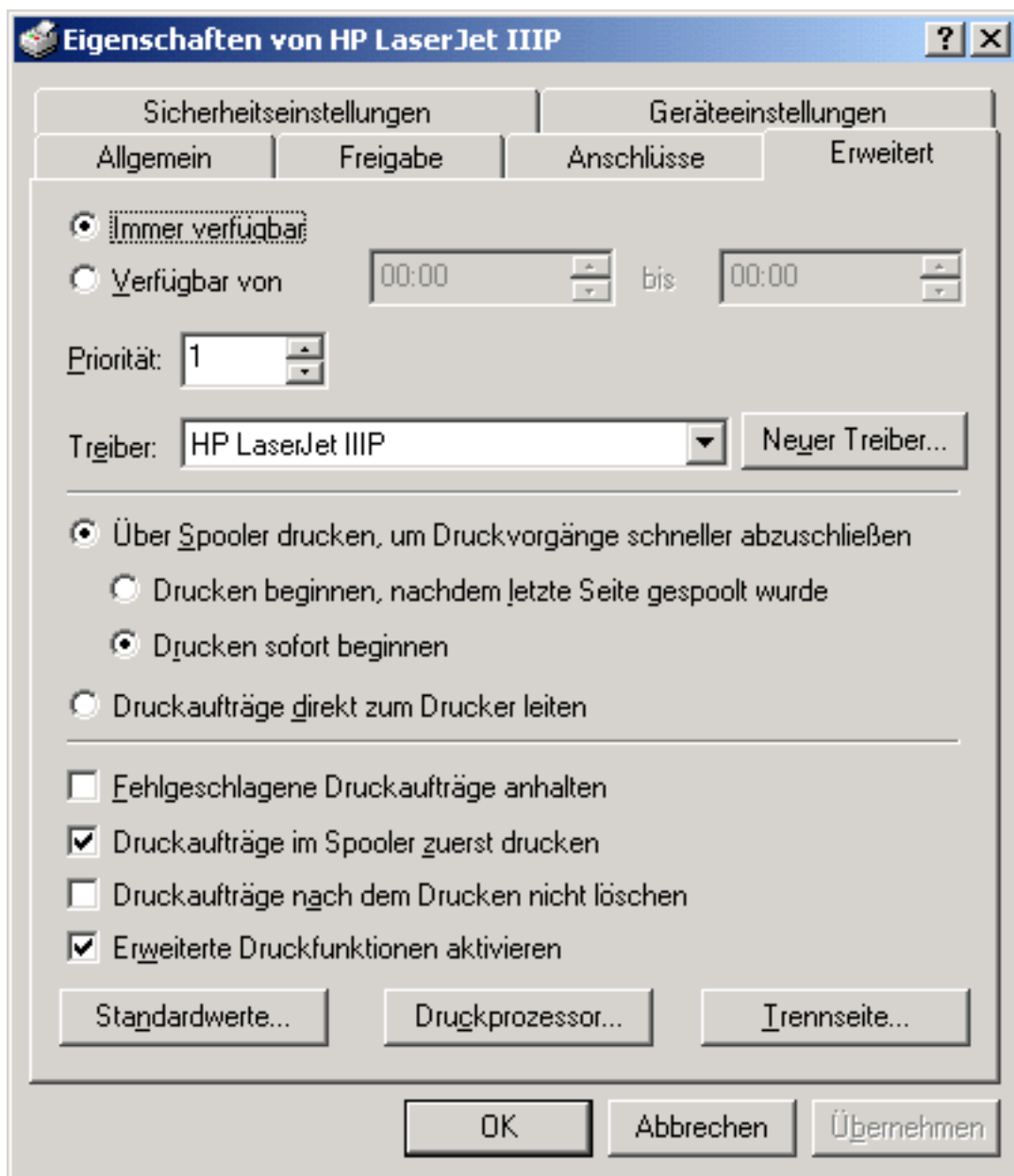


Abbildung 6.5: Die Registerkarte Erweitert im Eigenschaften-Dialogfeld des Druckers.

Auf der Registerkarte **Erweitert** können Sie auch den Treiber ändern, indem Sie entweder einen anderen aus dem Listenfeld **Treiber** auswählen oder auf die Schaltfläche **Neuer Treiber** klicken. Es öffnet sich der Assistent für die Druckertreiberinstallation, mit dem Sie einen Treiber von einer CD-ROM oder einen Treiber, den Sie aus dem Internet heruntergeladen haben, installieren können. Die Spooler-Optionen legen fest, wie das Druckspooling erfolgt. Normalerweise beginnt der Spooler sofort mit dem Ausdruck, nachdem die erste Seite gespoolt wurde. Wenn Druckaufträge häufig gelöscht

werden, sollte die Option **Drucken beginnen, nachdem letzte Seite gespooled wurde** aktiviert werden. Wenn der Benutzer warten möchte, bis der Drucker fertig ist, sollte er die Option **Druckaufträge direkt zum Drucker leiten** aktivieren. Der Spooler wird dann deaktiviert und die Anwendung wird gezwungen, auf den Drucker zu warten.

Die letzte Option auf der Registerkarte **Erweitert** bezieht sich auf den Spooler. Über das Kontrollkästchen **Fehlgeschlagene Druckaufträge anhalten** wird festgelegt, dass der Spooler Druckaufträge zurückhält, wenn die Einstellungen des Dokuments und des Druckers nicht übereinstimmen. Wenn für einen Druckauftrag z.B. festgelegt wurde, dass beide Seiten einer Seite bedruckt werden und der Drucker dies nicht unterstützt, wird der Druck angehalten, anstatt dass nur eine Seite bedruckt wird. Wird das Kontrollkästchen **Druckaufträge im Spooler zuerst drucken** aktiviert, werden die Druckaufträge gedruckt, die zuerst gespooled wurden, auch wenn sie eine geringere Priorität haben. Denken Sie daran, dass ein Druckauftrag ausgedruckt werden kann, bevor das Spooling beendet ist. Deshalb wird unabhängig von der Priorität immer zuerst der Druckauftrag beendet, der bereits gespooled wurde.

Wenn das Kontrollkästchen **Druckaufträge nach dem Drucken nicht löschen** aktiviert ist, wird ein Druckauftrag erst dann aus der Warteschlange entfernt, wenn er vollständig gespooled wurde. Auf diese Weise kann er bei Bedarf noch einmal gedruckt werden. Dies ist nützlich, wenn mehrere Dokumente mit mehreren Exemplaren ausgedruckt werden müssen, weil das Dokument von der Warteschlange aus noch einmal gedruckt werden kann und der Ausdruck nicht noch einmal über die Anwendung gestartet werden muss.

Über die Schaltfläche **Standardwerte** öffnet sich wie beim Befehl **Druckeinstellungen** das Dialogfeld **Druckstandardwerte für Drucker**. Über die Schaltfläche **Druckprozessor** kann ein anderer Druckprozessor ausgewählt werden. Ein Druckprozessor ist die Komponente, die die Ausgabe von einer Anwendung entgegennimmt, sie kompiliert und an den Druckertreiber sendet. Der Standarddruckprozessor heißt **WinPrint** und unterstützt verschiedene Optionen für einen Standarddatentyp. Normalerweise wird der Standarddatentyp nicht benutzt, sondern die Anwendung wählt einen Datentyp (normalerweise EMF) und sendet die Daten in diesem Datentyp. Am sichersten ist es, wenn die Standardeinstellung RAW beibehalten wird, weil der Druckauftrag dann nicht kompiliert wird, bevor er an den Drucker gesendet wird.

Über die Schaltfläche **Trennseite** lässt sich eine Trennseite festlegen, die vor jedem Druckauftrag gesendet wird, um die Ausdrücke der Druckaufträge leichter unterscheiden zu können.

Die Registerkarte Sicherheitseinstellungen

Auf der Registerkarte **Sicherheitseinstellungen** können Sie festlegen, wer den Drucker benutzen darf, wer die Einstellungen des Druckers verändern kann und wer die Dokumente in der Warteschlange verwalten darf. Standardmäßig haben nur die Mitglieder der Gruppe **Administratoren** und der Druck-Operator einen Vollzugriff auf den Drucker. Der **Ersteller-Besitzer** eines Druckauftrags darf nur Dokumente verwalten und Mitglieder der Gruppe **Jeder** dürfen nur drucken. Sie können entweder die Berechtigungen für die bereits vorhandenen Benutzer ändern, indem Sie die entsprechenden Kontrollkästchen aktivieren oder aber neue Benutzer hinzufügen. Abbildung 6.6 zeigt die Berechtigungen der Gruppe **Administratoren**.

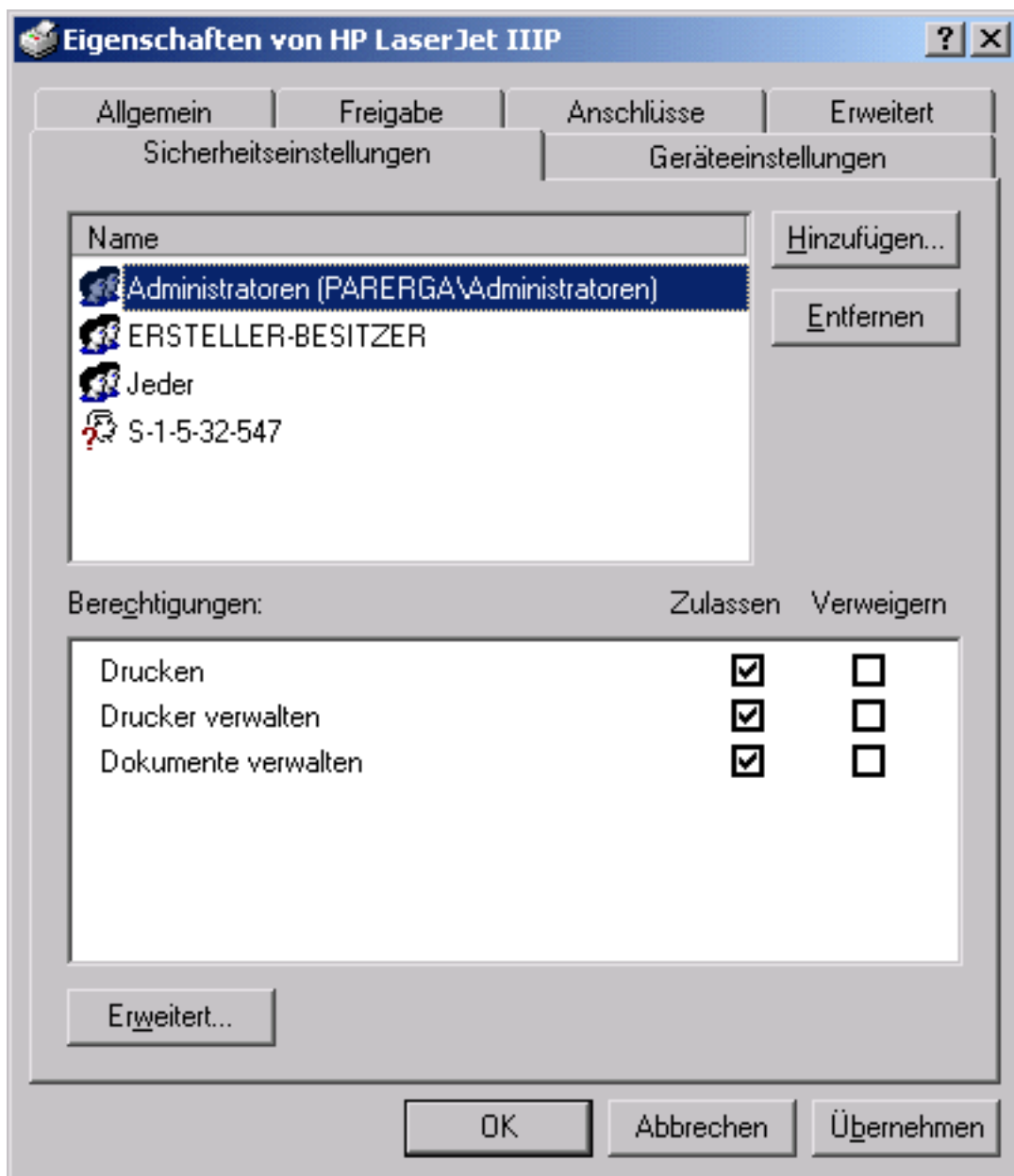


Abbildung 6.6: Die Standardsicherheitseinstellungen für eine Druckwarteschlange.

Die Registerkarte Geräteeeinstellungen

Auf der Registerkarte **Geräteeeinstellungen** stehen verschiedene Druckereinstellungen zur Auswahl. Die Geräteeeinstellungen sind vom Druckertyp abhängig. In der Regel handelt es sich um Einstellungen wie die Auswahl des Papierschachts, der Papierart und der installierten Schriftartkassette.

6.3.3 Die Befehle des Menüs Dokument

Das Menü **Dokument** der Druckerverwaltung enthält fünf Optionen, die nur dann aktiviert sind, wenn mindestens ein Dokument in der Warteschlange enthalten ist (und mindestens eines dieser Dokumente muss ausgewählt sein). Über die Befehle **Anhalten** und **Fortsetzen** lässt sich der ausgewählte Druckauftrag anhalten und der Ausdruck anschließend fortsetzen. Der Befehl **Neu starten** startet einen Druckauftrag noch einmal. Dies ist nützlich, wenn es einen Papierstau gibt und nur noch ein paar Seiten des Ausdrucks fehlen. Über den Befehl **Abbrechen** wird der markierte Druckauftrag aus der

Warteschlange entfernt.



Das Menü **Dokument** öffnet sich auch, wenn Sie mit der rechten Maustaste auf ein Dokument in der Warteschlange klicken. Das Kontextmenü entspricht dann dem Menü **Dokument** in der Menüleiste.

6.3.4 Die Eigenschaften eines Druckauftrags

Über den Befehl **Eigenschaften** können Sie die Eigenschaften des Druckauftrags betrachten (siehe Abbildung 6.7). Die einzigen Optionen, die Sie in diesem Dialogfeld ändern können, befinden sich auf der Registerkarte **Allgemein**. Im Feld **Benachrichtigen** können Sie einen Benutzer angeben, der benachrichtigt werden soll, wenn der Druckauftrag beendet ist. Über den Schieberegler im Bereich **Priorität** können Sie die Priorität des Druckauftrags verändern. Die Standardpriorität ist 1. Poweruser können also einfach die Priorität ihres Druckauftrags erhöhen und sich so vordrängeln. Über die Optionen im Bereich **Zeitplan** lässt sich festlegen, dass der Druckauftrag nur zu einer bestimmten Zeit gedruckt werden soll. Dies ist sehr nützlich, um umfangreiche Druckaufträge auf Zeiten zu verlegen, zu denen der Drucker nicht so stark ausgelastet ist.

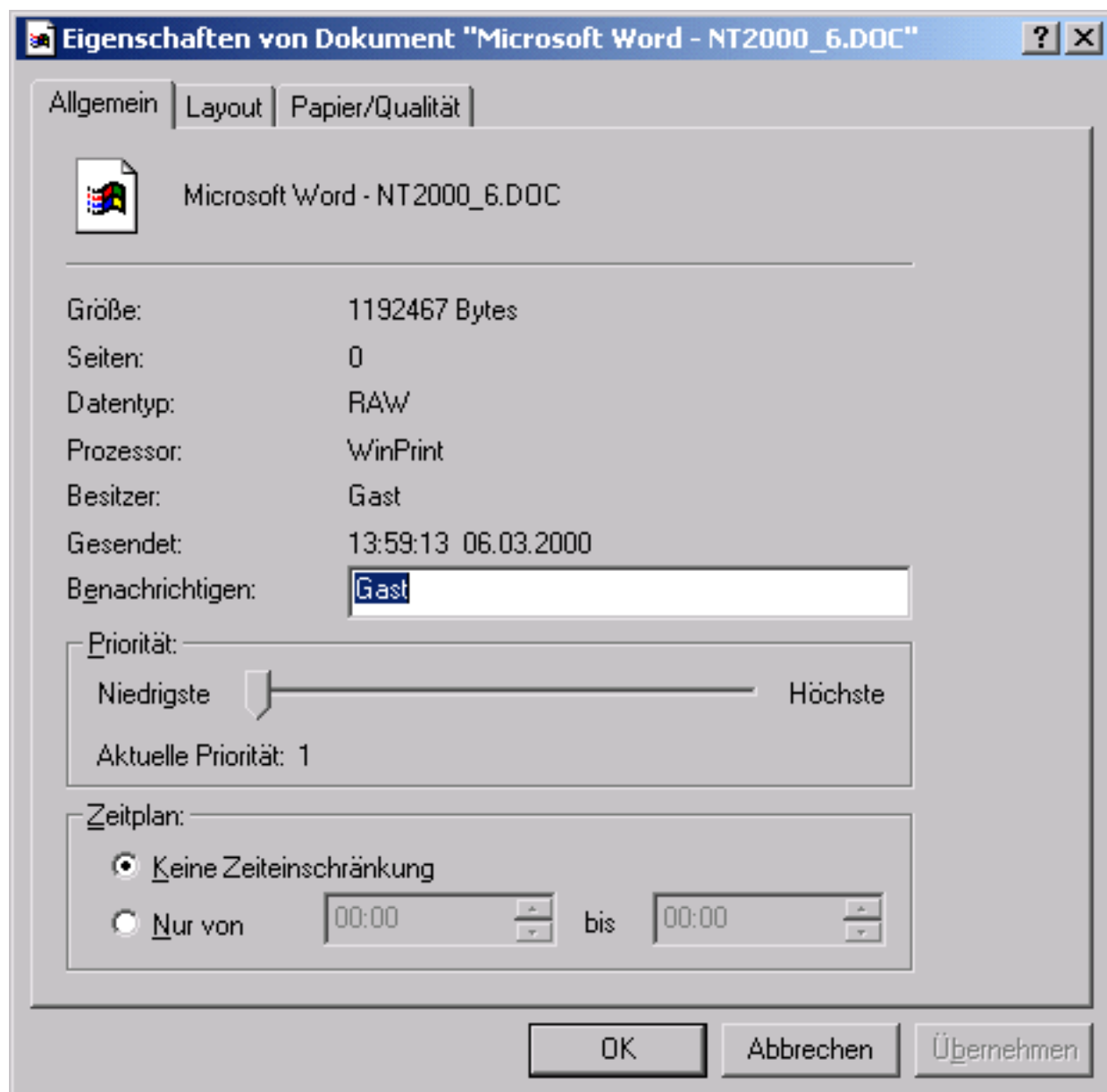


Abbildung 6.7: Die Eigenschaften eines Dokuments in der Warte-schlange. Es lassen sich die Benachrichtigung, die Priorität und der Zeitplan verändern.



Druckbenachrichtigungen werden über den Netzwerkbenachrichtigungsdienst versendet. Dieser entspricht dem alten WinPopup-Dienst in Windows für Workgroups 3.11. Sie können derartige Benachrichtigungen auch manuell versenden, indem Sie an der Eingabeaufforderung den Befehl `net send <Computer> <Nachricht>` eingeben, wobei <Computer> der Computernamen und <Nachricht> die Nachricht ist. Mit dem Befehl `net send millics Hallo` würden Sie z.B. dem Computer namens MILLCSS die Nachricht »Hallo« zusenden. Die Nachricht wird in einem Meldungsfenster angezeigt. Um Nachrichten zu deaktivieren, klicken Sie in der Systemsteuerung doppelt auf **Verwaltung** und dann auf **Dienste**. Deaktivieren Sie im Fenster **Dienste** den **Nachrichtendienst**.

Die Registerkarten **Layout** und **Papier/Qualität** sind schreibgeschützt. Die hier gezeigten Einstellungen können Sie verändern, wenn Sie im Menü **Drucker** der Druckerverwaltung den Befehl **Druckeinstellungen** wählen.

6.4 Warteschlangen über die Eigenschaften des Druckservers verwalten

Es gibt zwei verschiedene Methoden, um Druckwarteschlangen zu verwalten: über die Druckerverwaltung und über das Dialogfeld **Eigenschaften von Druckserver**. Die Druckerverwaltung wurde bereits ausführlich in diesem Kapitel beschrieben und bietet die Möglichkeit, die Anordnung von Druckaufträgen innerhalb einer Warteschlange und die Priorität der Druckaufträge zu verändern und Druckaufträge anzuhalten oder auch ganz aus der Warteschlange zu entfernen.

Um das Dialogfeld **Eigenschaften von Druckserver** zu öffnen, wählen Sie **Start/Einstellungen/Drucker** und im Ordner **Drucker** den Menübefehl **Datei/Servereigenschaften**. Das Dialogfeld **Eigenschaften von Druckserver** enthält die vier Registerkarten **Formulare**, **Anschlüsse**, **Treiber** und **Erweiterte Optionen**.

6.4.1 Die Registerkarte Formulare

Die Registerkarte **Formulare** (siehe Abbildung 6.8) stellt verschiedene Formulare zur Auswahl. Ein *Formular* bezieht sich auf die Papiergröße. Windows 2000 bietet Formulare für alle Standardpapiergrößen sowie Papiergrößen, von denen noch nie jemand gehört hat. Wenn Ihnen die vorhandenen Formulare nicht ausreichen, können Sie ein neues Formular erstellen, indem Sie das Kontrollkästchen **Neues Formular erstellen** aktivieren. Geben Sie den Namen des neuen Formulars und die Maßeinheiten des Papiers ein, d.h. die **Papiergröße** und die **Druckbereichsbegrenzungen**, und klicken Sie dann auf die Schaltfläche **Formular speichern**, um das neue Formular zu sichern.

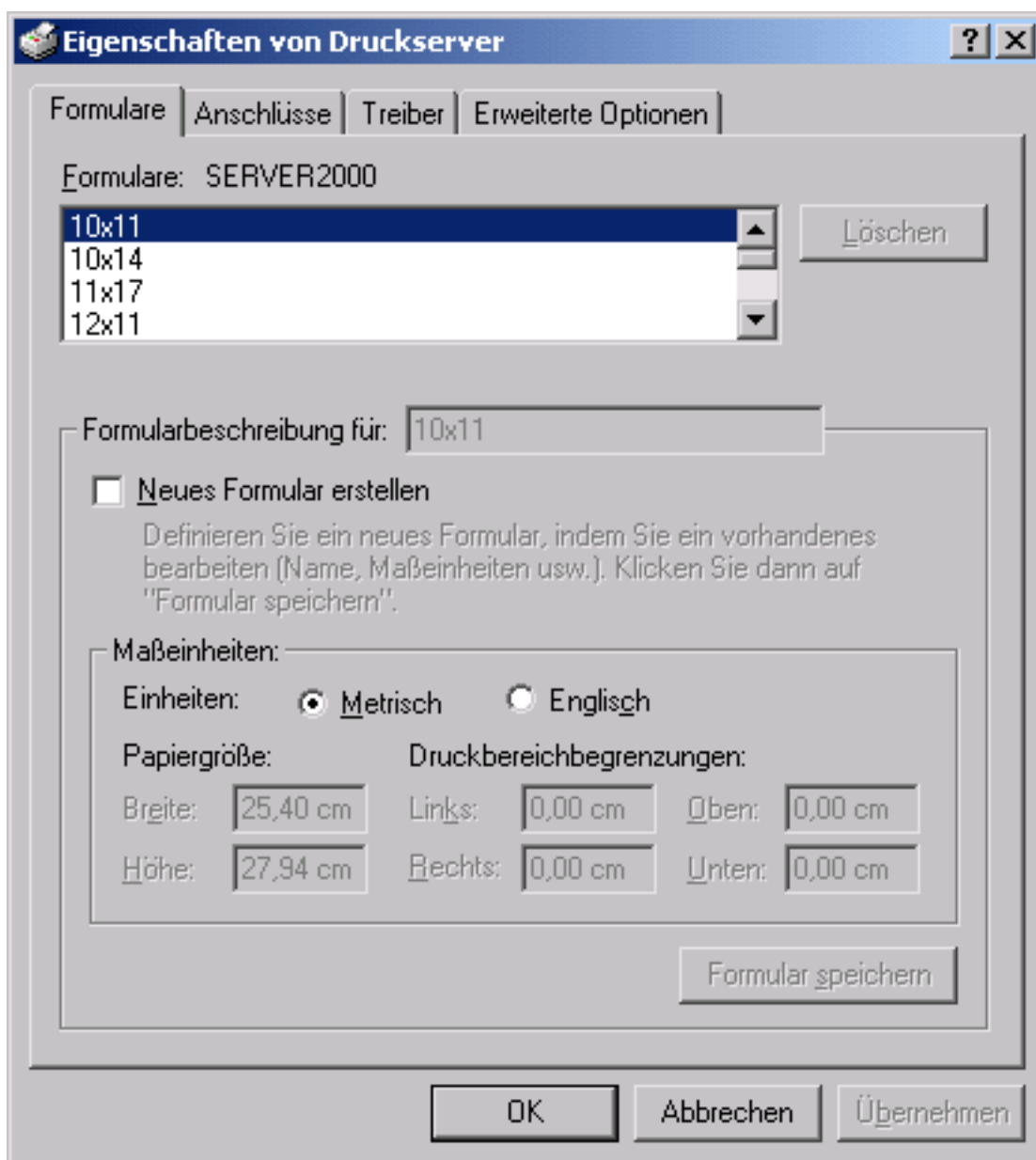


Abbildung 6.8: Auf der Registerkarte **Formulare** können Sie neue Seitenformate einrichten.

6.4.2 Die Registerkarte **Anschlüsse**

Wenn es zahlreiche Anschlüsse gibt, die keine Funktion haben, können sie auf dieser Registerkarte gelöscht werden (siehe Abbildung 6.9). Sie können auch neue Anschlüsse einrichten. Klicken Sie dazu auf die Schaltfläche **Hinzufügen**. Es öffnet sich das Dialogfeld **Druckeranschlüsse**. Wenn der gewünschte Anschlussstyp nicht in der Liste enthalten ist, klicken Sie auf die Schaltfläche **Neuer Anschlussstyp** und Sie werden aufgefordert, eine CD-ROM oder eine Datei anzugeben, die die Treiber für den neuen Anschluss enthält.

Ab jetzt öffnet sich ein für den Anschlussstyp spezifisches Dialogfeld, über das Sie den neuen Anschluss einrichten können. Für den Anschlussstyp **Standard TCP/IP Port** steht sogar ein Assistent zur Verfügung.

Um einen Anschluss zu löschen, wählen Sie diesen aus und klicken auf die Schaltfläche **Löschen**. Über die Schaltfläche **Konfigurieren** lässt sich, wie der Name schon sagt, der Anschluss konfigurieren. Bei

einem parallelen Anschluss kann z.B. das Intervall verändert werden, nach dem eine Zeitüberschreitung erfolgt und die Übertragung wiederholt wird. Bei einem seriellen Anschluss lassen sich die Geschwindigkeit der Datenübertragung und andere Einstellungen festlegen. Der Anschluss **File** lässt sich nicht konfigurieren.



Microsoft scheint alle Zeitüberschreitungsintervalle auf das Zehnfache des Werts zu setzen, der eigentlich gewählt werden sollte. Das Zeitüberschreitungsintervall von 90 Sekunden beim parallelen Anschluss ist ziemlich hoch. Wenn der Drucker innerhalb der ersten 10 Sekunden nicht antwortet, ist die Wahrscheinlichkeit hoch, dass er nicht aktiv oder nicht angeschlossen ist. Es ist dann ziemlich frustrierend, noch weitere 80 Sekunden warten zu müssen. Bei problematischen Druckern, wie z.B. bei tragbaren Geräten, sollte das Zeitüberschreitungsintervall verringert werden, um die Wartezeit zu verringern, wenn der Drucker nicht angeschlossen ist.

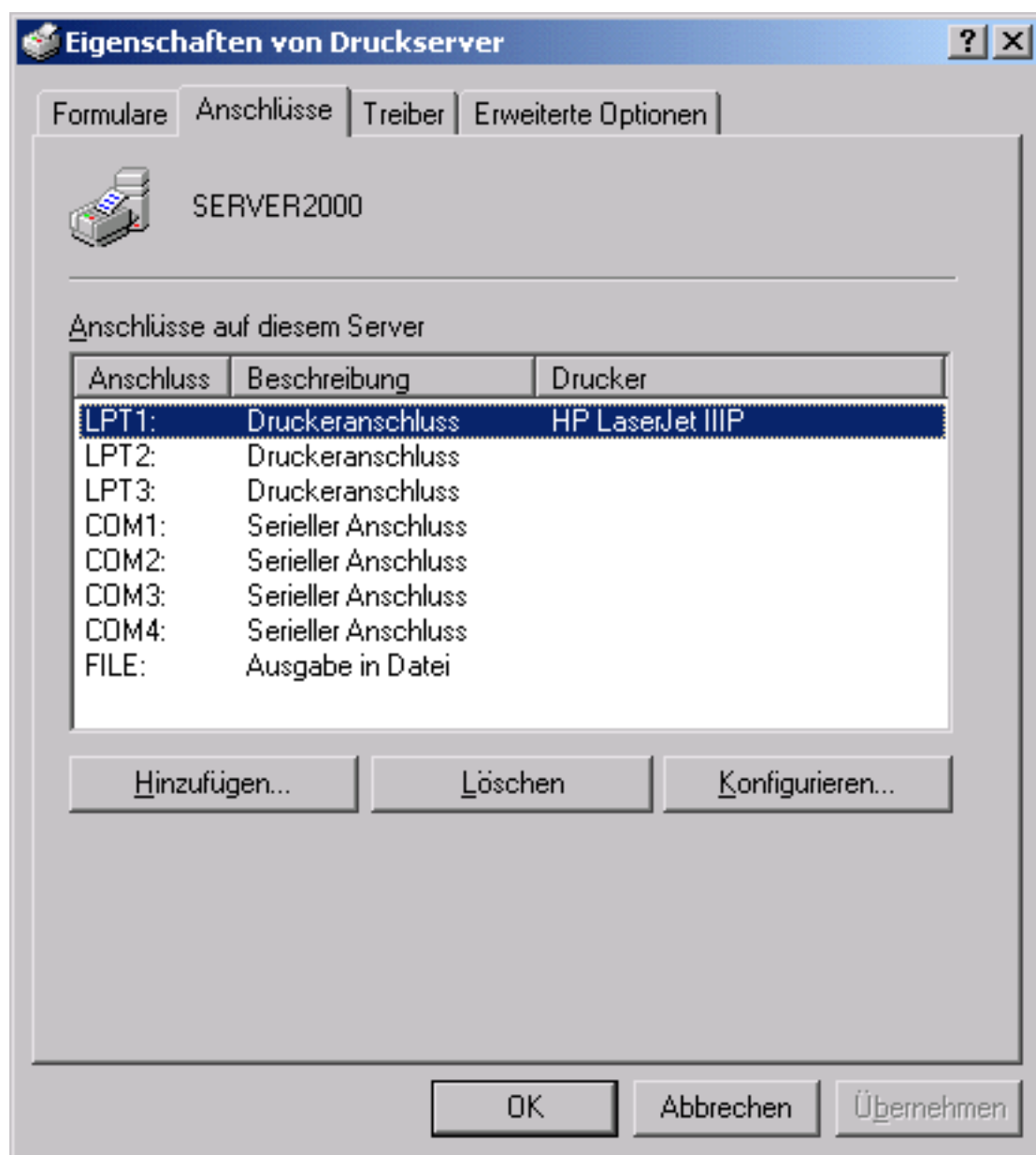


Abbildung 6.9: Die Registerkarte Anschlüsse im Dialogfeld Eigenschaften von Druckserver. Hier können Sie Anschlüsse entfernen und hinzufügen.

6.4.3 Die Registerkarte Treiber

Die Registerkarte **Treiber** (siehe Abbildung 6.10) ist sehr nützlich. Sie verwaltet die verschiedenen Druckertreiber, die auf dem Computer installiert sind. Hier lassen sich insbesondere Treiber entfernen, wenn sie nicht mehr benötigt werden. Außerdem lassen sich auch Treiber hinzufügen. Wie die Anschlüsse werden auch die Treiber üblicherweise über den **Druckerinstallations-Assistent** eingerichtet.

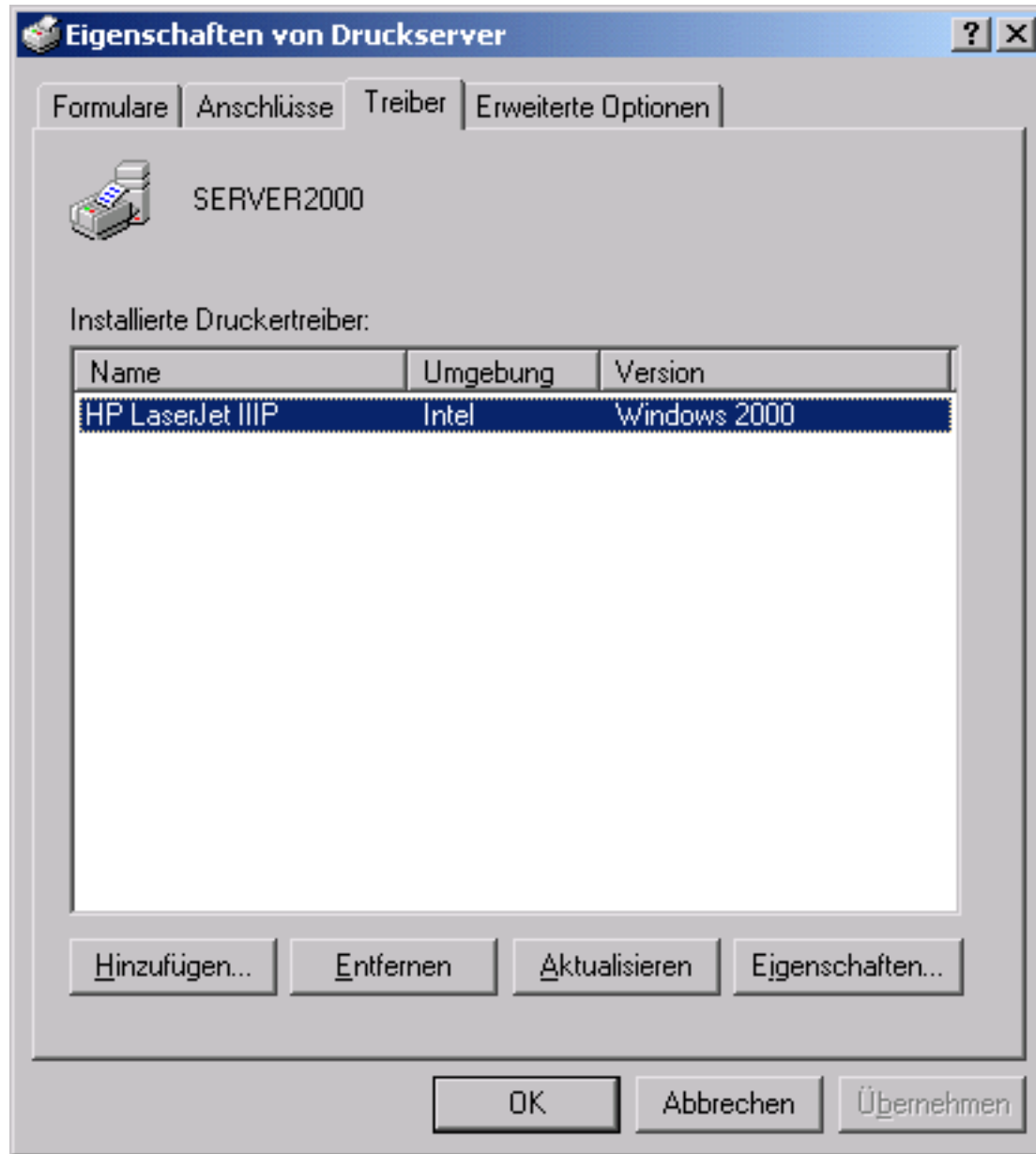


Abbildung 6.10: Die Registerkarte Treiber im Dialogfeld Eigenschaften von Druckserver enthält die auf einem Druckserver installierten Treiber.

Die Registerkarte **Treiber** enthält vier Schaltflächen. Über die Schaltfläche **Hinzufügen** lassen sich neue Treiber zum System hinzufügen. Diese Option ist nützlich, um Treiber für andere Betriebssystemarchitekturen wie beispielsweise Windows 98-Treiber für einen freigegebenen Drucker hinzuzufügen. Über die Schaltfläche **Entfernen** wird der markierte Druckertreiber entfernt.

Klicken Sie auf die Schaltfläche **Aktualisieren**, wird das lokale System nach einer neueren Version des

ausgewählten Treibers durchsucht und - falls vorhanden - sofort aktualisiert. Über die Schaltfläche **Eigenschaften** werden alle Dateien angezeigt, die mit dem ausgewählten Drucker verknüpft sind. Zu jeder Datei lassen sich außerdem Eigenschaften einblenden. Dies ist sehr nützlich, um Probleme mit DLL-Versionen zu verfolgen.

6.4.4 Die Registerkarte Erweiterte Optionen

Die Registerkarte **Erweiterte Optionen** (siehe Abbildung 6.11) enthält einige wenig bekannte und selten benutzte Optionen. Im Feld **Spoolordner** wird angegeben, wo die Druckaufträge gespooled werden. Über die drei Kontrollkästchen **Spoolerfehler protokollieren**, **Spoolerwarnungen protokollieren** und **Spoolerinformationen protokollieren** wird festgelegt, dass verschiedene Ereignisse im Ereignisprotokoll von Windows 2000 aufgezeichnet werden, das Sie über **Systemsteuerung/Verwaltung** und einen Doppelklick auf **Ereignisanzeige** öffnen. Normalerweise werden nur Fehler aufgezeichnet. Die Option **Signalton bei Fehlern von Remoteaufträgen** kann zwar ganz nützlich sein, wenn nur wenige Druckaufträge eingehen. Bei einem größeren Datencenter kann die Ausgabe von Signaltönen jedoch ziemlich nervtötend sein. Wird die Option **Benachrichtigen, wenn Remoteaufträge gedruckt wurden** aktiviert, erhalten die Benutzer eine Benachrichtigung, wenn der Druckauftrag fertig gestellt wurde. Wird das Kontrollkästchen **Computer benachrichtigen, wenn Remoteaufträge gedruckt wurden** aktiviert, erhält der Computer anstatt des Benutzers eine Benachrichtigung, dass der Druckauftrag beendet wurde. Dies ist nützlich, wenn der Druckauftrag von einem anderen Computer versendet wurde als dem, bei dem der Benutzer momentan angemeldet ist. Beachten Sie in Abbildung 6.11 den Pfad des Spoolordners, der im Teil Problembehandlung in diesem Kapitel benutzt wird.

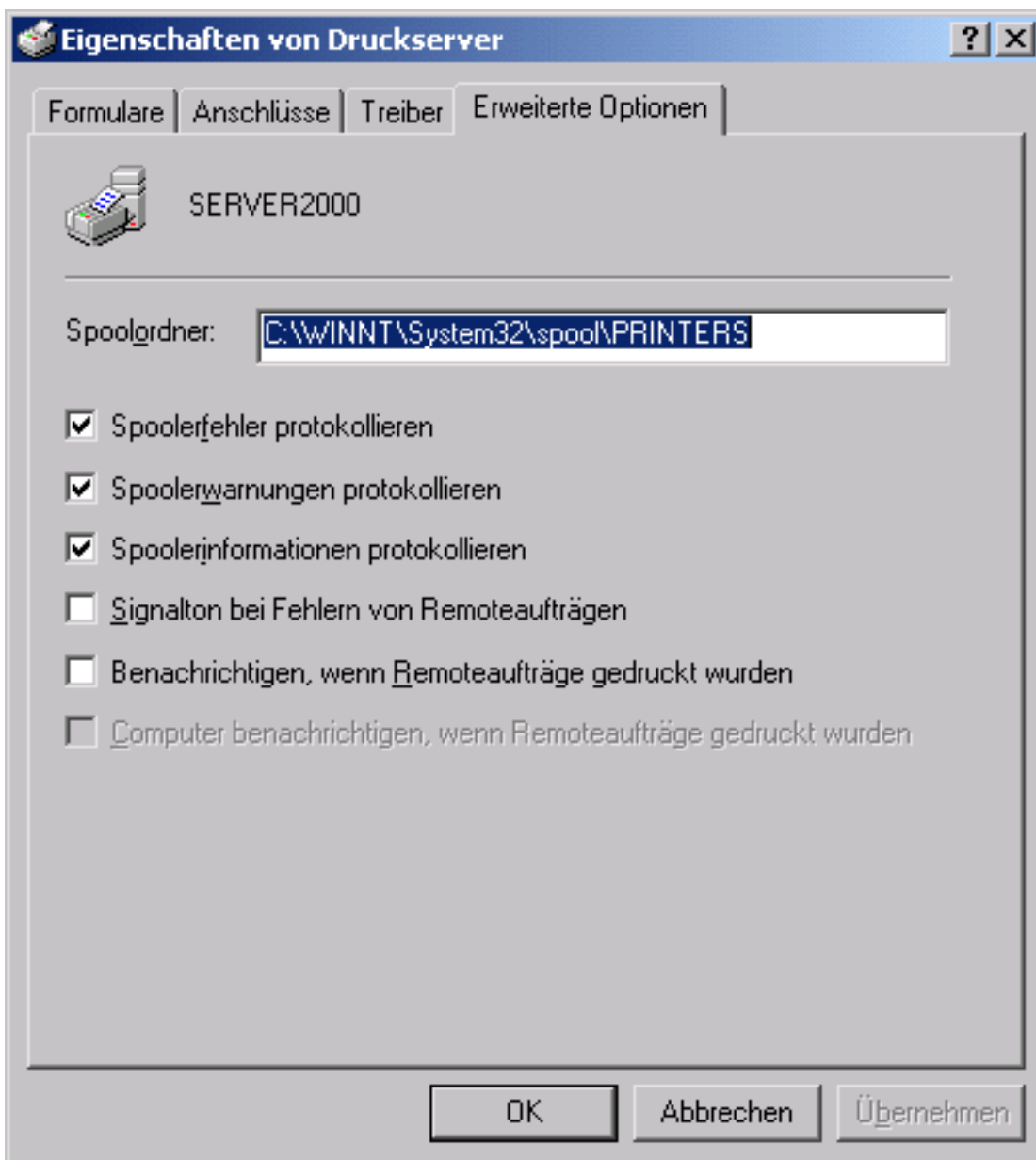


Abbildung 6.11: Die Registerkarte **Erweiterte Optionen** des Dialogfelds **Eigenschaften von Druckserver**.

6.5 Problembehandlung

Wie bereits in der Einleitung zu diesem Kapitel erwähnt, neigen Drucker im besten Fall zu Unzuverlässigkeit und zerstören im schlimmsten Fall den guten Ruf jedes Systemadministrators. Drucksysteme sind sehr komplex und beinhalten zahlreiche Teile, die aus verschiedenen Quellen stammen. Es gibt eine Folge von Problemen, für die kein Hersteller die Verantwortung übernehmen wird.

Beim Ausdruck treten zwei Arten von grundsätzlichen Problemen auf. Entweder kommt der Druckauftrag nicht beim Drucker an oder er wird nicht korrekt ausgedruckt. Als Erstes wird geprüft, was Sie tun können, wenn der Druckauftrag nicht gedruckt wird. Anschließend werden die Schritte genauer betrachtet, die Sie unternehmen müssen, wenn der Ausdruck nicht korrekt ist.

6.5.1 Probleme bei der Datenübertragung vom Client zum Server diagnostizieren

Eine Methode, um Druckprobleme zu behandeln, besteht darin, am einen Ende anzufangen und sich zum anderen Ende durchzuarbeiten, wie z.B. vom Client zum Drucker. Es ist jedoch wahrscheinlich besser, in der Mitte zu beginnen. Prüfen Sie, ob der Druckauftrag in der Mitte, d.h. in der Druckwarteschlange des Servers, ankommt. Falls nicht, können Sie die Suche auf die Verbindung zwischen Client und Server einschränken. Gehen Sie bei der Problembehandlung wie folgt vor:

1. Überprüfen Sie die Druckwarteschlange.
2. Überprüfen Sie den Server. Kontrollieren Sie dabei insbesondere die folgenden Dinge:
 - Stellen Sie fest, ob genügend freier Festplattenspeicher zur Verfügung steht.
 - Überprüfen Sie die Berechtigungen auf dem Server.
 - Werfen Sie einen Blick in das Ereignisprotokoll.
 - Prüfen Sie bei Netzwerkdruckern die Netzwerkumgebung.
 - Kontrollieren Sie den Drucker.
3. Überprüfen Sie den Client. Gehen Sie dabei jedes der nachfolgenden Elemente durch um sicherzustellen, dass es keine Probleme verursacht:
 - Prüfen Sie, ob auf dem Client genügend Festplattenspeicher zur Verfügung steht.
 - Nehmen Sie das Konto des Clients unter die Lupe.
 - Kontrollieren Sie die Druckereinstellungen.
 - Laden Sie die Druckertreiber neu.
4. Testen und diagnostizieren Sie andere Probleme.

Die Druckwarteschlange überprüfen

Gehen Sie zu einem Computer im Netzwerk und prüfen Sie, ob eine Verbindung zur Druckwarteschlange besteht. Wählen Sie dazu **Start/Einstellungen/Drucker** und gehen Sie die Liste der Drucker durch, die hier aufgeführt sind. Wenn der Drucker nicht verbunden ist, können Sie dies nachholen, indem Sie doppelt auf **Neuer Drucker** klicken und dann den neuen Drucker über den Druckerinstallations-Assistenten einrichten. Nachdem der Drucker installiert ist, öffnen Sie die Druckerverwaltung mit der Warteschlange, indem Sie doppelt auf den Drucker klicken.

Prüfen Sie als Erstes, ob irgendwelche Probleme angezeigt werden, wie z.B. Papierstau oder zu wenig Toner. Ob solche Nachrichten zur Verfügung stehen und wie genau sie sind, hängt vom Druckertreiber ab. Einige Druckertreiber geben an, dass Toner fehlt. Andere zeigen einfach nur eine Statusmeldung an, dass ein Eingriff durch den Benutzer erforderlich ist. In jedem Fall sollten Sie die Anzeige des Druckers und das Handbuch zum Drucker konsultieren um festzustellen, wie Sie den Drucker wieder funktionsfähig machen können.

Prüfen Sie anschließend, ob überhaupt Druckaufträge von dem Benutzer in der Warteschlange enthalten sind. Ist die Druckwarteschlange sehr lang, können Sie auch auf den Spaltenkopf **Besitzer** klicken, um die Warteschlange nach dem Besitzer zu sortieren. Wenn die Warteschlange Aufträge von dem Benutzer enthält, muss das Problem am Server liegen. Wenn überhaupt keine Aufträge beim Server angekommen

sind, liegen die Schwierigkeiten wahrscheinlich am Client.

Druckprobleme auf dem Server suchen

Wenn es Druckprobleme auf der Seite des Servers gibt, sollten Sie zunächst prüfen, ob für die Druckaufträge genügend Festplattenspeicher im Arbeitsverzeichnis des Spoolers zur Verfügung steht. Finden Sie als Erstes heraus, wo sich das Arbeitsverzeichnis des Spoolers befindet, indem Sie in der Systemsteuerung doppelt auf **Drucker** klicken und dann im Fenster **Drucker** den Menübefehl **Datei/Servereigenschaften** aufrufen. Aktivieren Sie die Registerkarte **Erweiterte Optionen** (siehe Abbildung 6.11) und betrachten Sie das Feld **Spoolordner**. In dem angegebenen Ordner legt der Spooler die Dateien ab, die ausgedruckt werden sollen. Um den verfügbaren Festplattenspeicher zu prüfen, öffnen Sie den **Arbeitsplatz** und klicken doppelt auf den Namen der Festplatte, auf der sich der Spoolordner befindet. Je nachdem, wie der Server eingerichtet wird, wird eine Grafik angezeigt, der Sie den verfügbaren Festplattenspeicher entnehmen können. Der Standardpfad ist `%SYSTEMROOT%\System32\Spool\Printers`.



Es ist sinnvoll, die Größe der Partition zu beschränken, die das Betriebssystem Windows 2000 auf dem Server enthält (siehe Kapitel 3). Weil der Spoolordner standardmäßig auf der Systempartition abgelegt wird, sollte die Systempartition jedoch vergrößert oder der Spoolordner auf einer anderen Partition abgelegt werden, wenn der Server sehr stark als Druckserver genutzt wird.

Wenn nicht genügend Festplattenspeicher zur Verfügung steht, sollten Sie entweder die nicht benutzten Dateien löschen oder den Spoolordner auf eine andere Festplatte verschieben. Wenn der Spoolordner verschoben wurde, muss der Spooler neu gestartet werden. Wenn sich der Spoolordner auf einer NTFS-Partition befindet, muss jeder, der den Drucker benötigt, die Berechtigung **Ändern** für diesen Ordner haben.

Wenn genügend Festplattenspeicher zur Verfügung steht und sich der Ordner auf einer NTFS-Partition befindet, sollten Sie prüfen, ob der Benutzer die Berechtigung **Ändern** für den Ordner hat. Die Benutzer benötigen diese Berechtigung, damit das Drucksystem die Druckaufträge in den Ordner schreiben kann.

Prüfen Sie als Nächstes das Ereignisprotokoll von Windows 2000 um festzustellen, ob dieses aufschlussreiche Nachrichten enthält. Diese Prüfung hätte zwar auch als Erstes erfolgen können, es geht aber wesentlich schneller zu prüfen, ob ausreichend Festplattenspeicher zur Verfügung steht. Das Ereignisprotokoll durchzusehen, kann etwas länger dauern und ziemlich mühselig sein. Öffnen Sie das Windows 2000-Ereignisprotokoll, indem Sie auf dem Server in der Systemsteuerung doppelt auf **Verwaltung** und im anschließend geöffneten Fenster doppelt auf **Ereignisanzeige** klicken. Wenn Sie von einem anderen Computer aus auf die Ereignisanzeige des Servers zugreifen wollen, wählen Sie in der Ereignisanzeige im Menü **Vorgang** den Befehl **Verbindung zu anderem Computer herstellen**. Geben Sie dann im Dialogfeld, das sich öffnet, im Feld **Anderen Computer** den Namen des Servers ein. Die Ereignisanzeige sehen Sie in Abbildung 6.12.

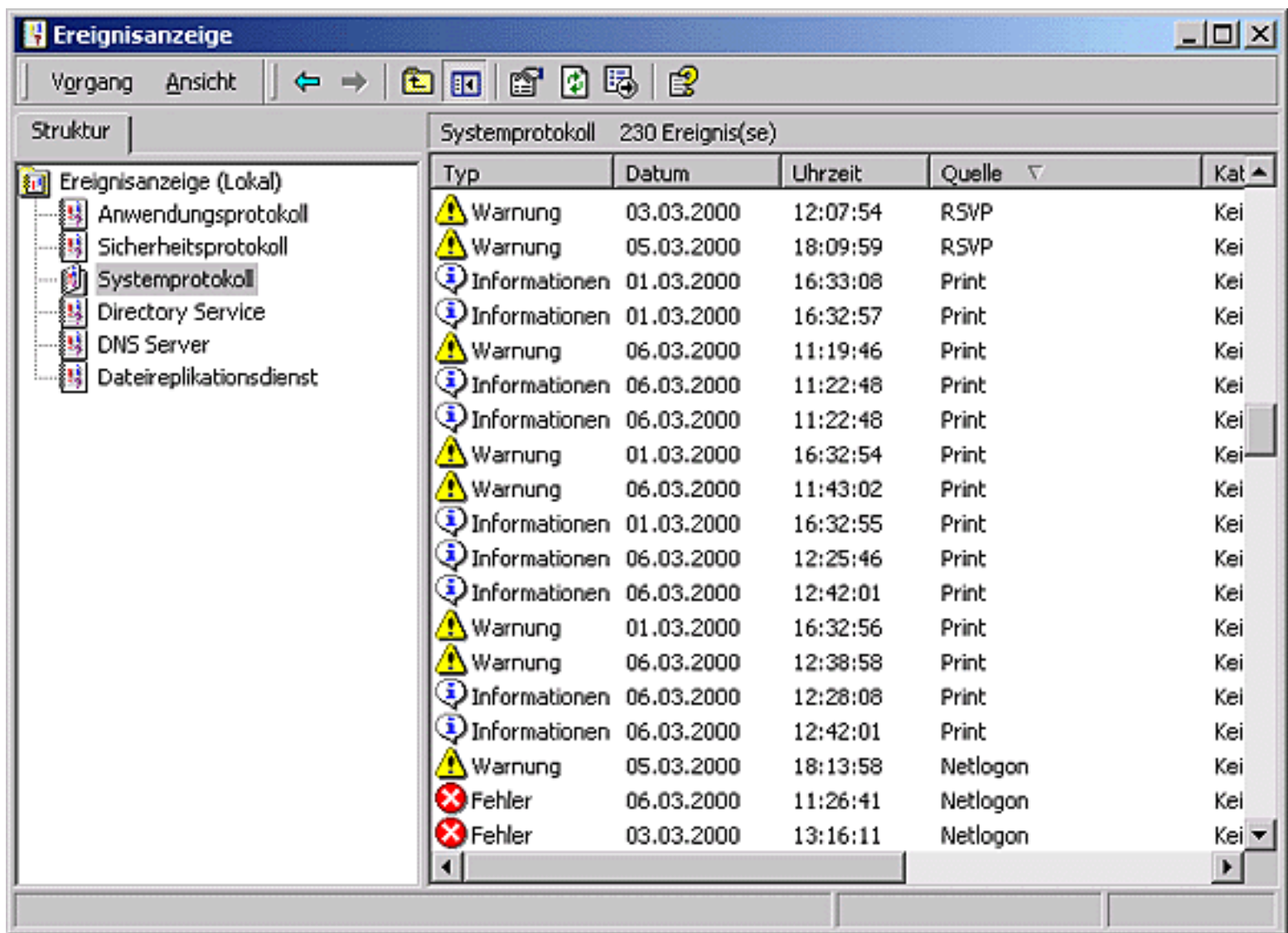


Abbildung 6.12: Die Ereignisanzeige dient dazu, Fehler zu finden. Hier wurden die Ereignisse nach der Quelle sortiert, um druckerbezogene Probleme zu finden.

Die Ereignisse, die für Druckprobleme relevant sind, stammen aus den Quellen **Spooler**, **Print** und möglicherweise auch **LPDSVC**. Der Spooler erzeugt Ereignisse, wenn Daten von der Druckwarteschlange auf den Drucker kopiert werden.

Die meisten Druckereignisse beziehen sich auf den Ausdruck vom Server und sind nicht besonders relevant, falls das Druckproblem nicht vom Server selbst stammt. Die Ereignisquelle LPDSVC ist der LPD-Dienst. Nach diesen Ereignissen müssen Sie Ausschau halten, falls der Client unter UNIX läuft und auf einem Windows 2000-Drucker druckt.

Typische Ereignisse, die Sie hier sehen werden, sind solche, die auftreten, wenn die Festplatte voll ist, ein Problem bei der Datenübertragung zum Drucker auftritt oder Probleme mit Berechtigungen auftreten. Wenn es keine relevanten Ereignisse gibt, sollten Sie den Spooler neu starten und fortfahren. Klicken Sie dazu in der Systemsteuerung doppelt auf **Verwaltung** und dann auf **Dienste**, klicken Sie mit der rechten Maustaste auf den Dienst **Druckwarteschlange** und wählen Sie den Befehl **Neu starten**.

Wenn es sich um einen TCP/IP-Drucker handelt, sollten Sie versuchen, die Adresse mit dem ping-Befehl zu überprüfen. Geben Sie dazu bei bestehender TCP/IP-Verbindung an der

Eingabeaufforderung den Befehl `ping <IP-Adresse>` ein. Um die Adresse herauszufinden, folgen Sie den Anweisungen, die Sie beim Druckserver finden. Die meisten Druckserver sind mit einer Diagnoseausgabe ausgestattet, die die Adresse nennt. Wenn die Adresse des Druckservers nicht auf einen ping-Befehl reagiert, kann niemand auf dem Drucker drucken. Dies liegt wahrscheinlich an einer fehlerhaften TCP/IP-Adresse des Druckservers oder der Workstation. Wenn die Workstation auf andere Netzwerkressourcen zugreifen kann, liegt das Problem am Druckserver. Ansonsten am Clientcomputer oder der Netzwerkinfrastruktur (Kabel, Hubs, Switches und Router) zwischen dem Client und dem restlichen Netzwerk.

Prüfen Sie als Nächstes den Status des Druckers. Wenn die Netzwerktests zeigen, dass der Drucker im Netzwerk erreichbar ist oder wenn der Drucker lokal an den Computer angeschlossen ist, sollten Sie versuchen, eine Testseite von einer anderen Workstation oder sogar vom Server zu drucken. Wählen Sie dazu **Start/Einstellungen/Drucker** und klicken Sie mit der rechten Maustaste auf den fraglichen Drucker. Wählen Sie im Kontextmenü den Befehl **Eigenschaften** und klicken Sie auf die Schaltfläche **Testseite drucken** am unteren Rand der Registerkarte **Allgemein** (siehe Abbildung 6.13). Wenn die Testseite korrekt ausgedruckt wird, ist alles bestens. Wird die Testseite nicht gedruckt (und auch von keiner anderen Workstation im Netz) und stapeln sich die Druckaufträge in der Warteschlange, sollten Sie den Drucker überprüfen.

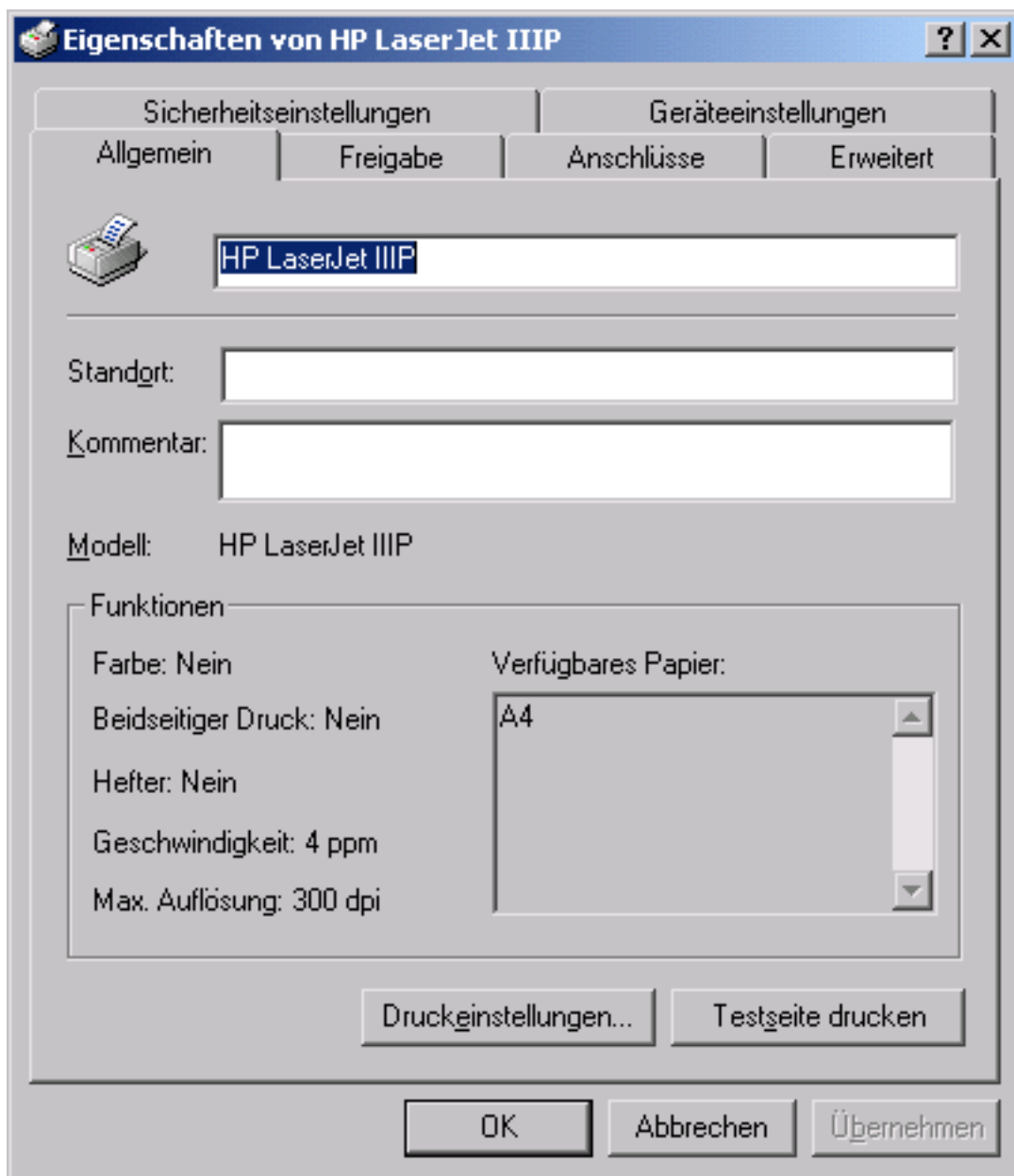


Abbildung 6.13: Klicken Sie auf die Schaltfläche Testseite drucken, um den Ausdruck zu prüfen. Der Druck von Testseiten kann bei der Diagnose sehr hilfreich sein.

Wenn Sie den Drucker überprüfen, sollten Sie als Erstes auf die Diagnosemeldungen auf der Druckerkonsole achten. Prüfen Sie anschließend die einfachen Dinge, nur um sicherzugehen, dass dem Drucker kein Papier fehlt und dass es keinen Papierstau im Drucker gibt. Prüfen Sie dann die Verkabelung zwischen Drucker und Computer und vergewissern Sie sich, dass alle Kabel fest verbunden sind. Manchmal führt eine lose Verbindung dazu, dass die Leitung glaubt, der Drucker sei in Betrieb, obwohl dieser keine Daten empfangen kann. Deshalb sollten Sie die Verbindungen immer mehrfach überprüfen.

Nun sollten alle Serverprobleme behoben sein. Der Server verfügt über genügend Festplattenspeicher und die passenden Berechtigungen, um die Druckaufträge auf die Festplatte zu spoolen. Die Kommunikation zwischen dem Server und dem Drucker wurde mit dem `ping`-Befehl überprüft und der Drucker ist betriebsbereit und mit ausreichend Papier und Toner ausgestattet. Nun sollten Sie noch zur letzten Sicherheit eine Testseite drucken. Der Dienst **Druckwarteschlange** wurde neu gestartet um

sicherzustellen, dass er aktiv ist. Wenn dies alles geprüft wurde, funktioniert der Serverpart des Drucksystems korrekt und Sie sollten den Client unter die Lupe nehmen.

Druckprobleme auf der Clientseite suchen

Druckprobleme auf der Clientseite lassen sich ziemlich leicht diagnostizieren. Dabei sollten Sie zuerst die grundlegende Funktionalität testen und sich dann nach oben arbeiten. Die einzelnen Schritte sollten Sie auf der Clientworkstation ausführen. Stellen Sie zuerst sicher, dass sich der Benutzer korrekt angemeldet hat. Normalerweise braucht sich der Benutzer dazu nur ab- und erneut anzumelden. Manchmal kommt es vor, dass ein Benutzer sein Kennwort auf einem Computer ändert, während er bei einem anderen Computer angemeldet ist. Die Sicherheitstoken auf dem anderen Computer sind dann nicht mehr gültig und müssen durch eine Neuansmeldung ersetzt werden.

Nachdem der Benutzer sich ab- und erneut angemeldet hat, wählen Sie **Start/Einstellungen/Drucker**. Klicken Sie doppelt auf den fraglichen Drucker, um sich zu vergewissern, dass der Benutzer die Druckaufträge sehen kann, die an den Drucker gesendet werden. Möglicherweise wurde einfach der Druckernamen falsch geschrieben. Betrachten Sie anschließend die Eigenschaftenseite und prüfen Sie folgende Einstellungen:

- Vergewissern Sie sich auf der Registerkarte **Anschlüsse**, dass der Drucker mit dem korrekten Anschluss mit dem Server verbunden ist (z.B. `\\Server\Drucker`).
- Stellen Sie auf der Registerkarte **Erweitert** sicher, dass das Kontrollkästchen **Fehlgeschlagene Druckaufträge anhalten** nicht aktiviert ist. Ist dieses Kontrollkästchen aktiviert, wird der Ausdruck von Dokumenten angehalten, die einen Druckdienst (wie beim beidseitigen Druck) benötigen oder eine Formulargröße haben, die vom Drucker nicht unterstützt wird.
- Prüfen Sie außerdem auf der Registerkarte **Erweitert** den Treibernamen und vergewissern Sie sich, dass er zum Drucker passt, der angeschlossen ist. Wenn der Druckertreiber nicht zum DruckermodeLL passt, müssen Sie den korrekten Treiber installieren.
- Prüfen Sie auf der Registerkarte **Sicherheitseinstellungen**, ob der Benutzer nicht irgendwie seinen Zugriff auf den Drucker aufgehoben hat.
- Klicken Sie auf der Registerkarte **Allgemein** auf die Schaltfläche **Testseite drucken** und prüfen Sie, ob die Testseite ausgedruckt wird.

Falls schließlich eine Testseite ausgedruckt wird, sollte das Problem eigentlich gelöst sein. Sie sollten aber trotzdem noch einmal überprüfen, ob der Benutzer von der Anwendung aus drucken kann, die die Probleme verursacht. Einige Grafikanwendungen sind sehr wählerisch, was den Ausdruck betrifft.

Wenn der Ausdruck noch immer nicht funktioniert, sollten Sie prüfen, ob auf der Systempartition des lokalen Computers genügend Festplattenspeicher zur Verfügung steht. Bei Windows 2000-Workstations sollten Sie den Spoolordner prüfen und, wie bereits beschrieben, sicherstellen, dass auf dem Laufwerk genügend Speicherplatz für den Spooler zur Verfügung steht. Ist dies nicht der Fall, sollten Sie die Festplatte aufräumen oder den Spoolordner in ein anderes Verzeichnis verschieben. Öffnen Sie bei einem Windows 9.x-Computer eine MS-DOS-Eingabeaufforderung und geben Sie den Befehl `set` ein. Suchen Sie nach Zeilen, in denen `TEMP=` steht und vergewissern Sie sich, dass im angegebenen Verzeichnis genügend Speicherplatz verfügbar ist. Prüfen Sie dann den Temp-Ordner. Wenn bereits sehr viele temporäre Dateien enthalten sind, sollten Sie das System neu starten und so viele Dateien wie möglich löschen. Beim FAT-Dateisystem gibt es eine Beschränkung für die Anzahl der Verzeichnisse, die in

einem Verzeichnis enthalten sein dürfen. Wenn die Grenze erreicht ist, können keine neuen Dateien mehr angelegt werden und somit kann auch nichts ausgedruckt werden. Es passieren dann auch andere seltsame Dinge (von Microsoft offiziell als unvorhersehbare Ergebnisse bezeichnet). Anwendungen werden beispielsweise unerwartet geschlossen, ohne dass Sie Ihre Daten speichern können.

Nachdem Sie die Eigenschaftenseiten und den Festplattenspeicher geprüft haben, gibt es normalerweise nur noch eines, was Sie tun können. Löschen Sie die Druckwarteschlange, indem Sie den Drucker im Ordner **Drucker** markieren und die (Entf)-Taste drücken. Richten Sie dann den Drucker neu ein. Achten Sie darauf, dass die Druckertreiber entweder vom Server stammen oder von einer anderen Quelle, von der Sie wissen, dass die Treiber funktionieren. Wenn Sie nun eine Testseite ausdrucken, sollte alles korrekt funktionieren.

Es hat alles nichts genützt. Was nun?

Wenn keine der beschriebenen Techniken zur Problembehandlung funktioniert hat, finden Sie hier noch ein paar Hinweise, die Sie ausprobieren können. Mit diesen Techniken werden die Druckertreiber im Wesentlichen umgangen, um das Problem besser isolieren zu können. Wenn der Drucker lokal an die parallele Schnittstelle angeschlossen ist, müssen Sie anders vorgehen als bei einem Netzwerkdrucker. Für beide Ansätze benötigen Sie einige Dinge. Handelt es sich nicht um einen PostScript-Drucker, benötigen Sie eine Textdatei. Eine Textdatei mit ein bis zwei Seiten Text reicht dabei völlig aus. Wenn Sie eine solche Datei neu erstellen müssen, öffnen Sie den Editor und tippen zwei Seiten Text ein. Wenn es sich um einen PostScript-Drucker handelt, müssen Sie eine Datei finden, die PostScript-Befehle enthält. Auf den Disketten oder der CD-ROM zu Ihrem Drucker sollten Sie etwas Passendes finden. Kopieren Sie die Datei (die Text- oder PostScript-Datei) in einen Ordner namens *C:\Prtest*.

Lokale Drucker testen

Wenn ein Drucker direkt über die parallele Schnittstelle an einen Server angeschlossen ist und nicht druckt, können Sie wie folgt einen Ausdruck erzwingen: Öffnen Sie eine Eingabeaufforderung und kopieren Sie die Datei direkt auf den Druckeranschluss. Für eine Textdatei namens *Test.txt* würde der Befehl wie folgt lauten:

```
Copy c:\prtest\test.txt lpt1:
```

Mit diesem Befehl wird der Druckauftrag direkt zum Drucker gesendet. Beim PostScript-Drucker müssen Sie die PostScript-Datei auf dieselbe Weise zum Drucker kopieren. Nachdem Sie die Textdatei an den Drucker geschickt haben, müssen Sie möglicherweise entweder die Form Feed-Taste an Ihrem Drucker (siehe das Druckerhandbuch) drücken oder den Befehl `Copy Con LPT1:` ausführen. Dieser Befehl kopiert das, was an der Eingabeaufforderung eingegeben wird, auf den Druckeranschluss LPT1. Tippen Sie, nachdem Sie den Befehl eingegeben haben, `Ctr l+L` ein und drücken Sie die (Enter)-Taste. Geben Sie dann `Ctr l+Z` ein und drücken Sie nochmals die (Enter)-Taste. Der Befehl `Ctr l+L` bewirkt einen Zeilenvorschub und mit dem Befehl `Ctr l+Z` wird das Dateiende gekennzeichnet. Der Drucker müsste nun ein Blatt Papier ausgeben, das die zweite Seite der Textdatei enthält.

Wenn dies nicht funktioniert, haben Sie vermutlich versucht, eine Textdatei an einen PostScript-Drucker

zu senden, was nicht funktioniert. Die Sprache PostScript verwendet einen speziellen Befehlssatz und wenn nicht die korrekten Informationen am Anfang und am Ende der Datei stehen, wird die Datei nicht ausgedruckt und der Drucker erzeugt eine Fehlermeldung. Wenn es sich definitiv nicht um einen PostScript-Drucker handelt, funktioniert entweder der Drucker nicht korrekt oder die Verkabelung zwischen dem Computer und dem Drucker ist defekt. Sie sollten es dann einmal mit neuen oder anderen Kabeln versuchen.

Über TCP/IP verbundene Drucker testen

Wenn ein Drucker über TCP/IP mit dem Computer verbunden ist, kann das Testen etwas schwierig sein. Als Erstes sollten Sie über den Druckserver eine Testseite zum Drucker senden. Es gibt zwei Arten von Druckservern: interne und externe. Die internen Geräte sind Karten, die in die einzelnen Drucker integriert sind, wie z.B. eine HP JetDirect-Karte in einem HP LaserJet-Drucker. Normalerweise müssen Sie die Statusseite über die internen Setup-Menüs des Druckers ausdrucken. Die externen Geräte sind schwarze Kästen mit einem oder mehreren parallelen Schnittstellen und normalerweise nur einer Taste, um den Drucker zu testen. Diese externen Geräte gibt es von HP, NetGeard und Intel. Lesen Sie die zugehörige Dokumentation um festzustellen, wie Sie mit diesen Geräten Statusseiten ausdrucken.

Nachdem die Statusseite gedruckt wurde, sollten Sie sich vergewissern, dass die TCP/IP-Adresse korrekt ist und über denjenigen Windows 2000 Server-Computer erreicht werden kann, der als Host für die Druckwarteschlange fungiert. Außerdem unterstützen externe Druckserver normalerweise die Konfiguration über Telnet. Mehr zu Telnet erfahren Sie in Kapitel 19. Lesen Sie die Anleitung zum Druckserver um zu erfahren, wie die Telnet-Schnittstelle zum Druckserver benutzt wird.

Wenn die Statusseite nicht gedruckt wird, funktioniert der Druckserver nicht korrekt. Prüfen Sie alle Setup-Informationen und rufen Sie bei Bedarf den Kundendienst des Herstellers an. Diese Geräte haben in der Regel ein sehr kompliziertes Setup. Wenn sie aber einmal korrekt konfiguriert sind, funktionieren sie prima. Wenn die TCP/IP-Adresse vom Server aus nicht zu erreichen ist, sollten Sie das TCP/IP-Kapitel in diesem Buch lesen um zu erfahren, wie Subnet-Masken funktionieren. Setzen Sie dann die TCP/IP-Adresse zurück. Weitere Einzelheiten finden Sie in Kapitel 8.

Drucker durch Protokollierung der Anschlüsse testen

Wenn die beiden letzten Tests nicht funktionieren, liegt der Fehler vielleicht an der Verbindung von Windows 2000 zum Drucker oder die Druckertreiber sind nicht korrekt. Prüfen Sie als Erstes die Verbindung zum Drucker. Die Behandlung von Treiberproblemen wurde bereits beschrieben.

Öffnen Sie die Eingabeaufforderung und geben Sie den folgenden Befehl ein:

```
Net use lpt1: \\Server\Drucker
```

Sie müssen natürlich den Server- und Druckernamen von Ihrem System einsetzen. Wenn an die Schnittstelle LPT1 bereits ein Drucker angeschlossen ist, geben Sie einen anderen Port an (LPT2, LPT3 oder LPT4).

Kopieren Sie als Nächstes mit dem Copy-Befehl eine Textdatei über die Netzwerkfreigabe auf den Drucker. Dadurch werden alle Druckertreiber umgangen und die Daten werden direkt an den Drucker

gesendet.

6.5.2 Probleme mit der Druckqualität diagnostizieren

Moderne Drucker sollten eine konsequent hohe Qualität bieten, die lesbar ist und die korrekten Schriftarten, Graustufen und Farben verwendet. Manchmal geht auch bei guten Druckern etwas schief und Windows 2000 füttert sie mit den falschen Informationen. In diesem Abschnitt wird beschrieben, wie Sie die Leistung und Qualität eines Druckers erhöhen. Das bestmögliche Ergebnis erzielen Sie, wenn Sie

- die Grenzen des Druckers kennen,
- die Druckerspezifikationen kennen,
- die Treiberversionen kennen,
- sicherstellen, dass alles zusammenpasst.

Bei den ersten drei Punkten müssen Sie herausfinden, was der Drucker leistet. Dazu gehören Angaben wie die Anzahl der gedruckten Seiten pro Sekunde, die Auflösung und die Farbtiefe. Mit dem letzten Punkt wird sichergestellt, dass Windows 2000 all diese Beschränkungen kennt und in die Druckausgabe einbezieht.

6.5.3 Die Grenzen des Druckers kennen

Ein Drucker hat alle möglichen Grenzen, wie z.B. die Druckgeschwindigkeit, die Anzahl der Grafiken, die er pro Sekunde erzeugen kann, die maximale Anzahl von Farben oder Graustufen, die er drucken kann und andere. Angaben zu diesen Beschränkungen finden Sie normalerweise im Druckerhandbuch. Die meisten Hersteller bieten Onlineversionen ihrer Handbücher, die sich durchsuchen lassen. Hier ein paar Dinge, die Sie in Erfahrung bringen sollten:

- Wie schnell sollte der Drucker drucken?
- Wie viele Farben kann der Drucker drucken?
- Welche Schriftarten sind im Drucker installiert?
- Um welches DruckermodeLL handelt es sich genau?

Die meisten Informationen finden Sie im Druckerhandbuch oder auf der Statusseite des Druckers.

6.5.4 Die Druckerspezifikationen kennen

Unternehmen kaufen häufig Drucker und stattdessen diese dann mit Schriftartkassetten und zusätzlichem Speicher aus. In einigen Fällen wird jedoch Speicher entfernt, um Geld zu sparen. Dies klingt zwar kurzsichtig, wenn ein Unternehmen jedoch tausend Drucker kauft, können ein paar hundert Mark pro Drucker schon eine ganze Menge ausmachen. Sie sollten also unabhängig vom Druckerhandbuch genau prüfen, wie viel Speicher im Drucker installiert ist und welche Schriftartkassetten vorhanden sind. Auch hier kann die Statusseite vermutlich einigen Aufschluss bieten. Manche Drucker drucken auch eine Seite mit allen Schriftarten aus, die im Drucker installiert sind.

6.5.5 Die Treiberversionen kennen

Es ist sehr wichtig zu wissen, welche Treiberversionen für einen bestimmten Drucker auf dem Server installiert sind. Sie sollten nicht nur die Versionen, sondern auch das Datum der Dateien kennen, weil manche Hersteller ihre Versionsnummern nicht korrekt vergeben. Die Version 2.2 kann also durchaus neuer sein als die Version 2.3. Prüfen Sie auf der Website des Herstellers, ob neue Treiberversionen vorliegen, und lesen Sie die Dokumentation der Treiber sorgfältig durch. Installieren Sie nur dann neue Treiber, wenn diese die Probleme lösen oder eine wesentliche Verbesserung bieten. Wenn Sie Treiber installieren, sollten Sie sicherstellen, dass Sie die Treiber für alle Betriebssysteme und Architekturen installieren, die unterstützt werden und die den Server zum Ausdruck benutzen. Wenn die Treiber auf dem Server aktuell sind, sollten die Workstations, die diese Treiber nutzen, ebenfalls immer auf dem neuesten Stand sein.

6.5.6 Sicherstellen, dass alles zusammenpasst

Nachdem Sie alle Informationen gesammelt haben, sollten Sie sich vergewissern, dass die Merkmale von Windows 2000 und dem Druckserver tatsächlich übereinstimmen. Öffnen Sie dazu das Dialogfeld **Erweiterte Optionen** (siehe Abbildung 6.14) über den Menübefehl **Start/Einstellungen/Drucker**. Klicken Sie doppelt auf den gewünschten Drucker und rufen Sie in der Druckerverwaltung den Menübefehl **Datei/Druckeinstellungen** auf. Klicken Sie dann im Dialogfeld **Druckeinstellungen** auf der Registerkarte **Layout** die Schaltfläche **Erweitert** an.

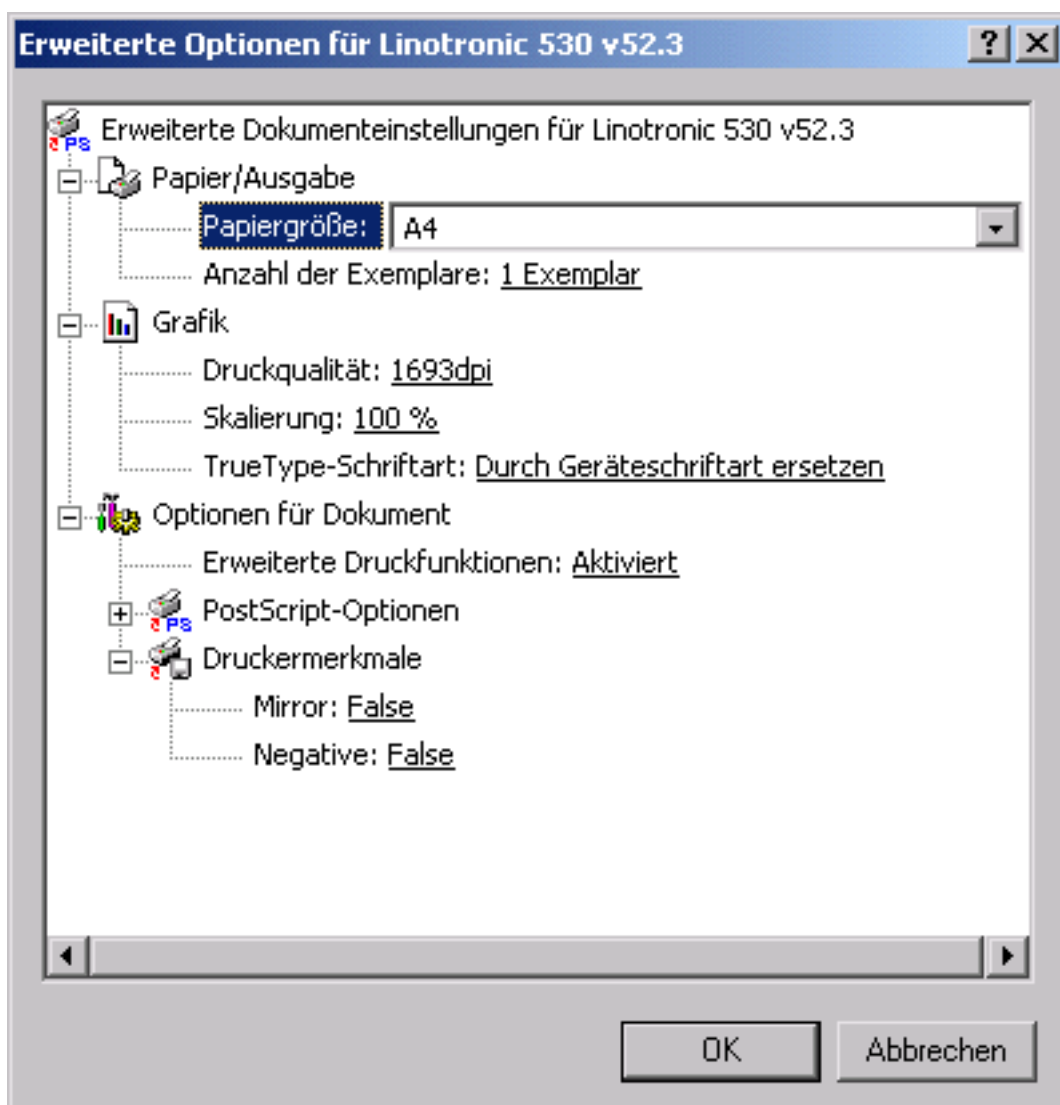


Abbildung 6.14: Im Dialogfeld **Erweiterte Optionen** können Sie prüfen, ob der Drucker genau das bietet, was Windows 2000 glaubt.

Im Dialogfeld **Erweiterte Optionen** werden alle Optionen des Druckers angezeigt. Die Optionen sind dabei vom Drucker abhängig. Vergewissern Sie sich, dass Windows 2000 über die korrekte Speichergröße informiert ist und dass die Schriftzuordnungen korrekt sind. Über die Schriftzuordnungen stellt der Drucker fest, ob eine Schriftart bereits installiert ist. Wenn eine Schriftart, die in einer Anwendung verwendet wird, einer Druckerschriftart zugeordnet werden kann, wird sie nicht auf den Drucker übertragen, sondern es wird die integrierte Schriftart des Druckers verwendet. Normalerweise resultiert dies in einer höheren Druckqualität und einem schnelleren Ausdruck, weil die Schriftart nicht übertragen werden muss. Sie sollten außerdem die Druckqualität für Grafiken und die Farbzusammenordnungen prüfen. Insbesondere bei älteren Druckern kann es manchmal zu Abweichungen bei den Angaben kommen.

Kapitel 7 Die Registrierung

Bei jedem, der mit Windows NT, Windows 95 oder Windows 98 vertraut ist, sollten beim Begriff *Registrierung* Bilder des Registrierungs-Editors und vieler anderer Dinge aufkommen. Die Registrierung wird einerseits unbedingt benötigt und Sie sollten sich damit auskennen. Andererseits ist der Umgang mit der Registrierung auch gefährlich und es entstehen ernsthafte Probleme, wenn die Registrierung falsch bearbeitet wird. An eines sollten Sie immer denken: Um einen Windows-Computer völlig unbrauchbar zu machen, brauchen Sie nur die Registrierung durcheinander zu bringen. Dieses Kapitel beschreibt sichere Methoden zum Umgang mit der Registrierung. Die Wahrscheinlichkeit, dass Probleme auftreten, ist damit geringer.

Dieses Kapitel behandelt die folgenden Themen:

- Was ist die Registrierung?
- Die Struktur der Registrierung.
- Wie verwenden Anwendungen die Registrierung?
- Die Benutzung des Registrierungs-Editors.
- Die zuletzt als gültig bekannte Konfiguration.

Als Erstes wird nun geprüft, welche Rolle die Registrierung in der Windows 2000-Architektur spielt.

7.1 Was ist die Registrierung?

Die Registrierung ist eine umfassende, hierarchische Datenbank, die permanente Informationen enthält, die sowohl vom Betriebssystem als auch von allen installierten Anwendungen benötigt werden. Die Registrierung ist im Ordner `%Systemroot%\system32\config` enthalten. Diese Dateien heißen *Security*, *System*, *Software* und *Default*. Und es gibt noch eine weitere Datei im Verzeichnis `%Userprofil%` namens *Ntuser.dat*.

Die Registrierung enthält alle Einstellungen, die vom Betriebssystem und den meisten Anwendungen verwendet werden. Das Betriebssystem speichert alles, wodurch sich das Setup eines Computers von dem anderer Computer unterscheidet, wie z.B. die TCP/IP-Adresse, den Computernamen, die installierten Drucker und Ähnliches in der Registrierung. Alle Einstellungen, die in Windows 2000 vorgenommen werden können, werden in die Registrierung eingetragen.

Die Registrierung wird in einem proprietären Format von Microsoft gespeichert. Sie lässt sich nur mit einem Registrierungs-Editor oder einer Anwendung öffnen, die die passenden Win32-API-Aufrufe vornimmt. Eine Anwendung darf auf alle Registrierungsschlüssel zugreifen, auf die der Benutzer, der die Anwendung gestartet hat, Zugriff hat.

7.2 Die Struktur der Registrierung

Ohne Ordnung herrscht das Chaos. Microsoft hat Standards dafür eingeführt, wie Informationen in der Registrierung strukturiert sein sollten und wie Daten in der Registrierung gespeichert werden. Die

Registrierung wird in Windows 2000 mit denselben Berechtigungen gesichert wie Dateien. Diese Berechtigungen existieren selbst dann, wenn die Systempartition keine Sicherheit auf Dateiebene unterstützt.

Die Registrierung ist hierarchisch aufgebaut. Deshalb gibt es eine oberste Ebene. Eigentlich sind es sogar vier oberste Ebenen, weil die Registrierung vier verschiedene Datenbanken enthält, die als *Teilstrukturen* bezeichnet werden. Diese vier Teilstrukturen heißen *Classes*, *Users*, *Local Machine* und *Current Configuration*. Die Registrierung enthält zwei Arten von Elementen: Schlüssel und Werte. Ein *Schlüssel* entspricht einem Ordner in einem Dateisystem. Der Ordner enthält jedoch keine Dateien, sondern Werte oder Teilschlüssel. Jeder Schlüssel hat mindestens einen Wert namens (*Standard*) und kann auch wesentlich mehr Werte enthalten. Jede Hierarchie ist etwas anders aufgeteilt und soll nun nachfolgend beschrieben werden.

7.2.1 Die Teilstruktur Classes

Die Teilstruktur *Classes* mit der Bezeichnung *HKEY_CLASSES_ROOT* wird in der Registrierungsdatei *System* gespeichert. Sie speichert die Einstellungen und die Registrierung für OLE oder ActiveX (Microsoft ändert die Bezeichnung dieser Architekturkomponenten häufiger). Diese Teilstruktur ist ziemlich umfangreich, selbst wenn keine Anwendungen geladen sind.

Haben Sie sich jemals gefragt, wie Microsoft Word gestartet wird, wenn Sie doppelt auf eine Datei mit der Erweiterung *.doc* klicken? Die Teilstruktur *Classes* enthält mehrere hundert Teilschlüssel, die festlegen, wie Programme für verschiedene Erweiterungen ausgeführt werden. Die Schlüssel beginnen alle mit einem Punkt und sind in alphabetischer Reihenfolge aufgelistet. Der gewünschte Schlüssel lässt sich also leicht finden. Jeder dieser Schlüssel hat einen Standardwert, der auf den Klassennamen zeigt, der verwendet werden soll (für *.doc* ist *Word.Document.8* der Standardwert, falls Microsoft Word 2000 auf dem System installiert ist).

Die nächste Gruppe von Schlüsseln in der Teilstruktur *Classes* enthält die Namen der Klassen, die auf dem Computer installiert sind, und eine Angabe, wie der Zugriff darauf erfolgt. Für viele dieser installierten Klassen existieren zwei verschiedene Schlüssel. Der erste Schlüssel ist versionsunabhängig und der zweite versionsabhängig. Für Microsoft Word 2000 gibt es z.B. einen Schlüssel *Word.Document* und einen Schlüssel *Word.Document.8*. Der Schlüssel *Word.Document* zeigt auf den Schlüssel *Word.Document.8*, der wiederum auf Microsoft Word zeigt.

Die meisten dieser Klassen verfügen über mindestens zwei Teilschlüssel, d.h. untergeordnete Schlüssel. Der erste heißt *CLSID* und der zweite heißt *CurVer*. Der Teilschlüssel *CLSID* hat einen Standardwert, der dem GUID (Globally Unique Identifier) für das Objekt entspricht. Der Standardwert des Teilschlüssels *CurVer* ist die Versionsbezeichnung der Anwendung. Der Teilschlüssel *CurVer* des Schlüssels *Word.Document* hat deshalb den Standardwert *Word.Document.8*. Wenn Sie weiter unten in der Liste einen Blick in den Schlüssel *Word.Document.8* werfen, sehen Sie die Teilschlüssel der Anwendung, den Pfad, in dem das Programmsymbol für die Verwendung im Explorer abgelegt ist und einen Schlüssel, der dem Betriebssystem erklärt, wie eine Datei geöffnet werden muss, wenn darauf doppelt geklickt wird. Der Schlüssel *Word.Document.8* enthält auch den GUIF für die Klasse, der wie folgt aussieht:

```
{00020906-0000-0000-C000-000000000046}
```

Alle Klassen sind mit einem ähnlichen GUID ausgestattet. Über den GUID wird die Klasse eindeutig identifiziert.

7.2.2 Die Teilstruktur Users

Die Teilstruktur *Users* mit der Bezeichnung *HKEY_CURRENT_USER* enthält die benutzerdefinierten Einstellungen für alle Anwendungen und für das Betriebssystem. Die Teilstruktur *Users* enthält auch das so genannte Benutzerprofil, das alle Einstellungen vom Hintergrundbild für den Desktop bis zur Platzierung eines Fensters am Bildschirm enthält. Die Benutzer werden ärgerlich, wenn bei diesen Einstellungen etwas schief geht, und das mit gutem Grund. Es dauert ziemlich lange, alles so einzurichten, dass es »passt«. Im Registrierungs-Editor, der in Kürze in diesem Kapitel behandelt wird, gibt es auch einen Eintrag *HKEY_CURRENT_USER*. Dieser Eintrag ist eigentlich eine Verknüpfung zur Teilstruktur *HKEY_USERS* und enthält die Einstellungen des Benutzers, der momentan beim Computer angemeldet ist.

Die Teilstruktur *Users* ist in zwei Bereiche aufgeteilt. Der eine Bereich heißt *.DEFAULT* und enthält die Standardeinstellungen, die einem neuen Benutzer präsentiert werden, wenn er sich das erste Mal bei dem System anmeldet. Die restlichen Einträge sind GUIDs für alle Benutzer und enthalten ein Profil für jeden Benutzer, der sich bei dem Computer angemeldet hat.

Wenn sich ein Benutzer anmeldet, wird überprüft, ob er sich das erste Mal bei diesem Computer anmeldet. Hat er sich bereits zuvor angemeldet, wird der *HKEY_CURRENT_USER*-Schlüssel mit dem GUID für diesen Benutzer verknüpft. Meldet sich der Benutzer zum ersten Mal an, wird ein neuer Eintrag mit dem GUID für den Benutzer erzeugt. Anschließend wird der Inhalt des Standardbenutzers im Schlüssel *.DEFAULT* in den Schlüssel des neuen Benutzers kopiert. Wenn Veränderungen für alle Benutzer vorgenommen werden sollen, die sich jemals bei einem Computer anmelden, sollten diese am Standardbenutzer im Schlüssel *.DEFAULT* vorgenommen werden. Die Änderungen gelten dann für alle Neuansmeldungen, nicht aber für bereits bestehende Benutzer.

Um ein Benutzerprofil aus der Teilstruktur *HKEY_USERS* zu entfernen, klicken Sie mit der rechten Maustaste auf das Symbol **Arbeitsplatz** auf dem Desktop und wählen im Kontextmenü den Befehl **Eigenschaften**. Wechseln Sie dann zur Registerkarte **Benutzerprofile**. Hier sehen Sie die Benutzerprofile, die auf dem lokalen Computer eingerichtet wurden. Löschen Sie Profile, indem Sie diese markieren und auf die Schaltfläche **Löschen** klicken. Manche Profile lassen sich nicht löschen. Das Profil des aktuell angemeldeten Benutzers und das des Administrators lassen sich nicht löschen.

Je nachdem, was auf dem lokalen Computer installiert ist, kann die Teilstruktur für einen einzelnen Benutzer zahlreiche verschiedene Einstellungen enthalten. Das Element *Network* enthält z.B. alle Schlüssel für Laufwerksbuchstaben, zu denen der Benutzer eine Verbindung hergestellt hat und die bei der nächsten Anmeldung wiederhergestellt wird. Jeder Schlüssel für einen Laufwerksbuchstaben enthält Einträge, deren Werte Windows 2000 mitteilen, wie die Verbindung zum Laufwerk bei der Anmeldung hergestellt werden kann, wie z.B. *RemotePath* mit dem Pfad zum verbundenen Laufwerk oder *ProviderName* mit dem Netzwerkanbieter (wie *Microsoft Windows-Netzwerk* für Windows 2000 oder Einträge für andere Netzwerkbetriebssysteme). Außerdem wird der Benutzername (*UserName*)

gespeichert (im Format *DOMAIN\USER*), sodass die Verbindung wiederhergestellt werden kann.

Ein weiterer interessanter Schlüssel heißt *Software*. Dieser Schlüssel enthält Daten für alle Anwendungen, die auf dem Computer gespeichert sind. Die Daten sind nach Softwarehersteller und Anwendung geordnet. Die Software Adobe Acrobat erzeugt z.B. einen *Schlüssel* für Adobe und einen Teilschlüssel für *Acrobat*. Unterhalb des Schlüssels für die Anwendung, wie z.B. *Acrobat*, werden zahlreiche Teilschlüssel eingerichtet. Diese gehören jedoch vollständig in den Zuständigkeitsbereich des Softwareherstellers und letztendlich den des Programmierers.

7.2.3 Die Teilstruktur Local Machine

Die Teilstruktur *Local Machine* enthält vom Benutzer unabhängige Informationen für den lokalen Computer. Dies bedeutet, dass alle Informationen, die den Start des Computers, Hardwareschnittstellen sowie Informationen betreffen und die die Software allgemein zur Ausführung benötigt, in diesem Teil der Registrierung gespeichert werden.

Der Teilschlüssel *Hardware* enthält Informationen über die Hardware, die im lokalen Computer erkannt wurde. Ein interessanter Teilschlüssel dieses Schlüssels heißt *DEVICEMAP*. Er listet die gesamte Hardware des Computers auf wie die Tastatur, parallele und serielle Anschlüsse und SCSI-Adapter.



Selbst wenn nur IDE- oder ATAPI-Laufwerke in den lokalen Computer eingebaut sind, ist der Teilschlüssel *Scsi* im Schlüssel *HKEY_LOCAL_MACHINE\Hardware* enthalten. Das Treibermodell von Windows 2000 behandelt IDE-Laufwerke wie SCSI-Laufwerke. Diese Vorgehensweise ist bei modernen Betriebssystemen üblich, weil der SCSI-Standard sehr ausgereift ist und alles unterstützt, was auch der IDE/ATAPI-Standard unterstützt.

Der Schlüssel *SECURITY*, der der Teilstruktur *HKEY_LOCAL_MACHINE* direkt untergeordnet ist, kann nur vom Betriebssystem gelesen werden. Er enthält alle Benutzerkonten und Sicherheitsinformationen wie die Namen der Benutzerkonten, der Gruppen, die verschlüsselten Kennwörter etc.

Der Schlüssel *SOFTWARE* ist dem gleichnamigen Schlüssel in der Struktur *HKEY_CURRENT_USER* sehr ähnlich, der bereits beschrieben wurde. Er enthält Informationen für Anwendungen auf dem lokalen Computer, die sich nicht von Benutzer zu Benutzer ändern. Der Pfad zu den Datendateien der Anwendung oder die Registrierungsinformationen für die Anwendung werden normalerweise in diesem Teil der Registrierung gespeichert.

Der Schlüssel *SYSTEM* ist der interessanteste Schlüssel der Struktur *HKEY_LOCAL_MACHINE*. Dieser Schlüssel enthält alle Windows 2000-Einstellungen für den lokalen Computer. Er enthält drei Teilschlüssel namens *CurrentControlSet*, *ControlSet001* und *ControlSet002*. Diese drei Teilschlüssel enthalten redundante Informationen darüber, wie das Betriebssystem eingerichtet ist. Der Grund für diese Redundanz ist, dass bei Änderungen in der Registrierung durch Software der Benutzer die vorherigen funktionierenden Einstellungen aus einer der Sicherungskopien wiederherstellen kann. Mehr zur letzten, als funktionierend bekannten Konfiguration erfahren Sie im letzten Abschnitt in diesem Kapitel.

Der Schlüssel *CurrentControlSet* enthält einige interessante Teilschlüssel. Der erste davon, der Teilschlüssel *Control*, enthält alle Hardwaretreibereinstellungen und Netzwerkeinstellungen für den lokalen Computer. Der Teilschlüssel *Class* enthält, nach GUID sortiert, einen Schlüssel für jeden

Gerätetreiber, der auf dem System installiert ist. Diese Teilschlüssel enthalten Informationen über den Treiber, wie z.B. Angaben zum Hersteller, zum Pfad des Treibers und einen benutzerfreundlichen Namen für den Treiber.

Der Schlüssel *ComputerName* enthält vor allem den Computernamen. Der Teilschlüssel *ActiveComputerName* ist der aktuelle Name des Computers und der Schlüssel *ComputerName* ist der Name, den der Computer beim nächsten Bootvorgang tragen wird.

Der Schlüssel *hivelist* enthält eine Liste aller Teilstrukturen der Registrierung und die Angabe, welche Dateien die Teilstrukturen enthalten. Die Informationen sind in einer Form gespeichert, die den Pfad zu den Dateien eindeutig identifiziert:

`\Device\HarddiskVolume1\WINNT\System32\CONFIG\SOFTWARE`

Dieses Format identifiziert die Lage der Datei ohne Laufwerksbuchstaben eindeutig. Auf diese Weise lässt sich der Laufwerksbuchstabe verändern und das Betriebssystem kann trotzdem noch starten.

Der Schlüssel *WOW* enthält Informationen, die vom System Windows in Windows benutzt werden. Dieses System dient dazu, 16-Bit-Windowsanwendungen unter Windows 2000 auszuführen. Er enthält Informationen darüber, wie dieses System gestartet wird und, was wahrscheinlich wichtiger ist, die DLLs, die benötigt werden, um die Software auszuführen.

Ein weiterer Schlüssel unter *CurrentControlSet* heißt *Services* und legt fest, wie die Dienste des Betriebssystems gestartet werden. Jeder Teilschlüssel des Schlüssels *Services* enthält bestimmte Werte, die dem Services-Teilsystem dabei helfen, die verschiedenen Dienste zu starten. Die meisten Schlüssel enthalten den Eintrag *DisplayName*, der angibt, wie ein Dienst in einer Dienstliste angezeigt wird. Der Schlüssel *ErrorControl* legt fest, was im Falle eines Fehlers zu tun ist. In den meisten Fällen ist dieser Schlüssel auf den Wert 1 gesetzt. Dadurch wird im Falle eines Fehlers ein Ereignis hervorgerufen und ein Hinweis eingeblendet, dass ein Dienst nicht gestartet werden konnte. Der Eintrag *ImagePath* enthält den Pfad zur ausführbaren Datei. Für Dienste, die über den Pfad *Winnt* gestartet werden, ist der angegebene Pfad relativ zur Variablen *%Systemroot%*. Für Dienste, die an einer anderen Stelle installiert sind, sind ein Laufwerksbuchstabe und ein vollständiger Pfad zulässig (nur mit 8+3-Dateinamen), wobei der Pfad *C:\Program Files* durch *C:\PROGRA~1* ersetzt wird.

Der Eintrag *Start* legt fest, wie oder ob ein Dienst startet. In dieser Liste sind einige Dienste aufgeführt, die ganz klar nicht für den lokalen Computer gelten. Bei den meisten handelt es sich um SCSI-Adapter. Diese Schlüssel haben einen Startwert von 0. Bei der Startreihenfolge der Dienste werden zuerst die Dienste mit dem Wert 1 gestartet, dann alle Dienste mit dem Wert 2 etc. Auf diese Weise lässt sich der Start von Diensten verzögern und es können Abhängigkeiten eingerichtet werden.

Die Teilstruktur *HKEY_LOCAL_MACHINE* enthält alles, was Windows 2000 wissen muss, um erfolgreich zu starten. Ein Großteil der Problembehandlung besteht darin, diese Teilstruktur zu prüfen und Änderungen vorzunehmen. Jedes Gerät, das installiert wird, nimmt Änderungen an dieser Teilstruktur vor und es ist sehr wichtig zu verstehen, wie diese Änderungen Windows 2000 beeinflussen.

7.2.4 Die Teilstruktur Current Configuration

Die Teilstruktur *Current Configuration* wird unter der Bezeichnung *HKEY_CURRENT_CONFIG* angezeigt. Sie enthält temporäre Informationen über die Konfiguration des lokalen Computers, wie z.B. Informationen zum PCI-Setup, Konfigurationsinformationen über PCMCIA, Einstellungen der aktuellen Bildschirmauflösung etc. Diese Informationen werden verworfen, wenn das System heruntergefahren wird und ändern sich, wenn andere Anwendungen ausgeführt werden.

7.3 Die Benutzung der Registrierung durch Anwendungen

Microsoft stellte Anwendungen die Registrierung zur Verfügung, damit diese allgemeine Einstellungen sowie Einstellungen, die vom Benutzer vorgenommen wurden, speichern konnten. Dies ermöglicht es Benutzern, Einstellungen des Betriebssystems wie den Hintergrund und das Farbschema zu verändern, ohne andere Benutzer zu beeinflussen.

Wenn sich eine Anwendung selbst installiert, verändert sie verschiedene Teile der Registrierung, die die Anwendung initialisieren. Die meisten Anwendungen installieren ihre Erweiterungen in der Teilstruktur *HKEY_CLASSES* und installieren dann grundlegende Benutzereinstellungen und Informationen zur Anordnung der Fenster in der Struktur *HKEY_CURRENT_USER*.

Für Dienste wie Microsoft SQL Server werden Informationen überall in der Registrierung gespeichert. Die Clienttools registrieren ihre Erweiterungen und die Serverkomponenten erzeugen Einträge im Schlüssel *HKEY_LOCAL_MACHINE/System/CurrentControlSet/Services*, um den Start des Dienstes zu steuern und im Schlüssel *HKEY_LOCAL_MACHINE/Software/Microsoft/MSSQLServer* für die Software selbst. Nachdem der Dienst mittels der Informationen im Schlüssel *Services* gestartet wurde, liest die Anwendung Informationen aus dem Schlüssel *Software*, um vollständig zu starten. Dies ist ziemlich typisch für Dienstsoftware.

Einige Anwendungen nutzen noch immer Ini-Dateien, um ihre Einstellungen zu speichern. Eine Ini-Datei ist eine Textdatei, die normalerweise im Ordner *Winnt* in reinem Textformat gespeichert ist. Jede Ini-Datei enthält die Einstellungen für eine Anwendung und das Format. Die Verwendung der Ini-Datei bleibt vollständig dem Programmierer überlassen.

Ein Benutzer kann festlegen, dass bestimmte Programme automatisch gestartet werden, wenn er sich bei einem Windows 2000-Computer anmeldet. Es gibt verschiedene Möglichkeiten, eine Anwendung bei der Anmeldung zu starten. Eine davon besteht darin, einen Eintrag für den Pfad der Anwendung im Schlüssel *HKEY_CURRENT_USER\Software\Microsoft\Windows\Run* oder im Schlüssel *RunOnce* anzulegen. Der Benutzer kann auch Anwendungen in der Gruppe *AutoStart* im Start-Menü ablegen. Die heimtückischste Methode - die meistens von Viren benutzt wird, die automatisch gestartet werden müssen - besteht darin, einen *Run*-Eintrag in der Datei *Win.ini* abzulegen. Das Programm wird dann automatisch ausgeführt und es lässt sich nur sehr schwer entdecken. Um festzustellen, ob derartige Einträge in der Datei *Win.ini* enthalten sind, öffnen Sie diese mit dem Editor. Die Datei *Win.ini* befindet sich im Ordner *C:\Winnt*.

Die Registrierungsdatenbank weicht vom typischen Betriebssystem ab. UNIX-typische Betriebssysteme

speichern Setup-Daten für den Computer in Textdateien im Verzeichnis */etc* und Benutzereinstellungen in Textdateien im Homeverzeichnis des Benutzers. Warum verwendet Windows 2000 die Registrierung, die nur mit einer speziellen Software bearbeitet und gewartet werden kann, und nicht reine Textdateien, die sich mit jedem Texteditor bearbeiten lassen? Auf diese Frage gibt es einige interessante Antworten. Erstens verwendet Windows 2000 einen speziellen Zeichensatz namens *Unicode*. Unicode-Zeichen beanspruchen pro Zeichen zwei Byte Speicherplatz und können nahezu jedes Zeichen in jeder Sprache dieser Erde repräsentieren. Wenn zwei Bytes 65.536 verschiedene Werte speichern können, sind das sehr viele Zeichen. Weil die Registrierung in der Lage sein muss, Zeichenfolgen in anderen Sprachen zu speichern, sollten diese am besten in Unicode gespeichert werden. Normale Texteditoren können Unicode-Daten nicht bearbeiten, der Registrierungs-Editor schon.

Der zweite Grund für den Einsatz der Registrierung ist, dass sie einen zentralen Ort für alle Systemeinstellungen bietet. Sie bietet Anwendungen einen einheitlichen Zugriffsmechanismus. Dies ist ein komfortabler Standarddienst für ein Betriebssystem.

Dieses System wird von vielen Programmierern angegriffen; es repräsentiert für sie eine Folge falscher Designentscheidungen. Deshalb benutzen diese Programmierer die Registrierung nicht, um Einstellungen zu speichern. Ein Grund für diese Entscheidung ist, dass die Installation einer Anwendung ziemlich komplex wird, wenn Einträge in der Registrierung abgelegt werden müssen. Um eine Anwendung zu installieren, muss ein Setup-Programm geschrieben werden, das alle Einstellungen in der Registrierung ablegt, anstatt einfach nur einen Stapel Dateien zu kopieren und das Programm auszuführen.

In einer Unternehmensumgebung ist es sehr aufwändig sicherzustellen, dass alle Benutzereinstellungen übernommen werden, wenn ein Programm eingerichtet, angepasst und an mehrere tausend Benutzer verteilt werden muss. Programme dokumentieren nicht, welche Registrierungseinstellungen sie benutzen. Es wird also ziemlich schwierig herauszufinden, was ein Programm benötigt. Eine neue Art von Dienstprogramm wurde einfach nur zur Analyse der Registrierung erzeugt um herauszufinden, welche Einstellungen ein bestimmtes Programm vornimmt, um das Setup-Programm für dieses Programm erzeugen zu können. Ein weiterer Industriezweig hat sich darauf spezialisiert, nicht benutzte Registrierungseinträge für Programme, die bereits gelöscht wurden, aus der Registrierung zu entfernen.

Ein Nachteil der Registrierung ist auch, dass sich alles auf einen Punkt konzentriert. Tritt ein Fehler auf, wenn z.B. eine der Dateien, die Registrierungsinformationen enthält, beschädigt wird, startet das Betriebssystem möglicherweise nicht mehr. Wenn also ein Benutzer z.B. ein Spiel spielt und der Teil der Registrierung, der die Einstellungen des Spiels enthält, durcheinander gerät, wird der Computer möglicherweise nicht mehr gestartet. Wenn die Einstellungen des Spiels dagegen in einer separaten Datei gespeichert würden und diese Einstellungen beschädigt sind, ließe sich zwar das Spiel nicht mehr starten, aber der Computer würde korrekt funktionieren. Ein weiterer Einwand gegen die Registrierung ist, dass mehr als hundert Hürden übersprungen werden müssen, um Software auf einer Win32-Plattform auszuführen. Deshalb benutzen viele Multiplattformanwendungen die Registrierung nicht oder nur in geringem Umfang.

7.4 Der Registrierungs-Editor

Mit dem Registrierungs-Editor kann die Registrierung bearbeitet und betrachtet werden. Da die Registrierung so empfindlich ist, gibt es im Startmenü keine Verknüpfungen zu Registrierungs-Editoren,

obwohl Windows 2000 zwei Registrierungs-Editoren enthält. Der eine ist ein Registrierungs-Editor namens *Regedit.exe* in der Art des Windows 95/98-Registrierungs-Editors mit der Möglichkeit zur Suche und einer sehr angenehmen Benutzeroberfläche. Der andere Registrierungs-Editor heißt *Regedt32.exe* und entspricht dem Registrierungs-Editor von Windows NT 3.51.

7.4.1 Wann sollte der Registrierungs-Editor benutzt werden?

Es wurde zwar bereits erwähnt, aber es kann nicht oft genug gesagt werden: Mit der Registrierung müssen Sie extrem vorsichtig sein. Wenn Werte in der Registrierung fehlen oder falsch gesetzt sind, können schlimme Dinge passieren. Dazu gehört, dass sich das Betriebssystem nicht mehr starten lässt, dass Dienste nicht gestartet werden, Hardware nicht korrekt funktioniert, Material beschädigt wird (insbesondere Monitore), die Leistung abfällt und die Karrierechancen natürlich auch. Bringen Sie die Registrierung auf keinen Fall durcheinander.



Sie wissen das zwar vielleicht bereits. Sie sollten aber den Registrierungs-Editor nur dann benutzen, wenn es keine andere Möglichkeit gibt, einen Wert zu ändern. Nehmen Sie in der Registrierung keine Einstellungen wie die Auflösung der Grafikkarte oder Ähnliches vor.

7.4.2 Regedit benutzen

Das Programm *Regedit.exe* sieht aus wie der Registrierungs-Editor von Windows 95/98. Die Benutzeroberfläche ist sehr ansprechend und es gibt eine Suchfunktion, mit der Sie Registrierungseinträge schnell finden können. Um den Registrierungs-Editor zu starten, wählen Sie **Start/Ausführen** und geben im Dialogfeld **Ausführen** den Befehl *Regedit* ein. Der Registrierungs-Editor, den Sie in Abbildung 7.1 sehen, wird daraufhin geöffnet. Beachten Sie, dass die Registrierung mit einer baumähnlichen Struktur angezeigt wird. Da die Registrierung nicht schreibgeschützt ist, sollten Sie sehr vorsichtig sein.

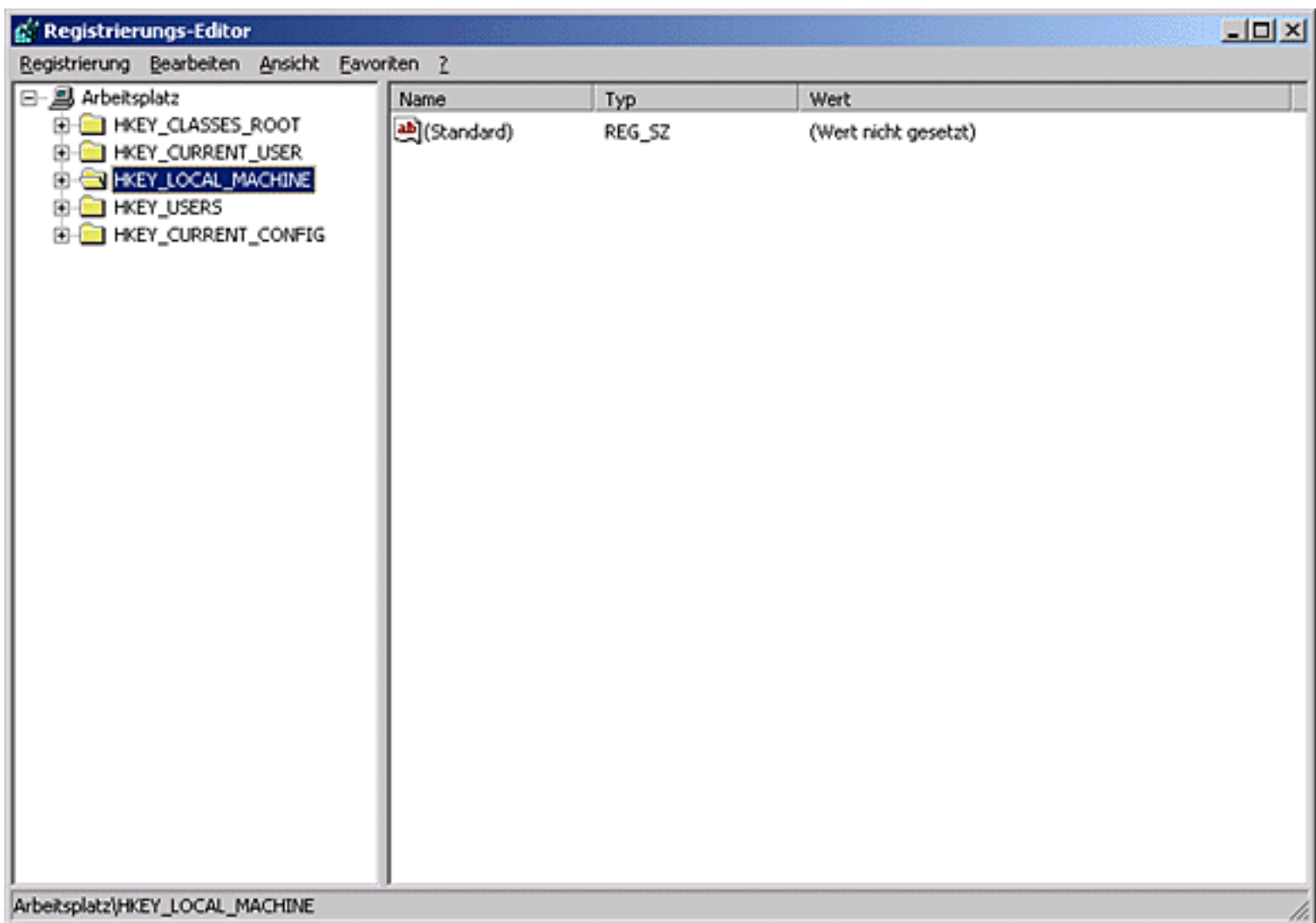


Abbildung 7.1: Regedit.exe ist der benutzerfreundlichere Registrierungs-Editor.

Die Registrierung arbeitet mit einer Dateistruktur wie im Windows-Explorer. Wenn einem Schlüssel ein Pluszeichen (+) vorangestellt ist, kennzeichnet dies, dass es Teilschlüssel für diesen Schlüssel gibt. Klicken Sie auf das Pluszeichen, wird der Schlüssel erweitert und alle Teilschlüssel sind sichtbar. Um die Teilschlüssel wieder auszublenden, klicken Sie auf das Minuszeichen. Um die Einträge für einen Schlüssel zu betrachten, wählen Sie den Schlüssel aus. Die Einträge und Werte werden nun auf der rechten Seite des Registrierungs-Editors angezeigt. Um einen Schlüssel zu finden, wählen Sie im Menü **Bearbeiten** den Befehl **Suchen** und füllen das Dialogfeld **Suchen** entsprechend aus. Nachdem der Editor den ersten Schlüssel gefunden hat, der mit dem Suchbegriff übereinstimmt, wählen Sie **Bearbeiten/Weitersuchen** oder drücken die (F3)-Taste, um die Suche mit dem angegebenen Begriff zu wiederholen.

Um einen Schlüssel zu löschen, markieren Sie diesen und drücken die (Entf)-Taste. Seien Sie jedoch vorsichtig. Wenn Sie den falschen Eintrag löschen, resultieren daraus erhebliche Probleme. Wird ein Schlüssel gelöscht, werden damit auch alle Teilschlüssel, Einträge und Werte gelöscht. Dies kann Windows 2000 völlig durcheinander bringen.

Um einen Schlüssel hinzuzufügen, wechseln Sie zum Schlüssel, dem der neue Schlüssel untergeordnet werden soll, und wählen im Menü **Bearbeiten** den Befehl **Neu/Schlüssel**. Der neue Schlüssel wird unter dem Namen **Neuer Schlüssel #1** hinzugefügt. Sie können ihn jedoch umbenennen. Den Namen können

Sie dabei frei wählen. Um den Namen eines vorhandenen Schlüssels zu ändern, klicken Sie auf den Schlüssel und wählen entweder im Menü **Bearbeiten** den Befehl **Umbenennen** oder drücken die (F2)-Taste. Ein Beispiel hierfür sehen Sie in Abbildung 7.2.

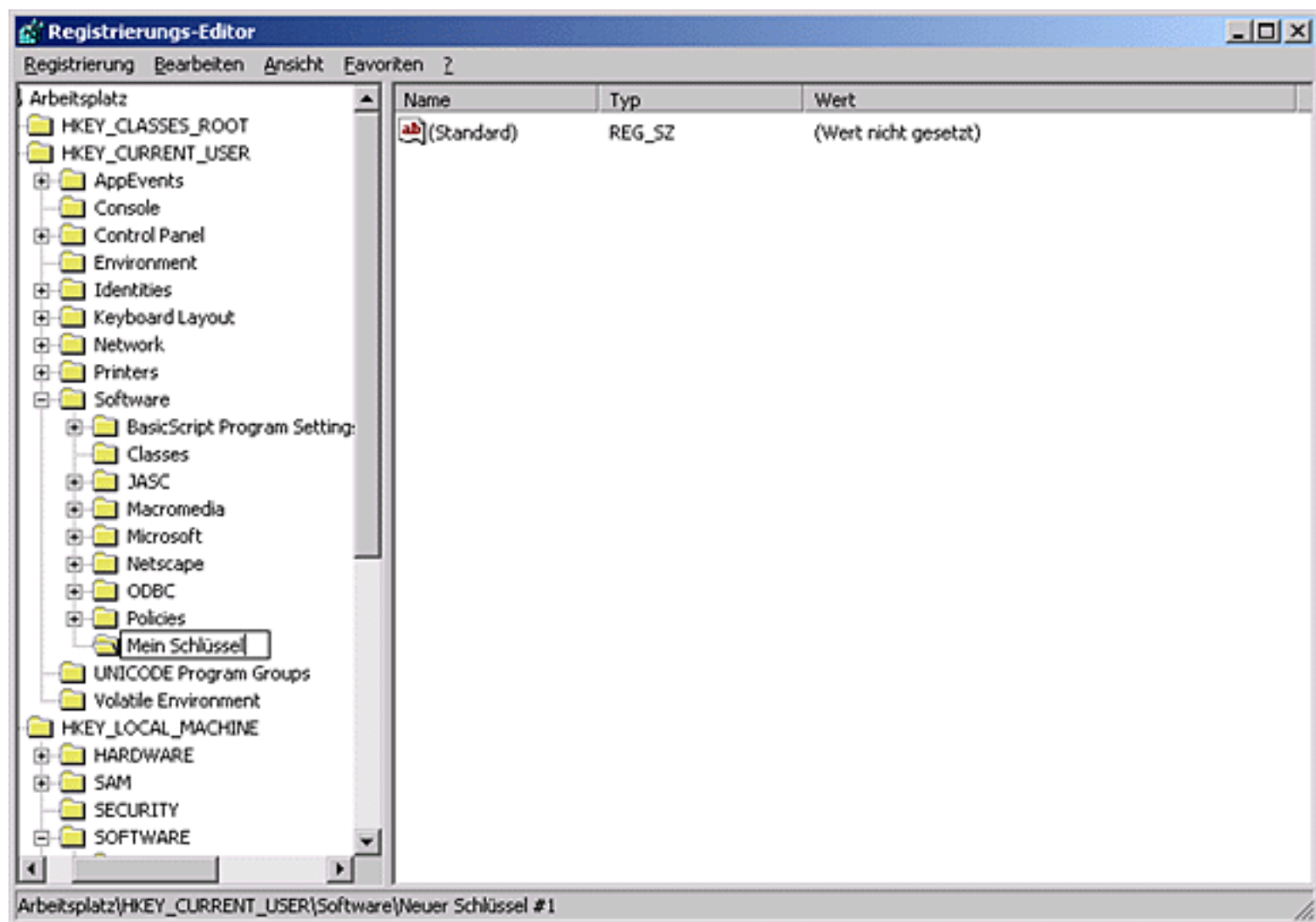


Abbildung 7.2: Um einen Schlüssel umzubenennen, wählen Sie im Menü Bearbeiten den Befehl Umbenennen und geben den neuen Namen ein, wie hier Mein Schlüssel.

Um einen Wert hinzuzufügen, klicken Sie auf den Schlüssel und wählen dann im Menü **Bearbeiten** den Befehl **Neu** sowie die Art des Wertes, den Sie hinzufügen möchten. Ein Wert des Typs **Zeichenfolge** kann eine Zeichenfolge speichern, ein **Binärwert** kann eine Folge von Zahlen speichern und ein **DWORD-Wert** enthält einen Doppelwortwert (ein aus vier Byte bestehender Integer-Wert). Standardmäßig trägt der neue Wert die Bezeichnung **Neuer Wert #1**. Sie können ihn jedoch über den Menübefehl **Bearbeiten/Umbenennen** oder durch Drücken der (F2)-Taste umbenennen. Um dem neuen Eintrag einen Wert zuzuweisen, klicken Sie doppelt darauf. DWORD-Werte werden für Wahr/Falsch-Werte benutzt, wobei 1 wahr ist und 0 falsch. In diesem Fall spielt es keine Rolle, ob Sie einen Wert als Hexadezimal- oder Dezimalzahl eingeben. Zeichenfolgewerte können Sie einfach eintippen. Binärwerte müssen jedoch als Hexadezimalzahl eingegeben werden. Zeichenfolgewerte dienen dazu, Pfadangaben oder andere Zeichenfolgeinformationen zu speichern. Binärwerte speichern Binärdaten wie z.B. codierte Zeichenfolgen. Abbildung 7.3 zeigt, wie ein neuer Zeichenfolgewert eingegeben wird.

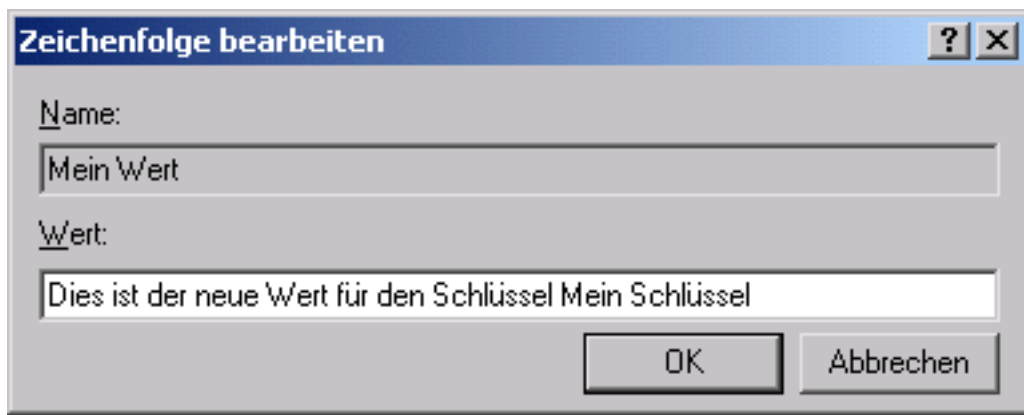


Abbildung 7.3: Um einen Zeichenfolgewert hinzuzufügen, wählen Sie Bearbeiten/Neu/Zeichenfolge. Benennen Sie den Eintrag um und klicken Sie doppelt darauf, um den Wert zuzuweisen.

Registrierungsschlüssel lassen sich auch in Textdateien exportieren und so an einer anderen Stelle nutzen. Wählen Sie dazu im Registrierungs-Editor den Schlüssel, den Sie exportieren möchten und dann im Menü **Registrierung** den Befehl **Registrierungsdatei exportieren**. Es öffnet sich das Dialogfeld **Registrierungsdatei exportieren**, in dem Sie die Option haben, die ausgewählte Teilstruktur oder die gesamte Registrierung zu exportieren.

Registrierungsdateien werden normalerweise exportiert, wenn eine Registrierungsdatei bei mehreren Computern identisch sein muss. Die Änderungen brauchen dann nur an einem Computer vorgenommen zu werden. Anschließend kann die exportierte Teilstruktur in die Registrierungen der restlichen Computer importiert werden. Um eine Registrierungsdatei zu importieren, wählen Sie im Menü **Registrierung** den Befehl **Registrierungsdatei importieren**.

Registrierungsdateien sind Textdateien. Sie lassen sich mit einfachen Programmen wie dem Editor öffnen. Wenn Sie mit der rechten Maustaste auf eine Registrierungsdatei klicken, öffnet sich ein Kontextmenü. Der Standardbefehl ist **Zusammenführen**. Damit wird der Inhalt der Registrierungsdatei zur Registrierung hinzugefügt. Mit dem Befehl **Bearbeiten** öffnet sich die Registrierungsdatei im Editor und es ist eine Liste mit Schlüsseln und Werten zu sehen. Die Schlüssel stehen in Klammern und die Werte stehen im Format »*Mein Wert*""=*Wert*« unter dem entsprechenden Schlüssel. Beim Import wird die Registrierungsdatei mit der Registrierung zusammengefügt. Wenn ein Schlüssel bereits vorhanden ist und Werte existieren, werden die neuen Werte einfach hinzugefügt und die alten bleiben erhalten. Wenn ein Registrierungsschlüssel namens *MeineAnwendung* z.B. die zwei Werte **Wert1** und **Wert2** enthält und die folgende Registrierungsdatei importiert wird,

Windows Registry Editor Version 5.00

```
[HKEY_CURRENT_USER\Software\MeinUnternehmen\MeineAnwendung]
"Wert3"="42"
```

enthält der resultierende Schlüssel **MeineAnwendung** die Werte **Wert1**, **Wert2** und **Wert3**. Eine Registrierungsdatei kann keine bestehenden Werte oder Schlüssel löschen. Sie kann nur Werte zu

bestehenden Schlüsseln hinzufügen oder mit neuen Werten überschreiben. Die Registrierung lässt sich dadurch nicht so leicht durch eine exportierte Registrierungsdatei durcheinander bringen.

Eine weitere nützliche Funktion des Registrierungs-Editors *Regedit* ist, dass Registrierungsdateien von der Befehlszeile importiert werden können. Mit dem Schalter */S* kann das Programm *Regedit* stillschweigend Registrierungsdateien und damit auch Registrierungseinstellungen ohne Benutzereingaben importieren. Dies ist nützlich, um Registrierungsdateien von einem Anmeldeskript zu importieren.

Das Programm *Regedit* eignet sich sehr gut für den Import und Export, es gibt jedoch auch einige Probleme. An erster Stelle steht dabei, dass es keine Sicherheit gibt. Bei allen Registrierungsschlüsseln kann Sicherheit nach dem Schema von NTFS zugewiesen werden. Das Programm *Regedit.exe* bietet jedoch keine Möglichkeit, die Berechtigungen, die den einzelnen Registrierungsschlüsseln zugewiesen wurden, zu bearbeiten. Der zweite Registrierungs-Editor namens *Regedt32* bietet diese Möglichkeit. Während *Regedit* nur die Datentypen Zeichenfolge, Doppelwort und Binärwert zulässt, gibt es im Registrierungs-Editor *Regedt32* die zwei zusätzlichen Datentypen *REG_MULTI_SZ* und *REG_EXPAND_SZ*.

7.4.3 Änderungen der Registrierung mit Regedit finden

Zu den unangenehmsten Dingen beim Umgang mit der Registrierung gehört es, Änderungen zu verfolgen, die bei der Installation neuer Software vorgenommen wurden. Um Software erfolgreich in einem großen Unternehmen installieren zu können, muss normalerweise ein angepasstes Installationsprogramm erstellt werden, das die Platzierung der Dateien behandeln kann, Verknüpfungen im Startmenü einrichtet und dann die Änderungen in die Registrierung importiert. Das Programm *Regedit* bietet einige Funktionen, mit denen diese Änderungen leichter vorgenommen werden können. Exportieren Sie vor der Installation der Anwendung die Teilstrukturen *HKEY_LOCAL_MACHINE* und *HKEY_CURRENT_USER* und führen Sie anschließend das Setup-Programm aus. Nachdem das Setup beendet wurde, müssen Sie den Computer bei Bedarf neu booten. Exportieren Sie anschließend die beiden Teilstrukturen noch einmal und führen Sie dann an der Eingabeaufforderung das Programm FC aus, das einen Dateivergleich durchführt:

```
FC UserPreInstall.reg UserPostInstall.reg > UserDiff.txt
```

Dieser Befehl schreibt die Unterschiede zwischen den beiden Teilstrukturen in eine Datei namens *UserDiff.txt*. Diese Datei können Sie dann in den Editor laden und die Registrierungseinträge betrachten, die verändert wurden. Viele dieser Einstellungen sind jedoch vielleicht nicht für die Installation relevant. Sie müssen die Datei also sorgfältig prüfen um festzustellen, welche Einstellungen angewendet werden.

7.4.4 Den Registrierungs-Editor Regedt32 nutzen

Die Benutzeroberfläche des Programms *Regedt32* ist nicht so angenehm wie die des Programms *Regedit*. Für jede Teilstruktur gibt es ein separates Fenster, sodass fünf Fenster geöffnet sind. Um *Regedt32* zu starten, wählen Sie **Start/Ausführen** und geben dann *regedt32* ein.

Die Navigation erfolgt im Registrierungs-Editor *Regedt32* auf die gleiche Weise wie in *Regedit*. Gehen Sie zum Fenster, das die fragliche Teilstruktur enthält, und suchen Sie dann in der Liste den gewünschten Schlüssel. Schlüssel werden mit Ordnersymbolen repräsentiert und Schlüsseln, die Teilschlüssel enthalten, ist ein Pluszeichen vorangestellt (siehe Abbildung 7.4).

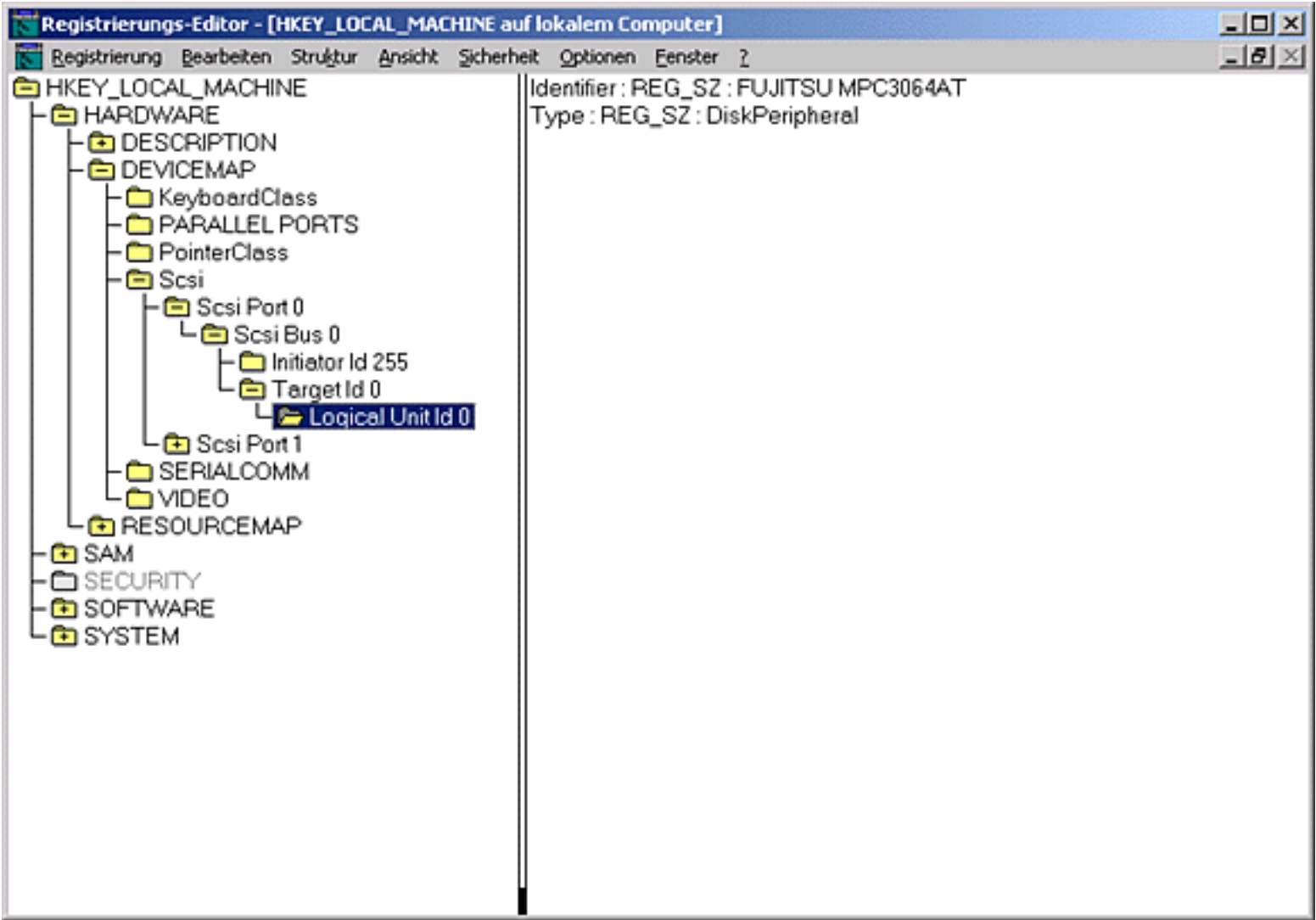


Abbildung 7.4: Der Registrierungs-Editor *Regedt32* sieht ganz anders aus als *Regedit*.

Um einen Schlüssel hinzuzufügen, wählen Sie im Menü **Bearbeiten** den Befehl **Schlüssel hinzufügen**, um einen Wert hinzuzufügen den Befehl **Wert hinzufügen**. Es öffnet sich das Dialogfeld **Schlüssel hinzufügen**, in dem Sie einen Namen für den Schlüssel eingeben müssen, bzw. **Wert hinzufügen**, in dem Sie den Namen und Typ des Werts eingeben müssen. *Regedt32* zeigt die Datentypen anders an als *Regedit* (siehe Tabelle 7.1).

Regedt32-Datentyp	Regedit-Datentyp
REG_BINARY	Binärwert
REG_DWORD	DWORD-Wert
REG_SZ	Zeichenfolge
REG_EXPAND_SZ	Nicht verfügbar

Tabelle 7.1: Datentypen für Registrierungseinträge.

Mit dem Datentyp *REG_MULTI_SZ* lassen sich mehrere Zeichenfolgen in einem Wert speichern und *REG_EXPAND_SZ* ist eine normale Zeichenfolge, die in eine Mehrfachzeichenfolge umgewandelt werden kann.

Regedt32 bietet nicht annähernd den Leistungsumfang von *Regedit*, wenn es um den Ex- und Import von Werten geht. Das Problem ist, dass *Regedt32* überhaupt keine Funktion bietet, um Dateien leicht zu importieren. Um einen Registrierungsschlüssel zu sichern, müssen Sie im Menü **Registrierung** den Befehl **Teilstruktur speichern unter** wählen und einen Dateinamen angeben. Die Datei, die beim Export erzeugt wird, lässt sich nicht importieren.

Um die Sicherheitseinstellungen eines Registrierungsschlüssels zu ändern, wählen Sie den Schlüssel und anschließend im Menü **Sicherheit** den Befehl **Berechtigungen**. Es öffnet sich das Dialogfeld **Berechtigungen**, das Sie bereits von Dateien her kennen. Wie beim Zugriff auf Dateien ist es auch hier möglich, den Zugriff auf die Registrierung zu überwachen. Die Überwachungsprotokolle werden wie die Überwachungsprotokolle für eine Datei in der Ereignisanzeige gespeichert. Dadurch lassen sich die Registrierungseinstellungen überwachen und Änderungen der Registrierung werden aufgezeichnet. Die Überwachungsprotokolle werden in der Ereignisanzeige unter den Sicherheitsprotokollen aufgeführt.

7.5 Die letzte, als funktionierend bekannte Konfiguration benutzen

Trotz aller Warnungen in diesem Kapitel und der offiziellen Warnungen von Microsoft nehmen Benutzer manchmal Änderungen an der Registrierung vor, durch die sich Windows 2000 nicht mehr erfolgreich starten lässt. Was passiert als Nächstes? Glücklicherweise haben die Entwickler von Windows 2000 diese Möglichkeit mit einbezogen und eine Funktion namens **Letzte als funktionierend bekannte Konfiguration** integriert.

Während des Startvorgangs liest Windows 2000 die Informationen, die benötigt werden, um den Teil der Registrierung auszuführen, der im Schlüssel *CurrentControlSet* enthalten ist. Wenn Windows 2000 den Startvorgang erfolgreich durchgeführt hat, wird zu dem Zeitpunkt, zu dem der Anmeldebildschirm eingeblendet wird, eine Verknüpfung zu den Schlüsseln *ControlSet001* und *ControlSet002* hergestellt und die aktuellen Einstellungen werden über diejenigen im Schlüssel *ControlSet001* kopiert. Wenn das System beim Startvorgang nicht bis zu dieser Stelle kommt, wird die letzte, als funktionierend bekannte Konfiguration benutzt. Dazu werden die Einstellungen aus dem Schlüssel *ControlSet001* statt aus dem Schlüssel *CurrentControlSet* gelesen und somit werden die fehlerhaften Registrierungseinträge umgangen.

Um auf die letzte, als funktionierend bekannte Konfiguration zuzugreifen, starten Sie den Computer neu und drücken im Betriebssystemauswahlmenü die Taste (F8). Sie können nun die Option **Letzte als funktionierend bekannte Konfiguration** wählen und mit den Registrierungseinstellungen starten, die vor dem letzten Neustart verwendet wurden. Wenn der Computer schon sehr lange nicht mehr neu gestartet wurde, sind die Einstellungen vielleicht völlig veraltet, aber es fehlen die Einstellungen, die den

Neustart verhindert haben. Deshalb sollten Sie vor jeder Veränderung der Registrierung den lokalen Computer neu starten.

© Copyright [Markt+Technik Verlag](#), ein Imprint der Pearson Education Deutschland GmbH
Elektronische Fassung des Titels: Windows 2000 Server Kompendium, ISBN: 3-8272-5611-9 Kapitel:
Die Registrierung

Kapitel 8 TCP/IP-Netzwerke

Der Gewinner des Protokollkriegs ist momentan TCP/IP. TCP/IP ist eigentlich kein Protokoll, sondern eher ein Protokollstapel, den es bereits seit den sechziger Jahren gibt. Merkwürdigerweise ist TCP/IP ein offener Standard, weil es von der Regierung der USA für ein weiteres kostenloses Medium, das Internet, erstellt wurde.

Das TCP/IP-Protokoll ist nicht nur wegen des Internets, sondern auch, weil niemand Copyright-Ansprüche darauf erhebt, mittlerweile zum De-facto-Standard geworden. Deshalb kann jeder Hersteller TCP/IP nutzen, verändern und in seine Einzelteile zerlegen.

8.1 TCP/IP-Konzepte kurz und knapp

TCP/IP steht für Transmission Control Protocol/Internet Protocol (Übertragungssteuerungsprotokoll/Internetprotokoll). Die wichtigsten Protokolle dieses Protokollstapels sind die Protokolle TCP und IP:

- TCP ist ein verbindungsorientiertes Netzwerkprotokoll, das Systemen die fehlerfreie Kommunikation über beliebige Medien erlaubt.
- IP ist das Protokoll der Netzwerkschicht, das für die Übertragung der Pakete zuständig ist, die von TCP erzeugt werden.

Diese beiden Protokolle werden in erster Linie für die Kommunikation zwischen unterschiedlichen Hardwareplattformen und Betriebssystemen verwendet. Der TCP/IP-Protokollstapel ist nicht auf eine bestimmte Hardware oder ein Betriebssystem beschränkt. Die Aufgabe der Protokollsammlung besteht darin, die Regeln für die Kommunikation bereitzustellen, die angewendet werden, nachdem eine physische Verbindung hergestellt wurde.

Wie die menschliche Sprache sorgt TCP/IP zunächst dafür, dass ein Kommunikationsmedium existiert, stellt dann eine allgemeine Sprache zur Verfügung und beginnt zu kommunizieren.

8.1.1 IP-Adressen

Das Adressierungsschema, das von TCP/IP verwendet wird, heißt IP-Adressierung und ist ziemlich einfach aufgebaut. Der Administrator wird in die Konfiguration und die Struktur aller Adressen einbezogen. Wenn Sie die Grundregeln verstehen, ist die Adressierung ziemlich einfach.

Die IP-Adresse ist eine Zahl, die sich aus vier 8-Bit-Zahlen zusammensetzt, die durch Punkte voneinander getrennt sind. Dieses Format wird manchmal auch als vier Oktette bezeichnet, weil ein Oktett aus acht Bits besteht. Daraus ergibt sich ein Wertebereich von 256 Zahlen, weil die 0 ebenfalls als möglicher Wert betrachtet wird.

Das Binärsystem

Wenn Sie nicht verstehen, wie sich acht Bits einem Wertebereich von 0 bis 255 zuordnen lassen, verstehen Sie höchstwahrscheinlich das Grundprinzip nicht, nach dem Computer Berechnungen

durchführen. Alles, was Computer berechnen, ist binär. Das Binärsystem ist das Zahlensystem zur Basis 2. Werte bestehen aus Kombinationen der zwei Ziffern 0 und 1.

Das Dezimalsystem ist das Standardzahlensystem zur Basis 10, das die meisten Menschen kennen. Jeder Binärwert lässt sich auch als Dezimalwert repräsentieren. Binärwerte eignen sich jedoch besser für die Verarbeitung durch den Computer und Dezimalzahlen können Menschen leichter interpretieren.

Hier eine Binärzahl, die aus acht Bits besteht:

00101100

Um diese Zahl ins Dezimalsystem zu übersetzen, müssen Sie einfach jede Spalte (von rechts nach links) als das Zweifache des vorherigen Werts betrachten. Beginnend mit der 1 ergibt sich folgendes Schema:

128 64 32 16 8 4 2 1

Um die obige Binärzahl in eine Dezimalzahl umzurechnen, »vergessen« Sie einfach die Vielfachen, in deren Spalte eine 0 steht, und berücksichtigen nur jene Zahlen, die einer 1 entsprechen. Addieren Sie diese, ergibt sich folgender Wert:

32 + 8 + 4 = 44

Hier noch ein paar weitere Beispiele:

- 00000001 = 1 = 1
- 10000000 = 128 = 128
- 10101010 = 128 + 32 + 8 + 2 = 170
- 01110111 = 64 + 32 + 16 + 4 + 2 + 1 = 119

So viel zum Binärsystem.

Die IP-Adresse

Nachdem Sie sich nun mit Binärzahlen auskennen und die IP-Adresse aus vier Oktetten besteht, die durch Punkte getrennt sind, müsste eine IP-Adresse eigentlich wie folgt aussehen.

10000000.10101010.00000001.01110111

Merken Sie sich dieses Format, weil IP-Adressen normalerweise nicht so aussehen. Wenn Sie versuchen,

Probleme zu berechnen oder eine ideale Konfiguration zu finden, ist dieses Format jedoch sehr nützlich.

IP-Adressen werden normalerweise als Dezimalzahlen dargestellt. Die obige Adresse sieht im Dezimalsystem wie folgt aus:

128.170.1.119

Netzwerke und Hosts

Die Computer in einem IP-Netzwerk werden als Hosts bezeichnet. Dabei spielt es keine Rolle, ob es sich um Server, Workstations, Drucker oder sogar Ihren Kühlschrank handelt (falls dieser an ein IP-Netzwerk angeschlossen ist).

Die IP-Adresse ist in zwei Teile unterteilt, um einen Host lokalisieren zu können. Das System kann damit feststellen, von welchem System ein Paket stammt oder an welches System das Paket geschickt werden muss. Wie die Telefonnummer, die aus einer Vorwahl und einer spezifischen Telefonnummer besteht, gibt es auch bei der IP-Adresse einen Teil, der das Netzwerk kennzeichnet, in dem das System enthalten ist und einen zweiten Teil, der den Host kennzeichnet.

Diese beiden Teile werden als der Netzwerk- und der Hostteil der Adresse bezeichnet. In ihrer einfachsten Form wird die Adresse entsprechend der Adressklasse bei den Punkten aufgeteilt.

Es gibt drei Klassen von IP-Adressen: Die Klassen A, B und C. Wenn das erste Oktett der IP-Adresse das Netzwerk kennzeichnet, handelt es sich um eine Adresse der Klasse A. Kennzeichnen die ersten beiden Oktette das Netzwerk, handelt es sich um eine Adresse der Klasse B. Kennzeichnen die ersten drei Oktette das Netzwerk, handelt es sich um eine Adresse der Klasse C. Das folgende Schema verdeutlicht dies:

- *Netzwerk.Host.Host.Host* = Klasse A
- *Netzwerk.Netzwerk.Host.Host* = Klasse B
- *Netzwerk.Netzwerk.Netzwerk.Host* = Klasse C

Um die verfügbaren Adressen zu organisieren, wurden ihnen Bereiche zugeteilt, in denen sie sehr wahrscheinlich operieren werden, wenn eine Verbindung zum Internet besteht. Damit lässt sich die Klasse einer Adresse auf einen Blick ermitteln.

- Klasse-A-Netzwerkadressen beginnen mit der Binärzahl 0
(z.B. 00000001.10101010.00000001.01110111 = **1**.170.1.119)
- Klasse-B-Netzwerkadressen beginnen mit der Binärzahl 10
(z.B. 10000000.10101010.00000001.01110111 = **128**.170.1.119)
- Klasse-C-Netzwerke beginnen mit der Binärzahl 110
(z.B. 11000000.10101010.00000001.01110111 = **192**.170.1.119)

Daraus resultieren Wertebereiche für die möglichen Adressen (in dezimaler Schreibweise) in jeder Klasse:

- Klasse A 1.X.X.X - 126.X.X.X

- Klasse B 128.0.X.X - 191.255.X.X
- Klasse C 192.0.0.X - 223.255.255.X



Beachten Sie, dass die Adressen des Bereichs 127.x.x.x fehlen. Dies liegt daran, dass die Adresse 127.0.0.1 zu Test- und internen Zwecken für den lokalen Computer reserviert ist. Diese Adresse wird aus diesem Grund auch als LOCALHOST bezeichnet. Um festzustellen, ob das TCP/IP- Protokoll vorhanden ist, können Sie auch den ping-Befehl an den LOCALHOST senden.

Aus welchem Grund sind die Netzwerk- und Hostteile der IP-Adresse variabel? Das liegt daran, dass einige Netzwerkverbünde mehr Netzwerksegmente beanspruchen, andere dagegen einen höheren Bedarf an Hostadressen haben. Hier einige Beispiele zur Verdeutlichung:

- Ein Internetprovider muss z. B. sehr viele Hostadressen bereitstellen. Alle Computer von Benutzern, die sich in diese Systeme einwählen, benötigen eine eindeutige IP-Adresse.
- Das WAN eines großen Unternehmens wird vielleicht einen größeren Bedarf für Netzwerkadressen haben, weil es viele geroutete WAN-Verbindungen, aber weniger Hosts an jedem Standort gibt.
- Netzwerkanbieter benötigen Netzwerk- und Hostadressen. Dies wird dadurch ermöglicht, dass Teilnetze oder Subnetze gebildet werden. Dies wird im Abschnitt »Adressierung von Subnetzen« ausführlicher beschrieben.

Die Anzahl der Hosts und Netzwerkadressen, die eine Klasse haben kann, lassen sich über die Anzahl der Adressen ermitteln, die auf jeder Seite der Leitung existieren, die das Netzwerk vom Host trennt. Sie müssen jedoch daran denken, dass Sie im Netzwerkteil der Adresse die Zahl 0 und die Zahl 255 nicht benutzen dürfen. Außerdem darf im Hostteil nicht nur die Zahl 0 oder die Zahl 255 vorkommen. IP-Adressen, die sich ausschließlich aus den Zahlen 0 und 255 zusammensetzen, haben bei der IP-Adressierung eine besondere Bedeutung:

- Die Klasse A verfügt über 126 mögliche Netzwerkadressen und 256 x 256 x 256 (oder 16.777.214) mögliche Hostadressen.
- Die Klasse B verfügt über 16.384 mögliche Netzwerkadressen und 256 x 256 (oder 65.534) mögliche Hostadressen.
- Die Klasse C verfügt über 2.097.152 mögliche Netzwerkadressen und 254 mögliche Hostadressen.

8.1.2 Subnetzmasken

Der Teil der IP-Adresse, der festlegt, welcher Teil eine Netzwerk- und welcher eine Hostadresse ist, wird als *Subnetzmaske* (oder Adressierungsmaske) bezeichnet. Hinter der Subnetzmaske verbirgt sich die Idee, die Teile der IP-Adresse zu maskieren, die das Netzwerk bezeichnen, sodass nur dieser Teil für die Hostadressen verfügbar ist.

Wenn Sie eine Subnetzmaske in binärer Schreibweise betrachten, werden Sie feststellen, dass sie entsprechend der Klassen in den Anfangsoktetten nur Einsen enthält. Betrachten Sie die folgenden einfachen Beispiele von Standard-IP-Adressklassen, um eine Vorstellung davon zu erhalten, wie die Subnetzmasken funktionieren.

Nachfolgend sehen Sie die Subnetzmasken für die Standardklassen:

- Klasse A = 255.0.0.0 = 11111111.00000000.00000000.00000000
- Klasse B = 255.255.0.0 = 11111111.11111111.00000000.00000000
- Klasse C = 255.255.255.0 = 11111111.11111111.11111111.00000000

Wenn der Computer die Adresse mit der Subnetzmaske vergleicht, verwendet er die Binärversion, um den Netzwerkteil vom Hostteil der Adresse zu trennen. Der Teil der Adresse, an dem die Einsen stehen, ist der Netzwerkteil und der Teil, an dem die Nullen stehen, ist der Hostteil. Ganz so einfach ist es zwar nicht, aber Sie erhalten eine Vorstellung davon, wie es funktioniert. Und wenn Sie bei den Standardklassen bleiben, ist es wirklich so einfach.

8.1.3 Adressierung von Subnetzen

Subnetzmasken können wesentlich komplizierter sein als die obigen Standardbeispiele. Diese Beispiele gelten für eine perfekte Welt, in der der Systemadministrator den Adressbereich auswählen kann, den er benötigt, ohne andere Netzwerke oder Systeme berücksichtigen zu müssen. Was ist mit dem Internet? Was ist mit Tochtergesellschaften von Unternehmen, die einen vorgegebenen IP-Adressbereich übernehmen und mit diesen Grenzen leben müssen?

Solche Umgebungen veranlassen Sie vielleicht dazu, das Subnetz in Teile mit ungünstigeren Adressen aufzuteilen. So haben Sie vielleicht die Subnetzmaske 255.255.255.128, damit Sie die Klasse C-Adresse, die Ihnen zugewiesen wurde, in zwei Netzwerke aufteilen können. Hier gelten dieselben Regeln. Sie sind jedoch vermutlich nicht so leicht zu verstehen.

Wenn Sie ein Subnetz weiter aufteilen, sollten Sie sich folgende Fragen stellen:

- Wie viele Hosts werden momentan und in Zukunft benötigt?
- Wie viele Netzwerke werden jetzt und in Zukunft benötigt?



Es ist nicht immer leicht, die Zukunft vorherzusagen, aber in diesem Fall sollten Sie lieber verschwenderisch sein. Wenn Sie ein IP-Schema einmal installiert haben, ist es ein enormes Unterfangen, dieses neu installieren zu müssen.

Wenn Sie Ihr Netzwerk in Subnetze aufteilen, die nicht der Standardunterteilung entsprechen, müssen Sie wissen, wie viele Netzwerk- und Hostadressen in dem Subnetz zulässig sind.

Hier eine Möglichkeit, um die Anzahl möglicher Hosts zu ermitteln:

Von der letzten Ziffer der Subnetzmaske (nicht die 0) 256 subtrahieren (der maximal zulässigen Anzahl an Hostadressen in einem Oktett). Das Ergebnis für jedes offene Oktett (.0), das von rechts her verbleibt, mit 256 multiplizieren. Den Wert 2 vom Ergebnis subtrahieren.

Hier ein paar Beispiele:

- Subnetzmaske = 255.192.0.0
- $256 - 192 = 64$
- $64 \times 256 = 16.384 \times 256 = 4194304$
- $4.194.304 - 2 = 4.194.302$ mögliche Hosts
- Subnetzmaske = 255.255.128.0

- $256 - 128 = 128$
- $128 \times 256 = 32.768$
- $32768 - 2 = 32.766$ mögliche Hosts
- Subnetzmaske = 255.255.255.252
- $256 - 252 = 4$
- Die Regel besagt, dass jedes offene Oktett (.0) mit 256 multipliziert werden muss. Es gibt hier aber kein offenes Oktett.
- $4 - 2 = 2$ mögliche Hosts



Denken Sie daran, dass nur das letzte Oktett, das einen Wert ungleich 0 hat, die Anzahl der Netzwerke beeinflusst, weil dies die einzige Stelle ist, an der die zugewiesene IP-Adresse verändert werden darf.

Hier zwei Möglichkeiten, die Anzahl möglicher Subnetze zu ermitteln:

- Die Binärposition von links (invertierte Position) verdoppeln und 2 subtrahieren. Daraus ergibt sich die Anzahl der Netzwerke.
- Beispiel: $224 = 11100000 = 4 \times 2 = 8 - 2 = 6$ (Anzahl der Subnetze)
- Die invertierte Position ist das Gegenteil der Standardbinärpositionen:
- 1 2 4 8 16 32 64 128

Weil 11111111 die Subnetzmaske komplett ausfüllt und 00000000 alles offen lässt, müssen sie nicht berechnet werden. Der Wert 00000000 (0) gestattet nur ein Netzwerk und der Wert 11111111 ist unzulässig.

Die nachfolgende Tabelle hilft Ihnen als Referenz bei der Berechnung.

Subnetzmaske	Binärzahl	Invertierte Position	Anzahl verfügbarer Netzwerke
192	11000000	2	2
224	11100000	4	6
240	11110000	8	14
248	11111000	16	30
252	11111100	32	62
254	11111110	64	126

Tabelle 8.1: Tabelle zur Berechnung.

Sie können auch Subnetze mit Subnetzmasken wie z.B. 255.255.184.0 erstellen, aber wenn Sie die Anzahl möglicher Hosts und Netzwerke ermittelt haben, habe ich bereits ein neues Buch geschrieben. Derartige Subnetzmasken sind sehr unüblich und sollten nur von sehr erfahrenen Administratoren verwendet werden.



Der Netzwerkbereich 10.x.x.x wurde für private Netzwerke reserviert (die keine Verbindung zum Internet haben). Dieser Bereich wird nicht in das Internet geroutet und eignet sich deshalb für interne Netzwerke. Außerdem lassen sich Subnetze leicht einrichten, weil der gesamte Bereich verfügbar ist. Dieser Netzwerkbereich verhält sich so wie eine Klasse-A-Adresse.

8.1.4 IP-Routing

Wenn Subnetzmasken berechnet werden, muss es im Netzwerk einen Bedarf für Routing geben, d.h. die Weiterleitung von Nachrichten zwischen Netzwerken. IP-Hosts kommunizieren miteinander, indem sie sich entweder gegenseitig im selben Segment entdecken (siehe Kapitel 5) oder indem sie den Standard-Gateway bitten (der Router, der in ihren IP-Einstellungen angegeben ist), die Anforderung an das passende Netzwerk weiterzuleiten (der Prozess ist etwas komplizierter, nachdem der Host verlassen wurde).



Router werden im Zusammenhang mit IP auch manchmal als Gateways bezeichnet, obwohl dies rein technisch gesehen falsch ist. Wenn Sie Windows-Systeme verwalten, werden Sie jedoch mit dieser Tatsache leben müssen. Wenn ein IP-Hostsystem die Standard-Gateway-Adresse abfragt, ist damit der erste Router gemeint, den der Computer abfragt, wenn er ein Zielsystem nicht in seinem eigenen Segment finden kann.

IP-Router übernehmen die Pakete, die von den Hostsystemen versendet wurden und senden diese an das passende Netzwerk oder den Zielhost. Der Router weiß, wo das korrekte Netzwerk zu finden ist, weil er entweder direkt damit verbunden ist, weil er Informationen von anderen Routern sammelt oder weil er eine integrierte Routingtabelle nutzt, die angibt, in welche Richtung die Daten gesendet werden müssen (siehe Abbildung 8.1).

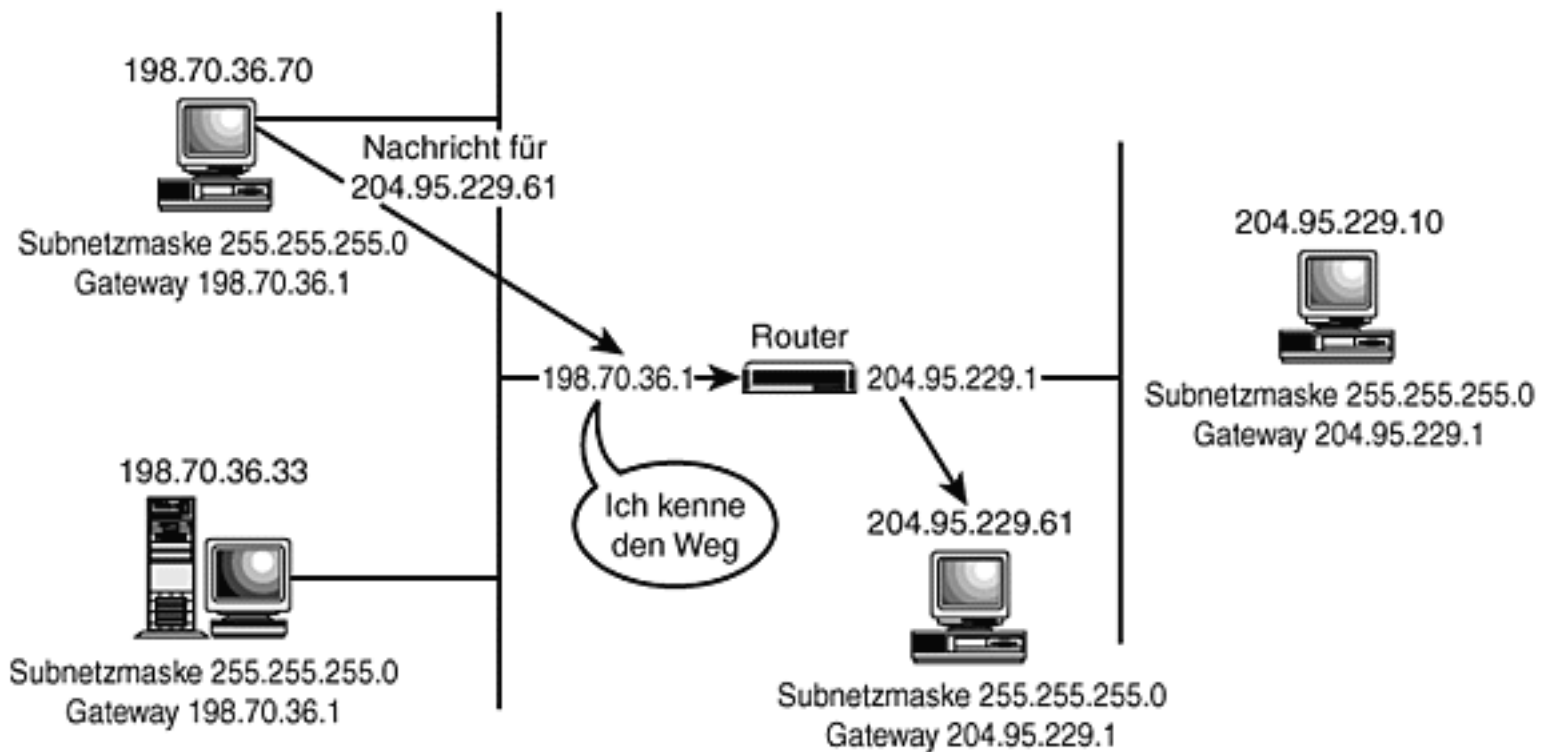


Abbildung 8.1: Ein Paket findet seinen Weg zum Host.

Jeder Host in einem IP-Netzwerk muss einen Router zur Verfügung haben, um mit einem Netzwerksegment kommunizieren zu können, mit dem er nicht direkt verbunden ist. Router, die nicht direkt mit einem Segment verbunden sind, müssen einen anderen Router benutzen, um die Verbindung zu dem Segment herzustellen. Jedes Mal, wenn ein Router eine Verbindung zu einem neuen Netzwerk herstellt, zeichnet er den Pfad auf, über den er zu diesem Netzwerksegment gelangt ist (siehe Abbildung 8.2). Im Laufe der Zeit kommt dabei eine umfassende Routingliste zusammen und der Router kann effizienter arbeiten. Für die Sammlung der Routen und die Nutzung der Routinginformationen werden viele verschiedene Protokolle benutzt. Aber alle verfolgen dasselbe Ziel. Das Internet ist ein Beispiel für dieses System.

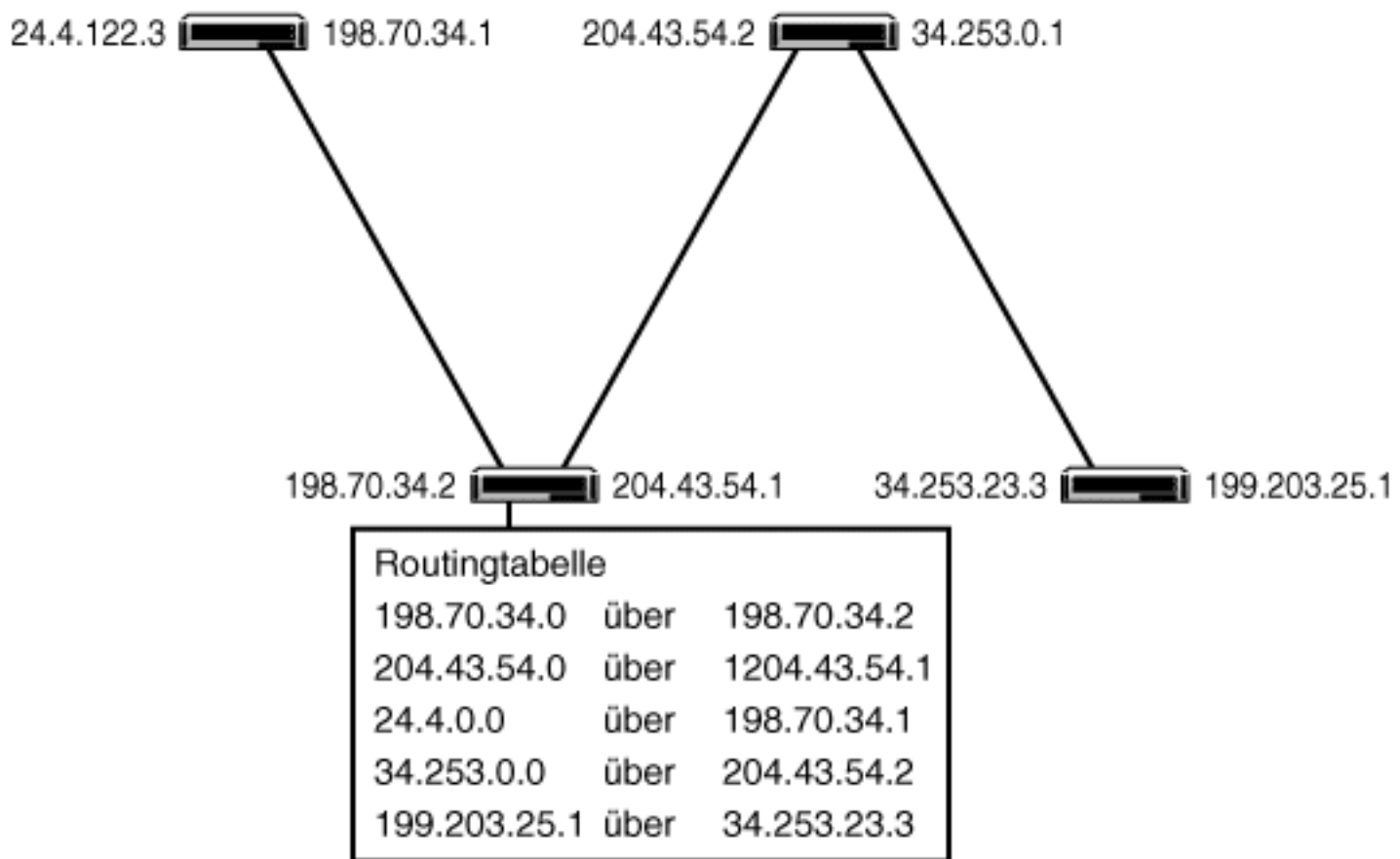


Abbildung 8.2: Ein Router, der eine neue Route findet und den Pfad aufzeichnet.

8.1.5 TCP-Ports

Wenn TCP/IP auf einem Host installiert wird, wartet der Server auf Nachrichten, die an den so genannten Ports eingehen. Ein *Port* entspricht einer geöffneten Tür, durch die Anforderungen ins System gelangen können, dass bestimmte Aktionen durchgeführt werden sollen. Wenn ein Server einen Dienst anbieten möchte, öffnet er einen Port und stellt den Dienst unter der Portnummer zur Verfügung. Clientanwendungen können dann Anforderungen an diese Portnummer senden und die Kommunikation kann beginnen.

Ein Beispiel ist der Port 80, der für die meisten Interaktionen mit dem World Wide Web verwendet wird. Der Port 80 wird von HTTP (Hypertext Transfer Protocol) benutzt, um den Webdienst (Webserver) bereitzustellen. Wenn ein Clientbrowser eine Webseite anfordert, sendet er die Anforderung an die HTTP-Adresse am Port 80.

Wenn ein Unternehmen eine private Seite präsentieren wollte, könnte sie HTTP einfach an einer anderen Portnummer präsentieren. Die Benutzer, die auf die Seite zugreifen wollen, müssen dann zunächst die spezifische Portnummer erfragen, um Zugriff auf die Seite zu erhalten. Das ist nützlich, weil Portnummern nicht immer dauerhaft zugeordnet werden. Wenn Pearson das HTTP-Protokoll z.B. am Port 465 anbieten würde, müssten die Benutzer die Webadresse <http://www.pearson.de:465> benutzen, um auf die Website zugreifen zu können.

Diese Regeln gelten für alle Ports. Hier nun einige »bekannte« Portnummern:

- 25 für SMTP (E-Mail)
- 21 für FTP (File Transfer Protocol)
- 80 für HTTP (Hypertext Transfer Protocol)
- 119 für NNTP (Network News Transfer Protocol)

Portnummern gibt es im Bereich zwischen 0 und 1023.

8.2 Microsoft-TCP/IP

Microsoft verpflichtete sich schon in der letzten Version von Windows NT zu TCP/IP, indem dieses Protokoll zum Standardprotokoll gemacht wurde. Bei Windows 2000 wurde dieser Trend noch verstärkt. Das gesamte Betriebssystem hängt nun von diesem Protokoll ab, um eine größtmögliche Funktionalität zu erzielen.

Wenn Sie bereits unter Windows NT mit TCP/IP gearbeitet haben, werden Sie in Windows 2000 auf viele altbekannte Gesichter stoßen. Wenn Sie eine lange Wunschliste für Windows-TCP/IP hatten, werden Sie nun feststellen, dass sich ziemlich viele Ihrer Träume verwirklicht haben.

8.2.1 Einführung in Microsoft-TCP/IP

Microsoft-Netzwerke hängen davon ab, dass ein Knoten im Netzwerk eine Ressource findet. Dateiserver, Mailserver, Drucker und sogar freigegebene Clients müssen sich selbst verfügbar machen, damit andere Computer sie sehen können. Dieser Vorgang wird als *Suche* bezeichnet.

Die Suche nach einem Server oder anderen Workstations erfolgt in Windows 2000, Windows 95/98 und Windows NT über die Netzwerkumgebung. Wenn Sie die Netzwerkumgebung öffnen, sehen Sie entweder die Systeme in Ihrem lokalen Segment oder eine Liste, die Ihnen bereitgestellt wurde.

Die Suche im Netzwerk ist nicht Bestandteil von TCP/IP. Sie muss vom Netzwerkbetriebssystem zur Verfügung gestellt werden. Das System, das Microsoft nutzt, um eine Suchfunktion im Netzwerk anbieten zu können, basiert auf einer Kombination verschiedener Tools von WINS bis zu Active Directory.

8.2.2 Installation von TCP/IP

Falls Sie nicht absichtlich versuchen, die Nutzung von TCP/IP auf Ihrem Server zu verhindern, wird TCP/IP während der Serverinstallation als Standardprotokoll eingerichtet. Über diesen Standard können Sie sich jedoch hinwegsetzen. Die Frage ist, wie Sie TCP/IP installieren können, wenn Sie die Installation übergangen haben? Weiterhin stellt sich die Frage, welche Dienste oder Optionen Sie für TCP/IP nutzen möchten, nachdem das Protokoll installiert ist.

TCP/IP lässt sich relativ leicht installieren. Besonders leicht ist die Installation, wenn Sie sich bereits mit der Installation von Protokollen und Netzwerkdiensten in Windows 95/98 auskennen. Die Benutzeroberfläche ist genau so einfach zu bedienen.

Um TCP/IP auf einer bestehenden Netzwerkkarte zu installieren, gehen Sie wie folgt vor:

1. Wählen Sie **Start/Einstellungen/Netzwerk- und DFÜ-Verbindungen**, um den Ordner **Netzwerk- und DFÜ-Verbindungen** zu öffnen.
2. Klicken Sie mit der rechten Maustaste auf die Verbindung, bei der Sie TCP/IP installieren möchten (siehe Abbildung 8.3) und wählen Sie im Kontextmenü den Befehl **Eigenschaften**.

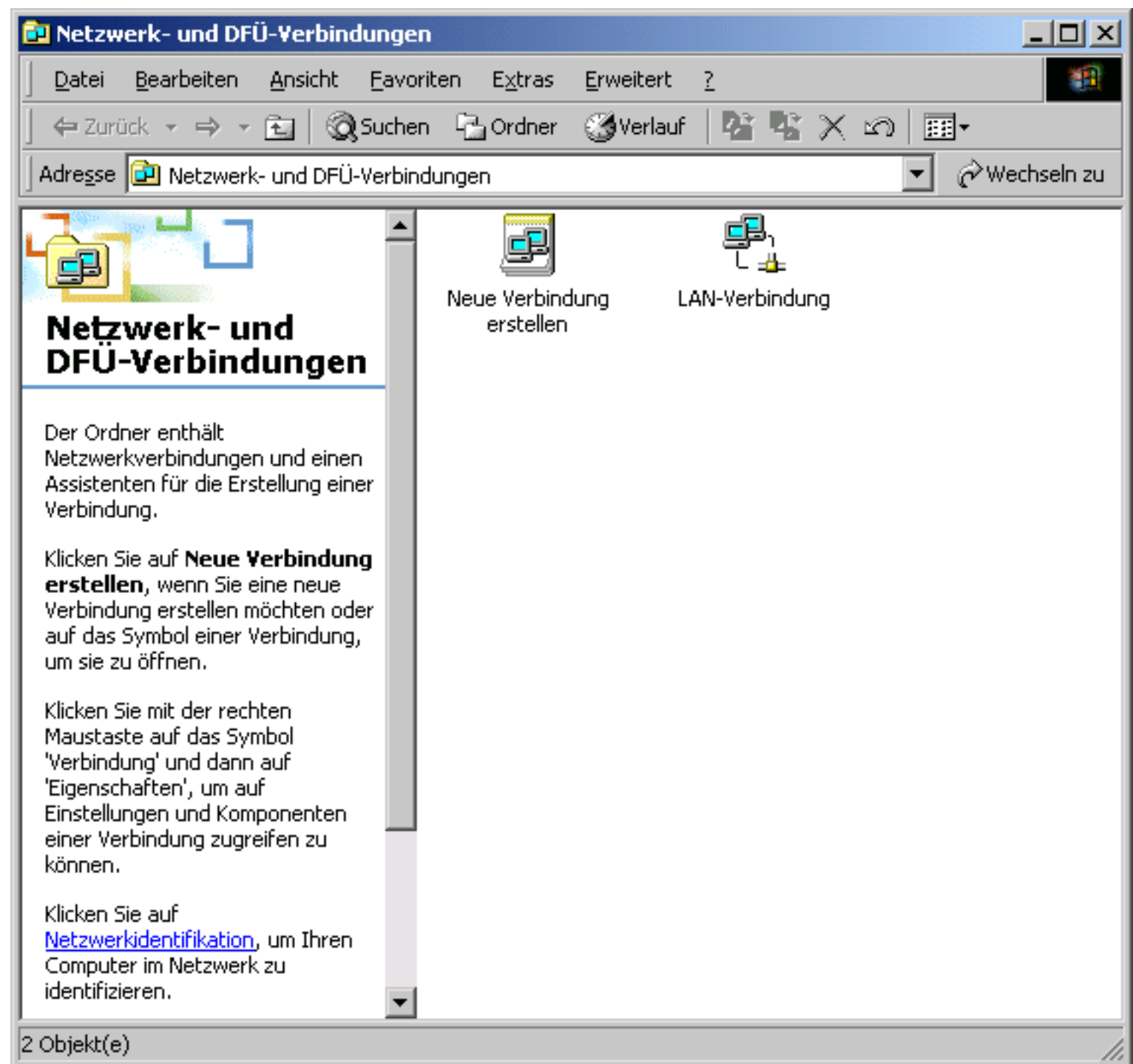


Abbildung 8.3: Der Ordner Netzwerk- und DFÜ-Verbindungen.

3. Klicken Sie im Fenster **Eigenschaften von LAN-Verbindung** auf die Schaltfläche **Installieren** und wählen Sie im Dialogfeld **Typ der Netzwerkkomponente auswählen** den Eintrag **Protokoll** (siehe Abbildung 8.4). Klicken Sie dann auf **Hinzufügen**.

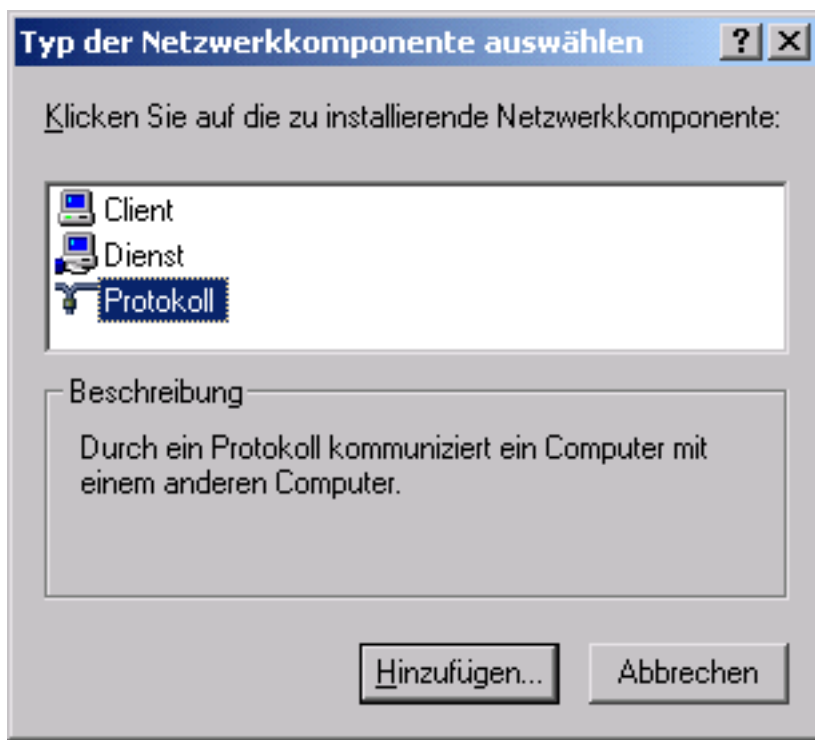


Abbildung 8.4: Das Dialogfeld Typ der Netzwerkkomponente auswählen.

4. Wählen Sie dann im Dialogfeld **Netzwerkprotokoll wählen**, das sich nun öffnet, den Eintrag **Internet-Protokoll (TCP/IP)** und klicken Sie dann auf OK.

8.2.3 Routing

Windows NT konnte bereits als Router eingesetzt werden, aber nicht in dem Maß, wie dies nun bei Windows 2000 möglich ist. Mit der Einführung von RRAS (Routing and Remote Access Service) ist das Routing über Windows nun eine wählbare Option. Windows 2000 wird sehr wahrscheinlich nie die erste Wahl als Router für umfangreiche Implementierungen sein. Bei kleinen Applikationen sollte es jedoch gut funktionieren.

Das Routing war im Rahmen von TCP/IP schon immer ein Bestandteil der Installation. Windows 2000 Server hat dies nicht geändert, sondern der Ort, an dem das Routing eingerichtet wird, wurde verändert. Die Routingfunktionen werden nun nicht mehr zusammen mit den Protokollen und Netzwerkkarten konfiguriert, sondern unter RRAS (Routing and Remote Access Service).

Windows 2000-Router

RRAS wird zusammen mit Windows installiert, ist aber nicht aktiviert. Um RRAS zu aktivieren, müssen Sie **Routing und RAS** öffnen (siehe Abbildung 8.5). Wählen Sie dazu **Start/Programme/Verwaltung/Routing und RAS**. Gehen Sie anschließend wie folgt vor:

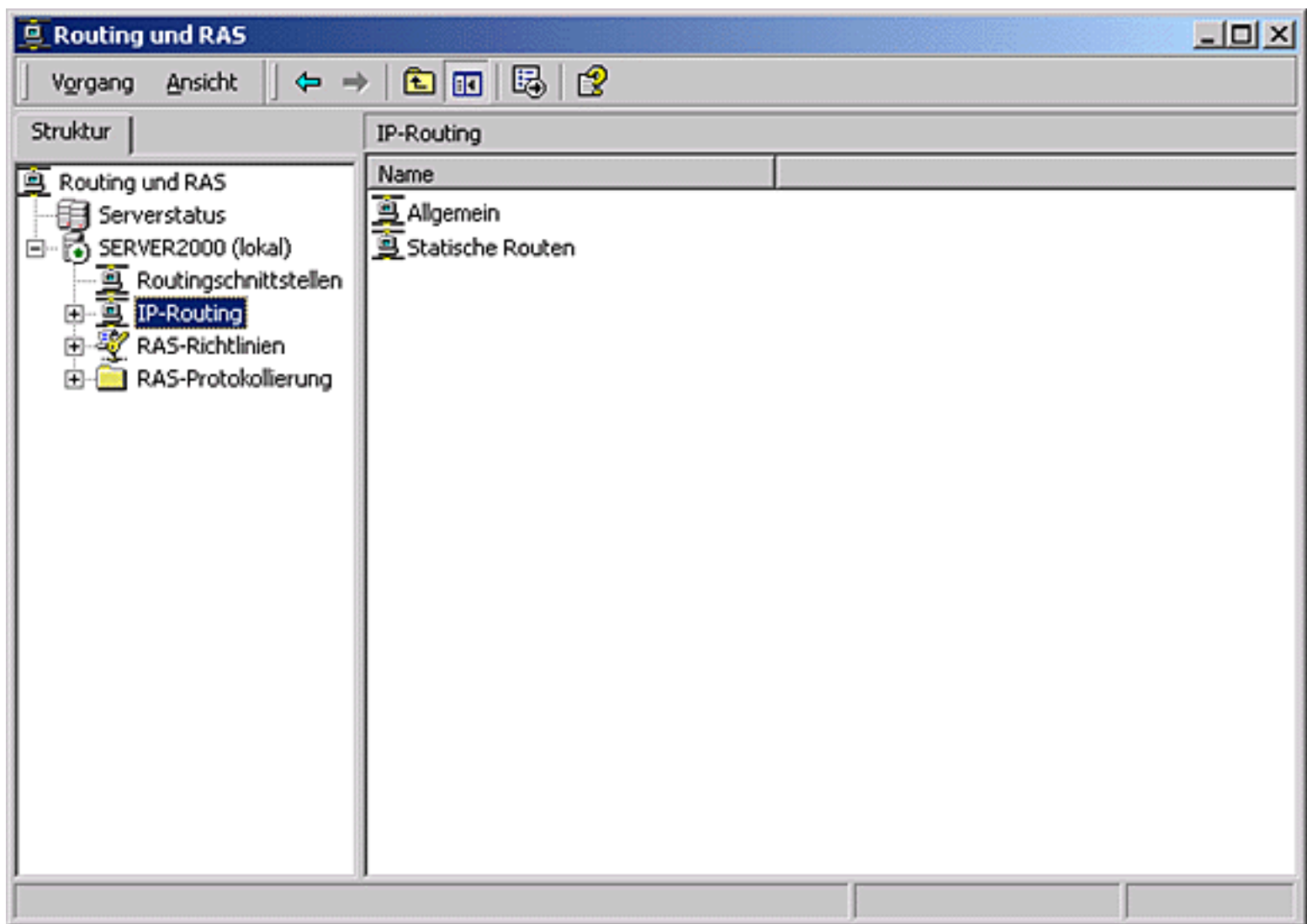


Abbildung 8.5: Die Anwendung Routing und RAS.

1. Klicken Sie mit der rechten Maustaste auf den Eintrag **Serverstatus** und wählen Sie im Kontextmenü den Befehl **Server hinzufügen**.
2. Wählen Sie im Dialogfeld **Server hinzufügen** die Option **Diesen Computer** und klicken Sie auf OK.
3. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf den neu hinzugefügten Server und wählen Sie im Kontextmenü den Befehl **Routing und RAS konfigurieren und aktivieren**.
4. Wählen Sie im **Setup-Assistent für den Routing- und RAS-Server** die Option **Netzwerkrouter**.
5. Wählen Sie das Protokoll, das für das Routing verwendet werden soll (standardmäßig TCP/IP).
6. Wählen Sie nun, ob eine **Bei Bedarf herzustellende Wählverbindung** eingerichtet werden soll, und stellen Sie den Router fertig.

Nachdem Sie den Router eingerichtet haben, können Sie ihn aktivieren, indem Sie mit der rechten Maustaste auf den Server klicken und im Kontextmenü den Befehl **Alle Tasks/Starten** wählen.

Für den RRAS-Dienst gibt es noch viele andere Verwendungszwecke. Die weiteren Optionen werden in Kapitel 14 ausführlich beschrieben. Erwähnenswert ist jedoch die Option **Bei Bedarf herzustellende Wählverbindung**. Für kleinere Unternehmen, für die eine Standleitung zwischen verschiedenen Niederlassungen zu kostspielig wäre, ist dies eine sehr gute Lösung, sofern die Bandbreite, die von einer

Standardtelefonleitung geboten wird, ausreicht.

Die Herstellung einer Wählverbindung bei Bedarf ist eine Einstellung von RRAS, die bewirkt, dass ein Modem eine Wählverbindung zur Gegenstelle herstellt, sobald eine Anforderung für eine Netzwerkadresse besteht, die sich auf der anderen Seite der Route befindet. Wenn ein Computer in Netzwerk A z. B. einen E-Mail-Server in Netzwerk B benötigt, stellt der RRAS-Server in Netzwerk A, der die Anforderung hört, eine Wählverbindung zu Netzwerk B her.



Denken Sie daran, dass eine Wählverbindung sich nicht eignet, um auf eine Anwendung zuzugreifen und auch nicht bei einem hohen Datenfluss. Die Internetconnectivity beansprucht in der Regel minimalen Datenverkehr.

8.2.4 DHCP

Ein sehr schwieriger Punkt beim Einsatz des TCP/IP-Protokolls ist die Tatsache, dass jeder Knoten im Netzwerk eine eindeutige Adresse haben muss. Andere Protokolle wie IPX/SPX weisen einem Client beim Start automatisch eine Adresse zu. IP-Adressen müssen extra zugewiesen werden. Das heißt jedoch nicht, dass diese Anforderung von einem Menschen überwacht werden müsste.

Grundlegende Informationen zu DHCP

DHCP (Dynamic Host Configuration Protocol) bietet TCP/IP-Netzwerken die Möglichkeit, Clientcomputern IP-Adressen bei Bedarf zuzuweisen. Dazu sendet das Betriebssystem einen Broadcast, der besagt, dass ein Host eine IP-Adresse benötigt. Jeder DNS-Server im Netzwerk kann hier weiterhelfen.

Die Anforderung, die versendet wird, wird als DHCP-Discover-Nachricht bezeichnet. Der DHCP-Server empfängt die Nachricht und übermittelt ein Angebot. Der Client kann diese Nachricht akzeptieren und antworten, dass er die angebotene Adresse behält oder eine neue Anforderung versenden. Sobald der Client das Angebot bestätigt, vervollständigt er seine IP-Informationen mit Einstellungen, die vom Server angeboten werden.

Adressen werden an Clients nicht dauerhaft vergeben. Im Allgemeinen wird einer Adresse eine Leasedauer zugewiesen, d.h. die Adresse läuft nach einer bestimmten Zeitspanne ab. Jedes Mal, wenn der Client neu gestartet wird, prüft er, ob seine Adresslease noch immer gültig ist. Wenn eine Bestätigung oder gar keine Antwort eintrifft, behält der Client die IP-Adresse. Falls der Client keine Antwort erhält, beginnt er, eine neue Lease zu suchen, nachdem 87,5 % der Zeitspanne der Lease abgelaufen sind.

Als Teil der Adresslease werden mehr als nur einfache IP-Adressinformationen gesendet. Die IP-Kommunikation hängt von mehr als der IP-Adresse ab und ein DHCP-Server kann so konfiguriert werden, dass er mehr als nur eine Adresse versendet. Clientcomputer können IP-Adressen und die damit verbundenen Daten sowie die folgenden Elemente empfangen:

- **Subnetzmaske.** Gibt die Subnetzmaske der Clientsubnetzmaske gemäß RFC 950, »Internet Standard Subnetting Procedure«, an. Der Wert für diese Option stammt aus dem Feld **Subnetzmaske** im Dialogfeld **Eigenschaften von Bereich**. Klicken Sie mit der rechten Maustaste auf den Bereich und wählen Sie im Kontextmenü den Befehl **Eigenschaften**, um dieses Dialogfeld zu öffnen.

- *Zeitoffset*. Gibt einen Offsetwert (in Sekunden) zur UCT-Zeit (Universal Coordinated Time) an, der auf das Clientsubnetz angewendet wird. Dieser Wert lässt sich als vorzeichenbehafteter 32-Bit-Ganzzahlwert konfigurieren. Positive Offsetwerte kennzeichnen ein Subnetz östlich des Nullmeridians und negative Werte kennzeichnen ein Subnetz westlich des Nullmeridians.
- *Router*. Gibt eine Liste der IP-Adressen für Router im Subnetz des Clients an. Wenn mehrere Router zugewiesen werden, interpretiert der Client die Adressen in der festgelegten Reihenfolge.
- *Zeitserver*. Gibt eine Liste mit IP-Adressen für RFC-868-Zeitserver an, die dem Client zur Verfügung stehen. Wenn mehr als ein Zeitserver zugewiesen wird, interpretiert und benutzt der Client die Adressen in der angegebenen Reihenfolge.
- *DNS-Server*. Gibt eine Liste der IP-Adressen für DNS-Namensserver an, die dem Client zur Verfügung stehen. Wurden mehrere Server zugewiesen, interpretiert der Client die Adressen in der angegebenen Reihenfolge und benutzt sie entsprechend. Mehrfach vernetzte DHCP-Clientcomputer, die mehrere DHCP-Leases erhalten, können nur eine DNS-Serverliste pro Hostcomputer erhalten und nicht eine pro Netzwerkkarte.
- *Hostname*. Gibt den Hostnamen für den Client an, der bis zu 63 Zeichen lang sein darf (siehe hierzu RFC 1035 für mögliche Beschränkungen des Zeichensatzes). In einigen Fällen lässt sich der Name auch, wie in der nächsten Option angegeben, vollständig qualifizieren, indem der hier mit dem DNS-Domänennamen bereitgestellte Namenswert angehängt wird. Für Windows-Clients wird diese Option beim Konfigurieren des Hostnamens des Clients nicht unterstützt. Diese Einstellung wird im Dialogfeld **Netzwerk** auf der Registerkarte **Identifikation** im Feld **Computername** vorgenommen.
- *DNS-Domänenname*. Gibt den Domänennamen an, den der DHCP-Client benutzen soll, wenn der Hostname mit Hilfe von DNS ausgewertet wird. Bei diesem Optionstyp werden ASCII-Zeichenfolgen als Datenwerte benutzt. Die Länge des Wertefelds hängt von der Anzahl der Zeichen ab, die im angegebenen DNS-Domänennamen verwendet werden. Wenn der Domänenname z.B. 20 Zeichen lang ist, sollte das Wertefeld für diese Option ebenfalls 20 Oktette lang sein.
- *IP-Layerweiterleitung Deaktivieren/Aktivieren*. Wird verwendet um festzulegen, ob der DHCP-Client die Weiterleitung von Datagrammen auf der IP-Ebene aktiviert oder deaktiviert.
- *Nichtlokales Quellrouting Deaktivieren/Aktivieren*. Wird verwendet um festzulegen, ob der DHCP-Client die Weiterleitung von Datagrammen auf der IP-Ebene aktiviert oder deaktiviert, wobei ein empfangenes Datagramm von einer lokalen oder nicht lokalen Quelle stammen kann.
- *Alle Subnetze lokal*. Gibt an, ob der Client annimmt, dass alle Subnetze seines Netzwerkverbunds dieselbe MTU verwenden wie das lokale Subnetz, mit dem der Client verbunden ist.
- *Broadcastadresse*. Normalerweise ist dies die eingeschränkte Broadcast-IP-Adresse (255.255.255.255), sie kann jedoch mittels zulässiger Werte für Broadcast-Adressen, die in Abschnitt 3.2.1.3 von RFC 1122, »Requirements for Internet Hosts - Communication Layers« angegeben sind, verändert werden.
- *Routersuche durchführen*. Gibt an, ob der Client Routeranfragen gemäß RFC 1256 durchführen soll.
- *Routeranfrageadresse*. Gibt die IP-Adresse an, an die der Client Routeranfrageanforderungen übergibt.
- *Statische Routenoption*. Gibt eine Liste statischer Routen an, die der Client in seinem

Zwischenspeicher für Routen installiert. Alle Routen zum selben Ziel werden nach absteigender Priorität aufgelistet. Die Standardroute 0.0.0.0 ist für eine statische Route kein zulässiges Ziel.

- *NIS-Domänenname*. Gibt den Namen der NIS-Domäne (NIS = Network Information Service) als ASCII-Zeichenfolge an.
- *NIS-Server*. Listet die IP-Adressen in der Reihenfolge der Verfügbarkeit von NIS-Servern für den Client auf.
- *NIS+ Domänenname*. Gibt den Namen der NIS+-Domäne (NIS+ = Network Information Service Plus) des Clients als ASCII-Zeichenfolge an.
- *NIS+ Server*. Listet die IP-Adressen in der Reihenfolge der für Clients verfügbaren NIS+-Server auf (NIS+ = Network Information Service Plus).
- *WINS/NBNS-Server*. Listet die IP-Adressen für WINS-Server (WINS = Windows Internet Naming Service) oder NBNS-Server auf (NBNS = NetBIOS Name Server).
- *NetBIOS über TCP/IP NBDD*. Konfiguriert den Clientknotentyp für NetBT-Clients (NetBT = NetBIOS über TCP/IP) gemäß RFC 1001/1002. Bei mehrfach vernetzten Computern wird der Knotentyp dem Computer und nicht einzelnen Netzwerkkarten zugewiesen.
- *IP-Adressenleasezeit*. Dieser Optionstyp wird zum Aushandeln und Austausch von Leasezeitinformationen zwischen DHCP-Clients und -Servern auf eine der beiden folgenden Weisen verwendet:
 - Kann bei der DHCP-Suche oder einer DHCP-Anforderungsmeldung verwendet werden, die von einem Client gesendet wird, um eine Leasezeit für seine IP-Adresse anzufordern.
 - Kann bei einer Antwort des Servers auf ein DHCP-Angebot verwendet werden, um dem Client eine vom Server angebotene Leasezeit anzubieten.

Installation

Zunächst sollten Sie wissen, dass alle Computer, die als DHCP-Server eingesetzt werden, eine statische IP-Adresse benötigen. Ein DHCP-Server kann nicht als Computer konfiguriert werden, der seine Adresse von einem DHCP-Server bezieht. Gehen Sie wie folgt vor, um einen DHCP-Server zu installieren:

1. Wählen Sie **Start/Einstellungen/Systemsteuerung**, um die Systemsteuerung zu öffnen.
2. Klicken Sie doppelt auf **Software**.
3. Wählen Sie die Option **Windows-Komponenten hinzufügen/entfernen**.
4. Aktivieren Sie das Kontrollkästchen **Netzwerkdienste** und klicken Sie auf die Schaltfläche **Details**.
5. Aktivieren Sie im Feld **Unterkomponenten von »Netzwerkdienste«** das Kontrollkästchen **DHCP-Protokoll (Dynamic Host Configuration Protocol)** und klicken Sie auf OK.
6. Klicken Sie auf **Weiter** und geben Sie den vollständigen Pfad zu den Dateien an (z.B. *D:\i386*), klicken Sie dann auf **Weiter**. Dadurch wird der DHCP-Installationsassistent gestartet.

Wenn der Assistent fertig gestellt wird, muss der Server neu gestartet werden, damit die Änderungen wirksam werden.

Bereich

Die Informationen, die der DHCP-Server dem Client anbietet, sind in einem so genannten *Bereich*

gespeichert. Bevor der Server die erste DHCP-Discover-Nachricht empfangen hat, benötigt er »Futter«.

Im Bereich sind die IP-Einstellungen enthalten, die der Server für die DHCP-Clients zur Verfügung stellt. Dieser Bereich wird entweder für alle Clients des DHCP-Servers (global) oder für einzelne Segmente erzeugt. Zu den Einstellungen, die in einem Bereich gespeichert werden, gehört die Verfügbarkeit der Lease (siehe hierzu den Abschnitt »Grundlegende Informationen zu DHCP« in diesem Kapitel).

Der Bereich wird über die DHCP-Konsole verwaltet. Der DHCP-Server wird entweder über das Menü **Verwaltung** oder über die Microsoft Management Console als Snap-In gestartet.

8.2.5 Einen Bereich einrichten

Wenn die DHCP-Konsole einmal geöffnet ist, können Sie wie folgt vorgehen, um einen Bereich einzurichten:

1. Markieren Sie in der DHCP-Konsole den DHCP-Server (siehe Abbildung 8.6).

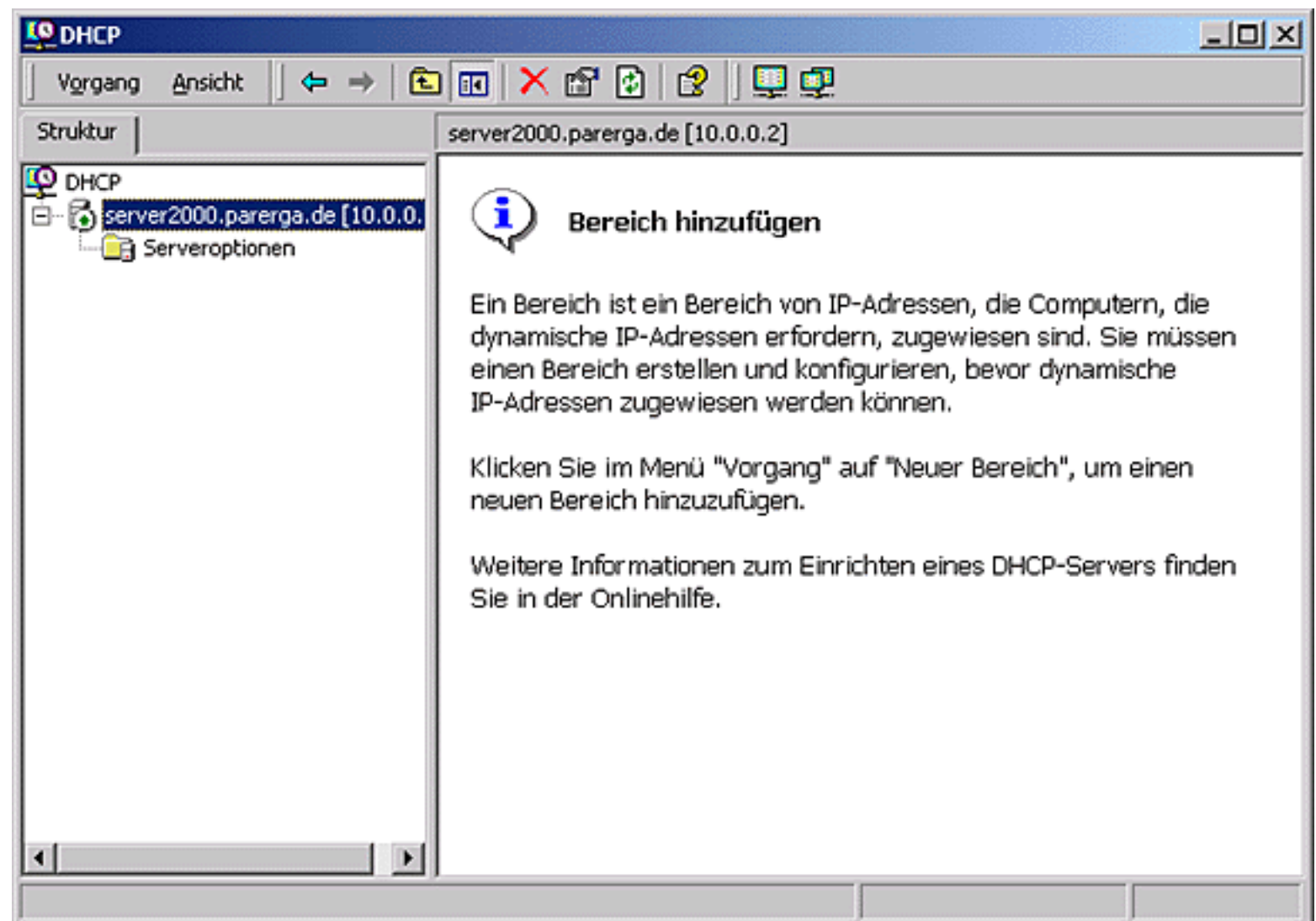
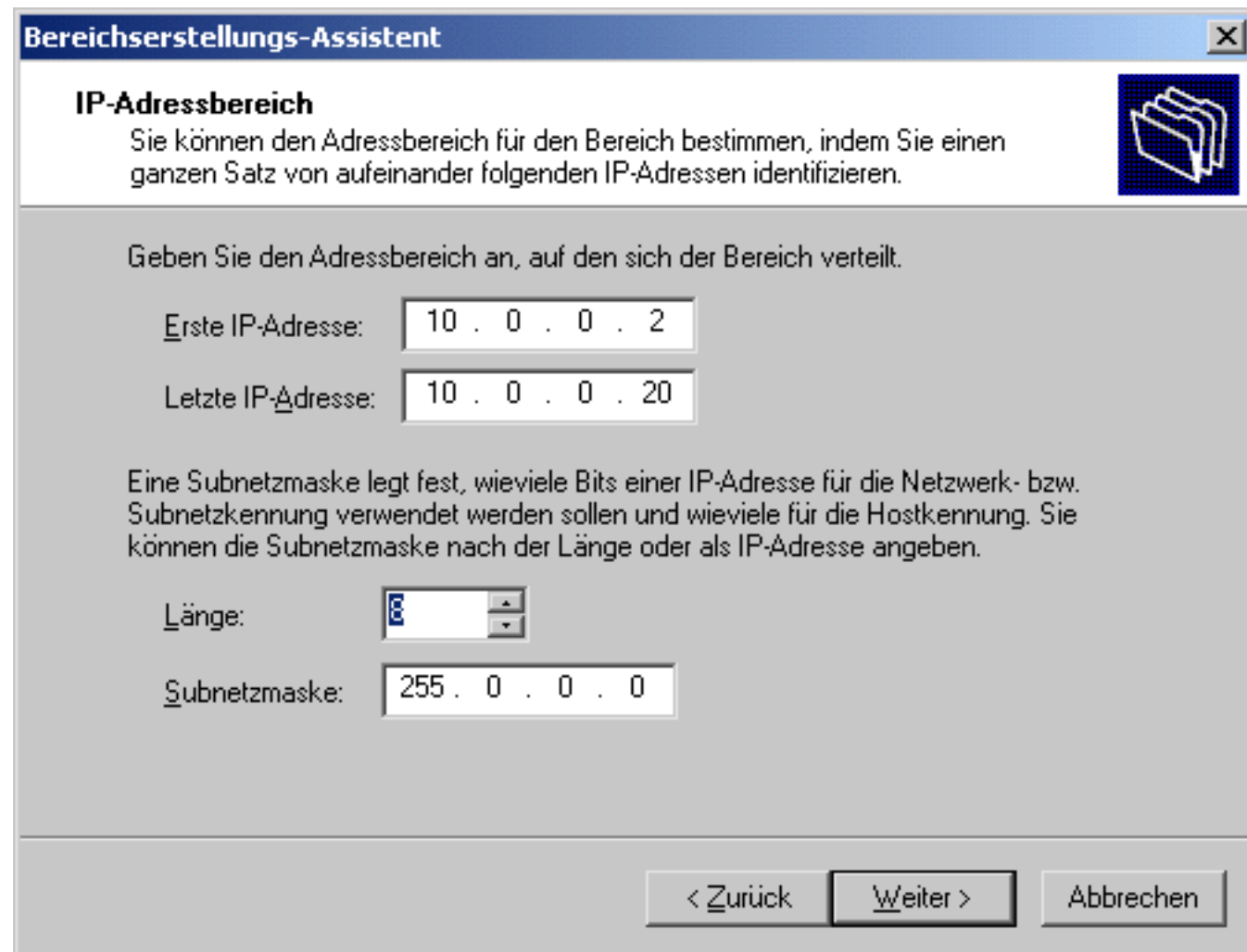


Abbildung 8.6: In der DHCP-Konsole einen neuen Bereich einrichten.

2. Wählen Sie im Menü **Vorgang** den Befehl **Neuer Bereich**. Es öffnet sich der **Bereichserstellungs-Assistent**. Klicken Sie auf **Weiter**.

3. Geben Sie einen Namen für den Bereich ein. Bei Bedarf können Sie auch noch eine Beschreibung eingeben, um den Bereich besser identifizieren zu können. Klicken Sie dann auf **Weiter**.
4. Geben Sie die erste und die letzte IP-Adresse für den Adressbereich ein, aus dem den Clients IP-Adressen zugewiesen werden sollen (siehe Abbildung 8.7).



Bereichserstellungs-Assistent

IP-Adressbereich

Sie können den Adressbereich für den Bereich bestimmen, indem Sie einen ganzen Satz von aufeinander folgenden IP-Adressen identifizieren.

Geben Sie den Adressbereich an, auf den sich der Bereich verteilt.

Erste IP-Adresse: 10 . 0 . 0 . 2

Letzte IP-Adresse: 10 . 0 . 0 . 20

Eine Subnetzmaske legt fest, wieviele Bits einer IP-Adresse für die Netzwerk- bzw. Subnetzkenung verwendet werden sollen und wieviele für die Hostkenung. Sie können die Subnetzmaske nach der Länge oder als IP-Adresse angeben.

Länge: 8

Subnetzmaske: 255 . 0 . 0 . 0

< Zurück Weiter > Abbrechen

Abbildung 8.7: Den IP-Adressbereich für die Clients konfigurieren.

5. Nun können Sie die Länge der Subnetzmaske in Bits eingeben. Es ist jedoch vermutlich einfacher, die (Tab)-Taste zu drücken und die Subnetzmaske manuell einzugeben. Klicken Sie anschließend auf **Weiter**.
6. Im Schritt **Ausschlüsse hinzufügen** können Sie bestimmte Adressen oder Adressbereiche angeben, die vom Server nicht zugewiesen werden sollen. Es werden also Adressbereiche ausgeschlossen. Füllen Sie dazu die Felder **Erste IP-Adresse** und **Letzte IP-Adresse** aus und klicken Sie auf **Hinzufügen**. Um nur eine Adresse auszuschließen, geben Sie diese in das Feld **Erste IP-Adresse** ein und klicken Sie dann auf **Hinzufügen**. Klicken Sie auf **Weiter**, um zum nächsten Schritt zu gelangen.
7. Im Schritt **Gültigkeitsdauer der Lease** (siehe Abbildung 8.8) können Sie angeben, wie lange eine Lease für einen Client gültig sein soll, d.h., wie lange die IP-Adresse einem Client zugewiesen wird. Der Standardwert liegt bei acht Tagen. Die Werte können Sie entweder direkt eingeben oder über die Pfeilschaltflächen auswählen.

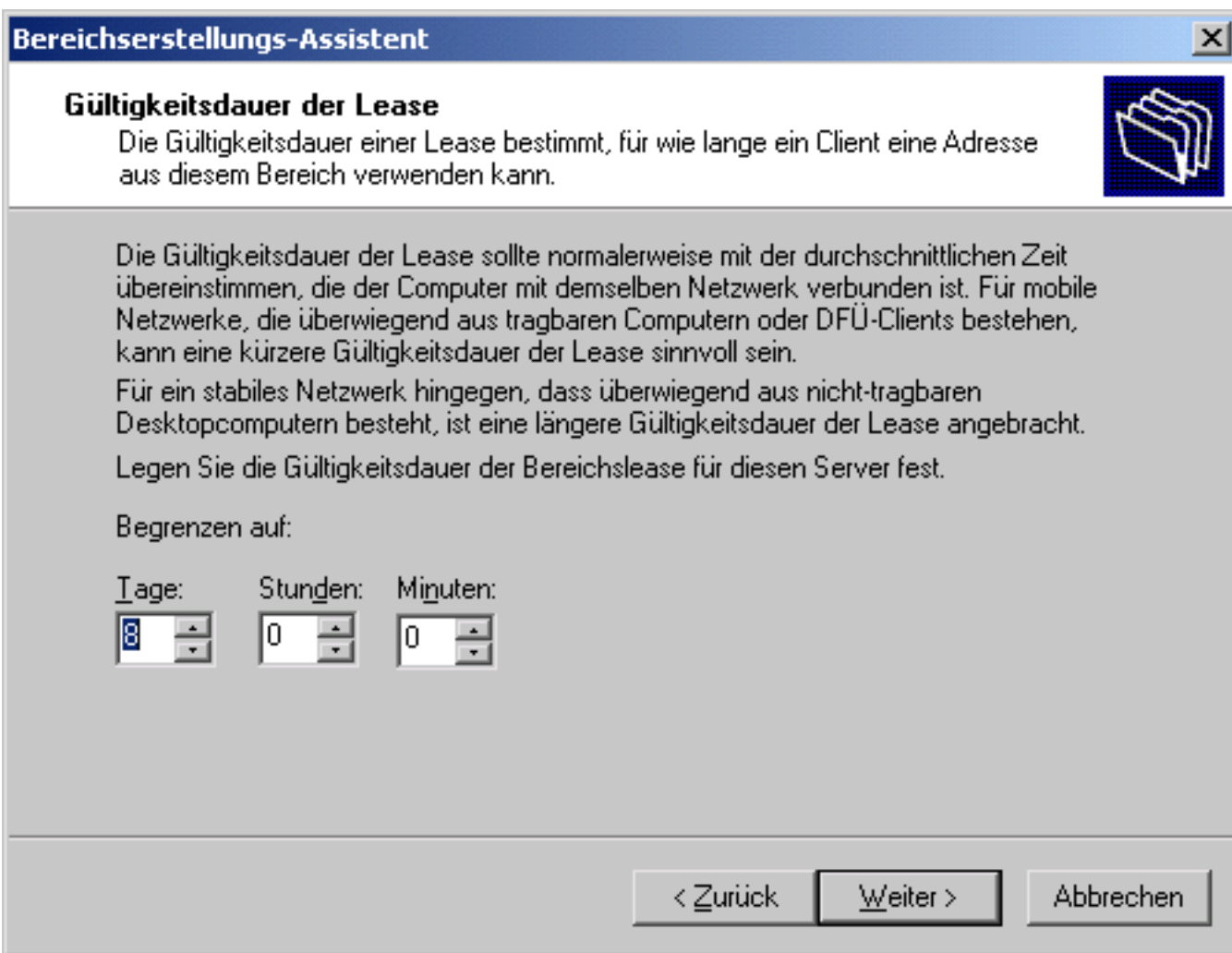


Abbildung 8.8: Die Gültigkeitsdauer der Lease festlegen.

8. Als Nächstes werden Sie gefragt, ob Sie die DHCP-Optionen nun konfigurieren möchten. Wählen Sie die Schaltfläche **Weiter** und stellen Sie die Installation fertig.
9. Geben Sie im Schritt **Router (Standardgateway)** die Adresse des Gateways oder Routers ein, den der Client benutzen soll. Klicken Sie dann auf **Hinzufügen**. Fügen Sie die Router in der Reihenfolge hinzu, in der sie durchsucht werden sollen. Klicken Sie dann auf **Weiter**.
10. Im nächsten Schritt können Sie Informationen zum Domännennamen und dem DNS-Server angeben (siehe Abbildung 8.9). Geben Sie zuerst den Namen der Domäne des Clientcomputers ein, drücken Sie die (Tab)-Taste und geben Sie dann die IP-Adresse des ersten DNS-Servers ein, den der Clientcomputer nutzen soll. Klicken Sie auf **Hinzufügen** und wiederholen Sie den Vorgang für alle benötigten DNS-Server. Klicken Sie dann auf **Weiter**.

Bereichserstellungs-Assistent

Domänenname und DNS-Server

Das DNS (Domain Name System) ordnet zu und übersetzt Domännennamen, die von Clients im Netzwerk verwendet werden.

Sie können die übergeordnete Domäne festlegen, die die Clientcomputer im Netzwerk für die DNS-Namensauflösung verwenden sollen.

Übergeordnete Domäne:

Geben Sie die IP-Adresse für die Server an, um Bereichsclients zur Verwendung von DNS-Servern im Netzwerk zu konfigurieren.

Servername: IP-Adresse:

Abbildung 8.9: Den Domännennamen und den DNS-Server angeben.

11. Der Schritt **WINS-Server** ist genauso aufgebaut wie der vorherige Schritt. Tragen Sie den oder die WINS-Server ein und klicken Sie auf **Weiter**.
12. Zum Schluss werden Sie gefragt, ob Sie den Bereich aktivieren möchten. Treffen Sie Ihre Wahl und klicken Sie auf **Weiter**.
13. Klicken Sie auf **Fertig stellen**.

Den Bereich verwalten

Die Verwaltung eines Bereichs, der soeben erstellt wurde, ist ganz einfach. Öffnen Sie die DHCP-Konsole und wählen Sie den Server sowie anschließend den Bereich, den Sie verwalten möchten. Der Bereich erweitert sich nun und Ordner für alle Optionen sind sichtbar (siehe Abbildung 8.10).

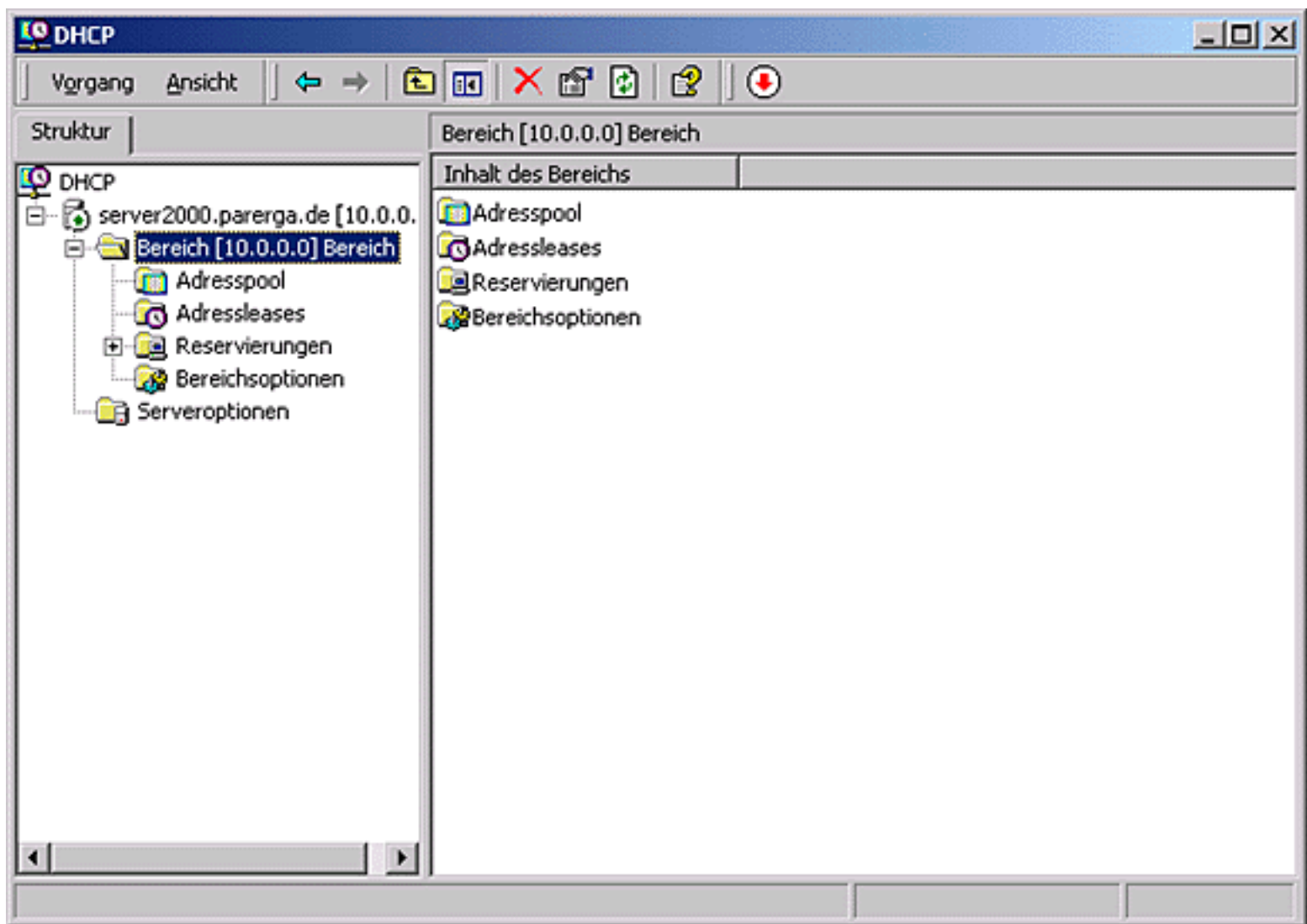


Abbildung 8.10: Der erweiterte Bereich.

Im DHCP-Server lassen sich mehrere hundert Einstellungen verändern. Um ein Beispiel zu geben und die häufigsten Optionen zu nennen, finden Sie nachfolgend eine Anleitung.

Gehen Sie wie folgt vor, um die Leasedauer zu verändern:

1. Klicken Sie mit der rechten Maustaste auf den Bereich und wählen Sie im Kontextmenü den Eintrag **Eigenschaften**.
2. Auf der Registerkarte **Allgemein** können Sie im Bereich **Gültigkeitsdauer der Lease für DHCP-Clients** Einstellungen zur Lease vornehmen. Klicken Sie anschließend auf OK.

Um einen weiteren Ausschlussbereich zu erzeugen, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf den Ordner **Adresspool** und wählen Sie im Kontextmenü den Befehl **Neuer ausgeschlossener Bereich**.
2. Geben Sie im Dialogfeld **Ausschluss hinzufügen** die erste und die letzte IP-Adresse des Ausschlussbereichs ein und klicken Sie auf **Hinzufügen**.

Gehen Sie wie folgt vor, um eine Reservierung vorzunehmen:

1. Klicken Sie mit der rechten Maustaste auf den Ordner **Reservierungen** und wählen Sie im

Kontextmenü den Befehl **Neue Reservierung**.

2. Geben Sie im Dialogfeld **Neue Reservierung** einen Namen und die IP-Adresse ein, die Sie für einen bestimmten Client reservieren möchten, und drücken Sie die (Tab)-Taste.

3. Geben Sie die MAC-Adresse des Computers ein, für den Sie die Reservierung erstellen möchten (siehe Abbildung 8.11).

4. Klicken Sie auf die Schaltfläche **Hinzufügen**.



Abbildung 8.11: Eine neue Reservierung einrichten.

 Um die MAC-Adresse eines Computers zu ermitteln, geben Sie an der Eingabeaufforderung den Befehl `net config wksta` ein und drücken dann die (Enter)-Taste.

Weitere Einstellungen von Bereichen lassen sich im Ordner **Bereichsoptionen** ändern. Klicken Sie mit der rechten Maustaste auf diesen Ordner und wählen Sie im Kontextmenü den Befehl **Optionen konfigurieren**, öffnet sich das Dialogfeld **Bereich-Optionen**, in dem Ihnen die Optionen zur Auswahl stehen, die im Abschnitt »Grundlegende Informationen zu DHCP« beschrieben sind. Nachdem eine Option ausgewählt wurde, wird ein Dateneingabepunkt geöffnet und es stehen Ihnen weitere Optionen zur Verwaltung des Bereichs zur Verfügung.

Bereichsgruppierungen

Eine Bereichsgruppierung umfasst mehrere DHCP-Bereiche in einem Netzwerk. Sie bietet den Vorteil, dass mehrere Bereiche gleichzeitig aktiviert oder deaktiviert werden können. Wenn keine Bereichsgruppierungen zur Verfügung stehen oder diese nicht benutzt werden, kann immer nur ein

DHCP-Bereich in einem Netzwerk aktiviert werden. Wurden auf einem DHCP-Server mehrere Bereiche definiert und aktiviert, wird trotzdem nur ein Bereich benutzt, um die Leases an die Clients zu vergeben. Die Bereichsgruppierung bietet die Möglichkeit, Leases aus mehreren Bereichen zu vergeben.

Um eine Bereichsgruppierung zu erstellen, klicken Sie in der DHCP-Konsole mit der rechten Maustaste auf den DHCP-Server, auf dem Sie die Gruppierung einrichten möchten, und wählen Sie im Kontextmenü den Befehl **Neue Bereichsgruppierung**. Der **Assistent zum Erstellen neuer Bereichsgruppierungen** führt Sie durch den Vorgang, bei dem Sie einfach einen Namen für die Gruppierung vergeben und die gewünschten Bereiche hinzufügen.

Clients aktivieren

Wenn ein Windows 2000-, ein Windows NT- oder ein Windows 95/98-Client mit dem TCP/IP-Protokoll installiert wird, erhält dieser die IP-Adresse standardmäßig automatisch von einem DHCP-Server und wird damit als DHCP-Client installiert. Bei Windows 2000 muss dazu die Option **IP-Adresse automatisch beziehen** ausgewählt werden (siehe Abbildung 8.12). Um den DNS-Server verwenden zu können, muss die Option **DNS-Serveradresse automatisch beziehen** aktiviert werden.

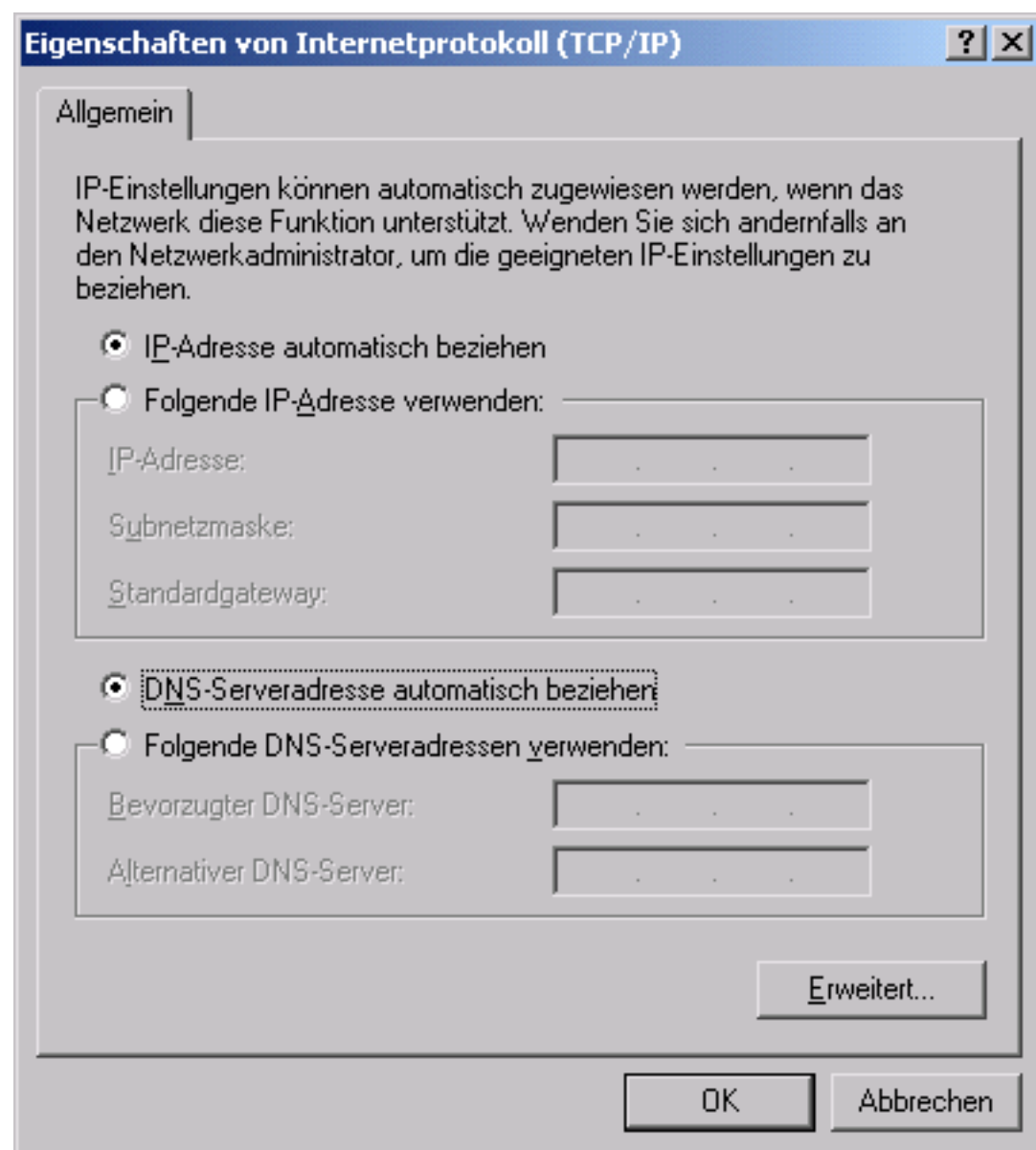


Abbildung 8.12: DHCP-Clients beziehen die IP-Adresse automatisch.

8.2.6 WINS

WINS (Windows Internet Naming Service) war die erste Lösung, die Microsoft entwickelte, um in TCP/IP-Netzwerken die Suche zu ermöglichen. WINS bietet den Computern im Netzwerk die Möglichkeit, die Namen und Adressen anderer Computer synchronisiert zu halten.

Wie bereits früher erwähnt, sind Windows-Netzwerke von einer Suchfunktion abhängig, mit der die anderen Computer im Netzwerk gefunden und angezeigt werden können.

Da ein ganzes Kapitel dieses Buches (Kapitel 13) der Suche im Netzwerk gewidmet ist, soll dieses Thema hier nicht überstrapaziert werden. Es soll hier genügen zu erwähnen, dass es eine Möglichkeit geben muss, die Netzwerkressourcen zu suchen, sodass sie im Ordner **Netzwerkumgebung** der Clients oder sogar über den Befehl `dos net` angezeigt werden.

Benennung und Suche

Wenn ein Computer in einem Netzwerk installiert wird, wird ihm ein Computernamen zugewiesen. Dieser Name wird auch als NetBIOS-Name bezeichnet (NetBIOS = Network Basic Input Output Service). Dieser Name wird Benutzern in der **Netzwerkumgebung** präsentiert. Er ist der zentrale Punkt bei der Suche nach Komponenten im Netzwerk.

Der Computernamen ist nicht mit dem Domänennamen eines Computers identisch. Der Domänenname ist der Name, der von den DNS-Servern (DNS = Domain Name Servers) verwendet wird. Domänen können in TCP/IP auch eingesetzt werden, um einen bestimmten Host zu kennzeichnen, wenn der Hostname zu dem Domänennamen hinzugefügt wird. Der Computer unter der IP-Adresse 10.1.23.44 ist möglicherweise mit dem Domänennamen proxy.microsoft.com verknüpft. Deshalb trägt dieser Computer in der Domäne den Namen »proxy«.

Die NetBIOS und Domänennamen können miteinander verknüpft werden. Sie sind aber eigentlich unabhängig voneinander.

Der Aufbau von Microsoft WINS 2000

Das Konzept von WINS ist es, einen Registrierungspunkt für die Computer zu bieten, die miteinander über NetBIOS-Namen in Verbindung bleiben müssen.

Der WINS-Dienst kann bei der Installation von Windows 2000 Server installiert oder später hinzugefügt werden. Ist der Dienst installiert, wartet er darauf, dass andere Computer ihm mitteilen, dass sie existieren; er übermittelt dann die NetBIOS-Informationen, die diese Computer ihm zur Verfügung stellen. WINS kann als eine Art NetBIOS-Telefonbuch betrachtet werden. Der Dienst empfängt neue Verbindungen und registriert die NetBIOS-Namen und IP-Adressen der Computer. Diese Informationen stellt er dann Clients oder anderen WINS-Servern zur Verfügung.

Immer, wenn ein neuer Computer in das TCP/IP-Netzwerk integriert wird, erhält er eine WINS-Serveradresse. Wenn ein Server TCP/IP startet, teilt er dem WINS-Server mit, dass er vorhanden ist, wie sein NetBIOS-Name lautet und welche IP-Adresse er erhält. Anschließend hält dieser Computer

den WINS-Server über alle Änderungen an der IP-Adresse oder dem NetBIOS-Namen auf dem Laufenden.

Ein WINS-Server kann immer nur ein Netzwerksegment überwachen. Wenn das Netzwerk mehrere Segmente enthält, muss ein WINS-Agent oder ein weiterer WINS-Server installiert werden, der mit dem ersten WINS-Server kommuniziert, um die Suche im Netzwerk weiterhin zu gestatten.

Nachdem sich die Computer beim WINS-Server registriert haben, haben Sie einige Vorteile:

- Die Anzahl der Broadcasts reduziert sich drastisch, weil die Computer eine direkte Quelle haben, um NetBIOS-Informationen zu beziehen.
- Der Computer läuft etwas schneller, weil er nach Anforderungen nicht mehr auf zufällige Antworten warten muss.
- NetBIOS kann nun über TCP/IP mehrere Netzwerksegmente übergreifen.

Windows 2000 funktioniert zwar auch ohne WINS, Microsoft empfiehlt jedoch, WINS zu verwenden, solange nicht alle Computer unter Windows 2000 betrieben werden. Bei umfangreichen Systemen wird es wohl eine Weile dauern, bis auf WINS verzichtet werden kann.

Replikation und ständige Verbindungen

Der WINS-Dienst erweitert seine Leistung dadurch, dass mehrere WINS-Server die NetBIOS-Namensliste warten können. Es können nun mehrere WINS-Server in einem Netzwerk (LAN oder WAN) miteinander kommunizieren und eine Art »NetBIOS-Antwortnetz« bilden.

Wenn ein WINS-Server als Replikationspartner eines anderen eingerichtet wird, zeichnen diese die Änderungen der Systeme auf, die bei ihnen registriert sind, und geben diese Informationen dann frei. Durch die Replikation der NetBIOS-Informationen, die jeder WINS-Server einbringt, lässt sich die Arbeitslast der beiden Server minimieren. Viele WINS-Server sind zwar miteinander verbunden, sie müssen jedoch auch von der Existenz der anderen WINS-Server wissen.

Unter Windows NT musste jedes Mal, wenn diese Verbindung benötigt wurde, eine neue Verbindung zwischen den Servern hergestellt und der Vorgang von neuem gestartet werden. Windows 2000 bietet nun so genannte ständige Verbindungen. Wird eine ständige Verbindung zwischen Replikationspartnern eingerichtet, können die Server die Informationen pünktlicher und genauer zur Verfügung stellen. Ständige Verbindungen werden auf der Basis von Verbindungen konfiguriert.

Veraltete Einträge manuell markieren

Wenn ein Eintrag für einen bestimmten NetBIOS-Host in einer WINS-Umgebung gelöscht werden soll, kann dies ziemlich schwierig oder zumindest zeitaufwändig sein. WINS bietet nun die Möglichkeit, veraltete Einträge manuell zu markieren. Der Status »veraltet« wird dann auf andere Server repliziert. Damit wird verhindert, dass gelöschte Einträge, die auf andere Server repliziert wurden, über die Replikation wieder auf den ursprünglichen WINS-Server übertragen werden.

Partner werden automatisch entdeckt

In früheren Versionen mussten die Replikationspartner in WINS manuell angegeben werden. In

Windows 2000 kann WINS die Replikationspartner nun automatisch erkennen und eine Auflistung aller WINS-Server erstellen. Alle neuen WINS-Server, die im Netzwerk gefunden werden, werden automatisch zur Partnerliste als Push/Pull-Partner hinzugefügt, was bedeutet, dass sie ohne Intervention des Administrators alle Informationen gemeinsam nutzen können.

Diese Funktion lässt sich ein- und ausschalten und sollte nicht benutzt werden, wenn mehr als drei WINS-Server in einem Segment enthalten sind.

Installation

Der WINS-Dienst kann während der Installation von Windows 2000 Server oder auch nachträglich installiert werden. Gehen Sie wie folgt vor, um den Dienst nachträglich zu installieren:

1. Klicken Sie in der Systemsteuerung doppelt auf **Software**.
2. Klicken Sie im Ordner **Software** auf **Windows-Komponenten hinzufügen/Entfernen**.
3. Aktivieren Sie die Option **Netzwerkdienste** und klicken Sie auf die Schaltfläche **Details**.
4. Aktivieren Sie im Dialogfeld **Netzwerkdienste** das Kontrollkästchen WINS (Windows Internet Naming Service) und klicken Sie auf OK und dann auf **Weiter**.
5. Geben Sie den Pfad zu den Windows 2000-Installationsdateien ein (z.B. *D:\i386*) und klicken Sie auf OK, um die Installation durchzuführen.

LMHOSTS-Dateien

Wenn Clients in der DNS-Umgebung einen Host im IP-Netzwerk nicht finden können, wird ihnen manchmal eine Datei namens HOSTS zur Verfügung gestellt. Diese enthält Datensätze für alle NetBIOS-Namen und die entsprechenden IP. Wenn ein Computer per Broadcast oder über den zuständigen DNS-Server nicht gefunden werden kann, benutzt der Client die Liste in der Datei HOSTS. Die NetBIOS-basierte Suche kann auf dieselbe Weise durchgeführt werden. Dazu wird eine Datei namens LMHOSTS benutzt.

Die Datei LMHOSTS enthält die NetBIOS-Namen und die zugeordneten IP-Adressen der Systeme, auf die der Client zugreifen möchte. Wenn keine Verbindung zu einem WINS-Server hergestellt werden kann oder wenn der WINS-Server nicht antwortet, kann der Client seine Anfrage selbst lösen.

Ein Beispiel für eine LMHOSTS-Datei ist im Verzeichnis *Winnt\System32\Drivers\Etc* enthalten. Unter Windows 95/98 befindet sich diese Datei im Windows-Verzeichnis.

Hier ein Auszug aus der Beispieldatei:

```
# 102.54.94.97    maestro
#PRE
#DOM:technik
#DC von "Technik"

# 102.54.94.102  "spiele  \0x14"
#besonderer Server
```

```
# 102.54.94.123    nordpol
#PRE
#Server in 3/4317
```

Die Angabe **#PRE** teilt dem Betriebssystem mit, dass der Computernamen bereits zu Anfang in den Namen-Cache geladen werden soll. Die Angabe **#DOM:<Domäne>** teilt dem System mit, dass der Computer Mitglied einer Domäne ist. Alle weiteren Angaben sind Kommentare.

8.2.7 DDNS (Dynamic Domain Name Service)

DNS (Domain Name Service) wird von TCP/IP-Systemen für die dynamische Namensauswertung von Computernamen in IP-Adressen verwendet. DNS übersetzt also einen für Menschen leicht verständlichen Namen wie www.Domäne.com in eine Adresse, die von Computern leichter interpretiert werden kann, wie z.B. 10.33.54.91. Computer können besser mit Zahlen umgehen, Menschen dagegen mit Namen.

So, wie WINS NetBIOS-Namen in IP-Adressen übersetzt, wertet DNS Domännennamen in IP-Adressen aus. Nachdem ein DNS-Server installiert wurde, können Clients diesen automatisch nutzen.

Anders als WINS ist DNS im klassischen Sinn nur ein System, das Eingaben für die Namensliste von anderen DNS-Servern erhält. Wird ein neuer Client neu eingerichtet, sind die IP-Adresse und der Domänenname dem DNS-Server noch nicht bekannt. Dadurch lässt sich das System nur schwer einsetzen, um alle Systeme und Freigaben aufzuzeichnen. Das System ist statisch. Wenn Namen und die zugeordneten Adressen nicht manuell eingegeben werden, existieren sie in der DNS-Welt ganz einfach nicht.

DNS-Domänen

Die grundlegendste Einheit von DNS ist die DNS-Domäne, die sich wie folgt zusammensetzt:

- *Domäne der obersten Ebene:* .com (Kommerziell), .edu (Erziehung und Bildung) und .gov (Regierungsbehörde) oder Länderkürzel wie .de oder .fr. Diese Domänen werden von DNS-Servern repräsentiert, die für die Domänen in jeder Kategorie Einträge enthalten.
- *Domäne der zweiten Ebene:* microsoft. (bei microsoft.com), yahoo. (bei yahoo.de) oder whitehouse. (bei whitehouse.gov). Diese Domänen sind die Namen von US-Unternehmen, US-Schulen, US-Regierungsbehörden oder Unternehmen und Organisationen in anderen Ländern, die den Domännennamen besitzen.
- *Subdomänen:* Jede zusätzliche Ebene der Domäne ist eine Subdomäne (z.B. beispiel. bei beispiel.unternehmen.com).

Die Domännennamen werden von einer Gruppe namens InterNIC (www.internic.net) zugewiesen. Organisationen, Individuen oder Gruppen registrieren bei InterNIC eine Domäne. Die Registrierung ist kostenpflichtig. Wurde eine Domäne einmal registriert, bestehen jedoch Exklusivrechte auf den Namen. Der Domänenname ist nun ein vollständig qualifizierter Domänenname (FQDN = Fully Qualified Domain Name).

DNS-Ressourcen

Es gibt verschiedene Arten von DNS-Ressourcen. Über den Typ kann der DNS-Server festlegen, welche Art von Dienst angeboten und/oder angefordert wird. Nachfolgend sehen Sie Beispiele für DNS-Ressourcen:

- *Hostressourceneinträge (A)*. Ein A-Ressourceneintrag ist die einfachste Form eines DNS-Eintrags, weil es sich dabei um den Eintrag für einen einzelnen Host handelt - ein Eintrag also, der einfach mitteilt, dass ein bestimmter Domänenname einer IP-Adresse zugeordnet ist.
- *PTR-Ressourceneintrag (Pointer) zu Reversezone*. Diese Art von Eintrag bildet das Gegenstück zum A-Eintrag. Mit diesem Eintrag kann der Domänenname eines Hosts anhand der IP-Adresse ermittelt werden.
- *MX-Ressourceneintrag (Mail Exchanger)*. Ein Administrator kann für jede Domäne einen Mail Exchanger-Eintrag festlegen. Dies ist die IP-Adresse, auf die der DNS-Server reagiert, wenn eine E-Mail-Anfrage an die Domäne gesendet wird. E-Mail-Server fragen den MX-Eintrag einer Domäne ab, bevor sie E-Mails weiterleiten.
- *Alias-Ressourceneintrag (CNAME)*. Ein Domänenname, der auf einen anderen Domänennamen verweist. Dieser Domänenname zeigt sehr wahrscheinlich auf eine IP-Adresse. Ein Administrator möchte vielleicht, dass zwei Domänennamen auf denselben Webserver verweisen. Er könnte dann einen A-Eintrag für den Domänennamen (wie z.B. Kinderkleidung.com) einrichten, der der IP-Adresse des Servers zugeordnet ist (123.43.64.100). Er könnte dann einen zusätzlichen C-Name-Eintrag unter dem Namen Babykleidung.com einrichten, der auf den A-Eintrag Kinderkleidung.com zeigt.

Dynamisches DNS

In Windows 2000 ist DNS nun dynamisch. Dynamisches DNS sollte jedoch nur in einer reinen Windows 2000-Umgebung eingesetzt werden, weil der Dienst auf Funktionen von DHCP 2000 und Active Directory aufbaut.

Die dynamische Registrierung von DNS-Einträgen für Windows 2000-Clients erfolgt über DHCP. Standardmäßig wird der DHCP-Server so eingerichtet, dass er die DNS-Clientinformationen automatisch aktualisiert. Wenn ein Clientcomputer eine IP-Adresse vom DHCP-Server zugewiesen bekommt, hängt sein Verhalten von der Windows-Version ab, unter der er läuft.

Verhalten bei Windows 2000-Clients:

- Die IP-Adressanforderung wird gesendet.
- Der DHCP-Server bietet eine IP-Adresse an und genehmigt den Lease.
- Der DHCP-Client registriert seinen A-Eintrag beim DNS-Server.
- Der DHCP-Server registriert den PTR-Ressourceneintrag zur Reversezone des Clients beim DNS-Server.

Um den Vorteil einer reinen Windows 2000-Umgebung zu erkennen, sollten Sie nun dieselbe Ereigniskette bei einem Windows NT- oder -95/98-Client betrachten:

- Die IP-Adressanforderung wird gesendet.

- Der DHCP-Server bietet eine Adresse an und genehmigt den Lease.
- Der DHCP-Server registriert den A-Eintrag des Clients beim DNS-Server.
- Der DHCP-Server registriert den PTR-Ressourceneintrag zur Reversezone beim DNS-Server.

Der Windows 2000-Client kann sich also selbst beim DNS-Server registrieren, während ansonsten der DHCP-Server eingreifen muss.

Installation von DNS-Server

DNS-Server können Sie selbstverständlich zusammen mit Windows 2000 installieren. Die Installation kann aber auch nachträglich erfolgen.

DNS-Server müssen Sie wie DHCP oder WINS auf einem Server mit einer statischen IP-Adresse installieren. Gehen Sie wie folgt vor, um DNS-Server zu installieren.

1. Klicken Sie in der Systemsteuerung doppelt auf **Software**.
2. Klicken Sie im Ordner **Software** auf **Windows-Komponenten hinzufügen/Entfernen**.
3. Aktivieren Sie die Option **Netzwerkdienste** und klicken Sie auf die Schaltfläche **Details**.
4. Aktivieren Sie im Dialogfeld **Netzwerkdienste** das Kontrollkästchen **DNS-Server (Domain Name System)** und klicken Sie auf OK und dann auf **Weiter**.
5. Geben Sie den Pfad zu den Windows 2000-Installationsdateien ein (z.B. *D:\i386*) und klicken Sie auf OK, um die Installation durchzuführen.

Startdatei

Die Datei, auf die DNS beim Start zugreift, heißt Startdatei. Sie enthält Informationen über die Pfade zu den DNS-Konfigurationsdateien und deklariert, für welche Domänen der Server zuständig ist.

Um Startdateien interpretieren zu können, müssen Sie das Dateiformat BIND kennen. Glücklicherweise übernimmt der Server die Verwaltung der Dateien für Sie. Sie sollten die Datei jedoch sichern, damit sie verfügbar ist, wenn der DNS-Server neu eingerichtet werden muss.

Die Zonendatei

Jede Domäne, für die der DNS-Server zuständig ist, muss in der Zonendatei eingetragen sein.

Cachedatei

Diese Datei enthält Hostinformationen, die eine grundlegende DNS-Verbindung aufrecht erhalten. Sie speichert die Adressen von Stammmamensservern (wie *.com* und *.edu*).

DNS konfigurieren

DNS das erste Mal zu konfigurieren, kann entweder einfach oder sehr schwierig sein. Dies liegt daran, dass Ihnen beim ersten Öffnen der DNS-Konsole einige Fragen gestellt werden. Wenn Sie die Antworten kennen, ist das kein Problem. Ansonsten ist die Installation etwas schwierig. Bereiten Sie sich also auf die Installation vor und gehen Sie dann wie folgt vor:

1. Der **Assistent für die DNS-Serverkonfiguration** öffnet sich.

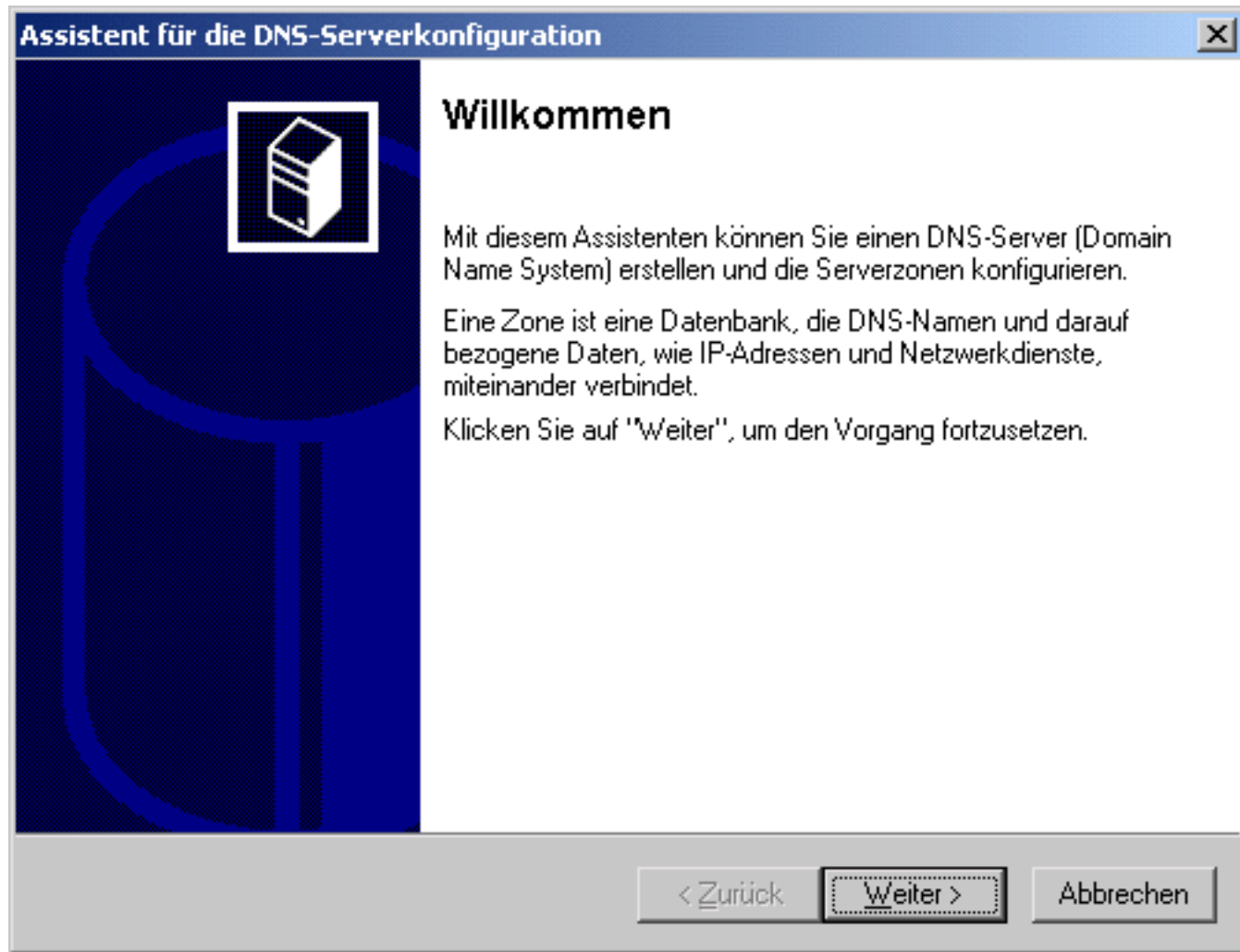


Abbildung 8.13: Der Assistent für die DNS-Serverkonfiguration.

2. Sie werden gefragt, ob der Server, den Sie installieren, der erste Server in der Domäne ist. Treffen Sie die entsprechende Auswahl und klicken Sie auf **Weiter**.
3. Behalten Sie im nächsten Schritt die Auswahl der Option **Ja, eine Forward-Lookupzone erstellen** bei und klicken Sie auf **Weiter**.
4. Wählen Sie als Zonentyp entweder **Primär** oder **Sekundär** und klicken Sie auf **Weiter**.
5. Geben Sie den Zonennamen ein und klicken Sie auf **Weiter**.
6. Erstellen Sie eine neue Zonendatei oder importieren Sie eine vorhandene Datei und klicken Sie auf **Weiter**.
7. Wählen Sie die Option **Ja, eine Reverse-Lookupzone erstellen**, und klicken Sie auf **Weiter**.
8. Wählen Sie als Zonentyp entweder die Option **Primär** oder die Option **Sekundär** und klicken Sie auf **Weiter**.
9. Geben Sie die Netzwerkkennung und den Namen für die Reverse-Lookupzone ein. Die Angaben sind gleich wie beim sekundären Domänennamen des FQDN. Klicken Sie anschließend auf **Weiter**.
10. Übernehmen Sie den Dateinamen und klicken Sie auf **Weiter**.
11. Klicken Sie auf **Fertig stellen**.

Sie sollten nun die Ergebnisse der Installation aufschreiben und zu den Akten legen. Diese Einstellungen können bei Problemen eine große Hilfe sein.

DNS-Server verwalten

Nach der Installation des Hauptservers beinhaltet die Verwaltung von DNS-Server drei Aufgaben (siehe Abbildung 8.14):

- Zonen hinzufügen und entfernen
- untergeordnete Domänen hinzufügen und entfernen
- neue Einträge hinzufügen und entfernen

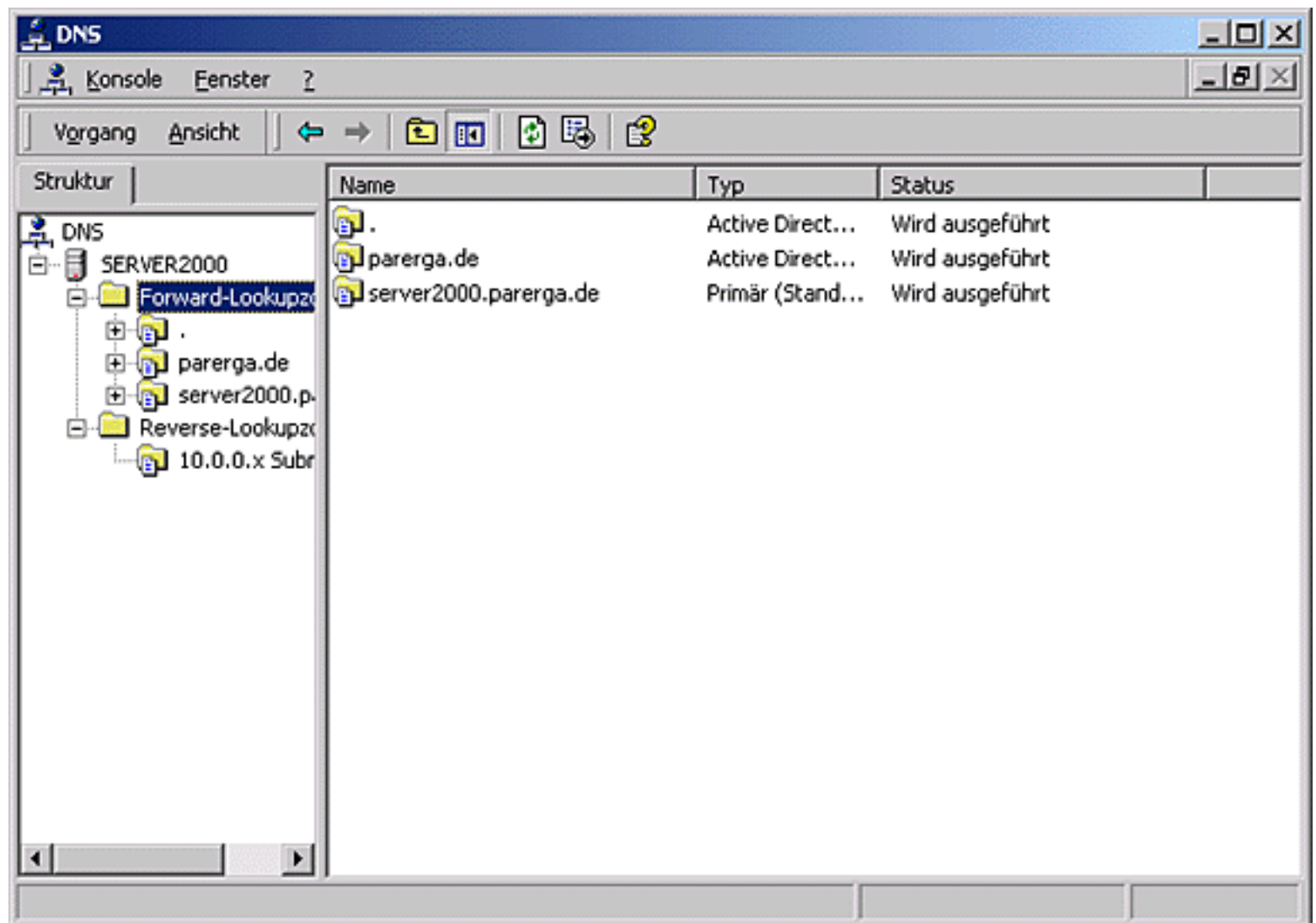


Abbildung 8.14: Die DNS-Konsole

Zonen bezeichnet im Zusammenhang mit DNS-Server die Domänen, die erstellt werden, sowie alle diesen untergeordneten Domänen. Diese Gruppierung wird als Zone bezeichnet, weil es sich um eine Verwaltungsgruppe, jedoch um mehrere Domänen handelt.

Wenn DNS installiert und erstmals geöffnet wird, wird die erste Zone und eine Reverse Lookup-Zone für sie eingerichtet. Um weitere Zonen hinzuzufügen, klicken Sie in der DNS-Konsole mit der rechten Maustaste auf das Serverobjekt und wählen im Kontextmenü den Befehl **Neue Zone**. Es öffnet sich der

Assistent zum Erstellen neuer Zonen, der auch beim ersten Start der DNS-Konsole sichtbar war.

Eine neue Domäne zu erstellen ist ähnlich einfach. Erweitern Sie die Zone, in der Sie eine neue Domäne einrichten möchten, und klicken Sie mit der rechten Maustaste auf die Zone. Wählen Sie im Kontextmenü den Befehl **Neue Domäne** und geben Sie im gleichnamigen Dialogfeld den Namen der neuen Domäne ein. Damit ist auch schon alles erledigt.

Neue Einträge werden ebenfalls über die DNS-Konsole erstellt. Gehen Sie dazu wie folgt vor.

1. Erweitern Sie das Serverobjekt und die Zone, in der Sie den Eintrag erstellen möchten, indem Sie auf die vorangestellten Pluszeichen klicken.
2. Klicken Sie mit der rechten Maustaste auf das Domänenobjekt. Im Kontextmenü stehen Ihnen nun einige Eintragsarten zur Verfügung, wie z.B. **Neuer Host**, **Neuer Alias**, **Neuer Mail-Exchanger** und **Andere neue Einträge**. Wählen Sie den gewünschten Typ, wie z.B. **Neuer Host**.
3. Es öffnet sich das Dialogfeld **Neuer Eintrag erstellen**. Füllen Sie dieses Dialogfeld aus.
4. Aktivieren Sie im Dialogfeld **Neuer Host** das Kontrollkästchen **Verknüpften PTR-Eintrag erstellen**. Dadurch wird automatisch ein Reverse-Lookup-Eintrag erstellt. Klicken Sie anschließend auf **Host hinzufügen**.

Bei einem MX-Eintrag müssen Sie wissen, an welchen Server E-Mail-Nachrichten gesendet werden sollen (siehe Abbildung 8.15).

Neuen Eintrag erstellen ? X

Mail-Exchanger (MX)

Übergeordnete Domäne:
parerga.de

Nachrichten, die an den nachfolgenden Host oder die nachfolgende Domäne adressiert sind, an den untenstehenden Mailserver senden (bei Nichtangabe wird übergeordnete Domäne verwendet).

Host oder Domäne:

Mailserver:
Durchsuchen...

Mailserverpriorität:
10

OK Abbrechen

Abbildung 8.15: Einen Mail-Exchanger-Eintrag erstellen

8.2.8 Von WINS zu DNS migrieren

Dynamic DNS kann WINS ersetzen und bietet die Vorteile, dass sich der Datenverkehr reduziert und das System mit einem Industrie- und Internetstandard eingerichtet wird. Den WINS-Dienst sollten Sie jedoch nur aus Netzwerken und Domänen entfernen, die keine Windows NT-, -95/98-, 3.x- oder DOS-Clients enthalten. Diese Systeme laufen besser mit WINS.

Bevor Sie WINS entfernen, sollten Sie sicherstellen, dass Ihre DNS-Umgebung vollständig implementiert ist und funktioniert. Wenn Sie ein funktionierendes WINS-System zugunsten der Bandbreite entfernen, könnte es Ihnen passieren, dass sich viele Benutzer beschweren.

Gehen Sie wie folgt vor, um von WINS zu DNS zu migrieren:

1. Entfernen Sie den WINS-Client von allen Workstations, indem Sie die Einträge für einen primären und einen sekundären WINS-Server aus den TCP/IP-Eigenschaften entfernen.



Denken Sie daran, dass einige Benutzer ihre IP-Informationen vom DHCP-Server beziehen.

2. Vergewissern Sie sich, dass alle Clients des WINS-Servers entfernt wurden und nun für DNS konfiguriert sind.
3. Beginnen Sie damit, die WINS-Server zu entfernen. Achten Sie darauf, dass zuerst alle Einträge entfernt werden müssen, die der WINS-Server besitzt, bevor er selbst entfernt werden kann. Vergewissern Sie sich dann, dass Sie eine Replikation von WINS haben, bevor Sie diese entfernen. Dadurch wird die Replikation der Einträge gestoppt.

8.2.9 Einer Netzwerkkarte mehrere Adressen zuweisen

Das mag zwar zunächst komisch klingen, aber Sie können Windows 2000 Server mit mehreren IP-Adressen verbinden. Dafür sprechen einige Gründe.

Ein Einsatzgebiet für diese Art von Konfiguration besteht darin, zwei Versionen desselben Dienstes bereitzustellen. Der Server kann dann Anforderungen der Clients auf der Basis der Adressen behandeln, an die die Anforderungen gesendet wurden. Ein Webserver könnte z.B. einen DNS-Eintrag für die Adresse einer öffentlichen und einen für eine interne Site haben. Die Tatsache, dass jede Site eine andere IP-Adresse registriert hat, bedeutet nicht, dass sich die beiden Sites auf unterschiedlichen Servern befinden müssen.

Mehrere Adressen lassen sich einfach konfigurieren:

1. Wählen Sie **Start/Einstellungen/Netzwerk- und DFÜ-Verbindungen**.
2. Klicken Sie doppelt auf die Verbindung, der Sie eine IP-Adresse hinzufügen möchten (siehe Abbildung 8.3), und klicken Sie auf die Schaltfläche **Eigenschaften**.
3. Klicken Sie im Dialogfeld **Eigenschaften von LAN-Verbindung** auf den Eintrag **Internetprotokoll (TCP/IP)** und klicken Sie dann auf die Schaltfläche **Eigenschaften**.
4. Klicken Sie im Dialogfeld **Eigenschaften von Internetprotokoll (TCP/IP)** auf die Schaltfläche **Erweitert**.
5. Klicken Sie im Dialogfeld **Erweiterte TCP/IP-Einstellungen** unter **IP-Adressen** auf die Schaltfläche **Hinzufügen** und geben Sie die neue IP-Adresse ein.

8.2.10 IPSec

Bestandteil der Grundinstallation von TCP/IP sind die sicheren IP-Verbindungen. Dies wurde durch das zunehmende Wachstum des Internets und das umfangreiche Wissen der Benutzerbasis nötig. Noch vor zehn Jahren hätte ein Administrator keine Gedanken daran verschwendet, dass ein Benutzer die Netzkleitungen abhören und die Kennwörter anderer Benutzer ausspionieren könnte. Heutzutage kann jeder Benutzer Netzwerküberwachungsprogramme aus dem Internet herunterladen, mit denen er das Netzwerk abhören kann. Die Benutzer haben aber nicht nur einen Zugriff auf das Internet, sondern auch umgekehrt. Deshalb wurde IPSec (IP Security) eingeführt. IPSec wird in Kapitel 22 ausführlicher behandelt.

Active Directory und Kontenverwaltung

Teil II

- 9. [Verzeichnis- und Zugriffskonzepte](#)
- 10. [Struktur des Active Directory](#)
- 11. [Erstellen und Verwalten von Benutzerkonten](#)
- 12. [IntelliMirror und Benutzersteuerung](#)

Kapitel 9 Verzeichnis- und Zugriffskonzepte

Active Directory bringt neue Gesichtspunkte in die Überlegungen bezüglich der Verwaltung von Benutzern, aber auch bezüglich der Steuerung von Ressourcen. Das Verzeichnissystem ermöglicht dem Administrator eine gründlichere Steuerung der Benutzerumgebung und der Präsentation der Ressourcen.

Microsofts Verwendung des Active Directory ist im Wesentlichen ein Schritt hin zu einem auf Normen basierenden Tool, das es schon seit Jahren gibt. Bei dieser Norm handelt es sich um die X.500-Verzeichnisstruktur. X.500 ist eine ISO-Norm (ISO = International Standard Organization), die definiert, wie globale Verzeichnisse aufgebaut sein sollten. Die hierarchische Struktur des Active Directory hat viele Dinge mit NetWare (ab Version 4.x) und vielen anderen Verzeichnissen gemein, da diese alle einer Norm entsprechen wollen. Diese Norm sorgt für Interoperabilität und leichte Erlernbarkeit. Wenn Sie ein NetWare-Administrator sind, werden Sie in diesem Kapitel und im gesamten Buch einige alte Bekannte wieder treffen.

In diesem Kapitel wird einiges aus Kapitel 5 wiederholt. Im Gegensatz zu Kapitel 5 soll hier jedoch die eigentliche Erstellung dieser einzelnen Komponenten ausführlich beschrieben werden. In den bisherigen Kapiteln ging es um Konzepte; hier geht es darum, wie und warum etwas getan wird.

9.1 Sicherheitskonzept

Wenn Benutzer versuchen, auf eine Ressource zuzugreifen, müssen sie zuerst von der Domäne, die für die jeweilige Ressource verantwortlich ist, authentifiziert werden. Die Authentifizierung kann einfach nur darin bestehen, dass geprüft wird, ob der Benutzer wirklich der ist, der er zu sein vorgibt. Die Authentifizierung kann jedoch auch sehr komplex sein, d.h., diese Referenzen werden über mehrere Server oder Domänen geleitet. In jedem Fall muss für diese Authentifizierung ein Protokoll eingerichtet werden.

Die Authentifizierung in Windows 2000 hat sich insofern geändert, als dieses Betriebssystem sowohl mit dem alten Protokoll, dem NTLM-Protokoll (Windows NT LAN Manager), als auch mit dem Sicherheitsprotokoll Kerberos ausgestattet ist. Beide Protokolle werden beim Starten von Windows 2000 geladen, um die große Anzahl an Windows NT- und 95/98-Clients zu berücksichtigen, die in einer Umgebung existieren können. In einer reinen Windows 2000-Umgebung ist Kerberos das einzige erforderliche Sicherheitsprotokoll. In diesem Kapitel werden die beiden Protokolle sowie die Beziehung zwischen diesen beiden Protokollen näher betrachtet.

9.1.1 Kerberos

Microsoft hat eine größere Änderung im Sicherheitsprotokoll, d.h. dem in Windows 2000 verwendeten Standardprotokoll, vorgenommen. Man hat sich für das Protokoll Kerberos entschieden. Ebenso wenig wie TCP/IP ist auch Kerberos eine neue Idee oder eine Innovation von Microsoft. Es gibt Windows jedoch eine sehr sichere Operationsgrundlage in einem Standard, der in der Host-Welt schon seit über zehn Jahren verwendet wird.

Kerberos ist eigentlich der Name des aus der griechischen Mythologie stammenden dreiköpfigen Hundes Zerberus, der die Tore zum Hades, also der Unterwelt, bewacht. Dieser Name wurde für das Protokoll aufgrund des dreistufigen, für die Verwaltung von sicheren Verbindungen zwischen Systemen erforderlichen Ansatzes gewählt. Das Protokoll wurde in den 80er-Jahren beim MIT entwickelt. Die Widerhaken und Pfeile, die über die Windows NT-Sicherheit auf Microsoft abgeschossen wurden, erforderten einen dreiköpfigen Wachhund, und das war Kerberos.

Bevor wir damit beginnen, das Protokoll Kerberos vorzustellen und seinen Platz in Windows 2000 zu beschreiben, möchte ich darauf hinweisen, dass Microsoft das Protokoll nur in reinen Windows 2000-Anwendungen standardmäßig verwendet. Das bedeutet nicht, dass dieses Protokoll sonst nicht verwendet wird. Das heißt nur, dass Windows 2000 Kerberos standardmäßig nur bei der Kommunikation mit anderen Windows 2000-Systemen verwendet. Windows NT-, Windows 95/98-, Windows für Workgroups- und andere Windows-Clients können nicht mit Kerberos auf Windows 2000 zugreifen. Sie verwenden für die Kommunikation das alte NTLM-Protokoll (Windows NT LAN Manager).



Da es sich bei Kerberos um ein öffentliches Standardsicherheitsprotokoll handelt, kann Windows 2000 Teil eines Kerberos-Sicherheitssystems werden, ohne von Windows 2000 gesteuert zu werden. Das System kann sowohl ein Host als auch ein Client für Nicht-Windows-2000- Systeme sein.

Man könnte sich vorstellen, dass Überlegungen getroffen werden, für ältere Betriebssysteme einen Kerberos-Client zu erstellen.

Der Kommunikationsprozess

Wenn zwei Systeme im Geheimen miteinander kommunizieren möchten, müssen diese dafür eine Vorgehensweise finden, bevor sie mit der Kommunikation beginnen können. Wenn beispielsweise Thomas eine verschlüsselte Nachricht an Renate senden möchte, müssen sich die beiden auf einen Verschlüsselungsschlüssel einigen, bevor die Nachricht gesendet wird.

Sie können einen einfachen Verschlüsselungsschlüssel verwenden, bei dem jeweils ein Buchstabe durch eine Zahl ersetzt wird wie z.B. 1 = a, 2 = b, 3 = c usw. Wenn Renate dann die Nachricht (20-8-15-13-1-19 12-9-5-2-20 18-5-14-1-20-5) empfängt, übersetzt sie diese mit dem vereinbarten Verschlüsselungsschlüssel. Diese Nachricht kann jedoch einfach entschlüsselt werden.

Die beiden müssen sich jedoch bewusst sein, dass ihre Nachricht abgefangen und ausgeklügelte Formen des Codeknackens angewendet werden können. Das Internet und andere öffentliche Netzwerke haben es erforderlich gemacht, dass ein Großteil unserer Verbindungen öffentlich gemacht werden. Daher muss die Verschlüsselung auf einer sehr komplexen Ebene erfolgen.

Der erste Schritt in diesem Prozess ist es, einfach eine Möglichkeit für den Empfänger zu finden, damit dieser weiß, dass die Nachricht vom Absender kommt. Dabei spricht man von einem *gemeinsamen Geheimnis*.

Authentifizierung kann realisiert werden, indem man sich vor der Kommunikation auf ein Kennwort einigt. Dann muss der Benutzer einfach vor der Kommunikation das Kennwort eingeben. Das Problem bei diesem Verfahren in der Vergangenheit war, dass das Signal abgefangen und rückübertragen werden konnte. Dieser Vorgang wird als Spoofing (engl. für »schwindeln«) bezeichnet, weil der »Schwindler«

das abgefangene Netzwerksignal verwendet, um vorzugeben, er sei nun der echte Benutzer. Er zeichnet einfach die ursprüngliche Nachricht auf und leitet sie weiter, wenn er vorgeben möchte, der echte Absender zu sein. Das ist in etwa so ähnlich, als würde man jemanden auf Band aufnehmen, der das Geheimwort an der Eingangstür zum Clubhaus sagt, und das Aufgenommene abspielen, wenn man selbst Zutritt zum Clubhaus haben möchte.

Dies lässt sich umgehen, wenn man diese beiden Lösungen (Verschlüsselung und Kennwörter) miteinander kombiniert. Die Idee dabei ist, dass das Kennwort verschlüsselt werden soll. Wenn der Server die Verschlüsselung versteht, kann das Kennwort wie jede andere Nachricht auch verschlüsselt werden. Aber auch verschlüsselte Nachrichten können abgefangen und rückübertragen werden, als wären es die ursprünglichen Nachrichten. Der Empfänger sieht sich in diesem Fall nur das Ergebnis an. Derjenige, der die Nachricht abfängt, spiegelt einfach Bit für Bit die verschlüsselte Nachricht, die das Kennwort enthält. Wie im obigen Beispiel werden Sie Zutritt bekommen, wenn Sie das aufgenommene Kennwort exakt so wiedergeben, wie es ursprünglich gesagt wurde.

Können Sie eine Computernachricht abfangen?

Nachrichten, die zwischen Computern ausgetauscht werden, sind nicht ganz, aber fast so einfach abzufangen wie Gespräche unter Menschen. Leute, die diese Nachrichten abfangen möchten, können sich Programme zu Nutze machen, die unter der Bezeichnung *Packet Sniffer* bzw. *Analyzer* bekannt sind. »Sniffer« ist ein umgangssprachlicher Ausdruck für eine sehr robuste Version des Hauptprodukts.

Mit Hilfe von Analyzern können Nachrichten im Netzwerk in Form von reinen Paketen (daher »Packet« Sniffer) abgefangen werden. Denken Sie daran, dass sämtliche Computer im Netzwerk sämtliche Pakete erhalten, die über das Netzwerk gesendet werden. Auch wenn die Computer nicht mit dem Netzwerk interagieren, sie empfangen dennoch sämtliche Nachrichten. In Reinform kann ein Paket, wenn es nicht verschlüsselt ist, so einfach gelesen werden wie eine Geburtstagskarte. Der Großteil des Inhalts eines Pakets besteht aus Klartext. Sogar Windows 2000 ist mit einem einfachen Netzwerk-Analyzer, dem Netzwerkmonitor ausgestattet. Sie finden ihn unter der Rubrik **Verwaltung**.

Der nächste Schritt in diesem Prozess besteht darin, sicherzustellen, dass die Übertragungen unmittelbar nacheinander vom ursprünglichen Absender erfolgen und dass die Antwort vom ursprünglichen Ziel gesendet wird. Hier wird nun deutlich, wie nützlich Kerberos ist.

Bei Kerberos geschieht dies mittels einer *Echtheitsbestätigung*. Der Teil der Nachricht, der die Echtheitsbestätigung umfasst, ist das Stück Information, das an die Nachricht angefügt wird und das sich in der Folge der Nachrichten ändert. Die beiden miteinander kommunizierenden Systeme müssen sich auf eine gemeinsame Echtheitsbestätigung einigen. Dabei muss es sich um eine Variable handeln, die beiden Seiten bekannt ist, sich aber im Laufe der Zeit ändert. Das kann einigermaßen verwirrend sein. Die Zeit selbst ist ein Beispiel dafür. Die Zeit ist niemals dieselbe. Sie ändert sich von einem Augenblick zum nächsten. Aber wir können uns auf den Verlauf der Zeit einigen und darauf, welche Zeit es zu einem bestimmten Moment gerade ist.

Wenn ich Ihnen eine Nachricht sende und die Uhrzeit anfüge, weiß nur ich, zu welcher Uhrzeit ich die Nachricht gesendet habe. Kerberos verwendet in der Regel die Uhrzeit, zu der die Nachricht gesendet wird, für die Echtheitsbestätigung. Damit können dieselben Pakete nicht noch einmal gesendet werden, denn wenn die Übertragung entschlüsselt wird, gibt diese zu erkennen, dass sie bereits empfangen worden ist. Die Uhrzeit sowie weitere statische client-spezifische Angaben (Benutzername,

Computernamen usw.) werden am häufigsten für die Echtheitsbestätigung verwendet.

Um die Übertragung fortzusetzen, sendet der Server einen Teil der Echtheitsbestätigung mit der Rückmeldung zurück. Damit wird bestätigt, dass die Nachricht vom gleichen Server stammt, an die der Client eine Nachricht gesendet hat.

Die Übertragungen könnten nun folgendermaßen aussehen:

- Der Client sendet sein Kennwort mit einer Echtheitsbestätigung (Uhrzeit und Client-Benutzername) an den Server. Alles in der Nachricht ist mit einem Verfahren verschlüsselt worden, das nur der Client und der Server kennen. Die Verschlüsselung ist das »gemeinsame Geheimnis«, von dem zu Anfang dieses Abschnitts die Rede war.
- Der Server empfängt die Nachricht und entschlüsselt sie. Er stellt fest, dass das Kennwort des Client mit dem vereinbarten Kennwort übereinstimmt und erstellt eine Rückmeldung, um zu bestätigen, dass die Übertragung beginnen kann. In dieser Meldung ist die Uhrzeit enthalten, zu der der Client die Nachricht gesendet hat, um zu bestätigen, dass es sich um eine gültige Antwort handelt (siehe Abbildung 9.1).

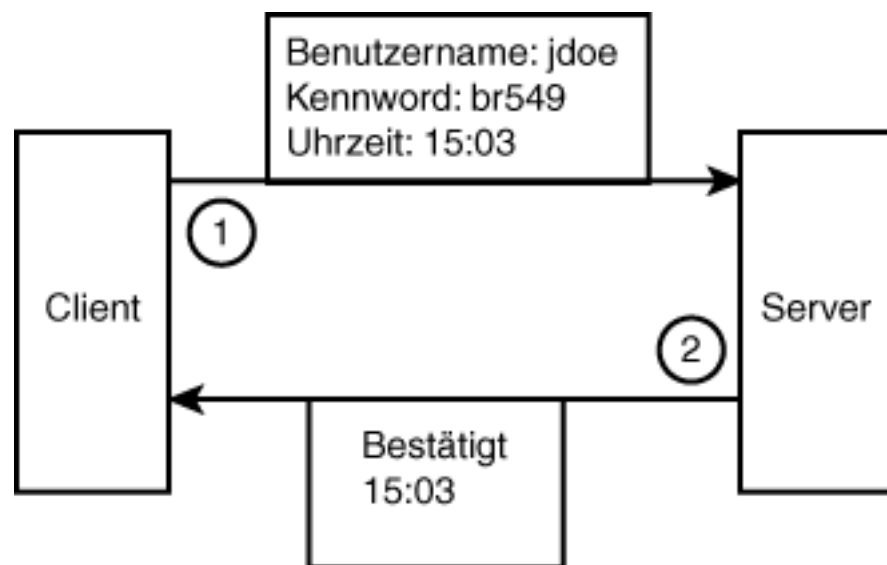


Abbildung 9.1: Authentifizierung und Bestätigung

Durch die Rücksendung der Uhrzeit sendet der Server eine Information, die nur das System mit dem richtigen Verschlüsselungsschlüssel (der Client) kennen kann. Dadurch, dass die Uhrzeit in den gesendeten Nachrichten ständig geändert wird, wird verhindert, dass die Nachricht abgefangen und später zum Eindringen in das System verwendet wird. Mit Hilfe der Echtheitsbestätigung ist es darüber hinaus für den Server möglich, sicherzustellen, dass es sich bei dem Client um den richtigen Antwortenden handelt.

Der Schlüssel

Zwei Köpfe hat unser Hund (Kerberos) schon. Der dritte Kopf ist derjenige, der ihn einzigartig macht. Bei vielen Übertragungsformen werden einfache Verschlüsselungsschlüssel verwendet. Der Trick liegt jedoch darin begründet, woher der Schlüssel kommt.

Es wäre einfach genug, jedem System manuell einen Schlüssel zur Verfügung zu stellen. Das wäre

jedoch unglaublich zeitaufwändig. Sie könnten einfach eine zentrale Stelle einrichten und allen Rechnern mitteilen, dass sie ihre Schlüssel von dort bekommen. Das würde jedoch bedeuten, dass der Schlüssel nicht chiffriert wäre. Kerberos in Windows 2000 richtet eine zentrale Stelle für die Vergabe von Verschlüsselungsschlüsseln ein. Diese wird als *KDC* (Key Distribution Center = Schlüsselverteilungscenter) bezeichnet.

Bei Windows 2000 wird das KDC auch als Domänencontroller bezeichnet. Domänencontroller (DCs) enthalten eine vollständige Informationsbasis der in der Domäne befindlichen Objekte. Jedem Objekt wird ein eindeutiger anfänglicher Verschlüsselungsschlüssel, ein so genannter *Langzeitschlüssel*, zugewiesen. Das bedeutet, dass der DC einzig für die Überwachung der Transaktionen eingesetzt wird. Aber wie gelangen die Schlüssel ohne Verletzung der Sicherheit zu den Clients und Servern?

Verteilen von Schlüsseln

Beim Verteilen von Schlüsseln geschieht im Prinzip Folgendes (siehe Abbildung 9.2 sowie die unten beschriebenen Schritte). Achten Sie darauf, dass es einen Unterschied zwischen einem *Sitzungsschlüssel* und einem *Sitzungsticket* gibt.

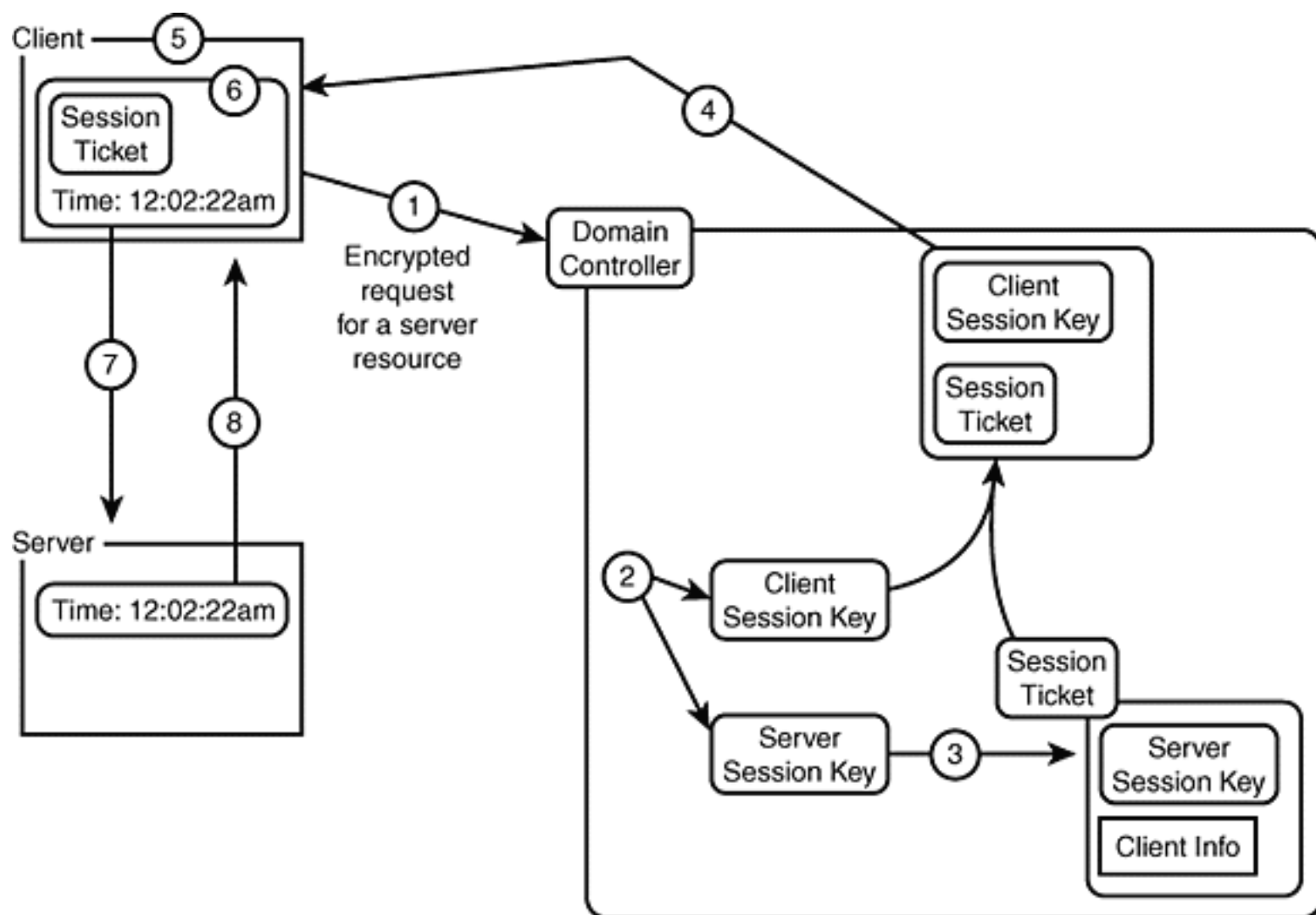


Abbildung 9.2: Erstellen und Verteilen von Schlüsseln

1. Der Client sendet eine Anforderung einer Server-Ressource an den Domänencontroller. Diese

Anforderung ist mit dem Langzeitschlüssel des Client verschlüsselt.

2. Das veranlasst den Domänencontroller dazu, zwei eindeutige Schlüssel, so genannte *Sitzungsschlüssel*, zu erstellen: einen für den Server und einen für den Client.

3. Der Sitzungsschlüssel des Servers wird zusammen mit Informationen über den Client gepackt und mit dem Langzeitschlüssel des Servers verschlüsselt. Dieses Paket wird als *Sitzungsticket* bezeichnet.

4. Die Kopie des Clients des Sitzungsschlüssels und das Sitzungsticket werden mit dem Langzeitschlüssel des Client verschlüsselt und dann an den Client gesendet.

5. Der Client entschlüsselt seinen Teil des Sitzungsschlüssels. Der Sitzungsschlüssel enthält das Sitzungsticket. Der Client kann dieses jedoch nicht lesen, da es mit dem Langzeitschlüssel des Servers verschlüsselt ist.

6. Der Client packt dann das Sitzungsticket zusammen mit einer Echtheitsbestätigung (Uhrzeit) und sendet dieses Paket an den Server, um die Kommunikation zu beginnen.

7. Der Server empfängt das Sitzungsticket und die Echtheitsbestätigung, die beide mit dem Langzeitschlüssel des Servers verschlüsselt sind. Der Server entschlüsselt dieses Paket.

8. Der Server antwortet mit der Echtheitsbestätigung des Client.

Aufgrund dieser Art der Schlüsselverteilung können sowohl der Server als auch der Domänencontroller ihre Informationen senden und müssen nicht die Schlüssel von Benutzern verfolgen, die die Kommunikation mit ihnen irgendwann begonnen haben. Da der Schlüssel vom Client verwaltet wird und der Client den Schlüssel für eine bestimmte Sitzung verwaltet, antwortet der Server einfach auf das Ticket. Tickets können während ihrer gesamten Gültigkeitsdauer (in der Regel acht Stunden) wiederverwendet werden, sodass der Domänencontroller nicht ständig durch Herausgabe neuer Sitzungstickets an diesem Vorgang beteiligt sein muss.

Sogar das Sitzungsticket erhält man über ein spezielles Sitzungsticket, das erstellt wird, wenn der Client zum ersten Mal auf den DC zugreift. Da der DC immer noch ein Server ist, muss es eine Möglichkeit geben, wie der Client innerhalb des Kerberos-Schemas mit dem DC kommunizieren kann. Dieses Ticket wird als *Ticket-genehmigendes Ticket (TGT)* bezeichnet.

9.1.2 NTLM

NTLM (Windows NT LAN Manager) ist möglicherweise sogar denjenigen nicht bekannt, die bereits Windows NT verwaltet haben. Aber *NT Challenge Response* sollte ein vertrauter Begriff sein.

Für die Echtheitsbestätigung mittels NTLM sind drei Informationen erforderlich:

- der Domänenname
- der Benutzername
- das Benutzerkennwort

SID

Die Domäne in diesem Protokoll ist die für die Echtheitsbestätigung zuständige Autorität. In der Domäne sind Angaben über die Benutzer und deren Berechtigungen zu finden. Die Angaben über die Benutzer sind in einem Paket enthalten, das als *SID* (Sicherheits-ID) bezeichnet wird. Die SID ist aus folgenden

Elementen zusammengesetzt:

- Kennwörter
- Gruppenmitgliedschaften
- Profilinformationen

Eine SID wird jeweils einem Benutzerkonto zugewiesen und wird niemals für einen anderen Benutzer neu generiert. Auch dann, wenn der Benutzer gelöscht und neu erstellt wird, wird die SID dieses Benutzers niemals einem anderen Benutzerkonto zugewiesen. Daher werden Sie, wenn Sie einen Benutzer in Windows NT löschen, darauf hingewiesen, dass der Benutzer nicht mehr völlig identisch erstellt werden kann.

Anfordern einer Ressource

Das Wichtigste ist, dass das Kennwort des Benutzers während der Echtheitsbestätigung niemals in Klartext übertragen wird. Das ist die Stärke (in Bezug auf die Sicherheit), zugleich aber auch die Schwäche von NTLM. Wenn eine Client-Anwendung eine SID zur Verfügung stellt, beginnt folgende Ereigniskette:

- Der Client-NTLMSP (Sicherheits-Provider) sendet Angaben über Domäne, Benutzer und Computer an den Server-NTLMSP.
- Der Server-NTLMSP erstellt mit Hilfe dieser Angaben eine eindeutige Challenge-Sequenz aus binären Bits.
- Der Client-NTLMSP empfängt diese Sequenz und verschlüsselt diese mit Hilfe des Benutzerkennworts. Das ist nun die Antwort.
- Der Client-NTLMSP sendet die verschlüsselte Antwort an den Server-NTLMSP.
- Der Server-NTLMSP ruft den DC mit der Benutzer-ID, der Challenge-Sequenz und der Antwortsequenz auf.
- Der DC verwendet das mit der Benutzer-ID verbundene Kennwort, um die Challenge-Sequenz zu verschlüsseln und mit der Antwortsequenz zu vergleichen und dadurch die Echtheit des Benutzers zu bestätigen.
- Ist dies erfolgreich, wird die Echtheitsbestätigung abgeschlossen und der Server-NTLMSP lässt die Kommunikation zu.

Es wird eine verschlüsselte Antwort, nicht jedoch das eigentliche Kennwort gesendet. Da der Server nie wirklich das Kennwort empfängt, gibt es für den Server keine Möglichkeit, das Kennwort für den Zugriff auf andere Ressourcen zu nutzen, auf die der Benutzer Zugriff hat. Dies können Netzwerkressourcen (Dateien, Datenbanken usw.) sein, auf die der Benutzer normalerweise zugreifen kann. Das ist eine Schwachstelle von NTLMSP, die die möglichen Aufgaben, die der Server für den Client übernehmen kann, deutlich einschränken.

9.1.3 Zugriffssteuerungsliste (ACL = Access Control List)

Um einen Platz für ein Objekt im Sicherheitssystem einzurichten, wird diesem eine Sicherheitsbeschreibung zugewiesen, die die Informationen enthält, die für die Kommunikation mit Benutzern und Gruppen erforderlich sind. Wenn ein Benutzer auf ein freigegebenes Objekt zuzugreifen

versucht, vergleicht das Objekt die SID des Benutzers mit seiner Zugriffssteuerungsliste.

Eine *Zugriffssteuerungsliste* ist eine Liste mit Berechtigungen, die mit einem Objekt verknüpft sind. In dieser Liste ist festgelegt, wer Berechtigungen für das Objekt hat und über welche Berechtigungen jeder Benutzer bzw. jede Gruppe verfügt. Die Zugriffssteuerungsliste besteht aus einer Liste von Einträgen, den so genannten *ACE-Einträgen* (Access Control Entries). Ein Eintrag kann beispielsweise besagen, dass Ben die Dateifreigabe lesen darf und dass die Gruppe Buchführung sowohl Lese- als auch Schreibzugriff auf die Freigabe hat. Dieses Beispiel erfordert zwei ACE-Einträge in der Zugriffssteuerungsliste.

Die ACE-Einträge geben entweder an: *Zugriff erlaubt* oder *Zugriff verweigert*. Sie enthalten eine Zugriffsberechtigung oder Zugriffsverweigerung für bestimmte Berechtigungen (lesen, schreiben usw.) und den entsprechenden Benutzer bzw. die entsprechende Gruppe.

Somit können Sie sich eine Zugriffssteuerungsliste wie eine Liste mit Einladungen zu einer exklusiven Versammlung vorstellen. Der Benutzer kommt an der Tür der Ressource an und ihm wird dann mitgeteilt, ob er über die gewünschte Berechtigung verfügt: »Ja, Sie dürfen reinkommen, aber nicht essen.«

9.2 Active Directory-Steuerung

Die Steuerung von Ressourcen und die Echtheitsbestätigung müssen natürlich auf eine bestimmte Art von Informationen zurückgreifen können. Kerberos und NTLM benötigen beide eine gemeinsame Liste mit Informationen über Benutzer, Gruppen und Objekten. Sie haben bereits erfahren, dass das Active Directory diese Informationsbasis darstellt. Lassen Sie uns jetzt die einzelnen Bereiche noch einmal etwas näher betrachten und sehen, wie sich diese in das Sicherheitsschema einfügen.

9.2.1 Arbeitsgruppen und Domänen

Domänen und Arbeitsgruppen sind die elementarsten Grundbestandteile der Windows 2000-Sicherheit. Das Domänenmodell ist die Basis für das Active Directory und die Unternehmenssicherheit. Das Arbeitsgruppenmodell ist im Wesentlichen auf die Installation zu Hause und in kleinen Büros beschränkt.

Wenn Sie an den Punkt gelangen, an dem Sie über eine hierarchische Verzeichnisstruktur für die Verwaltung von Benutzern und Gruppen nachdenken, sollten Sie keine Arbeitsgruppen mehr verwenden. Ich möchte die Arbeitsgruppen hier dennoch als Ausgangspunkt erwähnt haben.

Arbeitsgruppen

Arbeitsgruppen werden in Peer-to-Peer-Netzwerken verwendet, in denen fünf bis zehn Benutzer auf Ressourcen zugreifen. Das kommt daher, wie in Arbeitsgruppen Benutzer und Gruppen verwaltet werden.



Der Ausdruck *Peer-to-Peer* kommt daher, weil keiner der Rechner in einem solchen Netzwerk als Server oder Client dient. Sämtliche Rechner sind sowohl Server als auch Client. Daher werden sie als *Peers* (engl. Gleichrangiger) bezeichnet.

Das Arbeitsgruppenmodell, seine Erstellung und Verwaltung werden in Kapitel 5 ausführlich beschrieben. Hier reicht es, wenn Sie wissen, dass eine Arbeitsgruppe im Prinzip aus Windows-Rechnern (Windows 2000, 95/98 und/oder NT) besteht, die bestimmte Ressourcen gemeinsam nutzen. Diese Rechner sind miteinander verbunden, wobei jedoch jeder Rechner für die Verwaltung seines eigenen Sicherheitsschemas und seiner eigenen Freigaben selbst verantwortlich ist.

Wenn ein Rechner erst einmal ein Mitglied einer Arbeitsgruppe ist, ist es relativ einfach, die Arbeitsgruppe, der er angehört, zu ändern oder den Rechner zu einer Domäne hinzuzufügen.

Um die Arbeitsgruppenmitgliedschaft eines Rechners zu ändern oder um einen Rechner zu einer Domäne hinzuzufügen, gehen Sie wie folgt vor:

- Klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** und wählen Sie dann die Option **Eigenschaften**. Daraufhin öffnet sich das Dialogfeld **Systemeigenschaften**, das Sie auch über die Systemsteuerung und **System** aufrufen können.

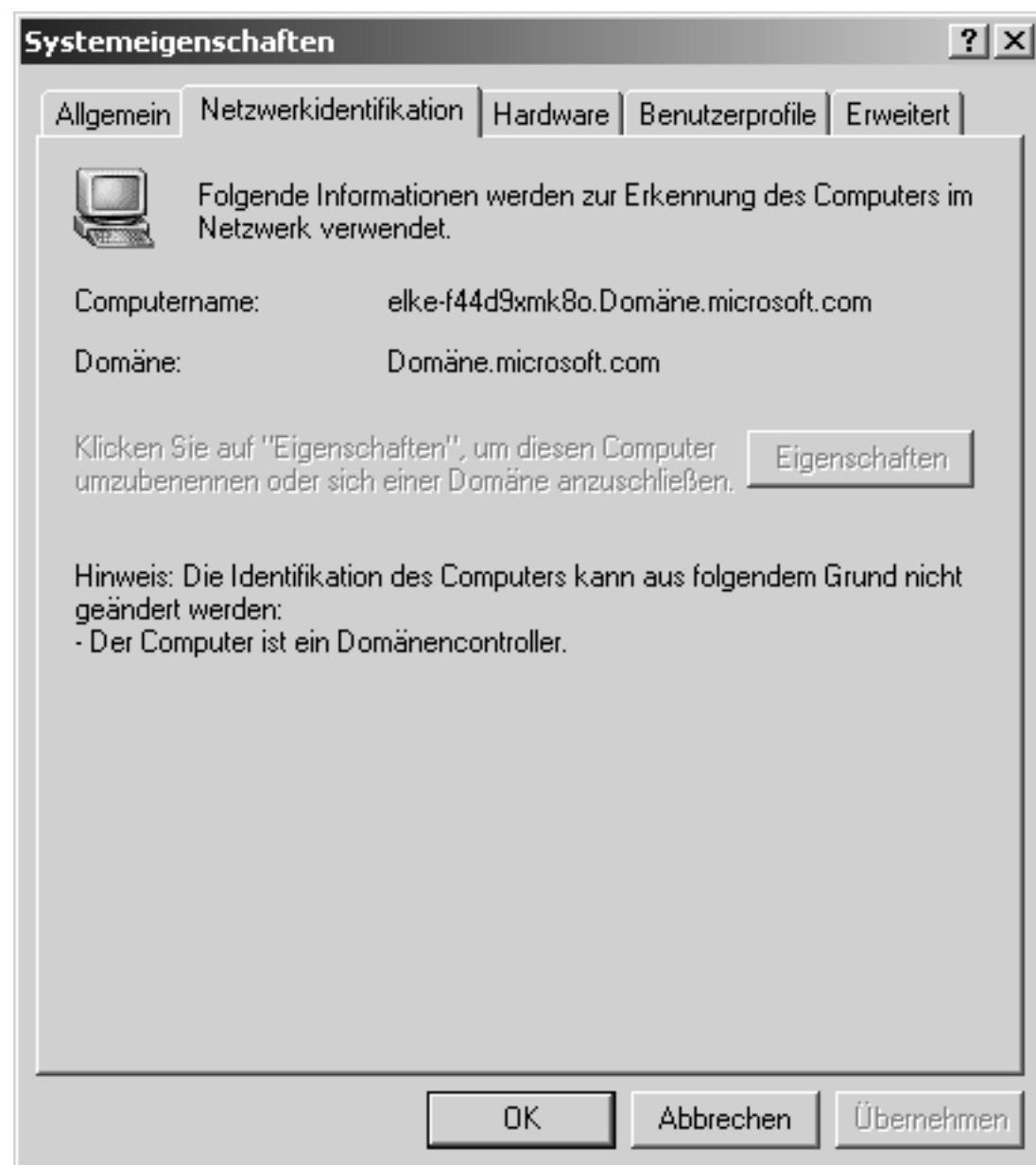


Abbildung 9.3: Die Registerkarte Netzwerkidentifikation

- Aktivieren Sie die Registerkarte **Netzwerkidentifikation** und klicken Sie auf **Eigenschaften**.

Wenn Sie einen Rechner zu einer Domäne hinzufügen, müssen Sie das Kennwort des Domänenadministrators kennen oder ein Administrator muss das Domänenkonto des Rechners zur Domäne hinzufügen, bevor Sie diesen Prozess beginnen.

Domänen

Innerhalb von Windows 2000 wurde das Domänenmodell Teil eines weitaus umfassenderen Schemas, nämlich des Active Directory. Hier soll es jedoch nur um den kleineren Teil gehen. Bevor Sie damit beginnen, Domänen als ein Werkzeug in dieser Version zu verwenden, sollten Sie wissen, dass diese Teil der Active Directory-Installation sind.

Wenn das Netzwerk aus einer großen Anzahl von Ressourcen und Benutzern besteht, ist das Domänenmodell zur Verwaltung besser geeignet als das Arbeitsgruppenmodell. Eine Domäne besteht aus Benutzerkonten und Gruppen von Benutzerkonten, die von mehreren Servern gemeinsam verwendet werden (siehe Abbildung 9.4). Damit ist es möglich, diese Rechner von einem Standort aus zentral zu verwalten. Administratoren können somit eine Vielzahl von verwaltungstechnischen Aufgaben auf die Domänen übertragen, anstatt umgekehrt. Das Domänenmodell ist für große Unternehmen und Universitäten weitaus attraktiver als das Arbeitsgruppenmodell.

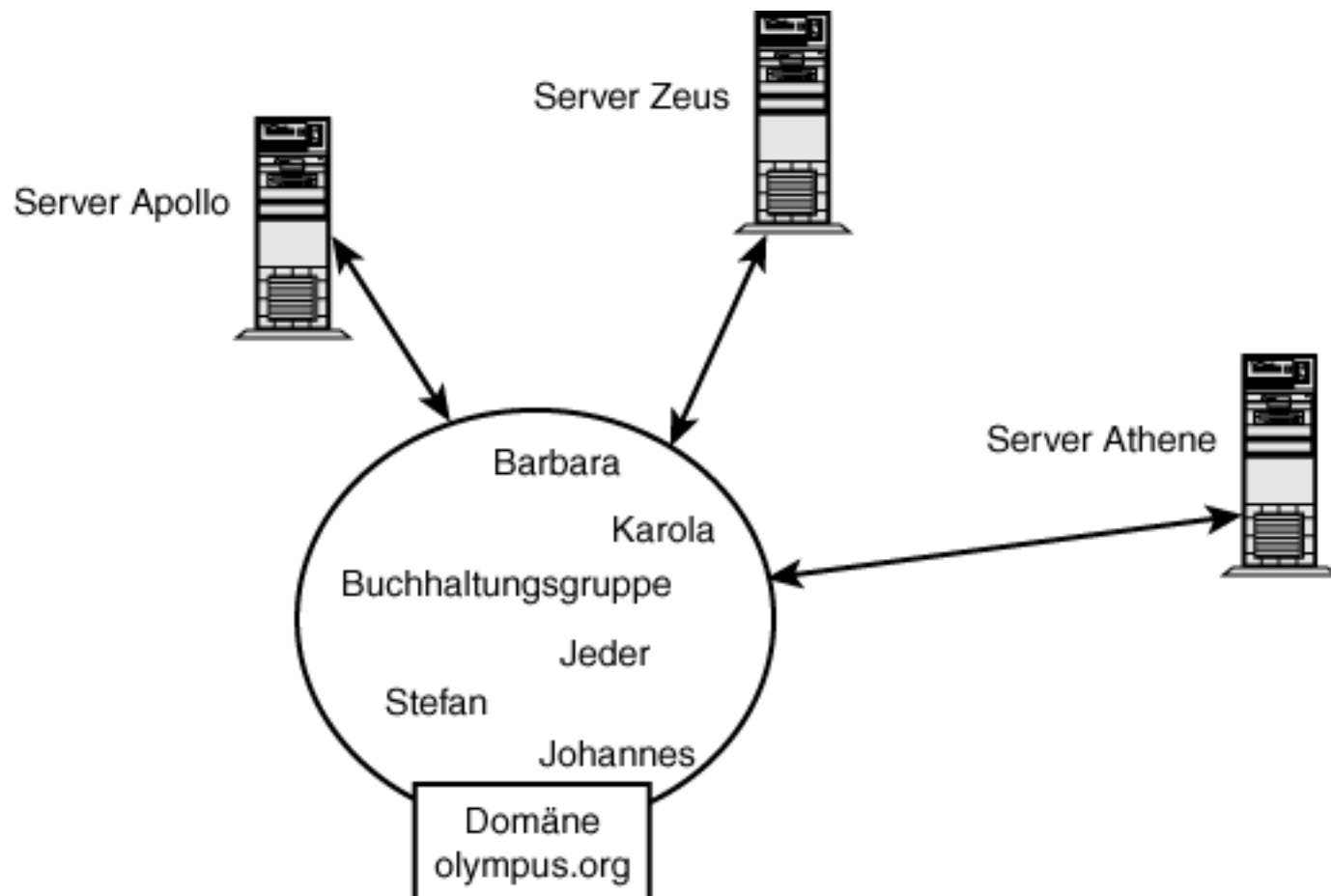


Abbildung 9.4: Der Aufbau einer Domäne

Der Domäne wird ein Name zugewiesen, der Ihnen bekannt sein wird, wenn Sie schon einmal im Internet waren. Bei Windows 2000 werden die Domänen nämlich mit dem DNS-Namenssystem nach

den im Internet geltenden Benennungsrichtlinien für Domänen benannt.

Beim DNS gibt es sechs Top-Level-Domänen, d.h. übergreifende Namenskategorien, für Domänen in den USA sowie Länderkürzel für Domänen in allen übrigen Ländern, wie z.B. `.de` für Deutschland oder `.fr` für Frankreich, denen alle weiteren Domänen untergeordnet sind. Diese Top-Level-Domänen und Länderkürzel sind den Domänennamen als Suffixe angehängt. Aus diesem Schema resultieren Domänennamen wie `microsoft.com` oder `yahoo.de`. Es gibt die folgenden Top-Level-Domänen:

- `.com` für kommerzielle Unternehmen
- `.edu` für Bildungsinstitutionen in den USA
- `.gov` für Regierungsbehörden in den USA
- `.mil` für militärische Organisationen in den USA
- `.net` für Netzerkanbieter
- `.org` für gemeinnützige Organisationen

Dadurch, dass in Windows 2000 nun das DNS-Benennungssystem zur Benennung von Domänen verwendet wird, steht ein globales Standardbenennungsschema zur Verfügung. Windows 2000-Server lassen sich damit global an jedem beliebigen Standort einsetzen, wenn der DNS-Server registriert und mit dem Internet verbunden ist. Einzelheiten zur Registrierung des Domänennamens bei InterNIC finden Sie in Kapitel 8 und Kapitel 21. In diesem Kapitel brauchen Sie nur zu wissen, woher die Benennungskonvention stammt.

Domänen werden bei der Installation eines Servers erstellt. Dabei werden Sie gefragt, ob der Rechner Mitglied einer Domäne werden soll. Wenn keine Domäne vorhanden ist, müssen Sie eine Domäne erstellen, um den Rechner zu einer Domäne hinzufügen zu können.

Sie werden darauf hingewiesen, dass Sie eine ungültige Domäne angegeben haben, und Sie werden gefragt, ob Sie dennoch fortfahren möchten. Um eine neue Domäne zu erstellen, klicken Sie einfach auf **Ja**.

Wenn Windows 2000 zum ersten Mal startet, öffnet sich ein Fenster, mit dessen Hilfe die Domänensituation geklärt werden soll (siehe Abbildung 9.5).



Abbildung 9.5: Das Eröffnungsfenster einer neuen Installation

Um mit dem Erstellen einer Domäne fortzufahren, gehen Sie wie folgt vor:

1. Klicken Sie auf **Das ist der einzige Server im Netzwerk**. Klicken Sie auf **Weiter**.
2. Lesen Sie, falls erforderlich, die Informationsseite und klicken Sie dann auf **Weiter**.
3. Geben Sie entsprechend der Richtlinien für die Benennung von Domänen den Namen Ihrer Domäne in das erste Textfeld ein und drücken Sie dann die (Tab)-Taste.
4. Wenn Sie Ihren Domänenamen beim InterNIC registriert haben, geben Sie diesen Namen (z.B. `mcp.com`, `indiana.edu` usw.) in das zweite Textfeld ein. Drücken Sie anschließend wieder die (Tab)-Taste, um eine Vorschau Ihres Domänennamens aufzurufen. Wenn Sie Ihre Domäne nicht registriert haben, geben Sie einfach `local` ein und drücken dann die Tabulatortaste.
5. Beobachten Sie die Vorschau Ihres Domänennamens (siehe Abbildung 9.6) und klicken Sie dann in diesem und dem folgenden Dialogfeld auf **Weiter** sowie schließlich auf **Fertig stellen**.



Abbildung 9.6: Domänenname und Vorschau

Bei älteren Versionen von Windows war die Entscheidung für eine Domäne eine Entscheidung für immer. Wenn ein Server als Domänencontroller installiert wurde, blieb er ein Domänencontroller, bis er entfernt oder neu installiert wurde. Bei Windows 2000 ist das anders. Das ist ein äußerst wichtiger Punkt, da aufgrund dessen eine größere Flexibilität ermöglicht wird. (Viele Windows NT-Administratoren werden dies zwei Mal lesen müssen, da dies eine derart unglaubliche Veränderung darstellt.)

Wenn Sie sich für eine Domäne oder Arbeitsgruppe entschieden haben und der Server läuft, haben Sie viele Möglichkeiten, diese Entscheidung zu ändern. Die einfachste Änderung besteht darin, einen Domänencontroller zu erstellen, wo zuvor keiner war, oder einen Domänencontroller von seiner Funktion als solchem zu entbinden.

Dies alles können Sie mit dem Assistenten zum Installieren von Active Directory tun. Um diesen Assistenten aufzurufen, klicken Sie auf **Start** und dann auf **Ausführen**. Geben Sie nun `dcpromo` ein und klicken Sie anschließend auf **OK**.

Um nach der Installation einen Domänencontroller hinzuzufügen, gehen Sie wie folgt vor:

1. Lesen Sie den Eröffnungsbildschirm und stellen Sie sicher, dass Sie die richtige Option gewählt haben.
2. Klicken Sie auf **Domänencontroller für eine neue Domäne** und dann auf **Weiter**.

3. Klicken Sie auf **Eine neue Domänenstruktur erstellen** und dann auf **Weiter**.
4. Klicken Sie auf **Neue Gesamtstruktur aus Domänenstrukturen erstellen** und dann auf **Weiter**.
5. Geben Sie den Namen der Domäne, die Sie erstellen, zusammen mit dem Namen der Top-Level-Domäne (wenn Sie registriert sind) in das Textfeld ein und klicken Sie dann auf **Weiter** (siehe Abbildung 9.7).

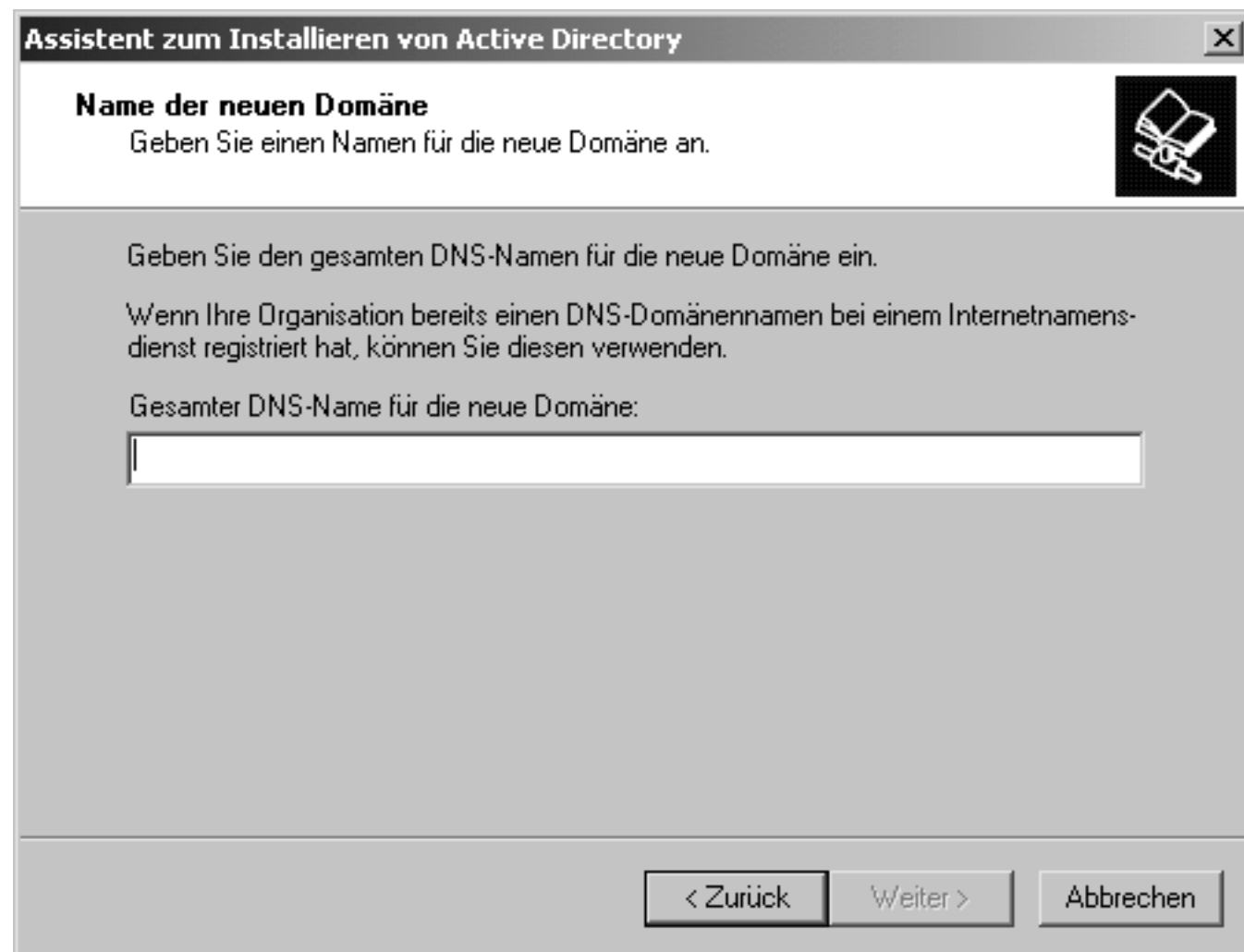


Abbildung 9.7: Fenster für die Eingabe des Domännennamens



Dies ist etwas Einmaliges bei der Erstellung einer Domäne. Wenn Sie den Assistenten verwenden, müssen Sie einen drei Ebenen bezeichnenden Domännennamen eingeben (z.B. `sams.mcp.com` oder `cs.purdue.edu`). Wenn Sie mit dem Programm DCPROMO arbeiten, können Sie einen zwei Ebenen bezeichnenden Domännennamen eingeben.

6. Geben Sie den NetBIOS-Namen der Domäne in das Textfeld ein und klicken Sie auf **Weiter**.
7. Bei den nächsten beiden Fenstern geht es um den Speicherort von Dateien. Sie können hier Änderungen vornehmen. Diese sind jedoch relativ nutzlos und können beim Suchen von Dateien und bei der Fehlersuche zu Problemen führen. Wenn Sie möchten, nehmen Sie Änderungen vor und klicken dann auf **Weiter**.
8. Wenn Sie für den Server, auf dem Sie Active Directory installieren, keinen DNS-Server haben, werden Sie aufgefordert, einen DNS-Server zu installieren (siehe Abbildung 9.8). Wenn Sie keinen

bevorzugten DNS-Server haben, sollten Sie auf **Ja** klicken und die Installation beginnen. Wenn Sie für Ihre Domäne bereits einen DNS-Server haben, sollten Sie auf **Nein** klicken und prüfen, warum dieser Server den aktuellen Server für die Domäne nicht erkennt. Klicken Sie auf **Weiter**.

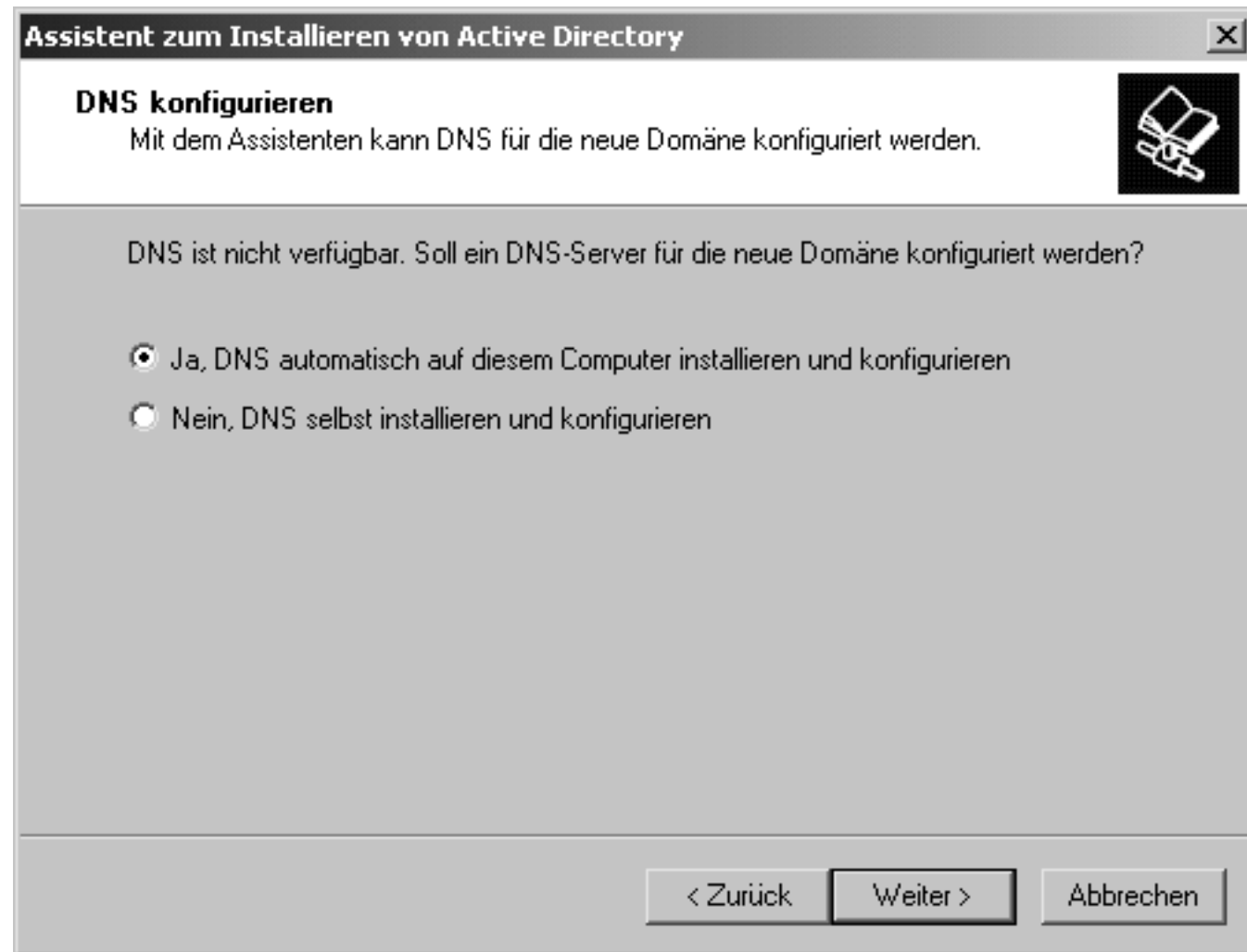


Abbildung 9.8: Es kann sein, dass Sie Angaben zum DNS-Server machen müssen.

Von nun an können die Optionen, abhängig davon, was auf Ihrem Server vor dem Hinzufügen des Domänencontrollers installiert worden ist, recht unterschiedlich sein. Wenn Sie sich von den Assistenten führen lassen, werden die meisten Ihrer Fragen beantwortet werden.

Um einen Domänencontroller von einem Server zu entfernen, rufen Sie wie zuvor das Programm DCPROMO auf und gehen dann wie folgt vor:

1. Lesen Sie den Eröffnungsbildschirm und stellen Sie sicher, dass Sie die richtige Option gewählt haben.
2. Wenn dieser Server der letzte bzw. einzige Server in der Domäne ist, klicken Sie auf das entsprechende Kontrollkästchen und dann auf **Weiter** (siehe Abbildung 9.9). Damit wird es möglich, dass das Betriebssystem die Domäne vollständig entfernen kann.
3. Geben Sie den Benutzernamen und das Kennwort des Administrators sowie den vollständigen Domännennamen (wird automatisch angezeigt) ein und klicken Sie dann auf **Weiter**.
4. Da der Server von nun an ein alleinstehender Server sein wird, müssen Sie das Kennwort des Administrators eingeben und bestätigen sowie anschließend auf **Weiter** klicken.
5. Zum Abschluss erscheint eine Zusammenfassung der von Ihnen gewählten Optionen. Wenn Sie auf

Weiter klicken, wird der Server aus der Domäne entfernt. Wenn Sie alle Dialogfelder des Assistenten durchlaufen haben, klicken Sie auf **Fertig stellen**.



Abbildung 9.9: Das Fenster für das Entfernen des einzigen Servers in der Domäne

Gesamtstrukturen und Strukturen

Eine *Domänenstruktur* ist eine Sammlung von Domänen, die weitere Domänen und untergeordnete Domänen in einer DNS-Hierarchie enthalten. Die Stammdomäne in einer Domänenstruktur kann einen DNS-Namen wie z.B. `yahoo.de`, `indiana.edu` oder `mcp.com` tragen. Der Name der untergeordneten Domänen wird auf der Basis der Domänenstruktur gebildet. Das heißt, der Name der untergeordneten Domäne wird dem der Stammdomäne vorangestellt, wie z.B. bei den Domänen `sams.mcp.com` und `architecture.indiana.edu`.

Die einzelnen Domänenstrukturen lassen sich zu übergeordneten Strukturen, so genannten *Gesamtstrukturen*, zusammenfassen, wobei diese keinen gemeinsamen Domännennamen benutzen müssen. Die Domäne `mcp.com` kann z.B. mit der Domäne `indiana.edu` zu einer Gesamtstruktur verknüpft werden. Die Stammdomäne kann dann z.B. `bellind.com` heißen. Der Name der Stammdomäne muss also nichts mit den Namen der einzelnen Domänenstämme zu tun haben.

Die meisten Unternehmen werden niemals eine Größe erreichen, bei der es nötig wäre, solche Gesamtstrukturen mit Stammdomänen einzurichten. Bei dem momentanen Trend zur Globalisierung von

Unternehmen wird diese jedoch zukünftig öfter erforderlich sein. Dank des neuen Domänenmodells und Benennungsschemas ist dies auch problemlos möglich.

Eine Struktur wird in dem Moment erstellt, in dem die erste Domäne erstellt wird. Dabei können Sie sich entscheiden, ob Sie eine neue Struktur erstellen oder einer bestehenden Struktur beitreten möchten. Die dritte Option, die Sie bei der Installation einer neuen Domäne haben, ist die Möglichkeit einer bestehenden Struktur beizutreten oder eine neue Gesamtstruktur zu erstellen.

Gesamtstrukturen werden im weitesten Sinne ebenfalls erstellt. Um jedoch zwei Strukturen mit unterschiedlichen Domänenkontextnamen zusammenzufügen, muss eine Gesamtstruktur manuell verbunden oder während der Installation von Strukturen erstellt werden. Einfach ausgedrückt bedeutet das, dass Gesamtstrukturen erstellt werden, indem Strukturen mit unterschiedlichen Namenskonventionen zusammengefügt werden.

Um Gesamtstrukturen zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie die Konsole **Active Directory-Standorte und -Dienste**.
2. Klicken Sie mit der rechten Maustaste auf **Active Directory-Standorte und -Dienste** und klicken Sie dann auf **Struktur ändern**.
3. Geben Sie im Textfeld **Stammdomäne** die Stammdomäne der Gesamtstruktur ein. Dies ist die Stammdomäne der ersten in der Gesamtstruktur erstellten Domänenstruktur.

Organisationseinheiten

Die Domänen sind größer geworden und sie lassen sich außerdem in kleinere Einheiten aufteilen. Diese Einheiten heißen Organisationseinheiten (abgekürzt OE bzw. im Englischen OU für »Organizational Units«). Wenn Sie mit der Welt von NetWare NDS vertraut sind, werden Sie hier etwas Altbekanntes wiedererkennen, das bereits seit Jahren existiert.

Es ist noch immer so, dass die Überwachung innerhalb der Domänengrenzen erfolgt. Aus diesem Grund wurde das Domänenmodell häufig kritisiert. Ein Domänenadministrator hatte alle Macht und es gab wenig Möglichkeiten, das Modell feiner zu gliedern.

Der Administrator einer Domäne kann nun aber Container (Organisationseinheiten) einrichten, Objekte in diesen Containern erstellen und verschiedenen Administratoren die Verantwortung für diese Container übertragen (siehe Abbildung 9.10). Der Administrator kann jedoch weiterhin den Domänenstamm überwachen. Dies verleiht dem Domänenmodell erheblich mehr Flexibilität als bisher und lässt auch ein Wachstum zu.

Durch die Aufteilung der Verwaltung kann die Arbeitslast von einem einzelnen Administrator genommen werden. Die Flexibilität der Informationsnetzwerke innerhalb von Unternehmen lässt sich so erhöhen.

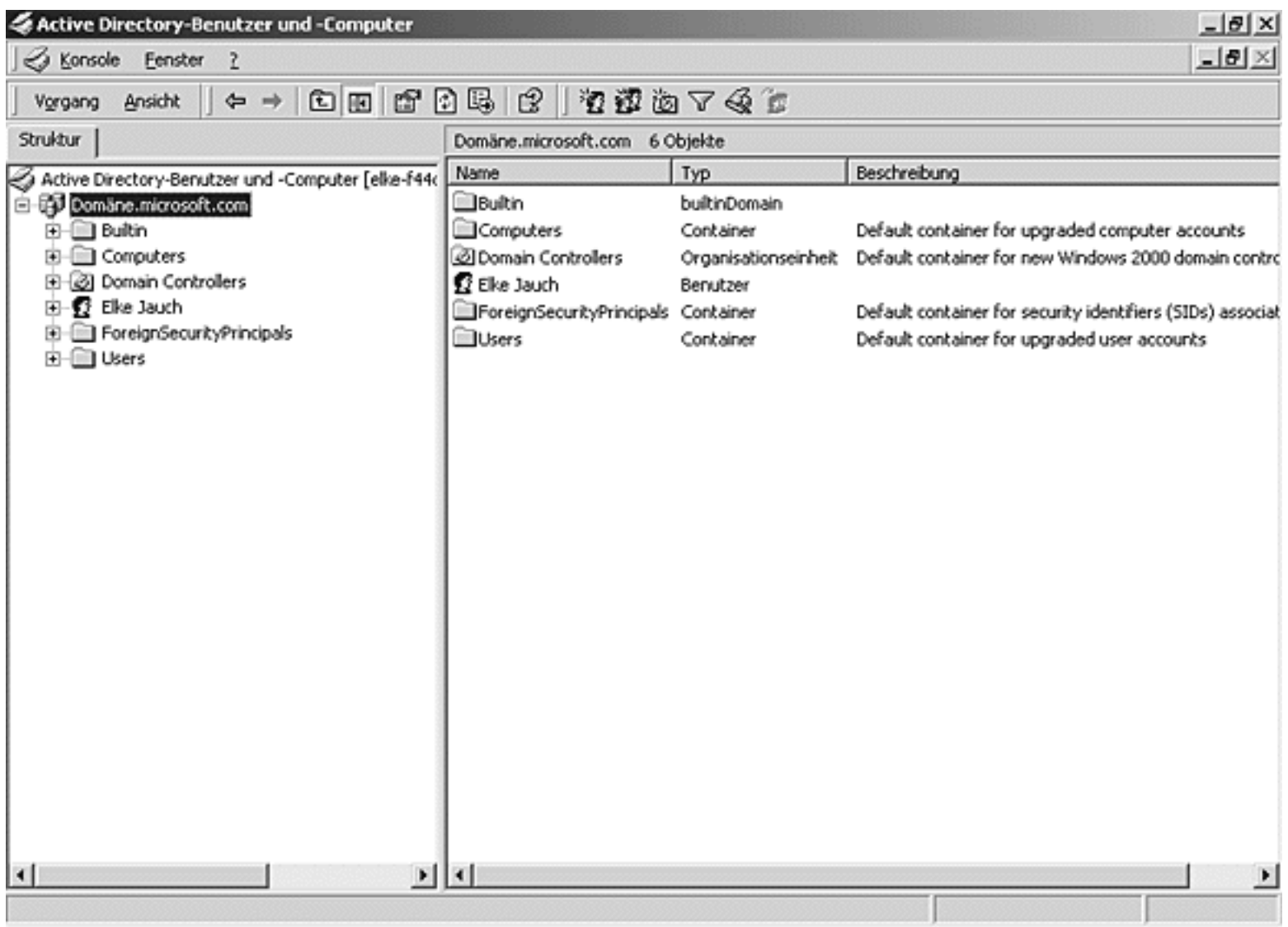


Abbildung 9.10: Domäne mit Organisationseinheiten

Eine Organisationseinheit erstellen Sie in der Konsole **Active Directory-Benutzer und -Computer**. Da eine Organisationseinheit Teil einer Domäne ist, wird sie innerhalb einer Domäne erstellt. Wie Sie eine Organisationseinheit erstellen, erfahren Sie weiter hinten in diesem Kapitel.

Domänenkontrolle

An dieser Stelle werden die Änderungen in Windows 2000 ganz offensichtlich und sie entsprechen auch dem, was sich schon lange jeder wünscht. Domänen sind nun, was die Anpassung der Größe und die sonstigen Möglichkeiten betrifft, erheblich flexibler. Aufgrund dieser Änderungen sind Administratoren nun in der Lage, Domänen in Bereiche auszuweiten, wie dies zuvor nicht möglich war.

Die Domänenkontrolle beinhaltet die Verwaltung und die Verteilung von Domäneninformationen auf den Servern im Netzwerk. Wenn an der Definition eines Benutzers oder einer Gruppe eine Veränderung vorgenommen werden muss, muss eine Autorität eingerichtet werden, damit dieses System funktioniert. Um Wachstum zuzulassen, muss ein Weg gefunden werden, die Veränderungen auf mehr als einem Computer zu speichern und den Zugriff auf diese Informationen zu erleichtern. Dies ist mit der Domänenkontrolle möglich.

Domänencontroller

Domänencontroller werden wie Betriebsmaster (siehe Kapitel 5) eingerichtet, wenn der erste Server in der Domäne installiert wird. Zu den Funktionen von Domänencontrollern gehören die Verwaltung der Benutzer- und Gruppenkonten sowie die Verwaltung des Zugriffs auf Verzeichnisse und auf freigegebene Ressourcen. Um die Fehlertoleranz zu erhöhen, sollte ein Verzeichnis mindestens zwei Domänencontroller enthalten (siehe Abbildung 9.11).

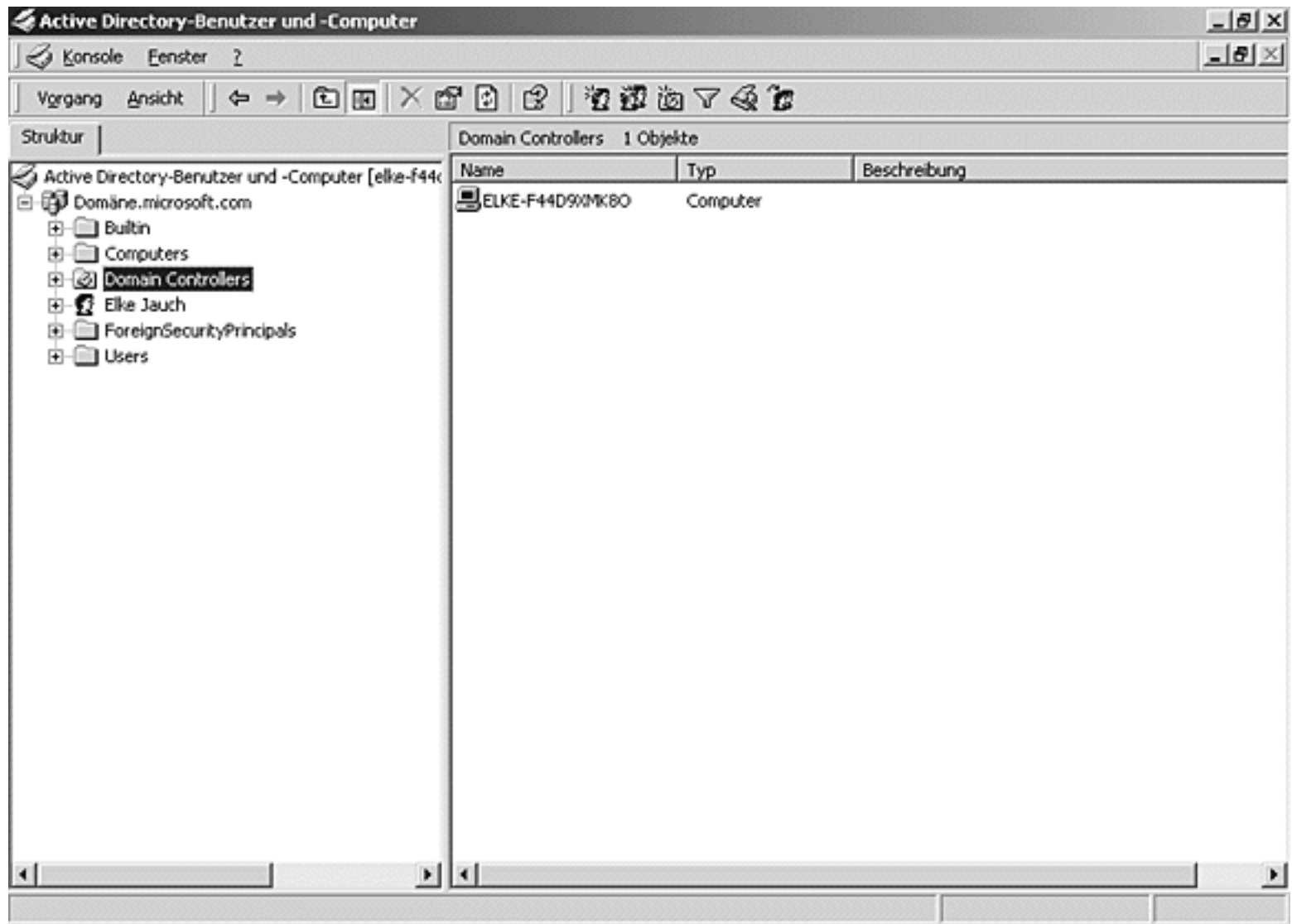


Abbildung 9.11: Auswahl eines Servers als Domänencontroller

Nachdem der erste Server installiert wurde, können andere Server in der Domäne installiert werden und an der Domänenkontrolle teilnehmen. Der Computer ist dann Bestandteil einer Multimaster-Systemdomäne. Dies stellt eine starke Veränderung gegenüber dem NT-Modell des allein stehenden Servers oder des primären Domänencontrollers dar.

Wenn der primäre Domänencontroller unter Windows NT heruntergefahren war, konnte kein Benutzer sein Kennwort ändern. Bei einem Multimastermodell kann ein Domänencontroller die Änderungen annehmen und Replikate an die anderen Domänencontroller in der Domäne verschicken.

Vertrauensstellungen

Eine *Vertrauensstellung* wird zwischen Domänen eingerichtet, damit die Benutzer und Gruppen aus einer Domäne auf Ressourcen einer anderen Domäne zugreifen können. In Windows 2000 gibt es zwei neue Formen von Vertrauensstellungen und das Konzept der Vertrauensstellungen wurde sehr stark verbessert.

Explizite Vertrauensstellungen (Klassische Vertrauensstellungen)

Domänen wurden bisher über so genannte *Vertrauensstellungen* miteinander verbunden. Diese werden nun als *explizite Vertrauensstellungen* bezeichnet. Eine explizite Vertrauensstellung ist eine einseitige Beziehung, mit der eine Verbindung zwischen den Ressourcen einer Domäne und den Benutzern und Gruppen einer anderen Domäne hergestellt wird. Die Bezeichnung »explizite Vertrauensstellung« stammt daher, dass die Vertrauensstellung von den Administratoren der teilnehmenden Domänen explizit eingerichtet werden muss.

Wenn z.B. der Administrator von Domäne A eine Vertrauensstellung für Domäne B einrichtet, erhalten die Benutzer und Gruppen aus Domäne B Zugriff auf die Ressourcen in Domäne A. Es handelt sich um eine *unidirektionale Vertrauensstellung*, die explizit eingerichtet wurde.

Wenn die Administratoren in den beiden Domänen A und B für die jeweils andere Domäne eine Vertrauensstellung erstellen, spricht man von einer *bidirektionalen* oder *vollständigen Vertrauensstellung*. In diesem Fall wird den Benutzern von beiden Domänen der Zugriff auf Ressourcen der jeweils anderen Domäne gewährt. In beiden Fällen muss die Vertrauensstellung, die eine explizite ist, manuell erstellt werden.

Klassische Vertrauensstellungen werden in Kapitel 5 ausführlicher beschrieben.

Nichttransitive Vertrauensstellungen

Eine *nichttransitive Vertrauensstellung* ist eine Vertrauensstellung zwischen zwei Domänen, die nicht in derselben Domänenstruktur enthalten sind oder bei denen eine teilnehmende Domäne keine Windows 2000-Domäne ist. Diese Vertrauensstellungen können unidirektional und bidirektional, nicht aber transitiv sein (siehe hierzu den nächsten Abschnitt).

Hier einige Beispiele für nichttransitive Vertrauensstellungen:

- Zwischen Windows 2000-Domänen und Windows NT-Domänen.
- Zwischen zwei Windows 2000-Domänen, die sich in unterschiedlichen Gesamtstrukturen befinden.

Transitive Vertrauensstellungen

Eine *transitive Vertrauensstellung* ist eine Vertrauensstellung zwischen zwei Domänen innerhalb einer Domänenstruktur oder einer Gesamtstruktur. Wenn untergeordnete Domänen in einer Domänenstruktur erstellt werden, besteht zwischen der untergeordneten und der übergeordneten Domäne automatisch eine transitive Vertrauensstellung. Diese ist immer bidirektional und wird automatisch eingerichtet.

Domänenmodus

Domänen werden bei Windows 2000 im so genannten *gemischten Modus* installiert. Das bedeutet, dass

die Domäne versuchen wird, sowohl mit Windows NT- als auch mit Windows 2000-Domänen zu kommunizieren. Das ist wichtig, weil viele Domänen, in denen Windows 2000 installiert wird, in Vertrauensstellungen beide Domänentypen adressieren werden. Dieser Modus ist zumindest für alle Aktualisierungsumgebungen erforderlich.

Das Gegenstück zum gemischten Modus ist der *native Modus*. Im nativen Modus kann eine Domäne sämtliche neuen Verzeichnisfunktionen von Windows 2000 nutzen. Für Features wie verschachtelte Gruppen ist der native Modus erforderlich.

Im gemischten Modus können Sie aus Gründen der Abwärtskompatibilität einige Funktionen von Windows 2000 nicht nutzen. Das ist ein bisschen so, als müssten Sie Ihren kleinen Bruder zum Einkaufsbummel mitnehmen. Sie müssen sich an sein Tempo anpassen. Features wie verschachtelte Gruppen oder universelle Gruppen sind in alten Domänen und somit auch für Sie nicht verfügbar.



Bevor Sie den Modus wechseln, sollten Sie daran denken, dass Sie diesen Vorgang nicht mehr rückgängig machen können. Wenn Sie den Modus gewechselt haben, bleibt dieser Modus dauerhaft so. Ich kann nicht oft genug darauf hinweisen: Sie können in keinem schlimmeren Dilemma stecken, als wenn Sie an einer Stelle ankommen, an der es kein Zurück mehr gibt.

Den Modus zu wechseln ist sehr einfach, aber überlegen Sie sich das genau. Gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf das Domänenobjekt und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie auf die Schaltfläche **Modus wechseln** (siehe Abbildung 9.12).
3. Starten Sie den Domänencontroller neu.

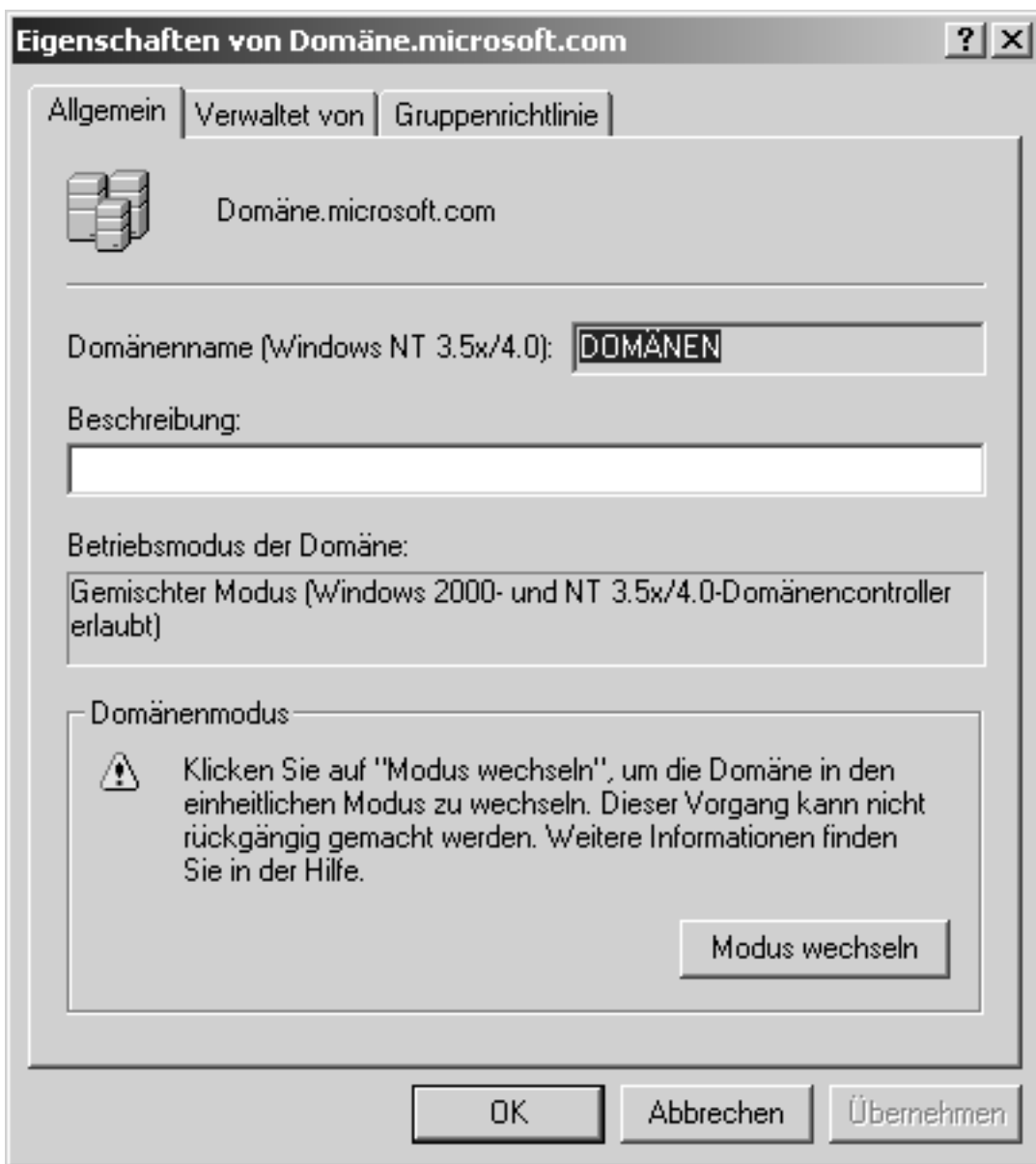


Abbildung 9.12: Die erste Registerkarte im Dialogfeld Eigenschaften von Domäne

Wenn Sie das Dialogfeld **Eigenschaften von Domäne** das nächste Mal öffnen, werden Sie sehen, dass die Domäne im nativen (ursprünglichen) Modus ist.

UPN (User Principal Name)

Wenn ein Benutzer auf die Domäne zugreift, kann er einen zugewiesenen Benutzernamen und ein Kennwort verwenden und in einer Umgebung mit nur einer Domäne problemlos eine Verbindung herstellen. In einer Umgebung mit mehreren Domänen oder über eine DFÜ-Verbindung ist es dagegen erforderlich, dass der Benutzer einen vollständigen Benutzernamen angibt, um eine Verbindung herstellen zu können. In diesem Fall sollte der Benutzer einen vollständigen Anmeldenamen zusammen mit dem Domänennamen eingeben. Dieser sieht ähnlich wie eine E-Mail-Adresse aus (z.B. zeus@olympus.org). Daher kann es sein, dass der Benutzer aufgefordert wird, sich mit seiner E-Mail-Adresse anzumelden. Dies ist jedoch nicht so offensichtlich, wie die Benutzer denken mögen.

Einige Unternehmen unterhalten aus vielen guten und berechtigten Gründen für denselben E-Mail-Server mehrere registrierte Domänennamen. Aus diesem Grund kann es vorkommen, dass es einige Benutzer

gibt, die sich in einer Domäne befinden, deren E-Mail-Adresse nicht mit dem Domänennamen übereinstimmt, in der sich das Benutzerobjekt befindet.

Nehmen wir beispielsweise einmal an, Pluto ist ein Mitglied der Domäne `olympus.org`. Aus politischen oder marktstrategischen Gründen möchte er seine E-Mails jedoch lieber unter `hades.com` empfangen. Die MX-Einträge beider Domänen so zu registrieren, dass die E-Mails an derselben Stelle ankommen, ist in Ordnung und zulässig (in Kapitel 8 erfahren Sie mehr über MX-Einträge). Da beide Domänennamen bei derselben Domäne registriert sind und ankommen, führt dies zu keinen Problemen. Aber wie kann sich Pluto bei der Domäne `olympus.org` anmelden?

Dieses Problem lässt sich mit einem UPN (User Principal Name) in der Active Directory-Domäne lösen. Damit können die Benutzer in dieser Domäne auf zahlreiche unterschiedliche `@DOMÄNENNAME`-Einträge zugreifen. Wenn Sie einen Benutzer erstellen, wählen Sie einfach den UPN, den Sie an den Anmeldenamen des Benutzers anfügen möchten. Wenn sich der Benutzer dann anmeldet, kann er seine normale E-Mail-Adresse verwenden und kommt dennoch in der Domäne an, die Sie festgelegt haben. Ich bin sicher, dass Pluto eine kleine Schwindelei zu seinen Gunsten verstehen wird.

UPNs werden auf der Registerkarte **Eigenschaften** der Domäne in der Konsole **Active Directory-Domänen und -Vertrauensstellungen** definiert. Klicken Sie dazu einfach mit der rechten Maustaste auf **Active Directory-Domänen und -Vertrauensstellungen** und klicken Sie dann auf **Eigenschaften**. Hier können Sie alternative UPN-Suffixe eingeben (siehe Abbildung 9.13). Weiter hinten in diesem Kapitel erfahren Sie, wie Sie den UPN zum Konto eines Benutzers hinzufügen.

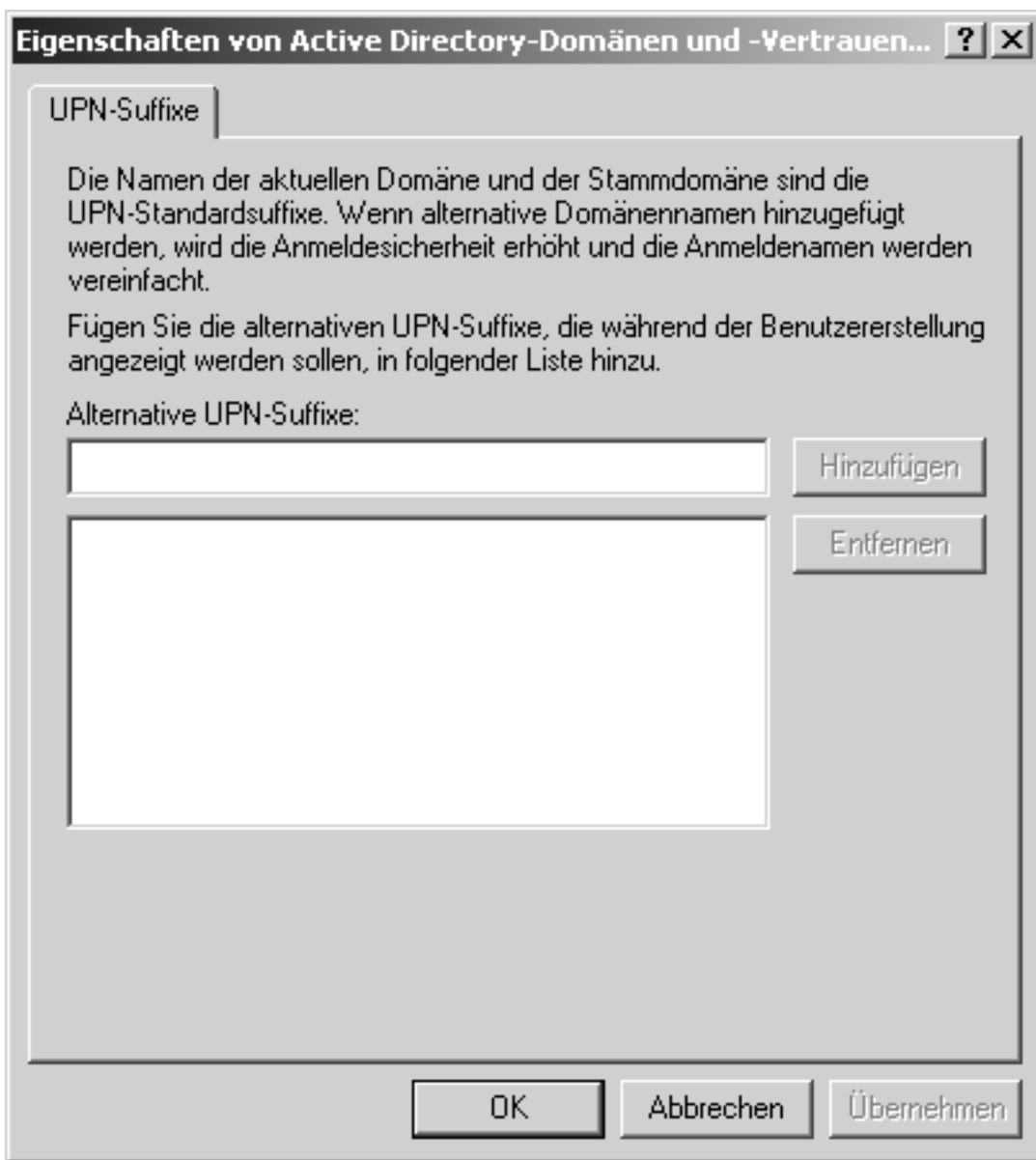


Abbildung 9.13: UPN-Suffixe

9.3 Active Directory- bzw. Domänenobjekte

Wenn eine Domäne erst einmal erstellt ist, kann sie mit Objekten gefüllt werden, weshalb sie ja schließlich erstellt worden ist. Benutzer, Gruppen und andere Objekte werden innerhalb der Konsole **Active Directory-Benutzer und -Computer** erstellt.

Zu den Objekten, die erstellt werden können, zählen folgende:

- *Benutzer*. Der Kontenname, der für den Zugriff auf die Domäne verwendet wird. Dies ist das Basisobjekt, dem Berechtigungen auf Ressourcen und Richtlinien gewährt werden.
- *Computer*. Das Konto, das für die Steuerung der Computerobjekte erstellt wird.
- *Gruppe*. Eine Reihe von Benutzerkonten und andere Gruppen, deren Benutzerberechtigungen und Richtlinien gemeinsam verwaltet werden, womit erreicht wird, dass nicht jedes Benutzerkonto einzeln geändert werden muss.
- *Kontakt*. Ein Verwaltungsobjekt, das erstellt wird, damit das System auf E-Mail-Konten außerhalb

des Systems zugreifen kann.

- *Organisationseinheit*. Ein administrativer Teil einer Domäne, der verwendet wird, um Domänenobjekte in verwendbare und einzeln verwaltete Bereiche zu gliedern.
- *Freigegebene Ordner*. Ein Active Directory-Objekt, das von Dateifreigaben erstellt wird, sodass die Freigabe als Teil des Verzeichnisses verwaltet werden kann.
- *Freigegebene Drucker*. Ein Active Directory-Objekt, das von Druckerfreigaben älterer Windows-Versionen (Windows NT, 95/98 und WFW) erstellt wird, sodass die Freigabe als Teil des Verzeichnisses verwaltet werden kann.

Eine ausführlichere Beschreibung der Benutzer- und Gruppenobjekte finden Sie in Kapitel 11.

9.4 Was kommt zuerst: Die Benutzer oder die Gruppen?

Für die Frage der Erstellung von Benutzer- und Gruppenkonten und welche Konten zuerst erstellt werden müssen, müssen wir uns etwas Zeit nehmen und zunächst einmal klären, wie sich die einzelnen Konten jeweils verzweigen.

Benutzerkonten werden für den Zugriff auf Domänen verwendet. Sie sind die Stammobjekte, denen Berechtigungen für Ressourcen und Richtlinien zugewiesen werden. Sie sind nicht wesentlich komplexer als hier beschrieben. Gruppen können dagegen deutlich komplexer aufgebaut sein.

Im Gegensatz zu Windows NT können Sie in Windows 2000 Gruppen, die Domänengrenzen überschreiten, sowie Gruppen, die in andere Gruppen verschachtelt sind, erstellen. Sie können dies nicht im gemischten, wohl aber im einheitlichen Modus tun.

Bei Windows 2000 gibt es drei Kategorien von Gruppen:

- *Universelle Gruppen*. Gruppen mit dem Bereich »Universal« können als Mitglieder beliebige Gruppen und Konten von beliebigen Windows 2000-Domänen in der Domänenstruktur bzw. in der Gesamtstruktur enthalten und ihnen können Berechtigungen in jeder Domäne in der Domänenstruktur bzw. in der Gesamtstruktur zugewiesen werden. Universelle Gruppen sind in Domänen im gemischten Modus nicht zulässig.
- *Globale Gruppen*. Gruppen mit dem Bereich »Global« können als Mitglieder beliebige Gruppen und Konten nur von der Domäne enthalten, in der die Gruppen definiert sind; ihnen können Berechtigungen in jeder Domäne in der Domänenstruktur bzw. in der Gesamtstruktur zugewiesen werden.
- *Gruppe der lokalen Domäne*. Gruppen mit dem Bereich »Lokale Domäne« können als Mitglieder beliebige Gruppen und Konten von einer Windows 2000- oder Windows NT-Domäne enthalten und sie können verwendet werden, um Berechtigungen nur innerhalb einer Domäne zuzuweisen.

Ob Sie nun Benutzer- oder Gruppenkonten zuerst erstellen, hängt von Ihrer Sichtweise zu Beginn ab. Microsoft empfiehlt, immer zuerst Gruppen zu erstellen, bevor Berechtigungen für eine Ressource zugewiesen werden. Es ist weniger wahrscheinlich, dass Ressourcen entfernt oder geändert werden, als Benutzer. Darüber hinaus werden Benutzer fast immer zu der Liste der für eine Ressource zulässigen Benutzer hinzugefügt.

Wenn Sie zuerst Gruppen erstellen, die die Aufgaben und Rollen ausfüllen, die erforderlich sind, um Netzwerkaufgaben zu erfüllen, und dann diesen Gruppen die erforderlichen Berechtigungen zuweisen, haben Sie ein einfacher zu befolgendes Sicherheitsparadigma. Wenn bei einem Benutzer in der Aufgabenverantwortlichkeit oder in einer Aufgabenliste Änderungen vorgenommen werden müssen, ist es einfacher, die Gruppenzugehörigkeit dieses Benutzers zu ändern, als all die Stellen zu suchen, für die dieser Benutzer als Einzelner über Berechtigungen verfügt.

Es scheint sehr aufwändig zu sein, immer jeweils eine Gruppe zu erstellen und dann Benutzer zuzuweisen. Aber wenn das Netzwerk gewachsen ist, werden Sie sehen, dass es so besser funktioniert. Aber es gibt natürlich auch Ausnahmen.

Windows 2000-Gruppen werden noch weiter unterschieden. Jede erstellte Gruppe ist entweder eine Sicherheitsgruppe oder eine Verteilergruppe. Der Unterschied zwischen diesen Gruppen besteht darin, dass Sicherheitsgruppen für die Anwendung von Berechtigungen und Sicherheitseinstellungen in der Domäne verwendet werden. Eine Verteilergruppe ist einem Kontaktobjekt sehr ähnlich. Sie hat eher einen informativen Charakter und kann für E-Mails verwendet werden.

9.4.1 Erstellen von Objekten

Die Konsole **Active Directory-Benutzer und -Computer** ist ein Tool, das so ähnlich wie der Windows-Explorer funktioniert, den Windows-Benutzer bereits gut kennen. Objekte im Active Directory werden ähnlich wie neue Ordner und/oder leere Dateien im Explorer erstellt. Mit ein bisschen gesundem Menschenverstand und den Informationen in diesem Kapitel können Sie wahrscheinlich selbst herausfinden, wo Sie mit dem Erstellen beginnen. In diesem Abschnitt wird das Erstellen von Objekten Schritt für Schritt beschrieben.

Um mit dem Erstellen von Objekten zu beginnen, öffnen Sie die Konsole **Active Directory-Benutzer und -Computer** entweder innerhalb der Microsoft Management Console (MMC) oder über **Start/Programme/Verwaltung**.

Erstellen einer neuen Organisationseinheit

Es ist möglicherweise erforderlich, die Autorität oder Verwaltung von Benutzern innerhalb einer Unternehmensstruktur zu delegieren. Aus informationstechnologischer Sicht mag es aber wenig sinnvoll sein, eine neue Domäne zu erstellen. In diesem Fall ist es angebracht, eine Organisationseinheit zu erstellen. Eine Organisationseinheit ist ein administrativer Teil einer Domäne, der verwendet wird, um Domänenobjekte in verwendbare und einzeln verwaltete Bereiche zu gliedern.

Um eine Organisationseinheit zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie die Domäne, in der Sie die Organisationseinheit erstellen möchten, indem Sie auf das Pluszeichen neben dem Domännennamen klicken.
2. Klicken Sie mit der rechten Maustaste auf die Domäne, dann auf **Neu** und anschließend auf **Organisationseinheit**.
3. Geben Sie den Namen der zu erstellenden Organisationseinheit ein und klicken Sie auf OK (siehe Abbildung 9.14).

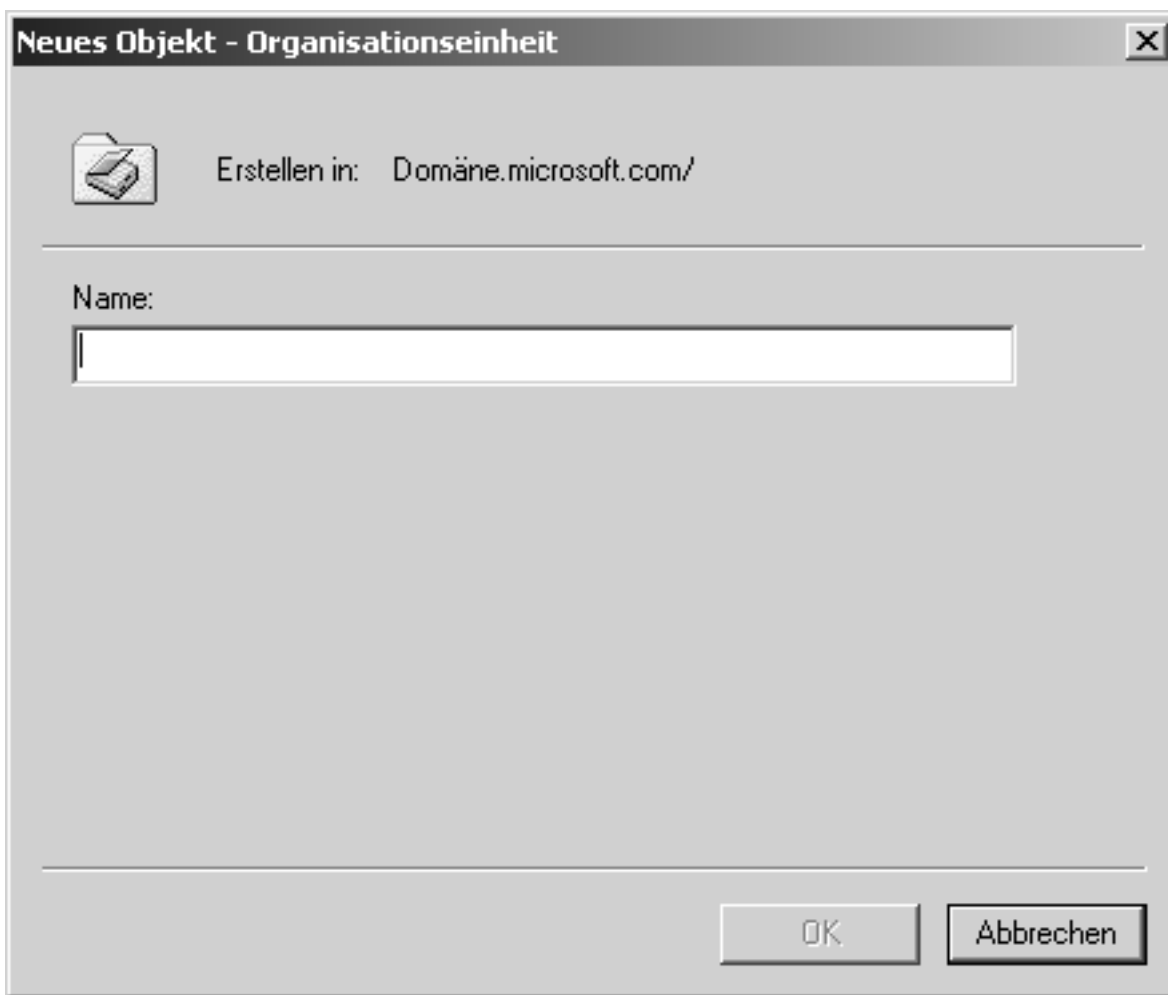


Abbildung 9.14: Das Dialogfeld zum Erstellen einer Organisationseinheit

Erstellen von Benutzern

Wie bereits erwähnt, sind Benutzerkonten die Basisobjekte für den Zugriff auf die Domäne in der Verzeichnisstruktur. Ein Benutzer muss authentifiziert werden und das machen die Benutzerkonten möglich. Benutzer ist der Kontoname, der verwendet wird, um auf die Domäne zuzugreifen. Dies ist das Basisobjekt, dem die Berechtigungen für Ressourcen und Richtlinien zugewiesen werden.

Um einen neuen Benutzer zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf die Domäne oder die Organisationseinheit, in der Sie den Benutzer erstellen möchten. Klicken Sie auf **Neu** und dann auf **Benutzer**.
2. Geben Sie den Vornamen ein und wechseln Sie in das Feld **Nachname**.
3. Geben Sie den Nachnamen ein und drücken Sie dann die (Tab)-Taste.
4. Das Feld **Vollständiger Name** wird entsprechend Ihren Angaben automatisch ausgefüllt.
5. Der Benutzeranmeldename ist der eigentliche Kontoname für den Zugriff auf die Domäne (z.B. tbraun, benutzer0129 usw.). Geben Sie den Benutzeranmeldenamen ein und drücken Sie dann die (Tab)-Taste.
6. Jetzt müssen Sie noch den Domänennamen oder das für diesen Benutzer gewählte UPN-Suffix eingeben. Drücken Sie anschließend die (Tab)-Taste.

7. Wenn Sie für den Benutzer einen anderen Benutzernamen haben möchten als den, der für ältere Systeme verwendet wird, können Sie diesen unter **Benutzeranmeldename (Windows NT 3.5x/4.0)** ändern. Wenn nicht, dann klicken Sie einfach auf **Weiter**.
8. Geben Sie das Kennwort des Benutzers ein, drücken Sie die (Tab)-Taste und bestätigen Sie dann das Kennwort.
9. Aktivieren Sie die gewünschten Optionen und klicken Sie dann auf **Weiter**.
10. Sehen Sie sich die Zusammenfassung an und klicken Sie auf **Fertig stellen**.

Erstellen von Gruppen

Damit Administratoren mehrere Benutzerkonten gleichzeitig bearbeiten können, verwendet der Verzeichnisdienst Gruppen. Unter einer Gruppe versteht man eine Reihe von Benutzerkonten und anderen Gruppen, deren Benutzerberechtigungen und Richtlinien gemeinsam verwaltet werden, womit erreicht wird, dass nicht jedes Benutzerkonto einzeln geändert werden muss.

Um eine Gruppe zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf die Domäne oder die Organisationseinheit, in der Sie die Gruppe erstellen möchten. Klicken Sie auf **Neu** und dann auf **Gruppe**.
2. Geben Sie den Gruppennamen ein und drücken Sie dann die (Tab)-Taste.
3. Wenn Sie einen Domänennamen haben, der mehr als 15 Zeichen umfasst, müssen Sie möglicherweise im Textfeld **Gruppenname (Windows NT 3.5x/4.0)** einen anderen Domänennamen eingeben. Drücken Sie dann die (Tab)-Taste.
4. Wählen Sie einen Gruppentyp aus und klicken Sie dann auf **OK**.

Erstellen von Computerkonten

Computer ist ein Konto, das für die Steuerung von Computerobjekten erstellt wird. Computerobjekte bieten dem Administrator die Möglichkeit, das Verhalten jedes Benutzers zu steuern, der sich an einem bestimmten Computer anmeldet. Auch wenn es sich bei dem Benutzer um einen Administrator handelt, gibt es möglicherweise bestimmte Aufgaben, für die ein Computer bestimmt ist, oder es gibt möglicherweise Sicherheitsgründe, derentwegen bestimmte Bereiche des Netzwerks für diesen Computer nicht zugänglich sind.

Um dieses Objekt zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf die Domäne oder die Organisationseinheit, in der Sie das Computerkonto erstellen möchten. Klicken Sie auf **Neu** und dann auf **Computer**.
2. Geben Sie den Namen des Computers ein, der Zugriff auf die Domäne haben soll.
3. Achten Sie darauf, dass Sie die Benutzer und Gruppen ändern, die Zugriff auf den Computer haben. Klicken Sie dazu auf **Ändern** und wählen Sie die entsprechende(n) Gruppe(n) und/oder Benutzer aus der Liste aus.
4. Klicken Sie auf **OK**.



Beachten Sie, dass die Standardeinstellung so ist, dass nur Mitglieder der Gruppe *Domänen- Admins* Zugriff haben. Das ist neu bei Windows und ein »geschlossen zu offen«-Teil des Systems. Windows-Systeme sind traditionell »offen zu geschlossen«, d.h., dass Ressourcen erstellt werden und dann zunächst für alle Benutzer offen sind.

Erstellen eines freigegebenen Ordners

Freigegebene Ordner ermöglichen Benutzern und anderen Verzeichnisobjekten über den Zugriff auf das Verzeichnis den Zugriff auf die auf dem Server freigegebenen Dateien. Ein freigegebener Ordner ist ein Active Directory-Objekt, das von Dateifreigaben erstellt wird, sodass die Freigabe als Teil des Verzeichnisses verwaltet werden kann. Das ist anders als bei der Netzwerkumgebung der Vergangenheit. Es stellt einen Fortschritt dar, da der Benutzer Ressourcen suchen kann, ohne das Netzwerk im klassischen Sinne von Microsoft tatsächlich zu durchsuchen.

Um dieses Objekt zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf die Domäne oder die Organisationseinheit, in der Sie das Ordnerobjekt erstellen möchten. Klicken Sie auf **Neu** und dann auf **Freigegebener Ordner**.
2. Geben Sie einen Objektnamen für den Ordner ein und drücken Sie dann die (Tab)-Taste.
3. Geben Sie die UNC-Adresse der Freigabe ein.
4. Klicken Sie auf **OK**.

Erstellen eines freigegebenen Druckers

Ebenso wie Ordnerobjekte Objekte sind, die Dateifreigaben über das Verzeichnis verfügbar machen, machen Druckerobjekte Druckerfreigaben verfügbar. Ein freigegebener Drucker ist ein Active Directory-Objekt, das von Druckerfreigaben älterer Windows-Versionen (Windows NT, 95/98 und WFW) erstellt wird, sodass die Freigabe als Teil des Verzeichnisses verwaltet werden kann.

Gehen Sie wie folgt vor, um ein Druckerobjekt zu erstellen:

1. Klicken Sie mit der rechten Maustaste auf die Domäne oder die Organisationseinheit, in der Sie das Druckerobjekt erstellen möchten. Klicken Sie auf **Neu** und dann auf **Drucker**.
2. Geben Sie die UNC-Adresse der Freigabe ein.
3. Klicken Sie auf **OK**.

9.5 Steuern des Benutzerzugriffs auf Ressourcen

Den Benutzer- und Gruppenkonten, denen Berechtigungen für den Zugriff auf eine Ressource zugewiesen werden sollen, werden diese Berechtigungen über das Dialogfeld **Eigenschaften** der entsprechenden Ressource zugewiesen. Wie bei vorhergehenden Versionen von Windows sollten Sie daran denken, dass jede Freigabe nach ihrer Erstellung für die Gruppe *Jeder* verfügbar ist (siehe Abbildung 9.15).



Abbildung 9.15: Anfängliche Berechtigungen

Für jede Freigabe gibt es das Dialogfeld **Eigenschaften**, das Sie aufrufen können, indem Sie wie bei jedem anderen Explorerobjekt zuerst mit der rechten Maustaste auf das Objekt klicken und dann die Option **Eigenschaften** wählen. Das trifft auch für Drucker- und Dateifreigaben zu. Dies ist allerdings die Stelle, an der viele Administratoren bei der Zuweisung von Berechtigungen Fehler machen.

9.5.1 Dateifreigabeberechtigungen

In diesem Dialogfeld gibt es zwei Bereiche, in denen Berechtigungen zugewiesen werden können. Auf der Registerkarte **Freigabe** befindet sich eine Schaltfläche mit der unschuldigen Aufschrift **Berechtigungen** (siehe Abbildung 9.16). Das ist etwas irreführend, da es eigentlich ein Überbleibsel vom alten Arbeitsgruppenmodell ist. Damit werden lediglich die Berechtigungen für den Ordner vom Netzwerk aus gesteuert. Wenn sich ein Benutzer lokal am Server anmelden kann, verwendet er die Berechtigungen auf der Registerkarte **Sicherheitseinstellungen**.

Am besten rufen Sie die Registerkarte **Sicherheitseinstellungen** auf. Dort können Sie Berechtigungen

sowohl für lokale als auch für Netzwerkbenutzer definieren. Sie müssen die Berechtigungen nicht auf beiden Registerkarten ändern, da die Berechtigungen auf der Registerkarte **Sicherheitseinstellungen** sowohl lokal als auch für das Netzwerk gelten. Wenn Sie auf eine Ressource über das Netzwerk zugreifen und auf einer oder auf beiden Registerkarten Einschränkungen definiert sind, gelten die strengsten Einschränkungen. Wenn beispielsweise auf der einen Registerkarte der Gruppe Buchhaltung die Berechtigung Vollzugriff zugewiesen ist, auf der anderen Registerkarte der Zugriff jedoch verweigert wird, dann haben die Mitglieder der Gruppe Buchhaltung keinen Zugriff. Wenn Sie sich dafür entscheiden, Berechtigungen über die Registerkarte **Sicherheitseinstellungen** zuzuweisen, haben Sie sich für die vollständige Kontrolle der Ressource entschieden.

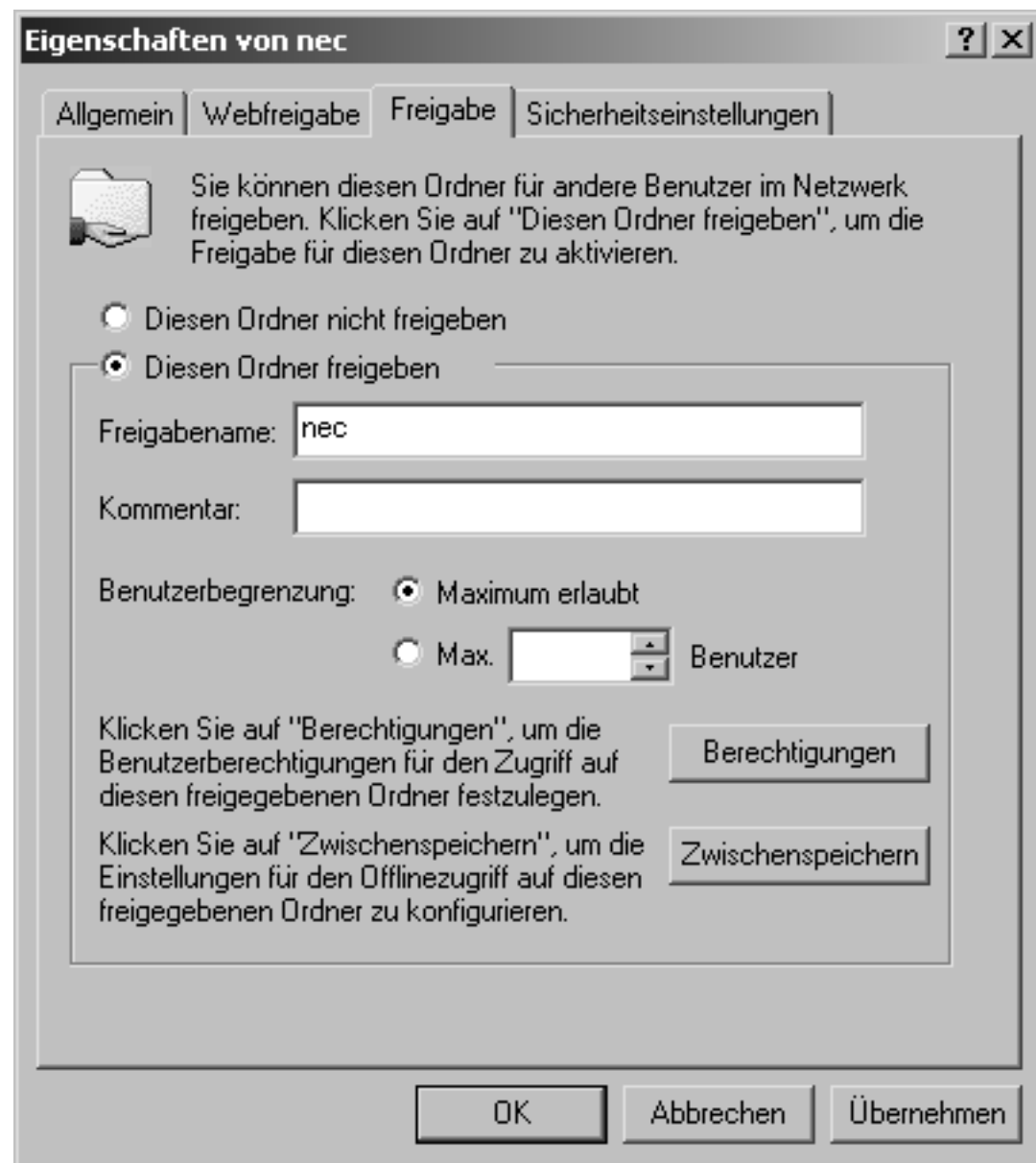


Abbildung 9.16: Die Registerkarte Freigabe



Die Registerkarte **Sicherheitseinstellungen** wird nur angewendet, wenn sich die entsprechende Freigabe in einer NTFS-Partition befindet. Es empfiehlt sich nicht, dass Sie einen Bereich in einer FAT-Partition freigeben. FAT-Partitionen sind auf lokaler Ebene nicht gesichert.

Objekte in einem Container erben bei ihrer Erstellung standardmäßig die Berechtigungen dieses

Containers. Wenn Sie beispielsweise den Ordner *Programme* erstellen, erben sämtliche in diesem Ordner erstellten untergeordneten Ordner und Dateien automatisch die Berechtigungen dieses Ordners. Somit verfügt der Ordner **Programme** über explizite Berechtigungen, während sämtliche untergeordneten Ordner und Dateien über vererbte Berechtigungen verfügen.

Berechtigungen für Active Directory-Objekte haben mit der Fähigkeit zu tun, auf Objekte zugreifen und Änderungen an diesen Objekten vornehmen oder Objekte innerhalb der Objekte erstellen zu können. Das alles hängt natürlich von der Art des Objekts ab.

Die Berechtigungen, die einem Ordner zugewiesen werden können, sind in Tabelle 9.1 aufgeführt.

Berechtigungen	Vollzugriff	Ändern	Lesen und Ausführen	Ordnerinhalt auflisten	Lesen	Schreiben
Ordner durchsuchen/Datei - ausführen	X	X	X	X		
Ordner auflisten/Daten lesen	X	X	X	X	X	
Attribute lesen	X	X	X	X	X	
Erweiterte Attribute lesen	X	X	X	X	X	
Dateien erstellen/Daten -schreiben	X	X				X
Ordner erstellen/Daten -anhängen	X	X				X
Attribute schreiben	X	X				X
Erweiterte Attribute schreiben	X	X				X
Untergeordnete Ordner und -Dateien löschen	X					
Löschen	X	X				
Berechtigungen lesen	X	X	X	X	X	X
Berechtigungen ändern	X					
Besitz übernehmen	X					

Synchronisieren	X	X	X	X	X	X

Tabelle 9.1: Ordnerberechtigungen

Es gibt zwei Arten von Berechtigungen:

- *Explizite Berechtigungen*: Berechtigungen, die einem Benutzer oder einer Gruppe im Dialogfeld **Eigenschaften** des jeweiligen Objekts zugewiesen werden, werden als explizite Berechtigungen bezeichnet.
- *Vererbte Berechtigungen*: Eine Berechtigung ist vererbt, wenn der Benutzer oder die Gruppe die Berechtigung von einem übergeordneten Container des Objekts übertragen bekommen hat.

Bevor Sie Berechtigungen von einem Benutzer für ein bestimmtes Objekt entfernen können, müssen Sie das Kontrollkästchen **Vererbbare übergeordnete Berechtigungen übernehmen** deaktivieren (siehe Abbildung 9.17). Danach können Sie die Berechtigungen nach Belieben an Ihre Bedürfnisse anpassen. Sie werden feststellen, dass die Gruppe Jeder aus der Liste der berechtigten Benutzer verschwindet.

Um Berechtigungen hinzuzufügen bzw. zu entfernen, gehen Sie wie folgt vor:

1. Klicken Sie auf **Hinzufügen**.
2. Wählen Sie einen Benutzer oder eine Gruppe aus, klicken Sie auf **Hinzufügen** und dann auf **OK**.
3. Nehmen Sie die gewünschten Änderungen vor, indem Sie die entsprechenden Kontrollkästchen aktivieren bzw. deaktivieren. Klicken Sie dann auf **OK**.

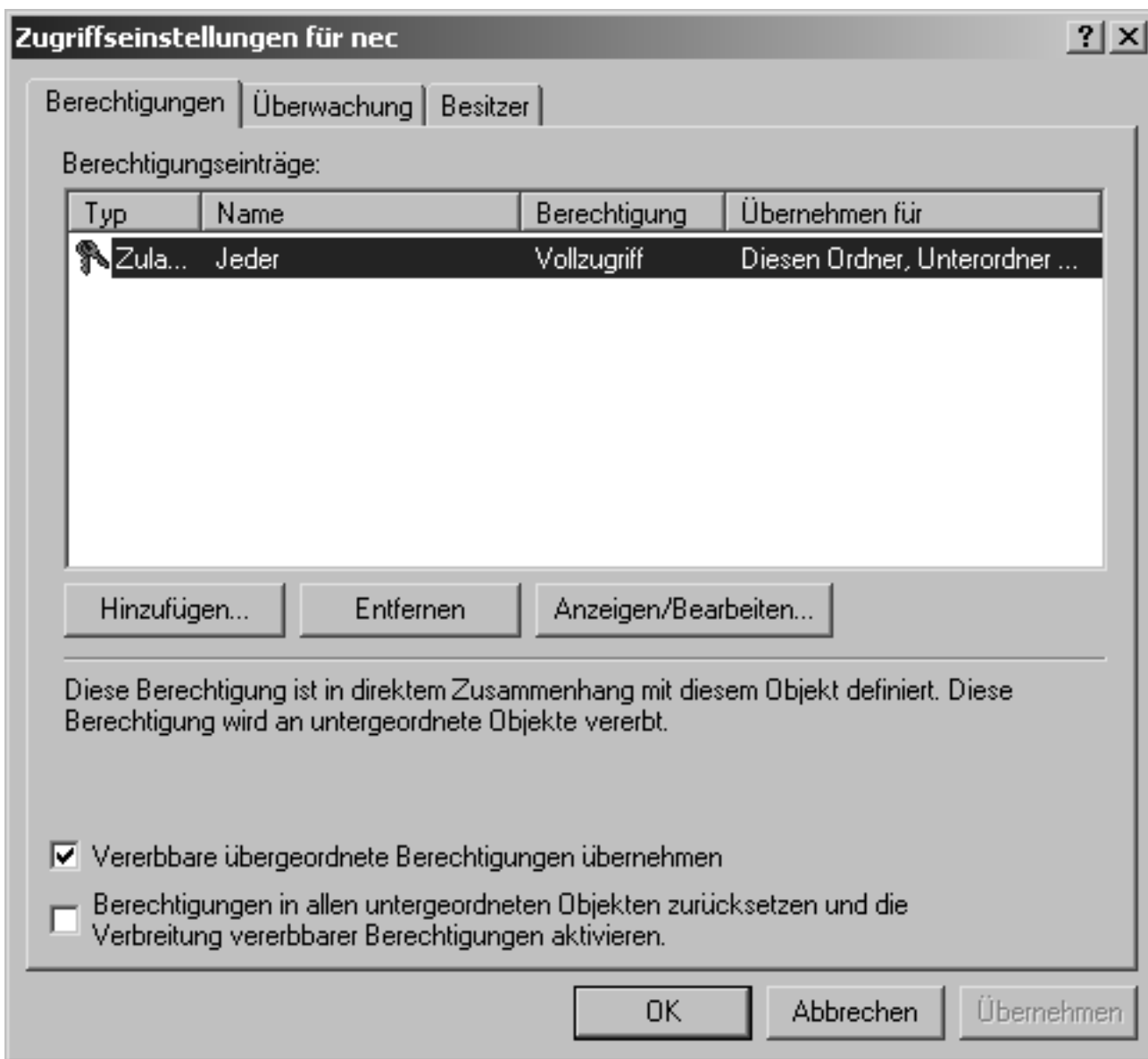


Abbildung 9.17: Vererbung deaktivieren



Denken Sie daran, dass Sie die Gruppe *Organisations-Admins* immer mit der Berechtigung Vollzugriff zur Liste der Berechtigungen hinzufügen, bevor Sie dieses Fenster schließen. Die Gruppe kann die Berechtigungen später immer noch ändern, um Zugriff zu bekommen, aber es wird sehr mühevoll sein, dies zu tun.

9.5.2 Druckerberechtigungen

Druckerberechtigungen können Sie nur über die Registerkarte **Sicherheitseinstellungen** zuweisen. Diese Berechtigungen sind nicht annähernd so kompliziert wie die bei den eben beschriebenen Objekten.

Mit den Druckerberechtigungen soll in der Regel eine kostspielige Ressource geschützt werden. Der neue 20.000-DM-Farbdrucker/Kopierer muss nicht unbedingt das persönliche Malbuch des neugierigen Fünfjährigen eines Angestellten (oder gar des Angestellten selbst) sein. Daher bietet Ihnen die Registerkarte **Sicherheitseinstellungen** die Möglichkeit zu bestimmen, wer auf dem Drucker drucken darf, wer für die Papierversorgung und Verwaltung zuständig ist und wer die Druckaufträge anderer überwachen soll.

Es gibt drei Kategorien von Druckerberechtigungen:

- *Drucken*. Die Berechtigung, Druckaufträge an eine Druckerfreigabe zu senden und die eigenen Dokumente zu kontrollieren.
- *Dokumente verwalten*. Die Berechtigung Drucken sowie die Berechtigung, die Dokumente anderer zu kontrollieren.
- *Drucker verwalten*. Die Berechtigung Dokumente verwalten sowie die Berechtigung, Druckereigenschaften zu ändern und Druckerfreigaben zu löschen.

© Copyright [Markt+Technik Verlag](#), ein Imprint der Pearson Education Deutschland GmbH
Elektronische Fassung des Titels: Windows 2000 Server Kompendium, ISBN: 3-8272-5611-9 Kapitel:
Verzeichnis- und Zugriffskonzepte

Kapitel 10 Struktur des Active Directory

Wenn Sie wissen, was Active Directory ist und wie es gestartet wird, bedeutet das noch lange nicht, dass Sie im Entwickeln von Verzeichnisstrukturen gut sind. Um da gut zu werden, benötigen Sie die Kenntnisse, die Sie in Kapitel 5 gewonnen haben und einige der Informationen über Verzeichnisse aus Kapitel 9 sowie gesunden Menschenverstand. Das Ganze ist ein bisschen so wie das Entwerfen von Gebäuden. Nur weil Sie ein Programm zum Entwerfen von Häusern kaufen können, bedeutet das nicht, dass das von Ihnen entworfene Haus gebaut werden kann, ohne dass die Wände einstürzen. Architekten müssen nicht nur wissen, wie man ein Gebäude schön gestaltet, sie müssen dafür sorgen, dass das Gebäude den täglichen Belastungen standhalten kann.

Auch das Active Directory ist täglichen Belastungen ausgesetzt. LAN-Verkehr kann das Verzeichnis verlangsamen, WAN-Verkehr kann es vollkommen lahm legen und aufgrund von unlogischen Anordnungen von Objekten kann es dazu kommen, dass das Verzeichnis praktisch nutzlos wird. Um ein Verzeichnisarchitekt zu werden, müssen Sie wissen, wo eine Stützmauer, wo ein Sturz und wo eine Stahlbetondecke erforderlich ist. Oder anders ausgedrückt: Sie müssen wissen, wo das gesamte Verzeichnis zu unterteilen ist, wann es nicht zu unterteilen ist und wie Sie den Wünschen der politischen Kräfte entsprechen können.

Witzig, aber wahr: Lassen Sie Active Directory-Designs nicht an der Wand hängen. Vorgesetzte und Manager könnten diese als Organisationsdiagramme missverstehen und sich einmischen. Wie Sie gleich erfahren werden, kann ein Verzeichnis, das allein auf politischen Strukturen basiert, nicht verwaltet werden und reicht selten an IT-Zielsetzungen heran.

:-)
TIPP

Aber nicht für jedes Verzeichnis ist ein »Architekt« erforderlich. Dieses Kapitel nützt vor allem denjenigen Administratoren, die Verzeichnisse mit mehr als einer Domäne oder zumindest mehreren Organisationseinheiten planen. Da bereits beschrieben wurde, wie ein Domänencontroller zu Beginn konfiguriert wird, wird dies hier nicht wiederholt werden. Stattdessen wird es hier um Verzeichnisse mit mehreren Domänencontrollern, um Organisationseinheiten, um Strukturen und Gesamtstrukturen gehen.

10.1 Standorte und Replikation

Die Replikation von Domäneninformationen über das Netzwerk ist der Hauptgrund dafür, dass Sie versuchen sollten, das Verzeichnis besser zu strukturieren. Damit sich Benutzer am Netzwerk anmelden und die Ressourcen sowie das Sicherheitssystem nutzen können, ist es erforderlich, dass die Domäneninformationen dort zur Verfügung stehen, wo die Benutzer sind. Wenn also Brigitte das Büro in Düsseldorf verlässt und in das Zweigbüro in München geht, muss sie immer noch in der Lage sein, sich anmelden und auf die Datenträger, die ihre Daten enthalten, zugreifen sowie die Verzeichnisressourcen nutzen zu können.

Domänencontroller in einer einzelnen Domäne replizieren Informationen zeitbasiert. Wenn am Kennwort von Brigitte in Düsseldorf eine Änderung vorgenommen wird, sollte der Domänencontroller in München die Aktualisierung der Informationen erhalten und die Änderung aufzeichnen. Wenn der Administrator in München Brigittes Kennwort zur gleichen Zeit ändert, werden die Änderungen aufgezeichnet und die

zeitlich zuletzt vorgenommene Änderung ist die Änderung, die letztlich aufgezeichnet bleibt.

Um verstehen zu können, wie die Replikation funktioniert, müssen Sie zwei grundlegende Elemente des Netzwerks verstehen: Standorte und Domänen. Domänen wurden bereits ausführlich beschrieben. Das, was Sie wissen müssen, um Replikationen und Verzeichnisstrukturen zu verstehen, ist die Tatsache, dass eine Domäne eine logische Einheit ist. Oder anders ausgedrückt: Ein Benutzer könnte denselben physikalischen Rechner und dieselbe IP-Adresse wie ein anderer Benutzer verwenden und dennoch als ein in einer anderen Domäne befindlicher Benutzer betrachtet werden. Die beiden Benutzer befinden sich physikalisch im gleichen Bereich, logisch jedoch nicht.

10.1.1 Standorte

Standorte bringen eine andere Art der Trennung mit sich. Systeme am gleichen Standort sind Standorte, die im Grunde eine physikalische Struktur gemein haben. Man kann sich diese am einfachsten als System im gleichen LAN vorstellen, weil ein Standort eine Sammlung von Systemen ist, die einander über ein Netzwerk mit einer schnellen WAN-Verbindung mit mindestens 1,5 Mbit/s erreichen können sollten.

Standorte können zahlreiche Domänen enthalten, da es sich vielmehr um einen physikalischen bzw. Netzwerkstandort als um einen logischen Standort handelt. Umgekehrt kann sich eine Domäne über mehrere Standorte erstrecken. Die zentrale Frage bei der Planung ist die Netzwerkgeschwindigkeit zwischen den Mitgliedern des Standorts.



Standorte werden häufig basierend auf IP-Subnetzen erstellt, da sich IP-Subnetze häufig im gleichen LAN und damit in einem Netzwerk befinden, das Geschwindigkeiten über 2 Mbit/s erreicht. Daher befinden sich zwei Server, die in unterschiedlichen Subnetzen konfiguriert worden sind, häufig an unterschiedlichen Standorten.

Domänencontroller replizieren Verzeichnisänderungen zuerst an Domänencontroller am eigenen Standort. Replikationen außerhalb des Standorts erfolgen weniger häufig. Standardmäßig erfolgen Replikationen zwischen Standorten alle 180 Minuten.

Wenn ein Client eine Verbindung zum Netzwerk herstellt, gibt er an, an welchem Standort er sich befindet. Wenn ein Client von einer Domäne aus eine Anforderung versendet, leitet der Client diese Anforderungen an Domänencontroller an seinem Standort. Dadurch wird vermieden, dass über die gesamte WAN-Struktur hinweg willkürlich Verkehr entsteht. Damit verfügt der Client über eine Active Directory-Beziehung, die so effektiv wie möglich ist.

Standorte unterscheiden genau zwischen der Implementierung von Verzeichnisdiensten von Microsoft und von anderen Anbietern (wie z.B. Novell), da Standorte dafür sorgen, dass Domänen, Strukturen und Gesamtstrukturen von der Replikation unberührt bleiben. Replikation bedeutet somit etwas anderes.

10.1.2 Replikation

Domänencontroller verfolgen die Änderungen, die im Verzeichnis vorgenommen wurden, sowie die Zeiten, zu denen diese Änderungen erfolgt sind. Basierend auf einem Zeitplan prüfen die Domänencontroller, ob andere Controller im Verzeichnis Änderungen im Verzeichnis vorgenommen haben. Wenn Änderungen erkannt werden, fordert der Controller eine Aktualisierung der Elemente, die

seit der letzten Aktualisierung geändert worden sind.

Damit dieselben Informationen nicht immer und immer wieder repliziert werden, unterstützen Domänencontroller die *Eigenschaft für ursprüngliche Schreibvorgänge*. Dabei wird verfolgt, welche Attribute in einer Aktualisierung geändert worden sind und wie häufig die Eigenschaft des Objekts für ursprüngliche Schreibvorgänge erhöht worden ist. Eine Änderung, durch die der Zähler »Eigenschaft für ursprüngliche Schreibvorgänge« erhöht wird, weist auf eine vom Client vorgenommene Objektänderung hin und nicht auf eine Änderung, die während der Replikation aktualisierter Verzeichnisinformationen von Active Directory vorgenommen wurde. Wenn der Domänencontroller in Denver die Mitteilung erhält, dass ein Objekt im Verzeichnis des Domänencontrollers in Indianapolis geändert wurde, überprüft dieser, ob die Eigenschaft für ursprüngliche Schreibvorgänge festgelegt wurde. Wenn dies nicht der Fall ist, erfolgt für das Verzeichnis in Denver keine Replikation.



Active Directory-Domänencontroller suchen automatisch die effizienteste Möglichkeit für die Replikation eines Standortes. Sie können Verbindungen manuell hinzufügen oder konfigurieren und die Replikation über eine bestimmte Verbindung erzwingen. Es ist jedoch besser, wenn die Replikation aufgrund der von den Active Directory-Standorten und -Diensten zur Verfügung gestellten Informationen automatisch optimiert wird.

Im Folgenden einige Funktionen zur Standortoptimierung:

- gelegentliche Neubewertung der verwendeten Verbindungen und die anschließende Nutzung des effizientesten Pfades
- Auswahl mehrerer Routen für die Replikation von Änderungen, und dadurch Gewährleisten von Fehlertoleranz
- Replikation nur von geänderten Informationen

10.1.3 Erstellen von Standorten

Standorte sind bei der Optimierung des Verzeichnisverkehrs sehr hilfreich. Das bedeutet jedoch nicht, dass Standorte automatisch aufgrund von Verkehrsbedürfnissen eingerichtet werden. Standorte dienen dem Administrator zur Verbesserung der Leistung des Verzeichnisses und des Netzwerks. Standorte werden in der Konsole **Active Directory-Standorte und -Dienste** erstellt (siehe Abbildung 10.1). Ein erster Standort mit der Domäne und dem Verzeichnis wird automatisch erstellt. Jeder weitere Standort muss dann jedoch vom Administrator manuell erstellt und aufgefüllt werden.

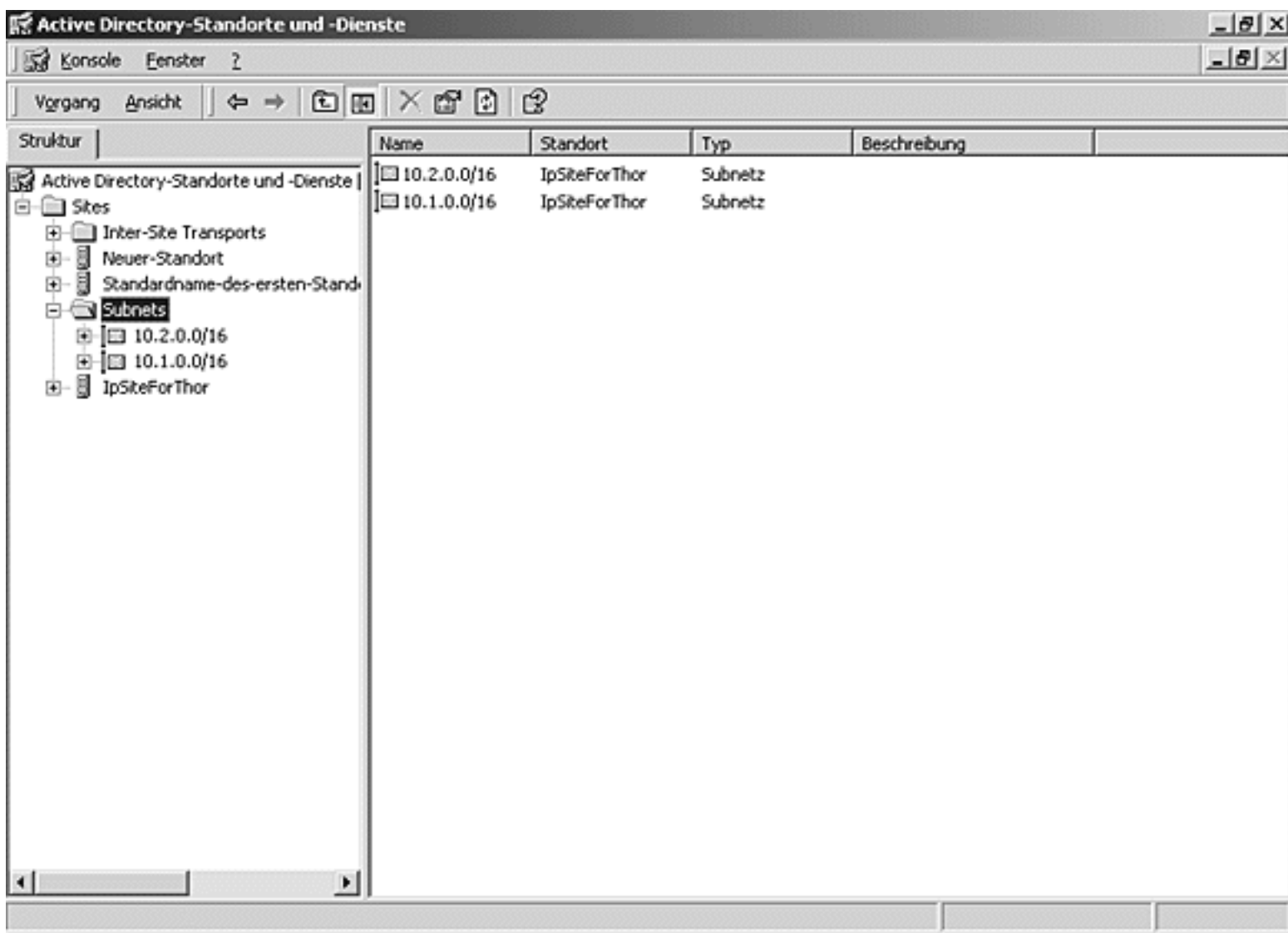


Abbildung 10.1: Erstellen eines Standorts

Um einen neuen Standort zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf den Ordner **Sites** und klicken Sie dann auf **Neuer Standort**.
2. Geben Sie den Namen des neuen Standorts ein.
3. Klicken Sie auf ein Standortverknüpfungsobjekt und dann zweimal auf **OK**, um die Dialogfelder zu bestätigen.
4. Klicken Sie mit der rechten Maustaste auf den Ordner **Subnets** und wählen Sie die Option **Neues Subnetz**.
5. Geben Sie die Subnetzadresse und Subnetzmaske ein und klicken Sie dann auf den Standortnamen, der mit dem Subnetz verknüpft werden soll. Bestätigen Sie über **OK** (siehe Abbildung 10.2).
6. Verschieben Sie einen Domänencontroller von einem bestehenden Standort, indem Sie mit der rechten Maustaste auf den Server-Namen klicken, dann die Option **Verschieben** und anschließend den gewünschten Standort wählen. Klicken Sie auf **OK**.

Neues Objekt - Subnetz

Erstellen in: Domäne.microsoft.com/Configuration/Sites/Subnets

Adresse: 10 . 1 . 0 . 0

Maske: 255 . 255 . 0 . 0

Name: 10.1.0.0/16

Geben Sie eine Subnetzadresse und -maske ein. Dies wird automatisch in einen Subnetznamen in Form von Netzwerk/Bits-Mask übersetzt.
Beispiel: Adresse 10.14.209.14, Maske 255.255.240.0 wird zu Subnetz 10.14.208.0/20.

Wählen Sie ein Standortobjekt für dieses Subnetz.

Standortname

- IpSiteForThor
- Neuer-Standort
- Standardname-des-ersten-Standorts

OK Abbrechen

Abbildung 10.2: Erstellen eines Subnetzes

Bei der Erstellung einer Standortverknüpfung verwenden Sie ein so genanntes *Standortverknüpfungsobjekt*. Dieses Objekt fällt nicht einfach so vom Himmel. Es wird erstellt, wenn das Verzeichnis erstellt wird. DEFAULTIPSITELINK wird beim Einrichten der Domäne und des Verzeichnisses erstellt. Diese Verknüpfung ist für den Standort Standard-Name-des-ersten-Standorts verantwortlich (so heißt der als Erstes erstellte Standort wirklich). Damit die Standortverknüpfung überhaupt einen Zweck erfüllt, benötigen Sie natürlich mehr als nur einen Standort.

TIPP :-)

Den fabelhaften Namen des ersten Standortobjekts (Standard-Name-des-ersten-Standorts und DEFAULTIPSITELINK) können Sie übrigens ändern, indem Sie mit der rechten Maustaste auf das Objekt klicken und die Option **Umbenennen** wählen.

Wenn zwischen physikalischen Standorten mehrere Kommunikationsmethoden verwendet werden, sollten Sie mehrere Standortverknüpfungen erstellen, um Fehlertoleranz zu gewährleisten. In einem Szenario, in dem ein Unternehmen über zwei WAN-Verbindungen verfügt, sollte eine weitere Standortverknüpfung erstellt werden, für den Fall, dass eine ausfällt.

Um die Nutzung dieser Verknüpfungen zu steuern, können Sie für jede Standortverknüpfung die Einstellungen **Kosten** und **Replizieren alle** definieren. Damit können Sie die gewünschte Verknüpfung festlegen (siehe Abbildung 10.3). Je geringer die Kosten, desto häufiger wird die Verknüpfung verwendet. Die Einstellung **Replizieren alle** wird verwendet, um die Replikationsfrequenz festzulegen.



Abbildung 10.3: Das Dialogfeld Eigenschaften der Verknüpfung

10.2 Strukturstandards

Die eigentliche Struktur der Verzeichnisobjekte ist in der Active Directory-Welt etwas offener. Die Entwicklung der Domänenstruktur erfordert dennoch ein ordentliches Maß an Planung.

Folgende Verzeichnisstrukturen stehen zur Verfügung:

- *Politische Struktur*. Dabei erfolgt die Strukturierung anhand der Abteilungen und anhand

politischer Strukturen im Unternehmen. In diesem Fall bilden die Abteilungen und Unternehmensbereiche eines Unternehmens die Domänen, die Domänenstrukturen und die Gesamtstrukturen (z.B. `Marketing.Unternehmen.com`, `Operationen.Unternehmen.com` und `Finanzierung.Unternehmen.com`).

- *Geografische Struktur*. Dabei erfolgt die Strukturierung anhand der geografischen Standorte. In diesem Fall bilden Gebäude und Länder die Domänen, die Domänenstrukturen und die Gesamtstrukturen (z.B. `Paris.Unternehmen.com`, `Asien.Unternehmen.com` und `Nordostamerika.Unternehmen.com`).

Der Einsatz politischer oder geografischer Grenzen erfolgt beiderseitig nicht ausschließlich. Damit Sie die Gründe für die Verwendung der einen oder anderen Struktur nachvollziehen können, sollen hier die Vor- und Nachteile dieser Basisstrukturen erläutert werden. Dann können Sie selbst entscheiden, ob es sinnvoll ist, eine Struktur wie

`Vizepräsidenten.Marketing.Ost.Paris.Unternehmen.com` zu haben.

10.2.1 Politische Struktur

Das politische Modell könnte als das »Abteilungs- oder Unternehmensbereichsmodell« bezeichnet werden, da es sich am besten für Unternehmen eignet, die rigoros nach Abteilungen oder Unternehmensbereichen gegliedert sind. Viele Unternehmen sind nicht so strikt nach Abteilungen oder Unternehmensbereichen gegliedert, sodass manche Angestellte nicht einmal wissen, dass bestimmte Unternehmensbereiche noch zum gleichen Unternehmen gehören. Die Strukturierung muss nicht so streng sein, um dieses Modell (oder Teile davon) zu realisieren, aber die Unternehmensbereiche müssen relativ stark sein.

Der Grund dafür ist der, dass sich dieses Modell an Unternehmensbereiche anlehnt, die ihre eigenen Systeme selbst verwalten müssen. Wenn der Server oder die Verteilung der Benutzer eines anderen Unternehmensbereichs nicht verwaltet wird, dann sollte dieses Modell angewendet werden.

Das Konzept ist relativ einfach. Domänen werden zunächst so erstellt, dass sie die organisatorische Struktur reflektieren. Dabei wird mit dem Namen des Unternehmens begonnen und nach und nach die darunter liegenden Unternehmensbereiche und danach die Abteilungen angeschlossen (siehe Abbildung 10.4).

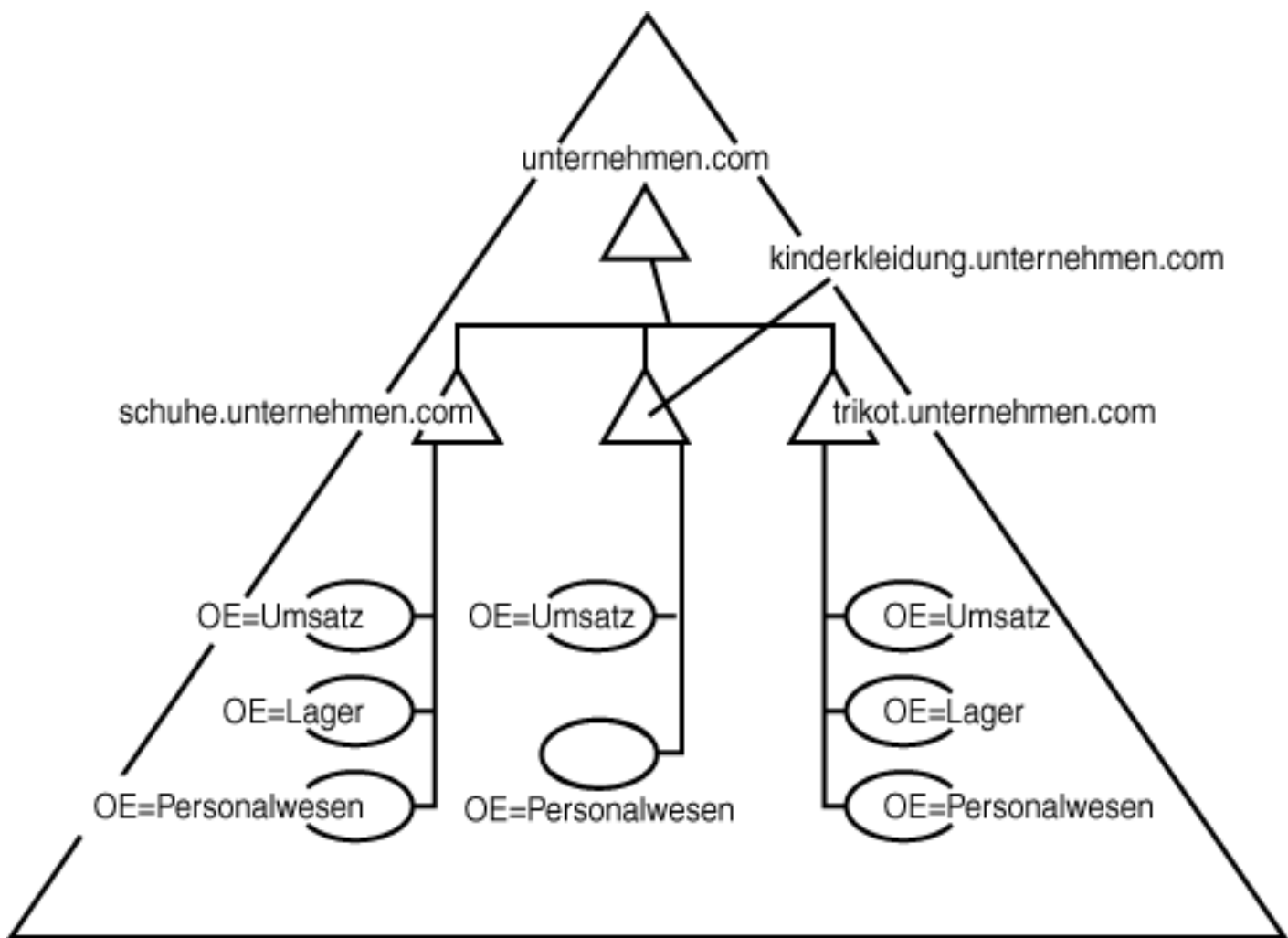


Abbildung 10.4: Ein politischer Plan

Aufgrund der Übereinstimmung mit den Unternehmensbereichen ist es sehr einfach, IT-Kosten und Verantwortung zu trennen. Es wird weniger über Router und Konnektivität als vielmehr darüber diskutiert, wer verantwortlich ist und wer wohin passt.

Bei diesem Modell ist es viel einfacher, die DNS-Namen zu erstellen und zu verwalten, weil die Benennung der internen Ressourcen dem Namensplan folgt, der verwendet wird, um die Unternehmensbereiche zu vermarkten. Es ist wirklich einfach zu sagen, was mit der Domäne `schuhe.unternehmen.com` gemeint ist.

Die Probleme, die bei diesem Plan entstehen können, ergeben sich aus dem Wachstum des Unternehmens, aus Firmenzusammenschlüssen und -aufteilungen. Wenn beispielsweise die Unternehmensbereiche »Kinderkleidung« und »Trikot« zusammengeschlossen und sämtliche Server, Benutzer, Drucker und möglichst alle Organisationseinheiten in den neu zusammengeschlossenen Unternehmensbereich verschoben werden, wird das Ganze schnell schwerfällig und schwierig zu verwalten.

Die Netzwerkeffizienz wird durch diesen Plan nicht verbessert. Wenn sämtliche Unternehmensbereiche eine gemeinsame Personalabteilung haben, die in einem Gebäude untergebracht ist, dann sollten Überlegungen bezüglich des WAN-Verkehrs angestellt werden. Dazu könnte das gesamte Unternehmen im gleichen Gebäude untergebracht werden, was zu einer lächerlichen Verwirrung für die Benutzer und

Administratoren gleichermaßen führen würde.

10.2.2 Geografische Struktur

Das geografische Modell ist für Unternehmen gedacht, die sich tatsächlich über geografisch unterschiedliche Bereiche erstrecken. Anders ausgedrückt: Wenn Ihr Unternehmen heute aus mehr als einem Standort besteht oder in Zukunft expandieren und mehrere Standorte einrichten möchte, dann sollten Sie ein geografisches Modell in die Planung Ihrer AD-Struktur einbeziehen. Wenn Ihr Unternehmen immer im gleichen Gebäude sein wird, werden Sie sich wohl kaum ausführlich mit der Erstellung einer großen Verzeichnisstruktur befassen.

Das Konzept, ein Verzeichnis anhand eines geografischen Modells zu strukturieren, basiert auf dem Gedanken, ein Verzeichnis aufgrund von IT- und Netzwerkgrenzen zu gliedern. Wenn also das Netzwerk entlang einer WAN-Grenze geteilt oder in Sicherheitsabschnitte unterteilt werden muss, sollte ein neues Containerobjekt erstellt werden (siehe Abbildung 10.5).

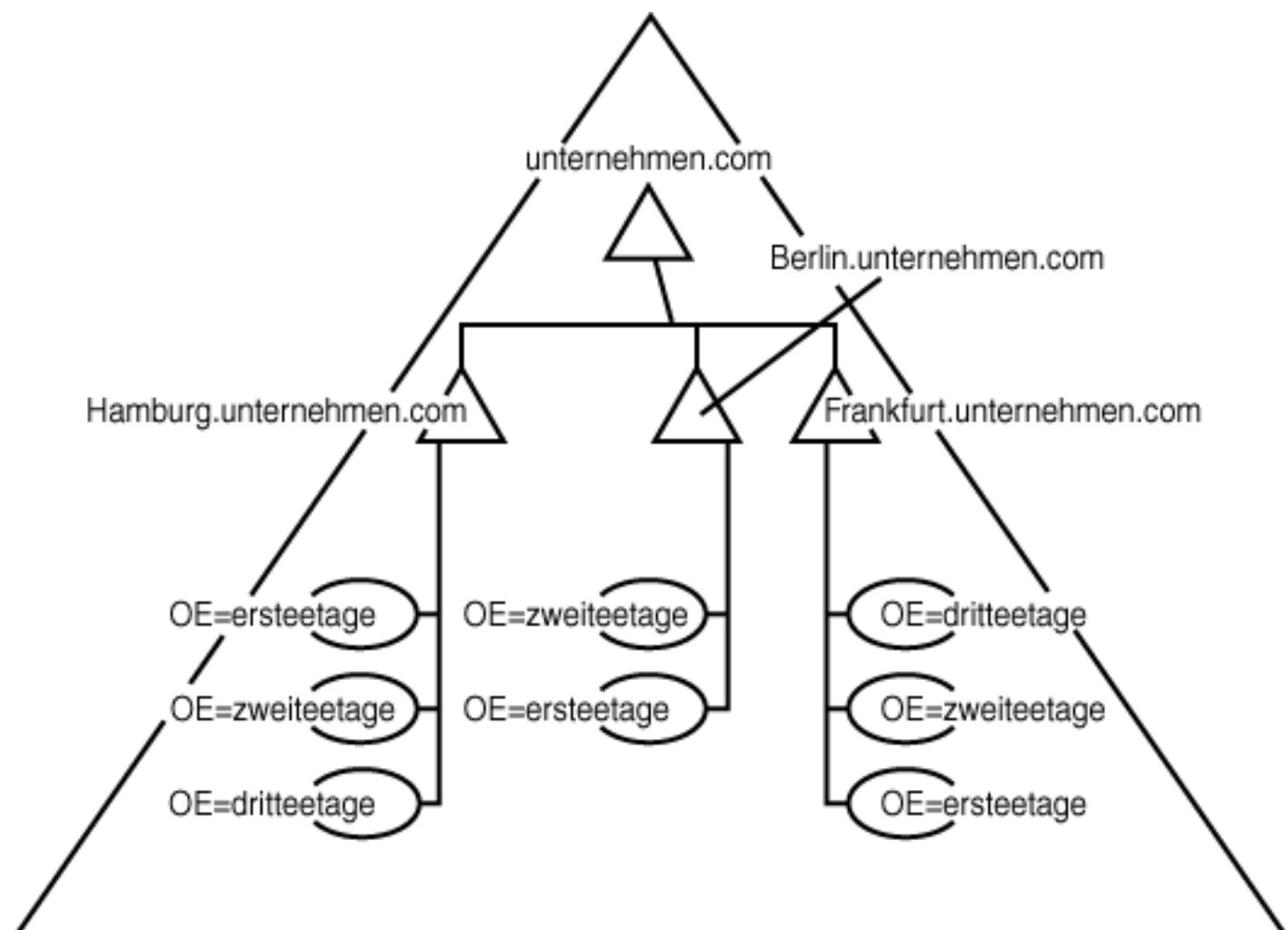


Abbildung 10.5: Geografisches Modell

Das geografische Modell macht es möglich, dass Benutzer und Systeme basierend auf den Standorten, an denen sie sich befinden, verwaltet werden. Dieses Modell eignet sich besser für das Paradigma, das von Netzwerkadministratoren bzw. IT-Abteilungen für die Verwaltung von Benutzern und Ressourcen verwendet wird. Wenn Bernd als Mitglied der Abteilung Buchhaltung für die Abteilung Schuhe

verantwortlich ist und ihm dann die Verantwortung für die Abteilung Trikots übertragen wird, hat das keine Auswirkungen auf den Verzeichnisplan. Wenn die Abteilungen Schuhe und Trikots zusammengeschlossen werden, haben lediglich die Versetzungen und Entlassungen von Angestellten Auswirkungen auf das System.

Die Replikation der Verzeichnisstruktur und sämtliche Änderungen werden ebenfalls vereinfacht, da die Standortverknüpfungen im Wesentlichen den Domänen entsprechen.

Das Problem dabei ist natürlich die Politik. Wenn sich die beiden Abteilungen Kinderkleidung und Schuhe nicht vertragen, wird es für den Administrator schwierig sein, für die gemeinsame Nutzung von Ressourcen Zustimmung zu bekommen. Wenn die Domänen und Organisationseinheiten, die diese Gruppen enthalten, miteinander vermischt sind, wird es nahezu unmöglich, die Benutzer und Gruppen auseinander zu halten.

10.2.3 Gemischte Struktur

Das Designpotenzial und die Grenzen von Active Directory werden in der Regel zu einer »gemischten Struktur« führen. Die Erläuterung der geografischen und politischen Modelle bedeutet nicht, dass die Umgebung nicht basierend auf weniger strikten Grenzen unterteilt werden kann. Es kann sinnvoller oder auch besser verwaltbar sein, wenn bestimmte Elemente anhand von nicht geplanten Grenzen gegliedert werden.

Wenn in dem Beispiel von oben den einzelnen Unternehmensbereichen die Abteilung Personalwesen gemein ist, diese Abteilung jedoch in allen Gebäuden vertreten sein muss, dann wurde eine gebräuchliche Trennlinie gefunden. Bei einem rein geografischen Modell wäre bei dieser Unterteilung nach Unternehmensbereichen die getrennte Verwaltung dieser Gruppe nicht möglich. Aufgrund des einheitlichen Bedarfs an einer Personalabteilung kann es erforderlich sein, dass diese Strukturierung trotz des Masterplans vorgenommen wird.

Der Schlüssel zum Erfolg Ihres Modells und Ihrer nachfolgenden Implementierung des Active Directory wird die politischen und geografischen Bedürfnisse ausgleichen und einfach vernünftig sein. Lassen Sie die Active Directory-Struktur für sich arbeiten. Wenn Sie bei einer Struktur bleiben, haben Sie eine bessere Kontrolle über die Umgebung. Wenn es jedoch mehr Arbeit macht, bei der Struktur zu bleiben, dann sollte dies natürlich berücksichtigt werden.

10.3 Organisationseinheiten

Organisationseinheiten werden in erster Linie erstellt, um die Verantwortung und Verwaltung aufzuteilen. Dabei handelt es sich nicht um Gruppen, die nur für die Zuweisung von Berechtigungen verwendet werden. Mittels Organisationseinheiten werden vielmehr administrative Bereiche zugewiesen.

Wenn beispielsweise die Personalabteilung in ihrer eigenen Abteilung Benutzer erstellen und die Berechtigungen für die Informationen in diesen Benutzerobjekten verwalten muss, sollte die Organisationseinheit Personalwesen erstellt werden.

Wenn der Supervisor der Gruppe Auftragsannahme Druckaufträge stoppen und Konten von Benutzern in seiner Abteilung deaktivieren können muss, ist es mit Hilfe einer Organisationseinheit möglich, dass der

Administrator diese Berechtigungen zuweist.

Um einer Organisationseinheit Berechtigungen zuzuweisen, gehen Sie wie folgt vor:

1. Öffnen Sie die Konsole **Active Directory-Benutzer und -Computer**.
2. Klicken Sie mit der rechten Maustaste auf die Organisationseinheit, der Sie Berechtigungen zuweisen möchten, und wählen Sie die Option **Objektverwaltung zuweisen**.
3. Klicken Sie auf **Weiter**, um den **Assistenten zum Zuweisen der Objektverwaltung** zu starten.
4. Klicken Sie auf **Hinzufügen**, um einen Benutzer oder eine Gruppe aus der Domäne auszuwählen (siehe Abbildung 10.6).
5. Klicken Sie auf den Benutzer, den Sie hinzufügen möchten, und klicken Sie dann auf die Schaltfläche **Hinzufügen**. Wiederholen Sie diesen Vorgang, bis Sie alle gewünschten Benutzer ausgewählt haben. Klicken Sie auf **OK**.
6. Klicken Sie auf **Weiter** und wählen Sie die Aufgaben, die Sie jeweils delegieren möchten. Klicken Sie schließlich auf **Weiter** und dann auf **Fertig stellen**.

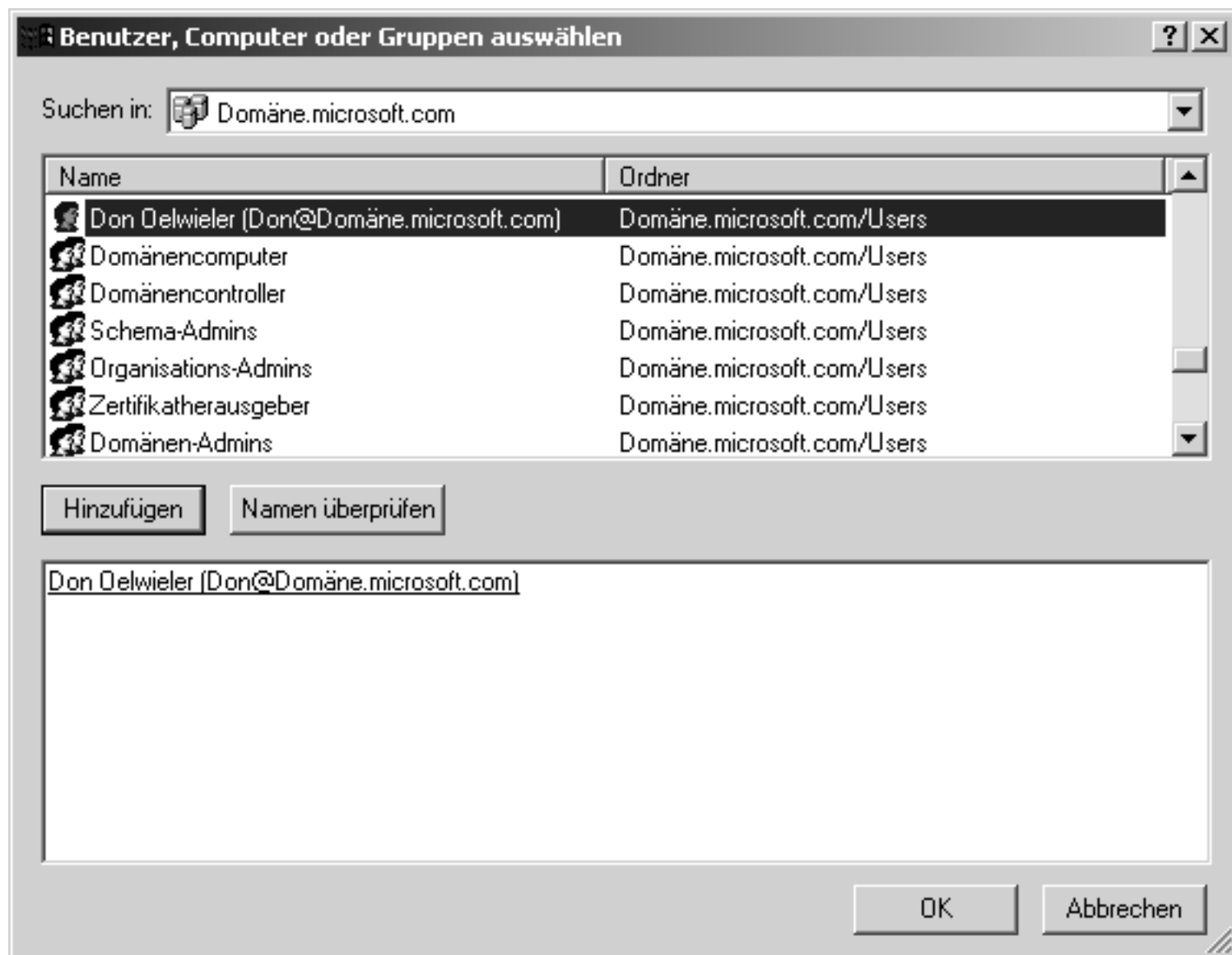


Abbildung 10.6: Zuweisen von Berechtigungen zu einer Organisationseinheit (in diesem Fall ein Benutzer)

10.4 Dynamisches DNS

Durch das dynamische DNS können DNS-Clients ihre eigenen A-Ressourceneinträge auf einem DNS-Server bei jeder Änderung registrieren und dynamisch aktualisieren. Dadurch verringert sich die Notwendigkeit der manuellen Verwaltung von Zoneneinträgen, insbesondere bei Clients, deren Standort häufig geändert wird und denen eine IP-Adresse anhand von DHCP zugewiesen wird.

Windows 2000 bietet Client- und Server-Unterstützung für die Verwendung von dynamischen Aktualisierungen, wie in RFC 2136 (<http://www.ietf.org/rfc/rfc2136.txt>) beschrieben. Bei DNS-Servern ermöglicht der DNS-Dienst das Aktivieren bzw. Deaktivieren der dynamischen Aktualisierung für jede Zone auf allen Servern, die zum Laden einer primären Standardzone oder einer Active Directory-integrierten Zone konfiguriert sind. In der Standardeinstellung aktualisieren Clients, die eine beliebige Version von Windows 2000 ausführen, ihre A-Ressourceneinträge in DNS dynamisch, wenn sie für TCP/IP konfiguriert sind.

Computer unter Windows 2000 versuchen standardmäßig, A-Einträge (Adresse) und PTR-Einträge (Zeiger) für die IP-Adressen dynamisch zu registrieren, die für den Computer konfiguriert sind und von diesem verwendet werden. Dabei registrieren die meisten Clients eine IP-Adresse, die auf dem vollständigen Computernamen beruht. Der vollständige Computernamen (vollqualifizierter Domänenname, FQDN) wird erstellt, indem der Computernamen an den wie unter **Systemeigenschaften** konfigurierten DNS-Domännennamen für den Computer angehängt wird.

Dynamische Aktualisierungen können aus folgenden Gründen oder bei folgenden Ereignissen gesendet werden:

- In der Konfiguration der TCP/IP-Eigenschaften für eine der installierten Netzwerkverbindungen wurde eine IP-Adresse hinzugefügt, entfernt oder geändert.
- Die Lease einer IP-Adresse ändert oder erneuert auf dem DHCP-Server eine der installierten Netzwerkverbindungen. Es wird z.B. der Computer gestartet oder der Befehl `ipconfig /renew` verwendet.
- Der Befehl `ipconfig /registerdns` wird zum manuellen Aktualisieren der Registrierung des Client-Namens in DNS verwendet.

Wenn von einem dieser Ereignisse eine dynamische Aktualisierung ausgelöst wird, sendet der DHCP-Client-Dienst (nicht der DNS-Client-Dienst) Aktualisierungen. Dies gewährleistet, dass bei Änderungen der IP-Adressinformationen, die durch DHCP hervorgerufen wurden, entsprechende Aktualisierungen in DNS ausgeführt werden, um die Zuordnung der Namen zu Adressen für den Computer zu synchronisieren. Der DHCP-Client-Dienst führt dies für alle im System verwendeten Netzwerkverbindungen aus, einschließlich der Verbindungen, die nicht für die Verwendung von DHCP konfiguriert sind.

10.4.1 Funktionsweise der dynamischen Aktualisierung

Unter Windows 2000 werden dynamische Aktualisierungen im Allgemeinen abgefragt, wenn auf dem Computer der DNS-Name oder die IP-Adresse geändert werden. Nehmen wir einmal an, ein Client mit dem Namen »alhost« wird zuerst in den **Systemeigenschaften** mit den folgenden Namen konfiguriert:

- Computername: `althost`
- DNS-Name: `beispiel.microsoft.com`
- Vollständiger Computername: `althost.beispiel.microsoft.com`

In diesem Beispiel werden keine verbindungs-spezifischen DNS-Domännennamen für den Computer konfiguriert. Später wird der Computer von »althost« in »neuhost« umbenannt, wodurch folgende Namen im System geändert werden:

- Computername: `neuhost`
- DNS-Name: `beispiel.microsoft.com`
- Vollständiger Computername: `neuhost.beispiel.microsoft.com`

Wenn die Namensänderung in die **Systemeigenschaften** übernommen wurde, führt der DHCP-Client-Dienst die folgenden Schritte zum Aktualisieren von DNS aus:

- Der Client sendet eine Abfrage nach dem Autoritätsursprung (SOA = State of Authority) unter Verwendung des DNS-Domännennamens des Computers.
- Windows 2000 legt den Namen der zu aktualisierenden Zone (`beispiel.microsoft.com`) basierend auf dem DNS-Domännennamen des Computers fest. Dann wird eine Abfrage nach dem Autoritätsursprung unter Verwendung des Zonnennamens gesendet.
- Der Server antwortet auf die Abfrage nach dem Autoritätsursprung (SOA).

Bei primären Standardzonen ist der in der Antwort auf die Abfrage nach dem Autoritätsursprung gesendete primäre Server (Besitzer) festgelegt und statisch. Dieser stimmt immer mit dem DNS-Namen überein, der im Ressourceneintrag für den Autoritätsursprung angezeigt wird, der mit der Zone gespeichert wird. Wenn die aktualisierte Zone Active Directory-integriert ist, können alle die Zone ladenden DNS-Server antworten und dynamisch ihren Namen als primärer Server (Besitzer) der Zone in die Antwort auf die Abfrage nach dem Autoritätsursprung einfügen.

Wenn der Client versucht, eine Verbindung zum primären DNS-Server herzustellen, verwendet er den in der Antwort auf die Abfrage nach dem Autoritätsursprung gesendeten Namen des primären Servers, um diesen Namen der IP-Adresse für den primären Server noch einmal abzufragen, nachzuschlagen und aufzulösen. Dann versucht der Client, eine Verbindung zum primären Server herzustellen. Wenn der primäre Server nicht verfügbar ist, kann der DHCP-Client-Dienst prüfen, ob es sich bei der Zone, von der die Aktualisierung abgefragt wird, um eine Single-Master- oder um eine Multi-Master-Zone handelt, indem er prüft, ob die Zone in Active Directory integriert ist.

Wenn die Zone Active Directory-integriert ist, fragt der DHCP-Client nach dem Name-Server-Ressourceneintrag für die Zone `beispiel.microsoft.com`, um einen anderen autorisierten primären Server zu finden, der eine Aktualisierung bearbeiten kann.

Wenn ein primärer Server die Aktualisierung bearbeiten kann, sendet der Client die Abfrage für die Aktualisierung und der DNS-Server bearbeitet diese. Der Inhalt der Abfrage für die Aktualisierung enthält Anweisungen zum Hinzufügen eines A- (und wahrscheinlich eines PTR-) Ressourceneintrags für `neuhost.beispiel.microsoft.com` und zum Entfernen der gleichen Eintragsstypen für `althost.beispiel.microsoft.com`, des vorher registrierten Namens.

Der Server überprüft auch, ob Aktualisierungen für die Client-Abfrage erlaubt sind. Bei primären

Standardzonen sind dynamische Aktualisierungen nicht gesichert, sodass alle Versuche von Clients für das Aktualisieren erfolgreich sind. Bei Active Directory-integrierten Zonen sind die Aktualisierungen gesichert und werden mit den entsprechenden Sicherheitseinstellungen durchgeführt.

Dynamische Aktualisierungen werden regelmäßig gesendet und erneuert. In der Standardeinstellung sendet Windows 2000 alle 24 Stunden eine Aktualisierung. Wenn bei der Aktualisierung keine Zonendaten geändert werden, bleibt die aktuelle Version der Zone erhalten und es werden keine Änderungen vorgenommen. Bei Aktualisierungen wird die Zone nur dann geändert oder die Zonenübertragung erhöht, wenn Namen oder Adressen geändert wurden.

Beachten Sie, dass Namen nicht vor Ablauf des Aktualisierungsintervalls (24 Stunden) aus DNS-Zonen entfernt werden, wenn sie nicht mehr aktiv sind oder nicht aktualisiert werden. In DNS werden Namen weder freigegeben noch als veraltet gekennzeichnet, obwohl DNS-Clients versuchen, alte Namen zu löschen oder zu aktualisieren, wenn ein neuer Name oder eine neue Adresse übernommen wird.

Wenn der DHCP-Client-Dienst A- und PTR-Ressourceneinträge für einen Windows 2000-Computer registriert, ist dafür ein Standardwert für die Gültigkeitsdauer (TTL, Time-To-Live) im Cache von 15 Minuten festgelegt. Für diese Dauer wird der Eintrag auf anderen DNS-Servern und -Clients zwischengespeichert, wenn diese in die Antwort auf eine Abfrage eingeschlossen sind.

10.4.2 Sichere dynamische Aktualisierung

Bei Windows 2000 ist die DNS-Aktualisierungssicherheit nur in Zonen verfügbar, die in Active Directory integriert sind. Wenn Sie eine Zone in Active Directory integrieren, stehen Ihnen die Bearbeitungsfunktionen der Zugriffssteuerungsliste (ACL) in der DNS-Konsole zur Verfügung, sodass Sie einer bestimmten Zone oder einem bestimmten Ressourceneintrag Benutzer oder Gruppen aus der ACL hinzufügen oder daraus entfernen können.

In der Standardeinstellung versuchen Clients unter Windows 2000 zuerst, nicht gesicherte dynamische Aktualisierungen zu verwenden. Wenn eine nicht gesicherte Aktualisierung verweigert wird, verwenden die Clients die gesicherte Aktualisierung. Außerdem verwenden Clients eine Standardaktualisierungsrichtlinie, die das Überschreiben eines zuvor registrierten Ressourceneintrags ermöglicht, wenn der Client daran nicht durch die Aktualisierungssicherheit gehindert wird.

Kapitel 11 Erstellen und Verwalten von Benutzerkonten

In diesem Kapitel geht es darum, wie Benutzerkonten erstellt, verwaltet und in Gruppen zusammengefasst werden. Die wesentliche Aufgabe bei der Benutzerverwaltung besteht darin, die Benutzerbasis zu erstellen und den Gruppen zuzuweisen, die in der Lage sein müssen, auf Ressourcen zugreifen zu können.

Auch wenn dieses Kapitel mit dem Erstellen von Benutzerkonten beginnt, sollten Sie sich davon im Umgang mit der Sicherheit nicht beeinflussen lassen. Wie bereits im vorhergehenden Kapitel erwähnt, sollten Sie zuerst die Gruppe für die Ressource erstellen und dann die Benutzer zuweisen. Es ist jedoch kein Fehler, wenn Sie wissen, wer zu der Gruppe gehören soll, die Sie erstellen.

Benutzerkonten bei Windows 2000 sind deutlich leistungsfähiger als sie das bisher waren. Dieses Kapitel soll Ihnen dabei helfen, die Verwaltung von Benutzerkonten zu verstehen. Wenn Sie bereits wissen, wie Benutzerkonten erstellt werden und jetzt wissen möchten, wie Richtlinien erstellt und verwendet werden, dann sollten Sie im folgenden Kapitel weiterlesen.

11.1 Benutzerkonten

Das Benutzerkonto ist die Stelle, an der das Gummi die Straße in der Welt des Netzwerkbetriebssystems berührt. Das Benutzerkonto ist die Schlüsselkomponente, die verwendet wird, um auf Netzwerkressourcen zuzugreifen, und es stellt den Kontrollpunkt für jede Berechtigung und jede Richtlinie dar. Bei Windows 2000 haben diese Konten enorm an Bedeutung gewonnen.

Bevor Sie damit beginnen, diese Konten zu erstellen, sollten Sie einige Grundregeln kennen lernen und einige wichtige Informationen erhalten. Das Erstellen von Gruppen und das Hinzufügen von Benutzern zu diesen Gruppen wird hier erwähnt, aber erst später ausführlicher behandelt. Wenn Sie als Administrator noch keine Erfahrung haben, sollten Sie diesen ausführlicheren Abschnitt zuerst lesen, bevor Sie sich daran machen, Konten zu erstellen. So können Sie verhindern, dass Sie Konten erstellen, die Sie später wieder löschen müssen.

11.1.1 Vordefinierte bzw. integrierte Benutzer

Wenn Windows 2000 installiert wird, werden einige Benutzerkonten sofort erstellt. Diese Konten werden vom System und von den ersten Benutzern des Systems verwendet, um überhaupt auf das System zugreifen zu können. Ebenso wie bei einem neuen Haus, bei dem es einen ersten Satz Schlüssel gibt, können diese Konten entweder geändert oder so wie sie sind verwendet werden. Es ist jedoch sinnvoll, diese Schlüssel so schnell wie möglich zu ändern.

Welche Konten automatisch erstellt werden, hängt davon ab, welche Dienste installiert sind. In jedem Fall werden auf jedem Server die Konten **Gast** und **Administrator** erstellt. Diese Konten werden erstellt, damit grundlegende Dienste zur Verfügung stehen. Wenn Sie die Konsole **Active Directory-Benutzer und -Computer** öffnen und anschließend auf **Users** klicken (siehe Abbildung 11.1), können Sie die vordefinierten Konten sehen.

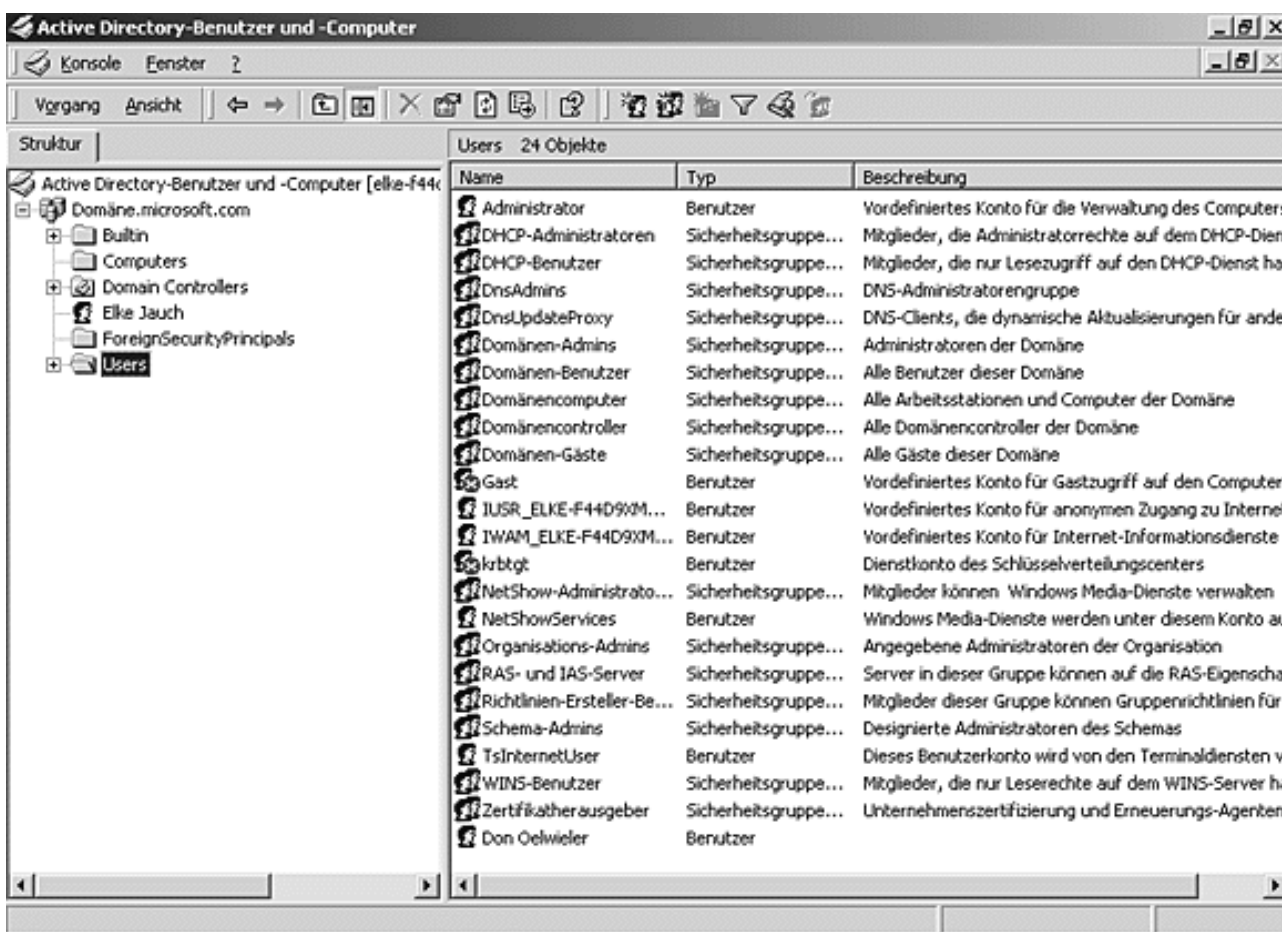


Abbildung 11.1: Standardkonten für Benutzer und Gruppen

Mit dem Gastkonto kann nichts installiert werden und das sollte auch so beibehalten werden. Dieses Konto sollte nur dazu dienen, Besuchern Ihres Systems Zugriff auf öffentliche Bereiche wie Drucker oder auch auf Freigaben zu gewähren. Das Beste an diesem Konto ist, dass es zur Gruppe **Domänen-Benutzer** gehört. Das bedeutet, dass dem Gastkonto der für die Gruppen **Domänen-Benutzer** bzw. **Jeder** freigegebene Dienst zur Verfügung steht.

Sie sollten wissen, dass Sie das Gast- und das Administratorkonto nicht löschen, aber umbenennen können.

Eine Ihrer ersten Aufgaben sollte es sein, die vordefinierten Konten umzubenennen. Eindringlinge, die sich auskennen, werden versuchen, sich im System mit Hilfe der vordefinierten Konten anzumelden. Wenn sie einen Kontonamen in Erfahrung bringen können, haben sie die Schlacht schon halb gewonnen. Wenn es sich bei dem Konto dann noch um das Administratorkonto handelt, ist der Krieg vorbei.

Das Administratorkonto wird für die Erstanmeldung und die Erstellung sowie für das Starten von Diensten erstellt. Das Administratorkonto wird auch dann erstellt, wenn der Server nicht in einer Domäne installiert ist. Das Konto wird in der Domäne nicht jedes Mal erstellt, wenn ein neuer Server oder Domänencontroller installiert wird. Wenn Sie einen neuen Server in einer bereits vorhandenen Domäne installieren, fragt das System nach einem Administratornamen und -kennwort, um das Computerkonto in der Domäne zu erstellen.

Benennen Sie das Administratorkonto so schnell wie möglich um. Wenn Sie sich in einer großen Unternehmensumgebung befinden, können Sie nie wissen, wer sich wie lange schon im System aufhält, bis Sie die Konten umbenennen.

Als Nächstes sollten Sie ein zweites Konto erstellen, das Mitglied der Gruppen **Domänen-Admins** und **Administrator** ist. Dadurch, dass Sie dieses Konto erstellen, lassen Sie sich eine Hintertür offen, falls das Administratorkonto einmal unbrauchbar werden sollte. Es kommt gar nicht so selten vor, dass das Kennwort des Administratorkontos geändert wird und sich keiner mehr an den Namen erinnern kann. Damit ist die Burg verschlossen und der Schlüssel auf Nimmerwiedersehen verschwunden.

Eine gute Übung für Systemadministratoren ist es, sich bei ihrer täglichen Arbeit mit der Domäne nicht als Administrator anzumelden. Oder anders ausgedrückt: Verwenden Sie kein Konto, das allmächtig ist, wenn Sie mit einem Textverarbeitungs- oder Tabellenkalkulationsprogramm arbeiten. Sie sollten immer daran denken, dass Sie Dateien ohne Kontrolle ändern können,

wenn Sie sich als Administrator anmelden. Dabei kann es Ihnen wie Gulliver bei den Liliputanern ergehen. Sie könnten auf etwas treten. Oder noch schlimmer: Wenn Sie Ihren Arbeitsplatz verlassen, ohne sich abzumelden, ist das Sicherheitssystem geöffnet.

Allzu häufig kennen die Besitzer oder leitende Angestellte eines Unternehmens das Administratorkennwort für die Domäne, in der ihre Daten enthalten sind, nicht. Es ist jedoch durchaus sinnvoll, den Besitzern oder leitenden Angestellten eines Unternehmens eine Liste dieser Kennwörter zur Verfügung zu stellen, für den Fall, dass ein Mitarbeiter das Unternehmen verlässt oder aus anderen Gründen nicht erreichbar ist. So ist es möglich, dass die Angestellten wieder an ihr System kommen.

11.1.2 Richtlinien für die Vergabe von Namen und Kennwörtern

Sie sollten die Aufgabe des Erstellens von Benutzerkonten ernst nehmen. Wenn Sie Robert Schmidt den Benutzernamen »Bert« und das Kennwort »Angela« (den Namen seiner Frau) zuweisen, ist das in einer kleinen Büroumgebung kein Problem. Wenn Sie jedoch 30 oder mehr Konten einrichten, wird es etwas schwieriger, sich solche netten Kombinationen auszudenken. Das ist allerdings die kleinste Sorge, die Sie in einem Szenario wie dem eben geschilderten haben werden. Die Sicherheit ist praktisch mit ihrer Einrichtung schon nicht mehr existent.

Bei Windows 2000 kann praktisch jede beliebige Methode für die Vergabe von Namen für Benutzer und Gruppen eingerichtet und verwendet werden. Das Programm ermöglicht dabei auch die Kontrolle darüber, ob ein Benutzer berechtigt ist, ein bestimmtes Kennwort zu verwenden. Bei Kennwörtern wird übrigens nach Groß- bzw. Kleinschreibung unterschieden.

Im Folgenden sind einige grundlegende Regeln aufgeführt, die dazu beitragen, dass Ihr System sicherer wird - vorausgesetzt, Sie befolgen diese Regeln:

- Verwenden Sie Kennwörter, die aus mindestens acht Zeichen bestehen. Dabei sollte es sich um alphanummerische Zeichen handeln, die Sie nach Möglichkeit groß schreiben sollten. Damit wird verhindert, dass Utilities verwendet werden, die einfach das Wörterbuch nach dem Server werfen, wenn ein Benutzername entdeckt wird. Wenn Sie diese Regel befolgen, können Sie die Zeit, die erforderlich ist, um das Kennwort eines Benutzers zu knacken, von einer Stunde auf vier Tage erhöhen. Beispiele dafür sind »492je429« und »7382jnne«.
- Weisen Sie Benutzern wann immer möglich Kennwörter zu. So können Sie genau nachvollziehen, was als Kennwort verwendet wird.
- Definieren Sie eine Richtlinie für Kennwörter, die Benutzer auffordert, ihre Kennwörter alle 30 bis 90 Tage zu ändern (siehe Abbildung 11.2).

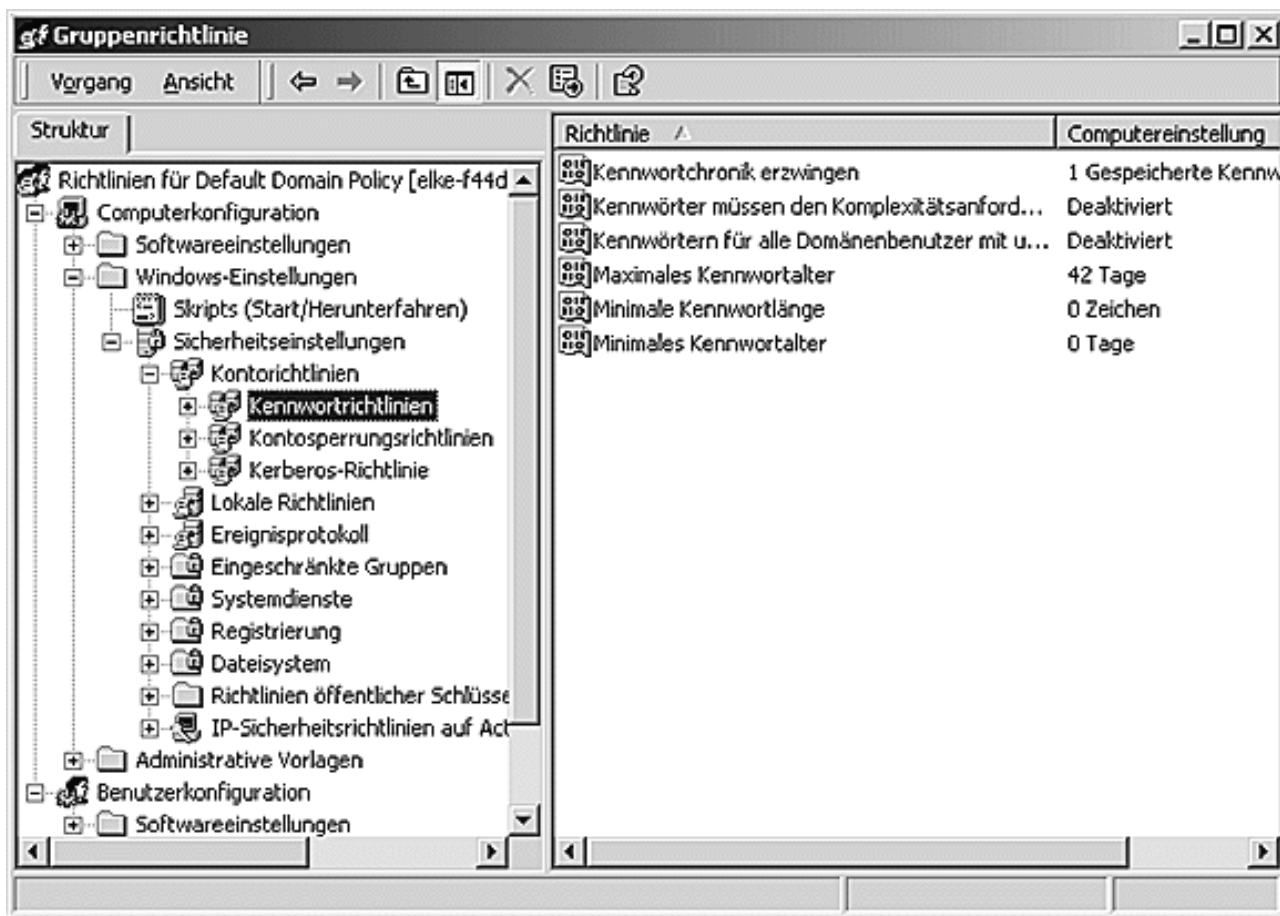


Abbildung 11.2: Richtlinie für Kennwörter

- Sorgen Sie für Eindeutigkeit in Bezug auf Kennwörter. Oder anders ausgedrückt: Achten Sie darauf, dass kein Benutzer den Namen seiner Katze als Kennwort verwendet. Lassen Sie darüber hinaus ebenso wenig zu, dass Benutzer zuerst den Namen ihrer Katze, dann den ihres Hundes und anschließend wieder den ihrer Katze verwenden. Das Kennwort sollte über mehrere Iterationen hinweg beibehalten werden.

Um diese Kennwortrichtlinien durchzusetzen, müssen Sie Änderungen in den Gruppenrichtlinien (insbesondere bei den Richtlinien für Kennwörter) für die Benutzer vornehmen, die Sie überwachen möchten. Mit **Default Domain Policy** können Sie die Richtlinie für sämtliche Konten standardmäßig durchsetzen.



Denken Sie immer daran, dass jeder Stein, den Sie den Benutzern in den Weg legen, mehr Arbeit für die Hotline bedeutet. Es ist daher ein schmaler Grad, den Sie gehen müssen, wenn Sie festlegen, ob die Richtlinien eher streng oder in der Anwendung eher einfach sein sollen. Sie werden wohl am meisten zu tun haben, wenn die Kennwörter von allen ablaufen.

Benutzernamen sind nicht annähernd so kompliziert wie Kennwörter. Die schwierigste Entscheidung, die Sie im Zusammenhang mit Benutzernamen treffen müssen, ist die, welche Regel angewendet werden soll, und ob es für das Unternehmen sinnvoll ist, wenn Benutzernamen verwendet werden, die mit den tatsächlichen Namen der Benutzer zu tun haben. Was das betrifft, gibt es grundsätzlich zwei verschiedene Ansichten.

Die eher konventionelle Ansicht in der heutigen, vom Internet geprägten Welt ist die, dass Benutzernamen vergeben werden sollten, die eine Abwandlung des tatsächlichen Namens der Benutzer darstellen. Ein Grund, der für diese Ansicht spricht, ist der, dass Benutzer einfacher erkannt und die Benutzernamen in andere Dienste integriert werden können - die Benutzernamen können den E-Mail-Adressen oder SQL Server-Konten entsprechen.

Das Problem dabei wurde bereits erwähnt. Wenn ein Hacker weiß, dass die Benutzerkonten in Ihrem Unternehmen aus dem ersten Buchstaben des Vornamens und dem Nachnamen (Robert Newton = rnewton) bestehen, weiß er schon die Hälfte dessen, was er wissen muss, um in Ihr System einzudringen.

Die diesem Ansatz entgegenstehende Ansicht ist die, dass für Benutzerkonten ähnlich wie bei den bereits erwähnten

Kennwörtern Zahlen oder alphanummerische Namen verwendet werden sollten. Die Idee, die dahinter steckt, ist dieselbe wie die, die sich hinter der Idee von Kennwörtern verbirgt: Je komplexer und unnatürlicher der Benutzername und das Kennwort, um so weniger wahrscheinlich ist es, dass ein Hacker die Kombination knackt.

Das Problem bei diesem System ist allerdings, dass Benutzer sich ihre Kombinationen häufig nicht merken können. Das führt zu einem oder zwei weiteren Problemen:

- Benutzer rufen häufiger bei der Hotline an, da sie sich die Kombination nicht merken können oder weil sie sich bei der Eingabe der Kombination vertippen.
- Benutzer notieren sich ihre Benutzernamen und/oder Kennwörter und geben diese auch an andere weiter. Diese Erfahrung machen und lassen viele Administratoren.



Denken Sie immer daran, dass die häufigste Sicherheitsverletzung im gemeinsamen Netzwerk ein Benutzer ist, der sich am System anmeldet und dann seinen Arbeitsplatz verlässt. Achten Sie daher darauf, dass Bildschirmschoner mit aktiviertem Kennwortschutz spätestens nach 15 Minuten Wartezeit aktiv werden. Dies können Sie übrigens ebenfalls mit Hilfe der Gruppenrichtlinien durchsetzen.

11.1.3 Erstellen von Benutzerkonten

Beim Erstellen von Benutzerkonten ist der schwierigste Teil der Aufgabe die Entscheidung, wo Sie die Benutzerkonten erstellen. Treffen Sie diese Entscheidung, indem Sie das wiederholen, was Sie in den vorhergehenden Kapiteln gelernt haben. Grundsätzlich müssen Sie entscheiden, in welchem Container Sie die Benutzerkonten erstellen möchten: in der Domäne oder in der Organisationseinheit?

Wenn Sie diese Entscheidung getroffen haben, müssen Sie während der Erstellung von Benutzerkonten mehrere Optionen wählen, die Sie aufzeichnen oder bereits kennen sollten, bevor das Dialogfeld für das Erstellen von Benutzerkonten (siehe Abbildung 11.3) geöffnet wird.

Abbildung 11.3: Erstellen von Benutzerkonten

- *Vorname*. Der Rufname des Benutzers.
- *Nachname*. Der Nachname des Benutzers.
- *Vollständiger Name*. Diese Option wird automatisch ausgefüllt, wenn Sie den Vor- und Nachnamen eingeben. Sie kann

jedoch für die Verwendung in einem anderen Feld bearbeitet werden.

- *Benutzeranmeldename*. Der Name, der bei der Anmeldung verwendet wird.
- *Benutzeranmeldename (Windows NT 3.5x/4.0)*. Wenn der von Ihnen gewählte Anmeldename aus mehr als 20 Zeichen besteht, erstellt dieser Eintrag automatisch ein mit älteren Versionen kompatibles Konto. Es kann bearbeitet werden, um den Namen etwas netter zu gestalten.

 Nicht alle Namensfelder müssen ausgefüllt werden. Lediglich das Feld **Vorname** oder **Nachname** und das Feld **Benutzeranmeldename** müssen ausgefüllt werden.

- *UPN-Suffix*. Wenn während der Installation der Domäne UPN-Suffixe erstellt werden, um bestimmten Benutzern eindeutige Domänenanmeldennamen zu geben, ist dies das Feld, in dem diese UPN-Suffixe angegeben werden.
- *Kennwort*. Das Kennwort, nach dem der Benutzer gefragt wird, wenn er sich bei der Domäne anmeldet.
- *Benutzer muss Kennwort bei nächster Anmeldung ändern*. Dabei handelt es sich um eine Option, mit deren Hilfe ein Kennwort erstellt werden kann, das nur für die erste Anmeldung verwendet werden kann. Danach wird der Benutzer aufgefordert, sein Kennwort zu ändern.
- *Benutzer kann das Kennwort nicht ändern*. Der Benutzer kann das Kennwort nicht ändern.
- *Kennwort läuft nie ab*. Wenn diese Option gewählt wird, werden die Richtlinien für Kennwörter nicht beachtet. Diese Option wird häufig für Systemkonten oder für selten verwendete Konten für Sicherheitsadministratoren verwendet.
- *Konto ist gesperrt*. Damit kann das Konto nicht mehr genutzt werden, es wird jedoch nicht gelöscht. Wenn ein Konto gelöscht werden muss, ist es häufig besser, es zuerst für eine gewisse Zeitspanne zu sperren. Damit ist es möglich, das Konto wieder zu aktivieren (möglicherweise sogar mit einem neuen Namen), falls ein Benutzer mit denselben Sicherheitsanforderungen ein solches Konto benötigt. (Das ist bei Zeitarbeitern, Praktikanten und auch bei Kündigungen, die u.U. wieder zurückgenommen werden, der Fall.)

Erstellen einer Konsole

Benutzerkonten werden in der Konsole **Active Directory-Benutzer und -Computer** erstellt. Wenn Sie eine große Anzahl von Benutzerkonten erstellen möchten, sollten Sie im folgenden Abschnitt nachlesen, wie Sie dies am besten tun können. Wenn Sie jedoch einzelne Benutzerkonten erstellen und verwalten müssen, eignet sich das Verfahren mit der Konsole am besten.

Um ein Benutzerkonto zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie die Konsole **Active Directory-Benutzer und -Computer** und wählen Sie das Containerobjekt aus, in dem Sie das Benutzerobjekt erstellen möchten. Das kann der Container **Benutzer** für die Domäne sein oder eine beliebige Organisationseinheit, die erstellt worden ist.
2. Klicken Sie mit der rechten Maustaste auf das Containerobjekt und wählen Sie die Option **Neu** und dann **Benutzer**.
3. Geben Sie die zuvor definierten Angaben zum Benutzernamen ein und klicken Sie dann auf die Schaltfläche **Weiter**.
4. Geben Sie die zuvor definierten Angaben zum Kennwort ein und klicken Sie dann auf die Schaltfläche **Weiter**.
5. Klicken Sie auf die Schaltfläche **Fertig stellen**.

Erstellen mehrerer Benutzerkonten

Wenn Sie 100 Benutzerkonten erstellen müssen, ist schon allein der Gedanke daran schmerzlich, dies mit Hilfe der Konsole tun zu wollen. Glücklicherweise gibt es eine Lösung zu diesem Problem: `net user`. Der Befehl `net` ist ein Allzweckbefehl, der in der Eingabeaufforderung eingegeben wird und mit dem Netzwerkressourcen schnell und effizient genutzt werden können. Mit Hilfe der unterschiedlichen Kombinationen des Befehls `net user` können Informationen über Benutzerkonten angezeigt und Benutzerkonten erstellt bzw. gelöscht werden.

Die Syntax für den Befehl lautet folgendermaßen:

```
NET USER [Benutzername [Kennwort | *] [Optionen]] [/DOMAIN]
NET USER Benutzername {Kennwort | *} /ADD [Optionen] [/DOMAIN]
NET USER Benutzername [/DELETE] [/DOMAIN]
```

Mit jedem Teil dieser Befehle können Sie bestimmte Informationen aufrufen oder einen gewünschten Effekt erzielen. Dieser Befehl ähnelt den Befehlen CD, RD und MD, mit denen Verzeichnisse in der Dateistruktur geändert werden. Im Folgenden ist eine Liste von Parametern mit ihren unterschiedlichen Auswirkungen aufgeführt:

- *Keine Parameter.* Wird der Befehl ohne Parameter verwendet, wird mit Hilfe von `net user` eine Liste der Benutzerkonten auf dem Computer angezeigt.
- **Benutzername.** Der Name des Benutzerkontos, das hinzugefügt, gelöscht, geändert oder angezeigt werden soll. Der Name des Benutzerkontos darf maximal 20 Zeichen umfassen.
- **Kennwort.** Weist dem Benutzerkonto ein Kennwort zu oder ändert es. Das Kennwort muss die mit der Option `/MINPWLEN` des Befehls `NET ACCOUNTS` festgelegte Mindestlänge aufweisen. Die maximale Länge beträgt 14 Zeichen.
- *****. Es erscheint die Eingabeaufforderung für das Kennwort. Das Kennwort wird bei der Eingabe nicht angezeigt.
- **/DOMAIN.** Führt den Vorgang auf einem Domänencontroller der aktuellen Domäne aus. Dieser Parameter ist nur auf Windows 2000 Professional-Computern gültig, die Mitglieder einer Windows 2000 Server-Domäne sind. Windows 2000 Server führen standardmäßig Vorgänge auf dem primären Domänencontroller aus.
- **/ADD.** Fügt ein Benutzerkonto der Benutzerkontendatenbank hinzu.
- **/DELETE.** Löscht ein Benutzerkonto aus der Datenbank.

Wenn der Befehl mit Optionen angegeben werden kann, wird die Art, wie die Daten geändert werden können, näher definiert. So kann beispielsweise die Option gewählt werden, dass zum neu erstellten Benutzerkonto eine Beschreibung hinzugefügt werden kann. Um eine dieser Optionen hinzuzufügen, ersetzen Sie einfach die Zeile `Option` in der Syntaxzeile durch die entsprechende Option. Und das sind nun die möglichen Optionen:

- **/ACTIVE: {YES | NO}.** Deaktiviert oder aktiviert das Konto. Wenn das Konto nicht aktiv ist, kann der Benutzer nicht auf den Server zugreifen. Standardeinstellung ist YES.
- **/COMMENT: "Beschreibung".** Es kann eine Beschreibung zum Benutzerkonto eingegeben werden. Diese Beschreibung kann bis zu 48 Zeichen umfassen. Der Text muss in Anführungszeichen stehen.
- **/COUNTRYCODE: nnn.** Verwendet die Landeskennzahl des Betriebssystems, anhand derer die Dateien der Online-Hilfe und der Fehlermeldungen in der jeweiligen Landessprache angezeigt werden. Bei der Eingabe des Wertes 0 wird die Standardländereinstellung gewählt.
- **/EXPIRES: {Datum | NEVER}.** Lässt ein Benutzerkonto zum angegebenen Datum ablaufen. Bei Eingabe von NEVER wird keine zeitliche Beschränkung für das Benutzerkonto festgelegt. Ablaufdaten können je nach angegebener Ländereinstellung in der Reihenfolge Monat/Tag/Jahr oder Tag/Monat/Jahr eingegeben werden. Monatsnamen können ausgeschreiben, mit drei Buchstaben abgekürzt oder als Zahlen geschrieben werden. Jahreszahlen können aus zwei oder vier Ziffern bestehen. Als Trennzeichen zwischen Tages-, Monats- und Jahreseingabe müssen Kommata oder Schrägstriche verwendet werden (keine Leerzeichen).
- **/FULLNAME: "Name".** Definiert den vollständigen Namen des Benutzers (nicht den Benutzernamen). Der Name muss in Anführungszeichen stehen.
- **/HOMEDIR: Pfad.** Bezeichnet den Pfad für das Basisverzeichnis eines Benutzers. Der Pfad muss bereits existieren.
- **/PASSWORDCHG: {YES | NO}.** Legt fest, ob Benutzer ihr eigenes Kennwort ändern können. Standardeinstellung ist YES.
- **/PASSWORDREQ: {YES | NO}.** Legt fest, ob ein Benutzerkonto ein Kennwort haben muss. Standardeinstellung ist YES.
- **/PROFILEPATH[:Pfad].** Bezeichnet den Pfad für das Anmeldeprofil des Benutzers. Dieser Pfad verweist auf ein Registrierungsprofil.
- **/SCRIPTPATH: Pfad.** Bezeichnet den Pfad für das Anmeldeskript des Benutzers. Der Wert Pfad darf kein absoluter Pfad sein. Pfad wird relativ zu `%systemroot%\System32\Repl\Import\Scripts` angegeben.
- **/TIMES: {Zeiten | ALL}.** Legt die Anmeldezeiten fest. Die Werte für Zeiten werden in der Form `Tag[-Tag][, Tag[-Tag]] , Uhrzeit[-Uhrzeit][, Uhrzeit[-Uhrzeit]]` angegeben, wobei die Angabe der Uhrzeit zu vollen Stunden erfolgen muss. Tage können ausgeschreiben oder abgekürzt werden. Beim 12-Stunden-Format muss nach der Uhrzeit AM, PM oder A.M., P.M. stehen. Bei ALL kann sich der Benutzer jederzeit anmelden. Ein Leerzeichen bewirkt, dass sich der Benutzer überhaupt nicht anmelden kann. Tag und Uhrzeit werden mit einem Komma getrennt, mehrere aufeinander folgende Zeitangaben mit einem Semikolon.

- `/USERCOMMENT:"Beschreibung"`. Hier kann der Administrator eine Beschreibung zum jeweiligen Benutzerkonto eingeben oder ändern. Der Text muss in Anführungszeichen stehen.
- `/WORKSTATIONS:{Computername[, ...] | *}`. Es können bis zu acht Computer angegeben werden, von denen aus sich der Benutzer am Netzwerk anmelden kann. Die unterschiedlichen Einträge werden durch Kommata voneinander getrennt. Wenn nach `/WORKSTATIONS` nichts oder `*` angegeben wird, kann sich der Benutzer von jedem Computer aus anmelden.

Diese Befehlszeile verwenden Sie für die Erstellung mehrerer Benutzerkonten am besten, indem Sie ein Beispiel Ihres gewünschten Kontos erstellen und dann in eine Stapelverarbeitungsdatei replizieren. Es kann nicht genügend betont werden, wie wichtig es ist, dass Sie dieses Verfahren ein-, zweimal ausprobieren sollten, bevor Sie die Stapelverarbeitungsdatei mit einer umfangreichen Gruppe von Benutzern füllen. Nach hundert falschen Benutzernamen zu suchen und diese zu berichtigen, kann sehr lästig sein.

So sieht beispielsweise eine Stapelverarbeitungsdatei aus, die Sie verwenden könnten:

```
NET USER bnewton 23nre32 /ADD /COMMENT:"Reisekoordinator"
NET USER jschmo 12nrw53 /ADD /COMMENT:"Reiseplaner"
NET USER snewton 2v2bt3 /ADD /COMMENT:"Reiseplaner"
NET USER jmeyer hrn598 /ADD /COMMENT:"Reisesekretärin"
```

Mit dieser Stapelverarbeitungsdatei werden Benutzerkonten, deren Kennwörter und Beschreibungen erstellt. Das ist ein einfaches Beispiel, das jedoch erkennen lässt, dass sich eine von nahezu jeder Textquelle exportierte Liste von Benutzern problemlos in eine importierte Liste für Windows 2000 konvertieren lässt.

11.1.4 Bedürfnisse der Benutzerumgebung

Bisher war der Umgang des Benutzers mit dem Netzwerk darauf ausgerichtet, den Benutzer nicht merken zu lassen, dass das Netzwerk überhaupt existiert. Seit es das Internet gibt, sind die Benutzer in Bezug auf Netzwerke etwas toleranter geworden.

Die Idee der *Benutzerumgebung* bezieht sich darauf, wie Benutzer mit ihren PCs und dem Netzwerk kommunizieren. Das hat sich während der letzten zwei bis drei Jahre stark verändert. Benutzerumgebung bedeutet nicht mehr nur, dass der Zugriff auf Ressourcen ermöglicht und überwacht wird, sondern dass das überwacht wird, was der Benutzer als verfügbar sieht (siehe Abbildung 11.4).

Eigenschaften von Phil Newton ? X

Mitglied von | Einwählen | Umgebung | Sitzungen

Remoteüberwachung | Terminaldienstprofile

Allgemein | Adresse | Konto | Profil | Rufnummern | Organisation

Phil Newton

Vorname: Initialen:

Nachname:

Anzeigename:

Beschreibung:

Büro:

Rufnummer:

E-Mail:

Webseite:

Abbildung 11.4: Benutzereigenschaften

Überwachung der Betriebssystemumgebung

Zu den in der Überwachung der Benutzereigenschaften für die Betriebssystemumgebung zur Verfügung stehenden Tools zählen die Benutzeranmeldeskripten, der Anmeldezugriff und die Zeitüberwachung.

Anmeldeskripten

Anmeldeskripten sind bei einigen Betriebssystemen schwierig zu lernen und anzuwenden. In der Welt von Windows wurden schon immer die guten alten Stapelverarbeitungsdateien verwendet. Die Befehlszeilen-Stapelverarbeitungsdatei gibt es schon seit rund zwei Jahrzehnten. Diese Schnittstelle wird schon seit den frühen Anfängen von DOS und in vielen anderen Betriebssystemen noch heute verwendet.

Eine *Stapelverarbeitungsdatei* ist eine Textdatei, die Befehle enthält, die zeilenweise ausgeführt werden. Wenn ich beispielsweise mit einem Befehl eine Anwendung ausführen, eine Anweisung über die Anwendung zurückübertragen und dann das Ergebnis der Anwendung löschen möchte, sollte ich eine Stapelverarbeitungsdatei erstellen.

Anmeldeskripten sind Stapelverarbeitungsdateien, die verwendet werden, um einen Benutzer in einer Umgebung zu definieren, die das Netzwerk besser nutzbar macht. Benutzern kann mittels Stapelverarbeitungsdatei ein Laufwerk, ein Druckeranschluss oder eine Anwendung zugewiesen werden.

Bei Windows 2000 wurden einige dieser Optionen erweitert. Der wichtigste Unterschied ist der, dass nun Containerobjekten Skripten zugewiesen werden können. Bei Windows NT gibt es so etwas wie *Gruppenanmeldeskripten* nicht. In der Familie der Skripten gibt es außerdem ein neues Mitglied, das so genannte *Abmeldeskript*.

Skripten werden zusammen mit sämtlichen anderen Windows 2000-Richtlinien für Benutzer und Profildaten in der folgenden

Reihenfolge ausgeführt:

- Standort
- Domäne
- Organisationseinheit
- untergeordnete Organisationseinheit usw.
- Benutzer

Speicherort im Verzeichnis

Skripten können von jeder beliebigen im Netzwerk freigegebenen Datei ausgeführt werden. Der Standardspeicherort von Skripten ist jedoch das Verzeichnis `\WINNT\System32\Repl\Import\Scripts`. Dies liegt in der möglichen Replikation dieser Skripten begründet.

Wenn kein bestimmter Pfad angegeben wird, erhalten die Clients eines Windows 2000- bzw. NT-Servers ihre Anmeldeskripten von dem DC, der sie im Netzwerk authentifiziert. Daher ist es in einem Netzwerk mit mehreren DCs sinnvoll, auf sämtlichen Servern eine aktuelle Liste von Anmeldeskripten zu verwalten. Wenn Sie die Skripten nicht nach jeder Bearbeitung für sämtliche Server kopieren möchten, müssen Sie eine Dateireplikation konfigurieren.

Die einzige Voraussetzung für ein Skript ist, dass darauf über eine Freigabe zugegriffen werden kann. Daher kann die Datei in der Freigabe `\\mcp\scripts` gespeichert und ebenso aufgerufen werden.

Wie bereits erwähnt, handelt es sich bei einem Skript in der Regel um eine Stapelverarbeitungsdatei (**.bat**). Damit Sie sich vorstellen können, wie ein Skript üblicherweise aussieht, sehen Sie sich folgendes Beispiel an:

```
***Beginn des Skripts
echo off
cls
echo Willkommen beim Macmillan Server-Cluster.
echo Die folgenden Ressourcenzuweisungen
echo wurden vorgenommen.
net use f: /home
net use g: \\mcp\data
net use m: \\mcp\apps
net use lpt2 \\mcp\laser_stock3
echo Einen schönen Tag!
pause
```

Mit diesem Skript wird zunächst die Befehlsanzeige ausgeschaltet. Anschließend wird der Bildschirm gelöscht und der Benutzer begrüßt. Darüber hinaus werden dem Benutzer die erstellten Umgebungsvariablen genannt. Abschließend wird dem Benutzer ein schöner Tag gewünscht. Aufgrund der Pause kann der Benutzer lesen, was auf dem Bildschirm steht, bevor er seine Arbeit fortsetzt und sich wundert, warum alles, was an LPT2 gesendet wird, über den Hewlett Packard 4MV ausgedruckt wird.

Ein Skript wird an einem von zwei möglichen Orten gespeichert: im Gruppenrichtlinienobjekt für einen Container bzw. für eine Gruppe oder im Benutzerobjekt. Das hängt natürlich davon ab, welche der Möglichkeiten jeweils am besten geeignet ist.

Bevor Sie nun Skripten erstellen, zunächst einmal ein paar zur Vorsicht mahnende Worte. Das Erstellen von Skripten ist so ähnlich wie das Erteilen von Berechtigungen. Es ist sinnvoller, wann immer möglich, Gruppenrichtlinienskripten zu erstellen. Darüber hinaus ist es immer einfacher, bestimmte Vorgänge für eine Gruppe, statt für jedes Benutzerkonto einzeln zu definieren. Auch Vorgänge für einen einzelnen Benutzer sollten möglichst in einem Gruppenrichtlinienskript definiert werden. Häufig wird das, was zunächst für einen Benutzer erforderlich ist, schon nach kurzer Zeit auch für andere Benutzer relevant.

Wenn Sie ein Gruppenrichtlinienskript zuweisen möchten, beginnen Sie in der Konsole **Active Directory-Benutzer und -Computer**. Gehen Sie dabei wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf den Container bzw. das Gruppenobjekt, in dem die Gruppenrichtlinie enthalten ist,

und wählen Sie dann die Option **Eigenschaften**.

2. Doppelklicken Sie auf der Registerkarte **Gruppenrichtlinie** auf die Gruppenrichtlinie, die Sie ändern möchten. (Wenn keine Gruppenrichtlinie vorhanden ist, müssen Sie eine erstellen, bevor Sie ein Skript zuweisen können.)

3. Klicken Sie auf das Pluszeichen (+) neben **Benutzerkonfiguration** und dann auf **Windows-Einstellungen**.

4. Wählen Sie die Option **Skripts (Anmelden/Abmelden)** und doppelklicken Sie anschließend auf das Symbol **Anmelden** bzw. **Abmelden**. Klicken Sie danach auf **Hinzufügen**.

5. Definieren Sie im Dialogfeld **Hinzufügen eines Skripts** die von Ihnen gewünschten Optionen und klicken Sie dann auf **OK**.

- **Skriptname**. Geben Sie den Pfad für das Skript ein oder klicken Sie auf **Durchsuchen**, um die Skriptdatei in der Netlogon-Freigabe auf dem Domänencontroller zu suchen.
- **Skriptparameter**. Geben Sie die gewünschten Parameter ein (wie in der Befehlszeile). Wenn das Skript beispielsweise die Parameter `//logo` (Vorspann anzeigen) und `//I` (interaktiver Modus) enthält, geben Sie folgende Zeile ein:

```
//logo//I
```

6. Definieren Sie im Dialogfeld **Eigenschaften von Anmelden** bzw. **Eigenschaften von Abmelden** sämtliche von Ihnen gewünschten Optionen:

- **Skripts zum Anmelden für**. Zeigt eine Liste aller Skripten an, die dem ausgewählten Gruppenrichtlinienobjekt derzeit zugewiesen sind. Wenn Sie mehrere Skripten hinzufügen, werden die Skripten in der angegebenen Reihenfolge abgearbeitet. Um ein Skript in der Liste nach oben zu verschieben, klicken Sie zunächst auf das Skript und dann auf **Nach oben**; mit **Nach unten** wird das Skript entsprechend nach unten verschoben.
- **Hinzufügen**. Öffnet das Dialogfeld **Hinzufügen eines Skripts**, in dem Sie weitere Skripten auswählen können.
- **Bearbeiten**. Öffnet das Dialogfeld **Skript bearbeiten**, in dem Sie Skriptdaten wie Name und Parameter ändern können.
- **Entfernen**. Entfernt das ausgewählte Skript aus der Liste der Skripten.
- **Dateien anzeigen**. Hiermit lassen Sie die Skriptdateien anzeigen, die im ausgewählten Gruppenrichtlinienobjekt gespeichert sind.

7. Klicken Sie auf **OK**.

Wenn Sie ein einzelnes Benutzerskript zuweisen möchten, beginnen Sie in der Konsole **Active Directory-Benutzer und -Computer**. Gehen Sie dabei wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf das Benutzerobjekt und wählen Sie die Option **Eigenschaften**.

2. Wählen Sie die Registerkarte **Profil**.

3. Geben Sie den Namen und den Pfad der Anmeldeskriptdatei ein, wenn sich diese vom Standardspeicherort auf den DCs unterscheidet.

4. Klicken Sie auf **OK**.

Der Befehl NET

Ein Administrator, der mit Befehlszeilanweisungen und Stapelverarbeitungsdateien umgehen kann, tut sich leichter, wenn es darum geht, Skripten zu verstehen. Es kann dennoch vorkommen, dass er die NET-Befehle nicht versteht. Der Befehl NET wird hier zum zweiten Mal in diesem Kapitel erwähnt, da mit diesem Befehl weitaus mehr gemacht werden kann, als nur Benutzerkonten zu erstellen und zu löschen. Der Befehl NET wird für Netzwerkressourcen ohne grafische Benutzeroberfläche verwendet und eignet sich daher hervorragend für Skripten oder jede andere Stapelverarbeitung.

Wenn Sie den Befehl NET verwenden möchten, müssen Sie lediglich NET mit der entsprechenden Variablen eingeben. Wie Benutzerkonten erstellt werden, wurde bereits beschrieben. Daher sollen hier nun einige Variablen genannt werden, die für ein Skript recht hilfreich sein können.

Die unten aufgeführte Liste ist eine unvollständige Liste der Variablen, die zusammen mit dem Befehl NET verwendet werden können, um eine Umgebung zu ändern oder Informationen abzurufen. Sie verwenden die Variablen einfach, indem Sie NET und dann den entsprechenden Befehl eingeben. Zu jeder Variablen ist ein Beispiel angegeben, damit Sie sehen, wie diese verwendet wird. Die Syntax entspricht folgendem Muster:

NET (Variable) (Parameter)

- **USE.** Verbindet einen Computer mit einer freigegebenen Ressource oder beendet diese Verbindung. Dieser Befehl steuert darüber hinaus auch die Wiederaufnahme von gespeicherten Netzwerkverbindungen. Beispiele:

```
NET USE [Gerätename | *] [\\Computername\Freigabename[\\Datenträger]] [Kennwort | *] [/USER:[Domänenname\]Benutzername] [/DELETE] | [/PERSISTENT:{YES | NO}]
NET USE Gerätename [/HOME[Kennwort | *]] [/DELETE:{YES | NO}]
NET USE [/PERSISTENT:{YES | NO}]
```

Hier nun eine Liste einiger USE-Parameter:

- **Kein.** Ohne Parameter zeigt NET USE eine Liste der Netzwerkverbindungen an.
 - **Gerätename.** Der Name der Ressource, zu der die Verbindung hergestellt oder das Gerät, das getrennt werden soll. Es gibt Gerätenamen für Laufwerke (D: bis Z:) und für Drucker (LPT1: bis LPT3:). Geben Sie einen Stern (*) anstatt eines bestimmten Gerätenamens an, wenn der nächste verfügbare Gerätename verwendet werden soll.
 - **\\Servername.** Der Name des Servers und der freigegebenen Ressource. Wenn der Computername Leerzeichen enthält, müssen die beiden umgekehrten Schrägstriche (\\) und der Computername in Anführungszeichen eingegeben werden. Die Länge des Computernamens kann 1 bis 15 Zeichen betragen.
 - **\\Datenträger.** Gibt einen NetWare-Datenträger auf dem Server an. Sie müssen den Client Service für NetWare (Windows 2000 Professional) oder den Gateway Service für NetWare (Windows 2000 Server) installiert und aktiviert haben, um eine Verbindung zu NetWare-Servern herstellen zu können.
 - **Kennwort.** Das Kennwort, mit dem Sie auf eine freigegebene Ressource zugreifen können.
 - *****. Erzeugt eine Eingabeaufforderung für das Kennwort. Das Kennwort wird bei der Eingabe nicht angezeigt.
 - **/USER.** Gibt einen anderen Benutzernamen an, mit dem die Verbindung hergestellt wird.
 - **Domänenname.** Der Name einer anderen Domäne. NET USE D:\\Server\\USER:admin\\marie1 verbindet beispielsweise die Benutzer-ID »Marie1«, als würde die Verbindung von der Admin-Domäne hergestellt. Ohne Eingabe eines Domännennamens gilt die aktuelle Domäne, an der der Benutzer angemeldet ist.
 - **Benutzername.** Legt den Benutzernamen fest, mit dem Sie sich anmelden.
 - **/DELETE.** Beendet eine Netzwerkverbindung. Wenn der Benutzer die Verbindung mit einem Stern angibt, werden sämtliche Verbindungen beendet.
 - **/HOME.** Verbindet den Benutzer mit seinem Basisverzeichnis.
 - **/PERSISTENT.** Steuert die automatische Wiederaufnahme von gespeicherten Netzwerkverbindungen. Standardmäßig wird die zuletzt eingestellte Verbindung verwendet.
 - **YES.** Speichert alle hergestellten Verbindungen und stellt sie bei der nächsten Anmeldung wieder bereit.
 - **NO.** Aktuelle und nachfolgende Verbindungen werden nicht gespeichert. Nur bestehende Verbindungen werden bei der nächsten Anmeldung wiederhergestellt. Verwenden Sie den Parameter /DELETE, um gespeicherte Verbindungen zu entfernen.
- **GROUP.** Fügt globale Gruppen auf Windows 2000 Server-Domänen hinzu, zeigt sie an oder ändert sie. Dieser Befehl steht nur auf Windows 2000 Server-Domänencontrollern zur Verfügung. Im Folgenden einige Beispiele:

```
NET GROUP [Gruppenname [/COMMENT:"Beschreibung"]] [/DOMAIN]
NET GROUP Gruppenname {/ADD [/COMMENT:"Beschreibung"] | /DELETE} [/DOMAIN]
NET GROUP Gruppenname Benutzername [ ... ] {/ADD | /DELETE} [/DOMAIN]
```

- **HELP.** Zeigt eine Liste mit Netzwerkbefehlen und Hilfethemen an. Darüber hinaus bietet dieser Befehl Hilfestellung bei bestimmten Befehlen und Themen. Die zur Verfügung stehenden NET-Befehle sind auch in der Befehlsreferenz im Dialogfeld **Befehle** unter **N** aufgeführt. Klicken Sie in der Windows 2000-Befehlsreferenz auf die Liste **Siehe auch**. Hier einige Beispiele:


```
NET HELP [Befehl]  
NET Befehl {/HELP | /?}
```

- **SEND.** Sendet Nachrichten an andere Benutzer, Computer oder Nachrichtennamen im Netzwerk. Um Nachrichten zu erhalten, muss der Nachrichtendienst aktiv sein. Hier ein Beispiel:

```
NET SEND {Name | * | /DOMAIN[:Name] | /USERS} Nachricht
```

- **TIME.** Synchronisiert die Systemzeit eines Computers mit der eines anderen Computers oder einer Domäne. Ohne die Option /SET wird die Uhrzeit für einen anderen Computer oder eine Domäne angezeigt. Hier ein Beispiel:

```
NET TIME [\\Computername | /DOMAIN[:Name]] [/SET]
```

- **USER.** Wurde bereits beschrieben.
- **VIEW.** Zeigt Domänen, Computer oder die von einem bestimmten Computer freigegebenen Ressourcen an. Hier einige Beispiele:

```
NET VIEW [\\Computername | /DOMAIN[:Domänenname]]  
NET VIEW /NETWORK:NW [\\Computername]
```

Basisverzeichnis

Das Basisverzeichnis eines Benutzers ist so etwas wie die Operationsbasis für jeden Benutzer in der Domäne. Es ist keine absolute Notwendigkeit, trägt jedoch dazu bei, dass der Benutzer das Gefühl hat, für seine eigenen Daten einen Speicherort in der Domäne zu haben.

Das Basisverzeichnis eines Benutzers wird auf der Registerkarte **Profil** im Dialogfeld **Eigenschaften** des Benutzerobjekts (siehe Abbildung 11.5) definiert. Bevor ein Basisverzeichnis erstellt werden kann, muss das freigegebene Verzeichnis, in dem das Basisverzeichnis erstellt werden soll, bereits bestehen. Der Administrator muss über Zugriffsberechtigungen verfügen, um in dieses Verzeichnis schreiben zu können und die Freigabe muss verfügbar sein. Außerdem sollte kein Verzeichnis mit dem Anmeldenamen des Benutzers existieren.

Abbildung 11.5: Die Registerkarte Profil im Dialogfeld Eigenschaften von [Benutzer]

Öffnen Sie die Konsole **Active Directory-Benutzer und -Computer**, um ein Basisverzeichnis auf einem Domänen-Server zuzuweisen und gehen Sie dann wie folgt vor:

1. Doppelklicken Sie auf das Benutzerobjekt und aktivieren Sie die Registerkarte **Profil**.
2. Klicken Sie auf das Optionsfeld **Verbinden von**.
3. Wählen Sie in der Dropdown-Liste einen Laufwerksbuchstaben, der verfügbar ist, wenn der Benutzer angemeldet ist. Drücken Sie auf die (Tab)-Taste.
4. Geben Sie die UNC-Adresse des Verzeichnisses ein, das das Basisverzeichnis für diesen Benutzer sein soll, und klicken Sie anschließend auf **OK**.

 Die Variable %USERNAME% kann in der UNC-Adresse für die Erstellung des Basisverzeichnisses (\\SERVERNAME\%USERNAME%) verwendet werden. Damit ist es möglich, dass Sie Vorlagen erstellen, die keinen Benutzernamen definieren, sondern Basisverzeichnisse erstellen, wenn ein neuer Benutzer kopiert wird.

Profil und Profilpfad

Mit dem Profil eines bestimmten Benutzers wird das Verhalten des Betriebssystems auf dem Arbeitsplatzrechner für diesen Benutzer definiert. Hier werden Software-Einstellungen, Hintergrundbild, Bildschirmschoner, manuelle Laufwerkzuordnungen und viele andere Dinge festgelegt. Wann immer sich ein Benutzer von Windows 2000, NT oder auch 95/98 (falls konfiguriert) an einem neuen System anmeldet, zeichnet dieses System den Benutzernamen auf und beginnt ein Profil für die Einstellungen dieses Benutzers.



Profileinstellungen können durch Richtlinien deaktiviert werden, die bestimmte Verhalten (wenn Sie beispielsweise Benutzern ein eigenes Startmenü zuweisen möchten) nicht zulassen oder diese provozieren. Diese Einstellungen sind kompliziert und werden in Kapitel 12 näher beschrieben.

Der Administrator einer Domäne kann Profile als Werkzeug für die Steuerung sowohl der Domäne als auch des Arbeitsplatzes des lokalen Arbeitsplatzrechners verwenden. Die Idee ist die, dass ein Profil erstellt werden soll, das zu der allen Benutzern präsentierten Umgebung passt und dass dieses Profil dann mit den Benutzern dahin mit wandert, wo diese sich anmelden. Daher wird dieses Profil auch als Roaming-Profil (engl. roaming = wandern) bezeichnet. Roaming-Profile bzw. servergespeicherte Profile können auch zu verbindlichen Profilen gemacht werden. Damit wird das Profil unveränderlich und stellt ein konsistentes und erzwingbares Profil dar.

Anmeldung und Kontooptionen

Außer der Umgebung, in der sich der Benutzer befindet, soll auch der Zugriff auf die Domäne gesteuert werden können. Über das Dialogfeld **Eigenschaften** des Benutzerobjekts (siehe Abbildung 11.4) können Sie den Zugriff und das Verhalten, angefangen bei den zulässigen Anmeldezeiten bis hin zu den Computern steuern, an denen man sich anmelden kann.

Anmeldezeiten

Die Anmeldezeiten können Sie definieren, indem Sie auf der Registerkarte **Konto** die Schaltfläche **Anmeldezeiten** anklicken (siehe Abbildung 11.6). Wenn Sie auf diese Schaltfläche klicken, können Sie Stunden auswählen, indem Sie auf die Stunden klicken und dann die Option **Anmeldung zulassen** bzw. die Option **Anmeldung verweigern** wählen. Danach wird der Zugriff auf dieser Basis zugelassen bzw. verweigert.

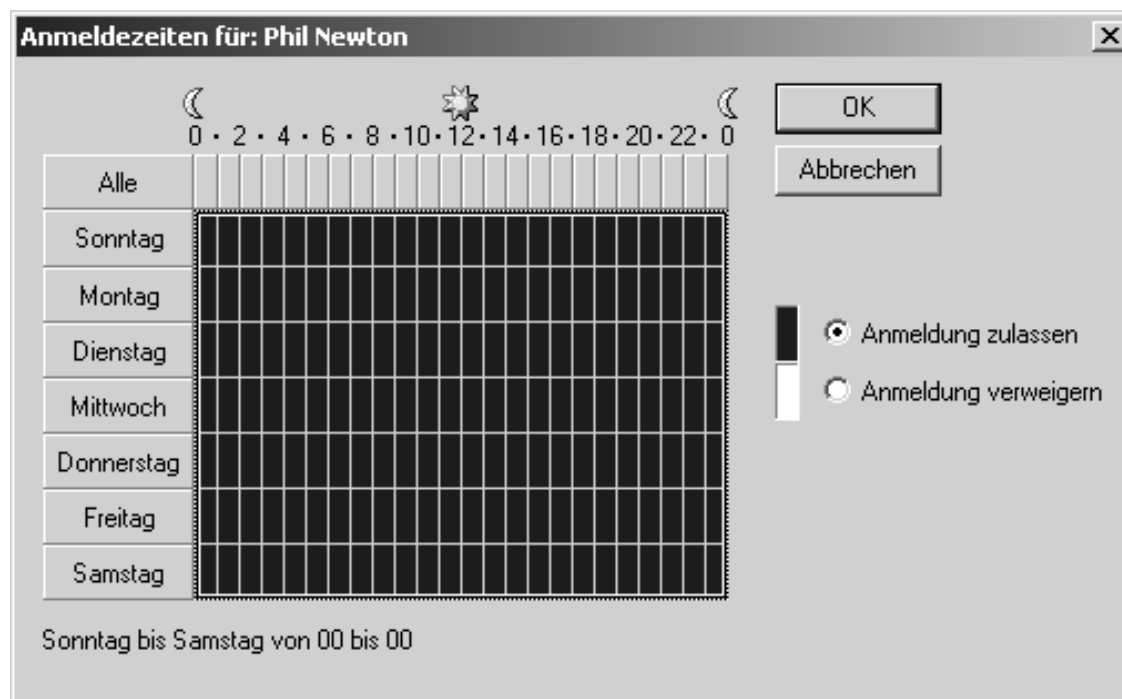


Abbildung 11.6: Das Dialogfeld Anmeldezeiten für: [Benutzer]

Remote-Zugriff

Den Remote-Zugriff der Benutzer können Sie mit Hilfe der Registerkarte **Einwählen** (siehe Abbildung 11.7) einzeln überwachen. Hier können Sie den Zugriff gestatten oder verweigern, indem Sie entweder die Option **Zugriff gestatten** oder die Option **Zugriff verweigern** wählen.

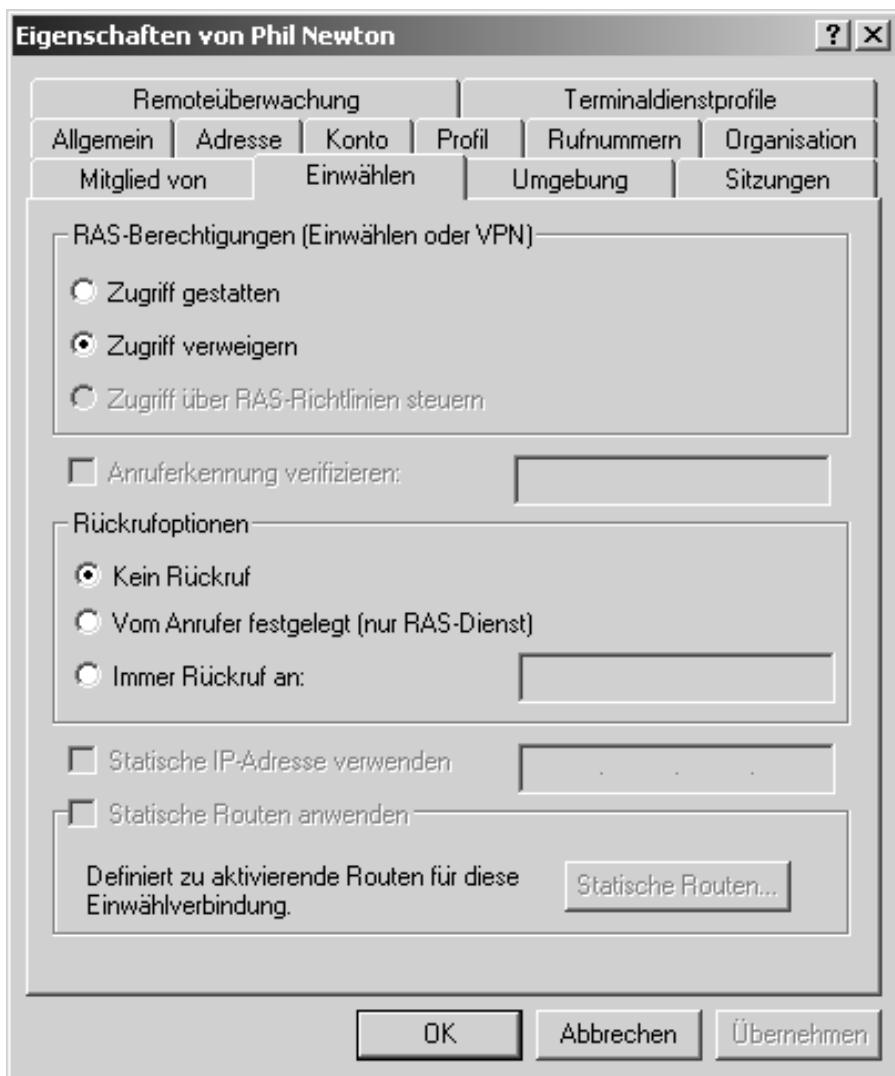


Abbildung 11.7: Die Registerkarte Einwählen im Dialogfeld Eigenschaften von [Benutzer]

Die andere hier zur Verfügung stehende Option dient der Sicherheit. Dabei handelt es sich um *Rückrufoptionen*. Die Idee dabei ist die, dass der Server Benutzer, die sich im Netzwerk einwählen, zurückruft, um sicher zu stellen, dass diese auch tatsächlich die Benutzer sind, die sie vorgeben zu sein bzw. dass diese sich an einem bereits geprüften Standort befinden.

Am sichersten ist es, wenn das System den Anrufer immer über eine bestimmte Rückrufnummer zurückruft. Es ist jedoch auch möglich, dass der Anrufer eine Rückrufnummer festlegt. Dabei geht es darum, dass der Benutzer wissen muss, dass die Rückrufoption erforderlich ist. Diese Option bietet allerdings auch die Flexibilität, dass einer Ihrer Benutzer zu einem Konkurrenten Ihres Unternehmens wechselt und von dort aus Ihre Kundenliste herunterlädt. Das ist natürlich unsinnig.

Computer-Einschränkungen

Es ist darüber hinaus auch möglich, den Computer zu schützen, auf den ein Benutzer über die Domäne zugreifen kann. Wenn beispielsweise ein Praktikant angestellt wird, der nur an seinem PC arbeiten soll, können Sie der Domäne mitteilen, dass sich der Praktikant nur über seinen PC anmelden darf. Wenn Sie sich vor Augen führen, dass die größte Bedrohung für die Sicherheit ein unbeaufsichtigter, angemeldeter Arbeitsplatzrechner ist, dann dürfte klar sein, wie wichtig diese Sicherheitsvorkehrung ist.

Die entsprechende Änderung können Sie im Dialogfeld **Eigenschaften** des Benutzers auf der Registerkarte **Konto** vornehmen, indem Sie auf die Schaltfläche **Anmelden** klicken (siehe Abbildung 11.8).

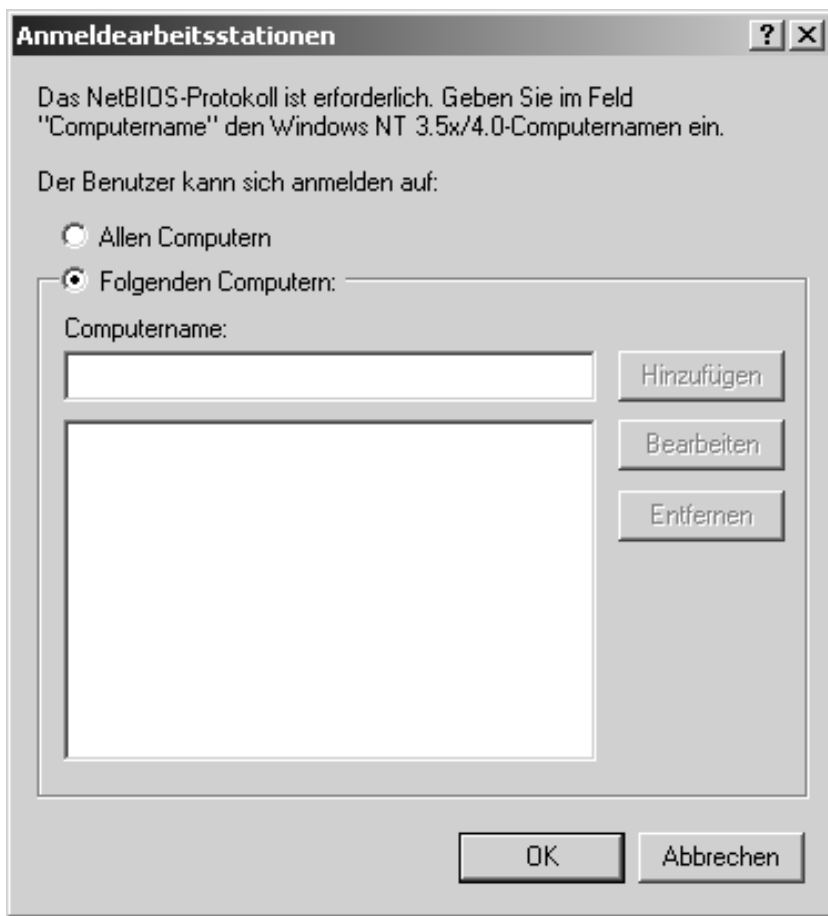


Abbildung 11.8: Das Dialogfeld Anmeldearbeitsstationen

Wenn Sie sich in diesem Dialogfeld befinden, geben Sie einfach den Namen des Computers ein, an dem sich der Benutzer anmelden darf, und klicken dann auf die Schaltfläche **Hinzufügen**.

Kontooptionen

Mit vielen der Optionen auf der Registerkarte **Konto** können unterschiedliche Arten von Konten gesteuert werden.

Mit den Kontooptionen auf dieser Registerkarte können viele Dinge gestattet bzw. verweigert werden. Die folgende Ausführung soll dazu beitragen, dass Sie diese Optionen verstehen und wissen, warum diese verwendet werden:

- **Benutzer muss Kennwort bei nächster Anmeldung ändern.** Der Benutzer wird aufgefordert, ein neues Kennwort zu verwenden, wenn er sich das erste Mal anmeldet. Damit soll ermöglicht werden, dass Sie zwar bei einer Einführung Kennwörter vergeben, die Benutzer die Kennwörter von da an jedoch selbst definieren. Damit wird die Sicherheit verstärkt, indem jeder Einzelne die Verantwortung für diese Aufgabe innerhalb seiner eigenen Konten selbst übernimmt.
- **Benutzer kann das Kennwort nicht ändern.** Wenn Sie sämtliche Kennwörter verwalten, muss diese Option gewählt werden, um zu verhindern, dass Benutzer ihre Kennwörter selbst ändern.
- **Kennwort läuft nie ab.** Das ist das Kennzeichen eines Unternehmens mit geringem Sicherheitsbedürfnis oder eines faulen Administrators. Damit gibt es aber natürlich weniger Nachfragen nach Kennwörtern.
- **Kennwort mit reversibler Verschlüsselung speichern.** Diese Option wird für Macintosh-Clients verwendet, die sich mit einem Apple-Client anmelden. Wenn sich Macintosh-Clients mit der Auswahl anmelden, muss diese Option aktiviert sein.
- **Das Konto ist deaktiviert.** Diese Option wird verwendet, um das Konto vorübergehend zu deaktivieren. Wenn ein Konto gelöscht werden soll, ist es besser, das Konto zunächst nur zu deaktivieren. Nehmen wir beispielsweise einmal an, Ihr Vorgesetzter sagt Ihnen, Sie sollen Pauls Konto löschen, weil Paul entlassen wird. Wenn Sie jedoch sehen, wie Paul aus dem Büro des Vorgesetzten mit einem Lächeln herauskommt und der Vorgesetzte und Paul einander die Hände schütteln, haben Sie bestimmt Zeit gespart, da Sie Pauls Konto nicht neu zu erstellen brauchen. Wenn Paul jedoch tatsächlich entlassen wird, dann können Sie sein Konto immer noch löschen.
- **Benutzer muss sich mit einer Smartcard anmelden.** Mit Hilfe von Smartcards ist es möglich, dass das System jedes

Mal, wenn sich ein Benutzer anmeldet, ein anderes Kennwort verwendet. Diese Option ermöglicht es dem Administrator, ausschließlich diese Art der Anmeldung zu verwenden.

- **Konto wird für Delegierungszwecke vertraut.** Mit diesem Konto können anderen Konten Berechtigungen innerhalb des Verzeichnisses zugewiesen werden.
- **Konto kann nicht delegiert werden.** Damit wird festgelegt, dass dem Konto kein delegierter Teil des Verzeichnisses zugewiesen werden kann. Sie mögen sich fragen, warum nicht einfach die Berechtigung delegiert wird. Mit dieser Option kann ein Administrator in einer großen Umgebung einen anderen warnen und damit verhindern, dass ein Konto delegiert wird.
- **DES-Verschlüsselungstypen für dieses Konto verwenden.** Aktivieren Sie diese Option, wenn Sie die DES-Unterstützung (Data Encryption Standard) aktivieren möchten. DES unterstützt mehrere Verschlüsselungsebenen.
- **Keine Kerberos-Präauthentifizierung erforderlich.** Aktivieren Sie diese Option, wenn das Konto eine andere Implementierung des Kerberos-Protokolls verwendet. Nicht alle Implementierungen oder Varianten des Kerberos-Protokolls unterstützen diese Funktion. Das Kerberos Key Distribution Center (Schlüsselverteilungscenter) verwendet für die Zuweisung der Netzwerkauthentifizierung innerhalb einer Domäne ticketgenehmigende Tickets. Der Zeitpunkt, zu dem ein ticketgenehmigendes Ticket vom Schlüsselverteilungscenter ausgegeben wird, ist für das Kerberos-Protokoll von Bedeutung. Windows 2000 verwendet andere Mechanismen zur Zeitsynchronisierung, sodass auch die Kerberos-Präauthentifizierung eingesetzt werden kann.

Die letzte Option auf der Registerkarte **Konto** dient lediglich dazu, für ein Konto ein Ablaufdatum festzulegen. Damit können temporäre Konten erstellt werden. Das ist dann recht nützlich, wenn für Zeitarbeiter oder Praktikanten Konten eingerichtet werden, die bei all den anderen verwaltungstechnischen Aufgaben leicht in Vergessenheit geraten können.

Die Anwendung dieser Option ist so einfach wie sie aussieht. Sie legen das Ablaufdatum fest, indem Sie einfach das Optionsfeld **Am** aktivieren und dann ein Datum angeben. Nach Ablauf dieses Tages kann sich der Benutzer nicht mehr am System anmelden.

11.2 Datenträgerkontingente

Das Netzwerkbetriebssystem Windows benötigt schon seit längerem eine Steuerungsfunktion der durch ständig anwachsende Benutzerzahlen kontinuierlich zunehmenden Nutzung der Festplatte. In Windows 2000 gibt es nun diese Funktion. Sie wird von einem Datenträger aus implementiert und stellt keine völlige Benutzerbeschränkung dar, wie das bei NetWare der Fall ist. Sie bietet jedoch weitaus bessere Steuerungsmöglichkeiten.

Um eine Beschränkung des Datenträgerkontingents zu definieren, müssen Sie zunächst einmal die Kontingentverwaltung auf dem Datenträger aktivieren. Dazu gehen Sie wie folgt vor:

1. Klicken Sie auf dem Server mit der rechten Maustaste auf das Symbol des Datenträgers und wählen Sie dann die Option **Eigenschaften**.
2. Aktivieren Sie die Registerkarte **Kontingent** (siehe Abbildung 11.9).

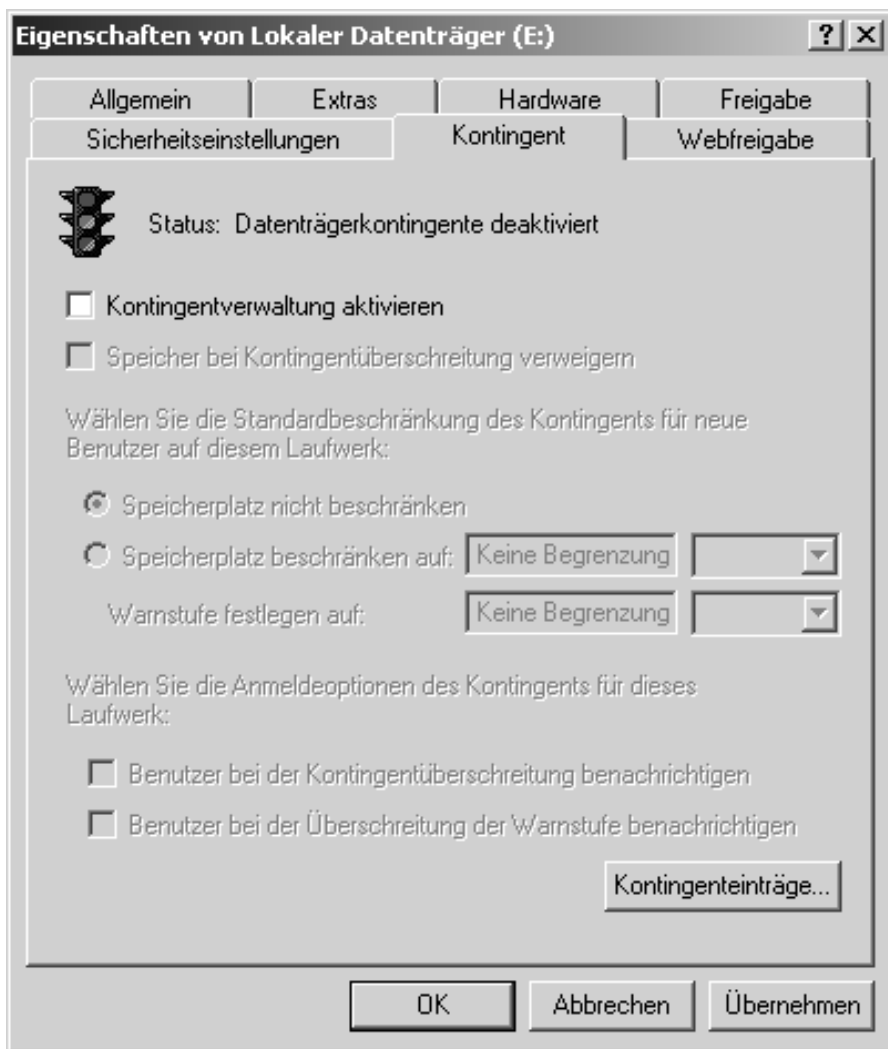


Abbildung 11.9: Die Registerkarte Kontingent im Dialogfeld Eigenschaften von [Datenträger]

3. Aktivieren Sie das Kontrollkästchen **Kontingentverwaltung aktivieren**.

4. Klicken Sie auf **OK**.

Wenn Sie das erledigt haben, können Sie damit beginnen, Kontingente zu definieren.

Im ersten Dialogfeld sind viele Einstellungen vorzunehmen, noch bevor Sie die eigentlichen Kontingente festlegen. Dabei handelt es sich um Anweisungen an das System in Bezug darauf, wie mit möglichen Überschreitungen der Kontingente umgegangen werden soll:

- **Speicher bei Kontingentüberschreitung verweigern.** Mit dieser Option wird verhindert, dass Benutzer weiter Daten auf dem Datenträger speichern, wenn sie das ihnen zugewiesene Kontingent überschreiten. Daraus könnte geschlossen werden, dass der Benutzer allein dadurch gestoppt wird, dass Sie eine Beschränkung definieren. Das ist jedoch nicht der Fall. Indem Sie Grenzen setzen, errichten Sie lediglich eine Schwelle für das Auslösen einer Reihe von Reaktionen, von denen eine verhindert, dass ein Benutzer Daten auf einem Datenträger speichert, wenn das Kontingent überschritten ist.
- **Wählen Sie die Standardbeschränkung des Kontingents für neue Benutzer auf diesem Laufwerk.** Mit den hier zur Verfügung stehenden Optionen stellen Sie sicher, dass für Benutzer eine Beschränkung definiert ist, falls für diesen keine Beschränkung manuell konfiguriert wurde.
- **Wählen Sie die Anmeldeoptionen des Kontingents für dieses Laufwerk.** Mit den hier gewählten Optionen können Sie festlegen, was geschehen soll, wenn ein Benutzer das Kontingent überschritten hat. Sie können damit Benutzer warnen, falls sie die Grenze ihres Kontingents erreichen.

Um ein neues Kontingent zu definieren, öffnen Sie zunächst das Dialogfeld **Eigenschaften** des Laufwerks und aktivieren die Registerkarte **Kontingent**. Gehen Sie dann wie folgt vor:

1. Klicken Sie auf die Schaltfläche **Kontingenteinträge**.

2. Klicken Sie anschließend auf **Kontingent** und wählen Sie dann die Option **Neuer Kontingenteintrag**.

3. Wählen Sie aus dem Dropdown-Menü **Suchen in** die Domäne aus, die den Benutzer oder die Gruppe enthält, deren Kontingent beschränkt werden soll.
4. Klicken Sie auf den Benutzer- oder Gruppeneintrag und dann auf die Schaltfläche **Hinzufügen**. Wiederholen Sie diesen Schritt, bis sich alle gewünschten Benutzer- bzw. Gruppenobjekte im unteren Feld befinden. Klicken Sie auf **OK**.
5. Wählen Sie in dem nun erscheinenden Dialogfeld **Kontingenteinträge** die Option **Speicherplatz beschränken auf** und geben Sie dann die Werte für den Speicherplatz und die Warnstufe ein (siehe Abbildung 11.10).
6. Klicken Sie auf **OK** und schließen Sie die Konsole **Kontingenteinträge**.

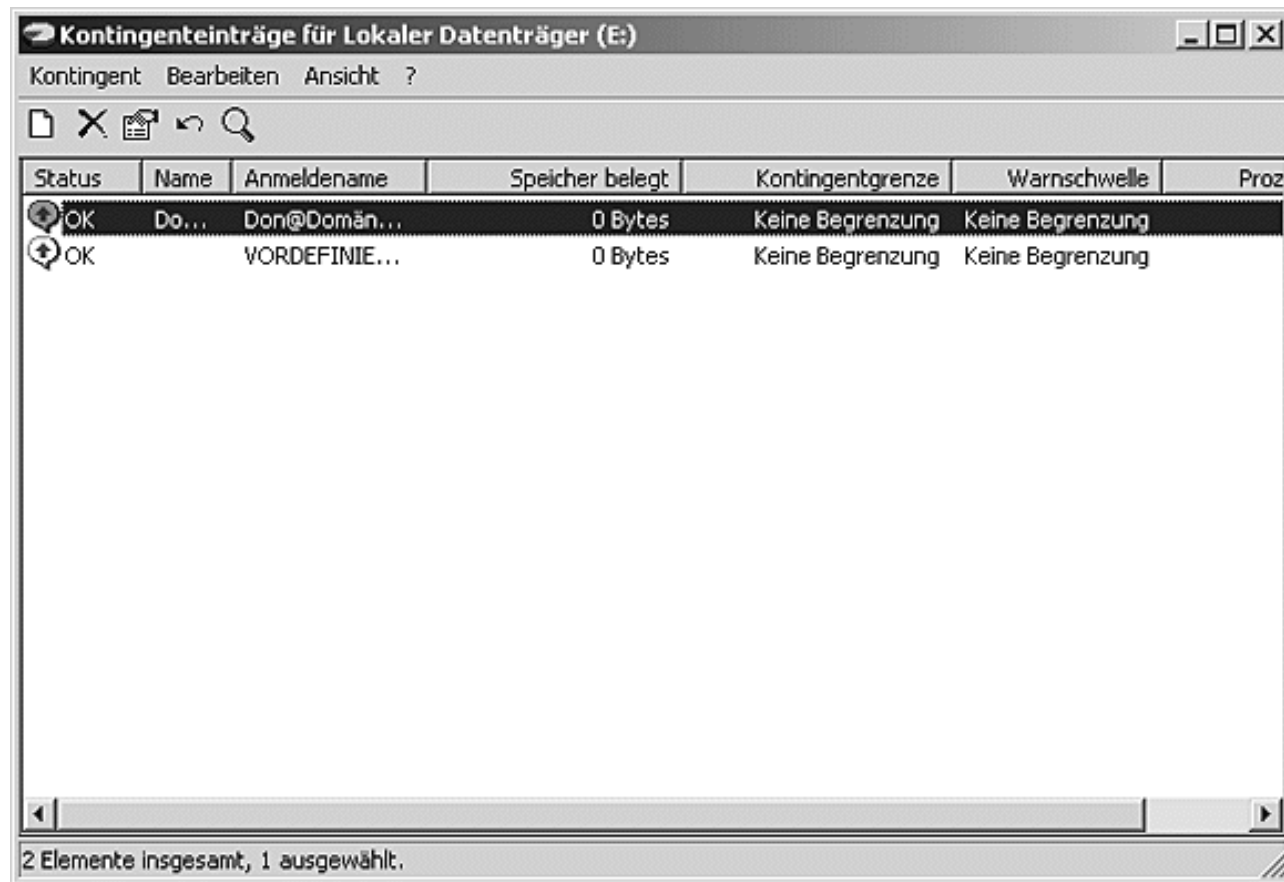


Abbildung 11.10: Die Konsole Kontingenteinträge

11.3 Gruppen

Gruppen von Benutzerkonten bei Windows 2000 bedeuten die Zusammenfassung von Benutzerkonten, um gleichzeitig mehrere Benutzerkonten überwachen zu können. Das ist wie bei Viehherden: Es dürfte ziemlich aufwändig sein, jede Kuh einzeln auf die Weide zu treiben. Daher sollten Sie sich, wenn Sie mit der Verwaltung von Benutzern beginnen, als Erstes darum kümmern, Benutzer zu Gruppen zusammenzufassen.

11.3.1 Gruppenbereich

Unter *Gruppenbereich* versteht man die Stelle im Verzeichnis, die der Gruppe zugewiesen wird, sowie mögliche Mitgliedschaften der Benutzer. Es gibt drei Gruppenbereiche: »Lokale Domäne«, »Global« und »Universal«.

Die Auswahl des Gruppenbereichs hängt vom Betriebsmodus ab, in dem sich das Sicherheitssystem derzeit befindet. Wenn sich die Domänencontroller im gemischten Modus befinden, stehen nur die Gruppenbereiche »Lokale Domäne« und »Global« zur Verfügung. Das kommt daher, weil Windows NT die Verschachtelung von Gruppen nicht zulässt. Im einheitlichen Modus sind alle drei Optionen verfügbar und Gruppen können Mitglieder von Gruppen sein, d.h., die Verschachtelung von Gruppen ist möglich.

Gruppenbereich »Lokale Domäne«

Der Gruppenbereich »Lokale Domäne« in Active Directory (Windows 2000) ist die Reinkarnation der guten alten lokalen Gruppen von Windows NT. Wenn lokale Gruppen von Windows NT übernommen werden, werden diese zu Gruppen der lokalen Domäne.

Gruppen der lokalen Domäne werden verwendet, um Ressourcen in der lokalen Domäne zu verwalten. Darin unterscheiden sich diese Gruppen von den alten lokalen Gruppen ein wenig. Dennoch ähneln sich diese beiden Gruppen in ihrer Grundkonzeption. Eine Gruppe der lokalen Domäne kann folgende Mitglieder enthalten:

- Gruppen mit dem Bereich »Global«
- Gruppen mit dem Bereich »Universal« (nur im einheitlichen Modus)
- Benutzerkonten
- andere Gruppen mit dem Bereich »Lokale Domäne« (nur im einheitlichen Modus)
- eine beliebige Kombination der oben genannten Objekte (abhängig vom Modus)

Die Idee, die dahinter steckt, ist die, dass Gruppen der lokalen Domäne verwendet werden, um darin Konten und Gruppen unterzubringen, die eine bestimmte Ressource gemeinsam nutzen. Wenn die Gruppe für die Ressource erstellt ist und die Konten zur Gruppe hinzugefügt sind, ist es einfach, Benutzer hinzuzufügen und in Erfahrung zu bringen, welche Benutzer bzw. Gruppen Zugriff auf die Ressource haben, indem man einfach in der Gruppe der Ressource nachsieht.

Wenn Sie die gesamte Gruppe der Buchhaltung zu den Gruppen hinzufügen müssen, die auf die Laufwerkfreigabe `\\Servername\Buchhaltung` zugreifen dürfen, ist es am einfachsten, die Gruppe Rechnungswesen zu erstellen und die globale Gruppe Buchhaltung zur Gruppe der Ressource zuzuweisen. Wenn mit der Freigabe eigenartige Dinge geschehen, ist es nun einfacher festzustellen, wer Zugriff auf die Freigabe hatte und Änderungen lassen sich leichter vornehmen.

Gruppenbereich »Global«

Eine globale Gruppe ist bei Windows 2000 nicht dasselbe wie bei Windows NT. Sie wird jedoch sehr ähnlich verwendet. Eine Gruppe mit dem Bereich »Global« ist eine Gruppe, die für das tägliche Hinzufügen von Benutzern oder anderen Gruppen zu Gruppen, denen später Ressourcen zugewiesen werden, verwendet wird.

Die Schlüsselwörter hier sind *Benutzer* und *täglich*. Eine globale Gruppe unterscheidet sich von einer universellen Gruppe dadurch, dass die globale Gruppe nicht über die Grenzen der Domäne hinaus repliziert werden kann. Außerdem kann eine globale Gruppe keine Mitglieder von außerhalb der Domäne haben. Eine globale Gruppe kann folgende Mitglieder enthalten:

- Globale Gruppen aus ihrer eigenen Domäne (nur im einheitlichen Modus)
- Benutzerkonten
- Eine beliebige Kombination der oben genannten Objekte (abhängig vom Modus)

Wenn die Mitgliedschaft von globalen Gruppen geändert wird oder wenn die einer globalen Gruppe zugewiesenen Berechtigungen geändert werden, werden diese Änderungen nur innerhalb der Domäne repliziert.

Aus diesem Grund ist es sinnvoll, Benutzer globalen Gruppen und dann die globalen Gruppen den Gruppen der lokalen Domäne zuzuweisen, die den Zugriff auf die Ressourcen steuern. Das Problem dabei ist jedoch, dass im gemischten Modus globale Gruppen von anderen Domänen nicht zu globalen Gruppen zugewiesen werden können, die erstellt worden sind, um sämtliche Benutzer zusammenzufassen.

Gruppenbereich »Universal«

Gruppen mit dem Bereich »Universal« stehen nur im Domänenmodus zur Verfügung. Universelle Gruppen in ihrer reinsten Form kann man sich als domänenübergreifende Lösung für Gruppen vorstellen, die Domänengrenzen überschreiten müssen. Es ist verlockend, sich universelle Gruppen als »magische« lokale Gruppen vorzustellen, die die Grenzen von Domänen überschreiten können. Universelle Gruppen können folgende Mitglieder enthalten:

- globale Gruppen aus einer beliebigen Domäne
- Gruppen mit dem Bereich »Universal«
- Benutzerkonten

Am besten ist es, wenn diese universellen Gruppen erstellt, diesen die globalen Gruppen zugewiesen und dann die universellen Gruppen der Gruppe der lokalen Domäne zugewiesen werden, die für die Ressource verantwortlich ist.

Untergliederung der Gruppen

Administratoren von lokalen Domänen können Benutzer zu den globalen Gruppen hinzufügen. Da diese globalen Gruppen Mitglieder der universellen Gruppen sind, die über Berechtigungen für den Zugriff auf die Ressource verfügen, haben die Mitglieder die Berechtigungen, die sie benötigen.

Für die domänenübergreifende Replikation sind lediglich die Namen der globalen Gruppen erforderlich, die den universellen Gruppen angehören. Da diese Mitgliedschaft sehr selten geändert werden muss, kommt es praktisch nicht zur Replikation. Domäneninterne Replikationen kommen vor, sind jedoch auf die Mitglieder der Domäne beschränkt.

Die Gruppen der lokalen Domäne tragen dazu bei, dass der lokale Administrator einen genauen Überblick über die Gruppen und Benutzerkonten hat, die Zugriff auf die Ressourcen haben. Darüber hinaus erleichtern diese Gruppen das Entfernen und Hinzufügen von Gruppen, da nicht jede einzelne Gruppe, der Berechtigungen zugewiesen worden sind, gesucht werden muss.

11.3.2 Erstellen einer neuen Gruppe

Um eine Gruppe zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie die Konsole **Active Directory-Benutzer und -Computer** und wählen Sie das Containerobjekt, zu dem Sie das Gruppenobjekt hinzufügen möchten. Dies kann der Benutzercontainer für die Domäne oder eine beliebige Organisationseinheit sein, die bereits erstellt ist.
2. Klicken Sie mit der rechten Maustaste auf das Containerobjekt und wählen Sie dann die Optionen **Neu** und **Gruppe**.
3. Geben Sie den Namen der neuen Gruppe ein und drücken Sie dann auf die (Tab)-Taste.
4. Geben Sie, falls erforderlich, den Gruppennamen für Clients mit älteren Windows-Versionen ein und drücken Sie dann auf die (Tab)-Taste.
5. Geben Sie den Gruppenbereich ein.
6. Klicken Sie auf **OK**.

11.3.3 Vordefinierte Standardgruppen

Wie Benutzerkonten, so verfügt auch das Betriebssystem Windows 2000 über vordefinierte Gruppen, die verfügbar werden, wenn ein Computer und/oder eine Domäne eingerichtet wird. Diese Gruppen werden als eine Art öffentliche Gruppenfunktion erstellt. Die grundlegenden Funktionen der Domäne gehören zu diesen Gruppen.

Einige der Gruppen sind Teil von Windows 2000 in jeder Form (Arbeitsgruppe oder Domäne), während andere erst erstellt werden, wenn eine Domäne eingerichtet wird.

Darüber hinaus gibt es so genannte *implizite Gruppen*, die nur für die zugewiesenen Berechtigungen verfügbar sind. Zu diesen Gruppen können keine Mitglieder hinzugefügt werden. Sie sind außerdem in der Konsole **Active Directory-Benutzer und -Computer** nicht zu sehen. Das kommt daher, weil sie vom Betriebssystem ausschließlich für das Betriebssystem erstellt werden. Wenn Sie sich die Beschreibungen der Gruppen einmal durchlesen, wird deutlich, wozu diese Gruppen benötigt werden.

Im Folgenden sind nun die vordefinierten Gruppen aufgeführt:

- *Konten-Operatoren (nur Domäne)*. Mitglieder dieser Gruppe können die Benutzer- und Gruppenkonten auf dem lokalen Computer ändern. Domänenbenutzer und Gruppen gehören nicht dazu.
- *Administratoren (Domäne und lokal)*. Mitglieder dieser Gruppe können sämtliche Aufgaben auf dem lokalen Computer ausführen. Mitglieder dieser Gruppe auf dem Domänencontroller sollten Mitglieder der Gruppe für alle Computer in der Domäne sein.
- *Sicherungs-Operatoren (Domäne und lokal)*. Mitglieder dieser Gruppe dürfen Dateien und Ordner des Systems sichern und wiederherstellen. Sie dürfen außerdem das System herunterfahren.
- *Ersteller-Besitzer (implizit)*. Der Ersteller eines Objekts (Datei, Druckauftrag, Ordner usw.) wird automatisch Mitglied der Gruppe Ersteller-Besitzer für dieses Objekt. Damit verfügt der Benutzer über sämtliche Berechtigungen für das Objekt.
- *Jeder (implizit)*. Eine integrierte und transparente Gruppe, die sämtliche im System authentifizierten Benutzer enthält.

Der Unterschied zwischen den Gruppen Benutzer und Jeder ist der, dass die Gruppe Benutzer Mitglieder der Domäne sind, während die Gruppe Jeder lokale Benutzer und/oder Domänenbenutzer enthält. Denken Sie daran, dass anonyme Benutzer über den IIS-Server ebenfalls dazu gehören.

- *Gäste (Domäne und lokal)*. Mitglieder dieser Gruppe dürfen auf alle Ressourcen zugreifen, auf die die Gruppen Jeder und Benutzer zugreifen dürfen.
- *Interaktiv (implizit)*. Jeder Benutzer, der an einem System lokal angemeldet ist.
- *Netzwerk (implizit)*. Jeder über das Netzwerk angemeldete Benutzer. Beachten Sie, dass anonyme Benutzer über den IIS-Server ebenfalls dazu gehören.
- *Druck-Operatoren (nur Domäne)*. Mitglieder dieser Gruppe dürfen sämtliche Druckerfunktionen steuern, d.h., sie dürfen Drucker freigeben, Drucker löschen und Druckaufträge starten, beenden und löschen.
- *Replikations-Operator (Domäne und lokal)*. Mitglieder dieser Gruppe dürfen Verzeichnisreplikationsaufträge erstellen, löschen und verwalten.
- *Server-Operatoren (nur Domäne)*. Mitglieder dieser Gruppe sind eigentlich Administratoren ohne die Kompetenzen von Konten-Operatoren. Server-Operatoren können sowohl Datei- als auch Druckerfreigaben steuern, erstellen und löschen. Sie sichern Dateien und stellen diese vom Server wieder her, aber sie können keine Berechtigungen für diese Aufgaben erteilen.
- *Benutzer (Domäne und lokal)*. Diese Gruppe ist eine lokale Gruppe auf dem Computer, auf dem diese Gruppe eingerichtet ist. Mitglieder sind sämtliche Benutzerkonten, die auf dem Computer erstellt wurden, und die Domänengruppe Domänenbenutzer, wenn der Computer Mitglied einer Domäne ist.
- *Domänen-Admins (nur Domäne)*. Eine globale Gruppe, die Mitglied der Gruppe Administratoren der lokalen Domäne ist. Die Mitglieder dieser Gruppe haben sämtliche Kompetenzen, die mit dieser Mitgliedschaft verbunden sind, und können darüber hinaus alles in der Domäne, in der Struktur und in der vertrauenden Gesamtstruktur steuern.
- *Domänencomputer (nur Domäne)*. Sämtliche in der Domäne erstellten Computerkonten werden automatisch Mitglied dieser Gruppe. Diese Gruppe kann an sämtliche Konten von Domänencomputern Änderungen vornehmen und für sämtliche Konten von Domänencomputern Eigenschaften festlegen.
- *Domänencontroller (nur Domäne)*. Sämtliche in der Domäne installierten Domänencontroller werden automatisch Mitglied dieser Gruppe. Diese Gruppe kann an sämtlichen Konten von Domänencontrollern Änderungen vornehmen und für sämtliche Konten von Domänencontrollern Eigenschaften festlegen.
- *Domänen-Gäste (nur Domäne)*. Eine globale Gruppe, die Mitglied der Gruppe Gäste der lokalen Domäne ist. Die Mitglieder dieser Gruppe haben sämtliche Kompetenzen, die mit dieser Mitgliedschaft verbunden sind.
- *Domänen-Benutzer (nur Domäne)*. Eine globale Gruppe, die Mitglied der Gruppe Benutzer der lokalen Domäne ist. Die Mitglieder dieser Gruppe haben sämtliche Kompetenzen, die mit dieser Mitgliedschaft verbunden sind.
- *Organisations-Admins (nur Domäne)*. Eine globale Gruppe, die Mitglied der Gruppe Administratoren der lokalen Domäne ist. Die Mitglieder dieser Gruppe haben sämtliche Kompetenzen, die mit dieser Mitgliedschaft verbunden sind, und können darüber hinaus alles in der Domäne, in der Struktur und in der vertrauenden Gesamtstruktur steuern.
- *Gruppenrichtlinien-Admins (nur Domäne)*. Mitglieder dieser Gruppe haben die Berechtigung, Gruppenrichtlinien innerhalb der Domäne zu bearbeiten und zu prüfen.
- *Schema-Admins (nur Domäne)*. Mitglieder dieser Gruppe können die Informationen im Schema bearbeiten. Dieses Active Directory-Schema kann verwendet werden, um Informationen zu speichern. Darüber hinaus kann es auch bearbeitet werden, um weitere Ressourcen innerhalb des Schemas zu definieren.
- *System (implizit)*. Vom Betriebssystem durchgeführte Operationen.

Kapitel 12 IntelliMirror und Benutzersteuerung

Das zu steuern, womit der Benutzer konfrontiert wird, wenn er sich an den PC setzt, ist eine der besten Möglichkeiten, jemanden zu kontrollieren. Bisher bestand die Steuerung des Benutzers darin, das Benutzerkonto zu erstellen und die Arbeitsumgebung zu steuern, indem Skripten erstellt und Berechtigungen verwaltet werden. Die neue Idee ist aus Sicht des Benutzers zwar »ausgefuchster«, kann dafür allerdings nützlicher sein. In diesem Kapitel geht es um die Verwendung von Richtlinien, Profilen und die direkte Installation von Software sowie die Verwaltung, um alles zu steuern, was der Benutzer bei seiner täglichen Arbeit vor sich hat. All dies wird in einer Gruppe von Technologien mit der Bezeichnung *IntelliMirror* zusammengefasst.

IntelliMirror kann man sich als die Realisierung von ZAW (Zero Administration für Windows) vorstellen. Die Idee, die sich hinter ZAW und IntelliMirror verbirgt, ist die, dass Administratoren mit Hilfe von Netzwerk-Tools ein weniger verwaltungsintensives Netzwerk einrichten können. Der Unterschied zwischen ZAW und IntelliMirror ist der, dass die IntelliMirror-Technologie integraler Bestandteil des Betriebssystems ist. IntelliMirror ist keine Gehhilfe für das Betriebssystem. IntelliMirror unterstützt wie ZAW-Tools, die das Betriebssystem zur Verfügung stellt.

IntelliMirror ist kein Programm, das Sie ausführen können, und keine Anwendung, die in Windows 2000 neu ist. ZAW enthält eine eigene Schnittstelle. IntelliMirror ist vielmehr eine Technologierichtung, die von Windows 2000 eingeschlagen wird. Wenn ein Administrator von der IntelliMirror-Technologie spricht, meint er damit eine Reihe von Technologien, die eine leistungsfähigere Verwaltung ermöglichen und für den Benutzer ein höheres Maß an Komfort bieten. IntelliMirror bedeutet die intelligente Spiegelung (engl. mirroring) der Benutzerumgebung über Arbeitsplatzrechner, LANs und sogar WANs hinweg.

12.1 Grundelemente von IntelliMirror

IntelliMirror vereint drei unterschiedliche Technologiegruppen, die Sie in diesem Kapitel kennen lernen werden:

- *Verwaltung der Benutzereinstellungen.* Durch die Verwendung von Richtlinien kann der Administrator die Arbeitsumgebung des Benutzers steuern und er kann Active Directory nutzen, um diese Richtlinien über das Netzwerk verfügbar zu machen.
- *Verwaltung der Benutzerdaten.* Mit Hilfe der Funktionen von Active Directory für die Steuerung der Einstellungen für Benutzerprofile, Anmeldeskripten und Gruppenrichtlinien kann der Administrator sicherstellen, dass der Benutzer über eine einheitliche Speicherstruktur verfügt. Diese Plattform sorgt darüber hinaus auch für die Replikation und Sicherung der Benutzerdaten.
- *Installieren und Warten von Software.* Durch die Verknüpfung der Software-Installation mit der Leistungsfähigkeit von Active Directory können Sie sicherstellen, dass eine Anwendung auch vorhanden ist, wenn sich der Benutzer an der Domäne anmeldet, und dass diese auch betriebsbereit ist.

12.2 Steuerungskonzepte

Bei der Steuerung dessen, was der Benutzer täglich in seiner Arbeitsumgebung sieht, spielt sowohl die Sicherheit als auch der Komfort eine Rolle.

Aus sicherheitstechnischer Sicht ist das Haus, in das am wenigsten wahrscheinlich eingebrochen wird, dasjenige, das nicht zu sehen ist. Ein guter Mensch, der den Ordner für die Gehälter nie auf dem Server sieht, wird aller Wahrscheinlichkeit nach ein guter Mensch bleiben. Ein Hacker, der das Symbol **Netzwerkumgebung** nicht sieht, wird sich die Liste der Server wohl eher nicht ansehen. Wenn die Eingangstür nicht zu sehen ist, ist die Versuchung einzubrechen nicht so groß.

Das zweitsicherste Haus ist das, das gut beleuchtet ist. Wenn der Dieb davon ausgehen muss, von allen gesehen zu werden, wenn er in das Haus eindringt, ist die Versuchung weitaus geringer. Wenn Benutzern ein bestimmtes Aussehen und Gefühl gegeben wird, wird ihnen bewusster, dass sie sich an einer Stelle befinden, an der sie sich eigentlich nicht befinden dürften.

Ein Beispiel dafür ist ein Schulsystem, bei dem für die Anmeldung der Lehrer und Administratoren andere Symbole und ein anderer Hintergrund verwendet wird, als für die der Schüler. Wenn ein Lehrer an einem Computer vorbeigeht und einen Schüler mit dem Hintergrund für Lehrer auf dem Bildschirm sieht (nehmen wir einmal an, einen hellblauen Hintergrund), ist der Schüler ertappt. Der Schüler wird auch nicht lange vor einem Bildschirm sitzen, der ruft: »Ich will gerade einbrechen.«

Für die meisten Benutzer ist es ein Alptraum, in einer Umgebung arbeiten zu müssen, in der sie die Daten von anderen vernichten oder vertrauliche Daten versehentlich sehen können. Der Computer macht ihnen schon so genügend Angst. Daher ist es am besten, diese Benutzer in einer Arbeitsumgebung unterzubringen, die nur deren Tools und Daten enthält. So befinden sich Benutzer in einer Umgebung, in der sie alle dargestellten Ressourcen nutzen können, ohne derartige Missgeschicke fürchten zu müssen.

Wenn Sie Angestellte für die Auftragsverwaltung vor Computer setzen, in denen sie Produkte suchen, Aufträge vergeben und mit ihren Vorgesetzten kommunizieren können, arbeiten diese gerne mit dem Computer. Wenn Sie diese Angestellten jedoch vor einen Computer setzen, auf dem ein Web-Browser, Solitär und ein Tabellenkalkulationsprogramm installiert sind, dürfen Sie sich nicht wundern, wenn die Angestellten im Internet surfen, Karten spielen und Berechnungen durchführen. Wenn sie die Gelegenheit zum Zeitverschwenden haben, verschwenden Menschen eben Zeit.

Windows 2000 bietet wie Windows NT auch schon Tools, mit denen die Benutzerumgebung gesteuert und einige dieser Möglichkeiten besser verfügbar und nutzbar gemacht werden können. Zu diesen Tools gehören die Benutzerprofile und die Richtlinien. Diese wiederum sind Teil des Active Directory.

Bei Windows NT mussten Richtlinien mit einem eigenen Hilfsprogramm erstellt und an einer zentralen Stelle gespeichert werden. Es war außerdem sehr schwierig, diese mit Benutzern und Gruppen zu koordinieren. Wie Sie sehen werden, lassen sich Richtlinien wesentlich einfacher integrieren und Profile sind nicht mehr schwierig.

12.2.1 Profile

Profile gibt es schon seit den Anfängen von Windows NT und Windows 95. Mit Profilen wird definiert, wie sich das Betriebssystem je nach angemeldetem Benutzer verhält. Wenn sich der erste Benutzer an Windows 95 anmeldet, wird er gefragt, ob das System die Einstellungen dieses Benutzers getrennt speichern soll. Der Benutzer wird außerdem aufgefordert, ein Kennwort einzugeben. Wenn er dies getan hat, wird ein Profil erstellt. Im Profil sind die Druckeroptionen, Anwendungseinstellungen, Desktop-Einstellungen usw. gespeichert. Wenn sich dieser Benutzer wieder anmeldet, werden wieder dieselben Einstellungen aktiviert.

Windows 2000 setzt diese Tradition fort. Wenn sich ein Benutzer an einem Windows 2000-Computer anmeldet, werden die Einstellungen des Benutzers auf dem System in einem Profil gespeichert. Das Profil, das ursprünglich erstellt worden ist, befindet sich auf dem lokalen Rechner. Es enthält das Menü **Start**, die Desktop-Symbole, das Menü **Programme** und sämtliche individuellen Anwendungseinstellungen für den Benutzer. Ein Administrator stellt beispielsweise fest, dass der Internet Explorer jedes Mal, wenn sich ein neuer Benutzer am System anmeldet, persönliche Einstellungen definiert und fragt, wie auf das Internet zugegriffen werden soll. Dies ist eine Eigenschaft von Profilen, die sich ändert, wenn sich die Benutzer ändern.

Benutzer gewöhnen sich mit der Zeit sehr an Profile. Es ist sogar so, dass sie aufgrund der durch das Profil gesteuerten Elemente denken, der Computer sei ihr eigener. Ein Bildschirmschoner, ein Foto vom letzten Angelausflug des Benutzers und eine Liste der Favoriten im Internet Explorer tragen dazu bei, dass der Benutzer meint, es handle sich um seinen eigenen Computer. Wenn sich dieser Benutzer nun an einen anderen Rechner setzt, an dem es all diese Elemente nicht gibt, tut sich dieser Benutzer schwer, mit diesem System zu arbeiten.

Generell gibt es zwei Arten von Profilen: lokale Profile und servergespeicherte Profile sowie eine Reihe von Variationen dieser Profile. Hier sollen nun zuerst einmal die lokalen und servergespeicherten Profile näher beschrieben werden.

Lokales Profil

Ein lokales Profil ist ein Profil, das vom lokalen Rechner angezeigt wird, wenn sich der Benutzer anmeldet. Wenn der Administrator keine andere Art von Profilen erstellt, ist dies das einzige Profil, das erstellt wird. Das Profil wird als *lokal* bezeichnet, da es sich auf dem lokalen Rechner befindet und jeweils pro Rechner erstellt wird. Daher wirken sich die Einstellungen, die auf einem Rechner definiert wurden, auf einem anderen Rechner nicht aus.

Bei Windows 2000 sind lokale Profile im Verzeichnis *Dokumente und Einstellungen\[USERNAME]* im Ordner des Betriebssystems gespeichert (siehe Abbildung 12.1). Wenn Sie diesen Ordner öffnen, können Sie die Elemente im Startmenü und auf dem Desktop anzeigen und ändern.

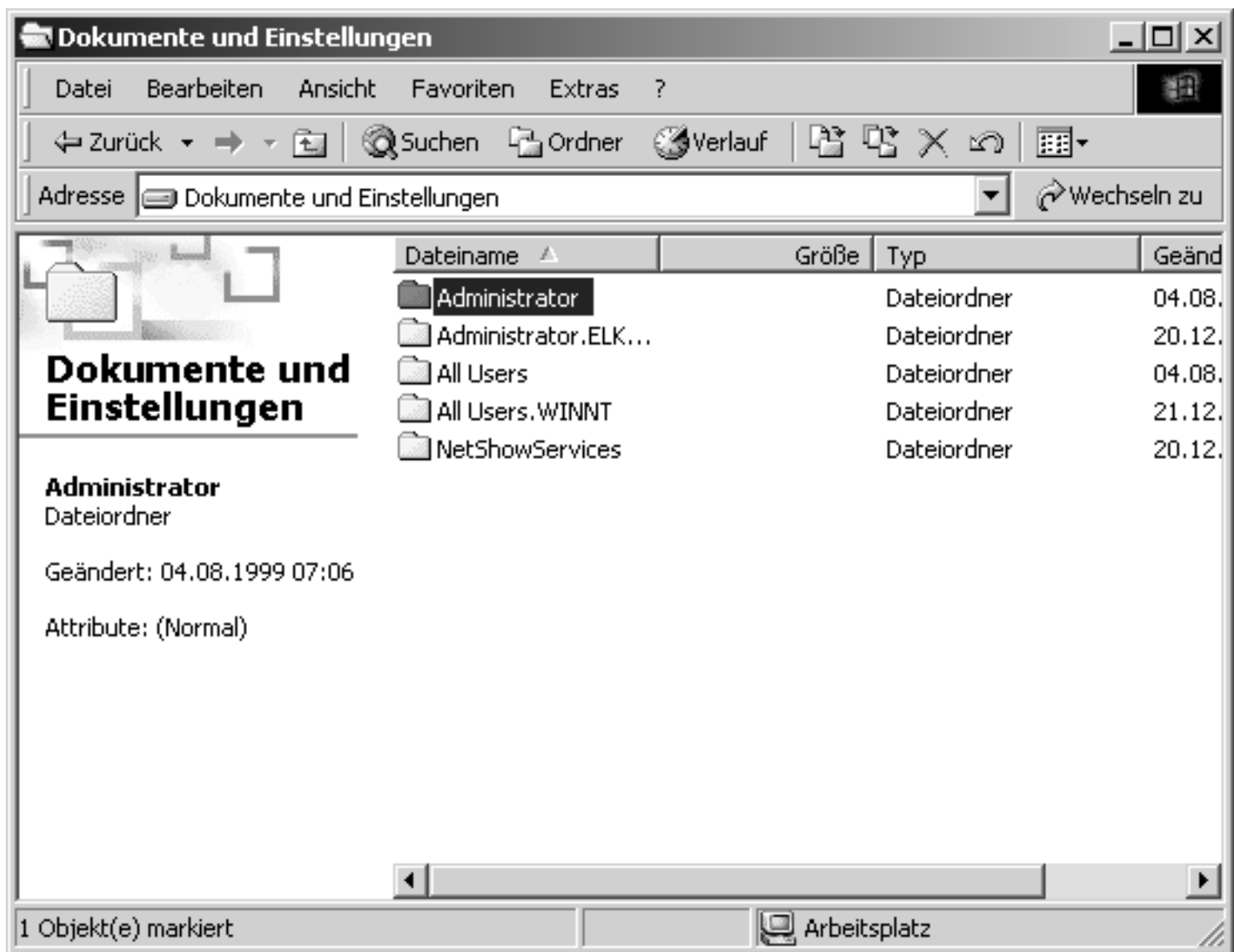


Abbildung 12.1: Profile im Verzeichnis Dokumente und Einstellungen

Beachten Sie, dass es Profile für »All Users« und »All Users.WINNT« gibt. Diese Profile definieren allgemeine Profilelemente, sodass das System allgemeine Elemente nicht immer wieder neu definieren muss.



Windows NT-Administratoren sollten wissen, dass der Speicherort der lokalen Profile geändert wurde. Das ist eine der wenigen Änderungen im Profilschema. Wenn Sie das jedoch nicht wissen, werden Sie viel Zeit mit Suchen vergeuden. In einigen technischen Beschreibungen von Windows 2000 wird nämlich immer noch der alte Speicherort genannt.

Servergespeichertes Profil

Servergespeicherte Profile bieten eine Möglichkeit, die Profileinstellungen auf jedem Arbeitsplatzrechner, an dem sich der Benutzer anmeldet, verfügbar zu machen. Ein servergespeichertes Profil muss nicht von einem kontrollierten Konto aus erstellt werden. Es kann von jedem Konto aus erstellt werden, das über ein Profil verfügt, das unter **Arbeitsplatz** auf der Registerkarte **Benutzerprofile** aufgeführt ist. Daher sieht der Reisebezirksleiter seinen Desktop auch dann, wenn er wieder in einem

neuen Büro ankommt, denn sein Profil wird direkt von seinem Computer kopiert.

Das, was im Eifer des Gefechts bei servergespeicherten Profilen häufig vergessen wird, ist, dass die erforderlichen Ressourcen am neuen Standort auch verfügbar sein müssen. Wenn beispielsweise das Logo des Unternehmens im Profil als Hintergrundbild gewählt wird und dieses auf dem Rechner, an dem sich der Benutzer anmeldet, nicht vorhanden ist, wird das Logo nicht als Hintergrundbild erscheinen. Das ist so einfach. Wenn die Netzwerkfreigabe für die Zuweisung eines Laufwerks nicht verfügbar ist, wird das Laufwerk nicht zugewiesen.

Schwierig wird es, wenn die »fehlende Ressource« dazu führt, dass eine Anwendung nicht mehr richtig oder überhaupt nicht mehr funktioniert. Servergespeicherte Profile funktionieren in einer Umgebung mit Systemen am besten, die mit identischer Software arbeiten. Identische Hardware wäre ideal, ist jedoch nicht erforderlich.

Verbindliches Profil

Ein servergespeichertes Profil kann aus Gründen eines einheitlichen Aussehens von vielen unterschiedlichen Benutzern verwendet werden. Diese Art von Profil wird allgemein definiert, sodass keiner der Benutzer dauerhafte Änderungen an diesem Profil vornehmen kann. Man spricht hier von einem *verbindlichen Profil*. Dabei ist es Benutzern nicht möglich, ihre persönlichen Einstellungen dauerhaft zu ändern, bzw. die Benutzer können diese Einstellungen ändern, werden jedoch, wenn sie sich am nächsten Tag am System anmelden, wieder die Standardeinstellungen vorfinden.

Verbindliche Profile verhindern, dass Benutzer freigegebene Profile so ändern, dass diese von anderen Benutzern nicht mehr verwendet werden können. Nur weil Hannes die BSE-Seite als seine Homepage haben möchte, bedeutet das noch lange nicht, dass jeder mit der Seite über die Auswirkungen von BSE konfrontiert werden möchte. Ziel ist es, alles allgemein und für alle ansprechend zu gestalten.

Aus einem servergespeicherten Profil ein verbindliches zu machen, ist sehr einfach. Dazu müssen Sie lediglich die Datei NTUSER.DAT im Verzeichnis **Profiles** in NTUSER.MAN umbenennen. Diese Datei kann an unterschiedlichen Stellen gespeichert sein, je nachdem, wie Sie die Einstellungen der Benutzerprofile gespeichert haben. Der Standardspeicherort der Datei ist jedoch die NETLOGON-Freigabe des Domänencontrollers. Geben Sie in der Eingabeaufforderung einfach folgenden Befehl ein:

```
ren ntuser.dat ntuser.man
```

Bestätigen Sie mit der (Enter)-Taste. Wenn sich der Benutzer das nächste Mal anmeldet, ist das Profil verbindlich.

Ein verbindliches Profil kann auch auf lokaler Ebene erstellt werden. Der Vorgang ist derselbe. Das ist jedoch weitaus weniger gebräuchlich.

Windows NT-Profil

Windows NT 4.0-Profile funktionieren so wie Windows 2000-Profile. Sie können ein Windows 2000-Profil erstellen, freigeben und davon ausgehen, dass sowohl NT- als auch 2000-Benutzer mit diesem Profil arbeiten können.

Windows 95/98-Profil

Servergespeicherte Windows 95/98-Profile sind zu Windows 2000-Profilen nicht kompatibel und werden anders gespeichert. Sie müssen folgende Änderungen am Netzwerk vornehmen, um servergespeicherte Profile für ein Windows 95/98-System zu verwalten:

- Sie müssen Benutzerprofile in Windows 95/98 aktivieren. Diese Einstellung finden Sie im Dialogfeld **Eigenschaften von Kennwörter** (siehe Abbildung 12.2).

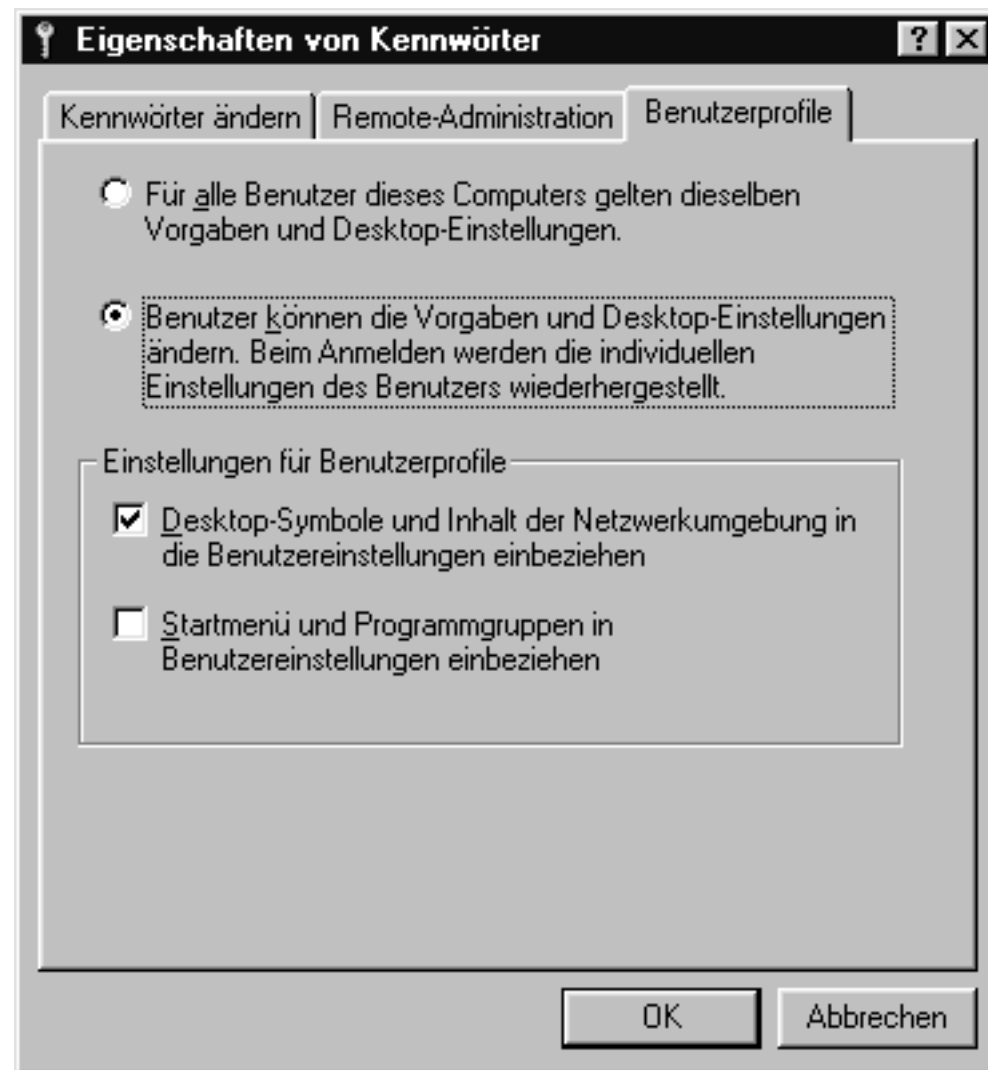


Abbildung 12.2: Dialogfeld für die Aktivierung von Profilen bei Windows 95

- Sie müssen Basisverzeichnisse für die Benutzer verwalten.
- Sie müssen einen 32-Bit-Netzwerk-Client (Microsoft-Client für Windows-Netzwerke) verwenden.
- Sie müssen Windows 95/98 so konfigurieren, dass es sich an der Domäne anmeldet.

Benutzerprofile werden bei Windows 95/98 in Ordnern im Verzeichnis *PROFILES* im Betriebssystemverzeichnis (*\Windows\Profiles*) erstellt. Wenn Profile aktiviert worden sind, gibt es hier für jeden Benutzer, der sich am Rechner angemeldet hat, ein Verzeichnis.

Anders als bei Windows 2000 und NT ist bei Windows 9x für das Erstellen eines servergespeicherten Profils kein spezieller Kopiervorgang erforderlich. Sie brauchen jedoch einen bestimmten Speicherort für Ordner und Dateien. Bei Windows 9x muss das Profil im Basisverzeichnis des Benutzers gespeichert

werden. Daher muss ein Benutzer mit einem servergespeicherten Profil über ein Basisverzeichnis verfügen.

Für diese Benutzer können Sie auch ein verbindliches Profil erstellen. Aber auch dafür ist ein Basisverzeichnis erforderlich. Um ein verbindliches Profil zu erstellen, erstellen Sie einfach ein servergespeichertes Profil und benennen Sie die Datei *USER.DAT* in jedem Verzeichnis, in das die Datei kopiert wird, in *USER.MAN* um.

12.2.2 Richtlinien: Eine allgemeine Einführung

Eine Benutzer- oder Gruppenrichtlinie steuert entsprechend der gewählten Optionen die Registrierung von Windows 2000 sowie das Verhalten des Betriebssystems. Der Hauptunterschied zwischen einer Richtlinie und einem Profil besteht darin, dass bei einer Richtlinie aus einem Menü von Elementen die Elemente gewählt werden können, die gesteuert werden sollen, und dass die Richtlinien Einzelnen oder Gruppen zugewiesen werden können.

Ein Vergleich, der vielleicht hilft, dass Sie sich unter Windows 2000-Richtlinien etwas vorstellen können: Stellen Sie sich diese Richtlinien einfach wie einen Unterbrecherschalter vor. Wenn jede Funktion des Betriebssystems an einer großen Schalttafel mit einem Schalter zu aktivieren bzw. zu deaktivieren wäre, dann wäre die Schalttafel vergleichbar mit den Richtlinien. Mit Hilfe der Richtlinien kann ein Administrator eine Funktion aktivieren, deaktivieren oder unverändert lassen. Wie bei Schalttafeln bleiben die Richtlinien von Windows NT und Windows 95/98 so, wie sie definiert wurden, bis sie wieder geändert werden.

In Abbildung 12.3 sind die Richtlinien für den Benutzer und den Desktop dargestellt. In diesem Beispiel kann der Administrator die Funktion deaktivieren, die dafür sorgt, dass das Symbol für die Netzwerkumgebung auf dem Desktop zu sehen ist. Es ist nicht viel Phantasie notwendig, um zu erkennen, wie sinnvoll es ist, die Ressourcen zu verstecken, die sich hinter diesem Symbol verbergen - es reichen nur wenige Tage als Administrator eines umfangreichen Netzwerks oder einer Gruppe von Schülern.

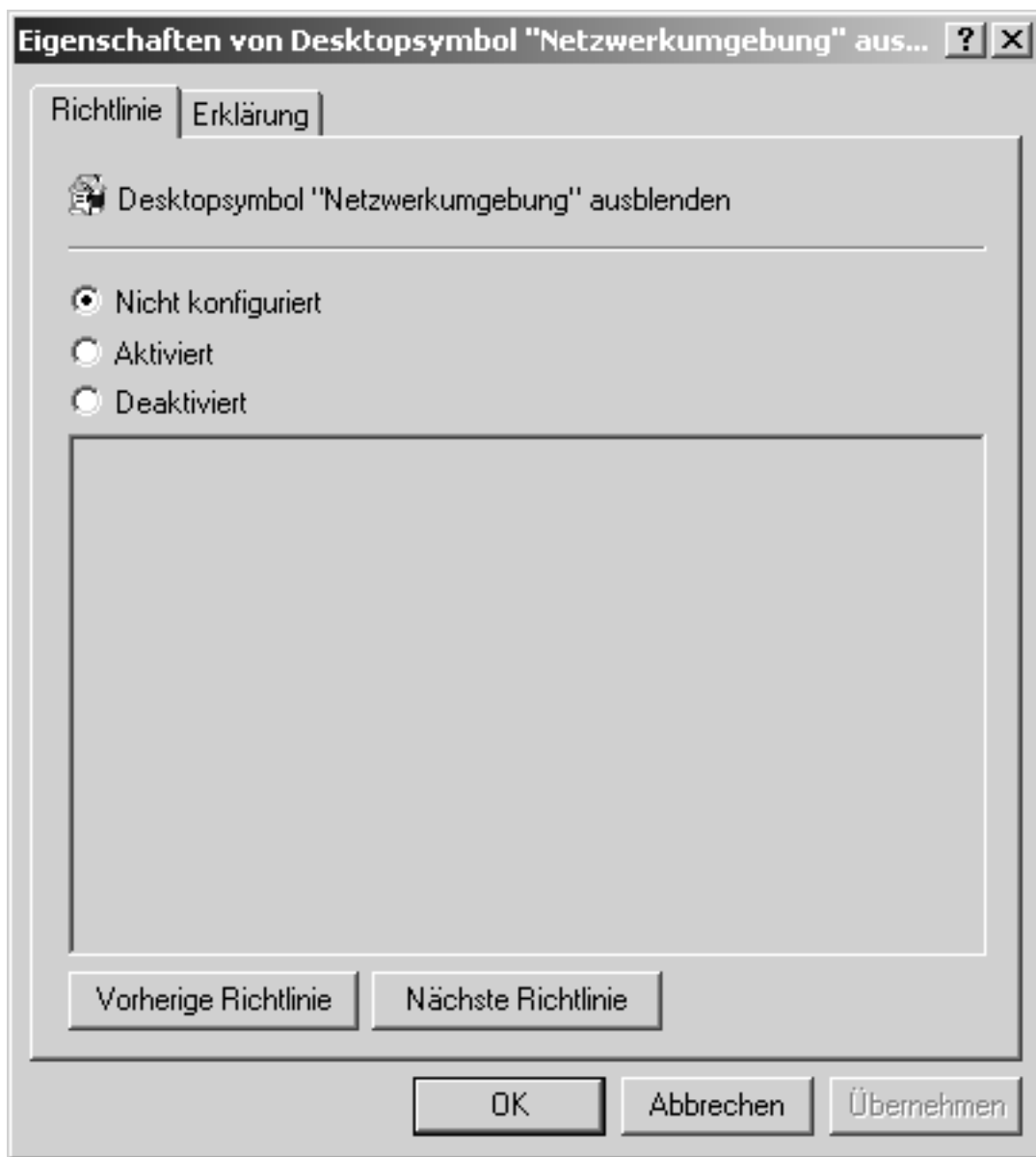


Abbildung 12.3: Beispiele für Beschränkungen durch Richtlinien

Windows 2000-Richtlinien beziehen sich nun auf Gruppen in Containerobjekten. Benutzergruppen werden in der Tat nur in Gruppenrichtlinien aus Gründen der Sicherheit und zum Filtern von Gruppenrichtlinien (darüber werden Sie später mehr erfahren) verwendet. Bei einer *Gruppe* in *Gruppenrichtlinien* kann es sich um das Containerobjekt Standort, Domäne oder Organisationseinheit handeln. Ebenso wie Anmeldeskripten Teil der Gruppenrichtlinie sind, ist die Gruppenrichtlinie Teil des Containerobjekts.

In jedem Containerobjekt werden so genannte Gruppenrichtlinienobjekte erstellt. Sämtliche Gruppenrichtlinienobjekte sehen zunächst gleich aus: leer, ohne Änderungen der Registrierungen. Die Objekte werden erst nützlich, wenn sie so bearbeitet werden, dass an der Registrierung des Windows 2000-Rechners, mit dem der Container in Kontakt kommt, Änderungen vorgenommen werden. Ein Container kann zahlreiche Gruppenrichtlinienobjekte enthalten, die unabhängig voneinander geändert werden können. Das kann sehr verwirrend sein. Wenn Sie weiterlesen, werden Sie erfahren, wie Sie das verhindern können.

Richtlinien werden, basierend auf der Verzeichnisstruktur, hierarchisch und im Gesamten angewendet.

Das bedeutet, dass der Benutzer sämtliche Richtlinien von jedem Container, auf den diese sich beziehen, zugewiesen bekommt, und dass diese Richtlinien in der Reihenfolge Standort, Domäne, Organisationseinheit und dann untergeordnete Organisationseinheiten, denen der Benutzer angehört, angewendet werden. Das ist die Reihenfolge, die bereits für Anmeldeskripten gilt. Das kommt daher, weil Anmeldeskripten Teil der Richtlinienstruktur sind.



Wenn es in der NETLOGON-Freigabe (die Datei *NTCONFIG.POL*) noch Windows NT- Richtlinien gibt, werden diese vor den Richtlinien von Standort, Domäne und Organisationseinheit angewendet. Wenn auf dem lokalen Computer, an dem sich der Benutzer anmeldet, lokale Computer-Richtlinien definiert sind, werden diese Richtlinien ebenfalls vor den Richtlinien von Standort, Domäne und Organisationseinheit angewendet. Dies ist zwar eher unwahrscheinlich, dennoch können diese Informationen bei der Fehlersuche recht hilfreich sein. So wissen Sie, dass die Richtlinien in einer anderen Reihenfolge, nämlich in der Reihenfolge *NTCONFIG.POL*, lokale Computer-Richtlinien, Standortrichtlinie, Domänenrichtlinie und Richtlinie der Organisationseinheit, angewendet werden.

Es ist nicht nur so, dass Richtlinien in jedem Container eine Anwendungsreihenfolge haben, sondern jeder Container kann mehrere Gruppenrichtlinien enthalten (siehe Abbildung 12.4). Diese Richtlinienobjekte werden entsprechend der Reihenfolge angewendet, in der Sie diese festlegen. Wenn Sie die Richtlinie auswählen, die als erste angewendet werden soll, und dann auf die Schaltfläche **Nach oben** klicken, können Sie die Reihenfolge ändern, in der die Richtlinien angewendet werden.

Der wichtige Hinweis hier ist der, dass es nicht am besten ist, erster zu sein. Wenn die Richtlinie für den Standort eine Einstellung enthält, mit der das Bild der drei Gründerväter des Unternehmens als Hintergrundbild definiert wird und mit der Richtlinie für die Organisationseinheit festgelegt wird, dass das Hintergrundbild die drei »Heinis« darstellt, dann werden die Benutzer die Kollegen Heinrich, Heinzi und Heinz zu sehen bekommen, nicht aber die drei Gründerväter. Das trifft für jede Reihenfolge der Richtlinien, auch innerhalb des Containers zu. Aus diesem Grund empfiehlt es sich, dafür zu sorgen, dass die wichtigsten Einstellungen zuletzt angewendet werden.

Damit leuchtet es auch besser ein, dass es besser ist, eine Richtlinie unabhängig vom Container zu erstellen und die Richtlinie dann dem Container zuzuweisen. Wenn Sie die beiden Vorgänge voneinander trennen, können Sie eine einheitliche Richtlinie definieren und diese dann den Containern auf der unteren Ebene zuweisen, um deren Anwendung sicherzustellen.



Abbildung 12.4: Mehrere Gruppenrichtlinien in einem Containerobjekt

Grundsätzlich wird zwischen zwei Arten von Richtlinien unterschieden:

- *Benutzerkonfiguration*. Einstellungen, die sich auf die Benutzer im Container beziehen und auf jedem Computer gelten.
- *Computerkonfiguration*. Einstellungen, die sich auf den Computer beziehen und unabhängig von dem an diesem Computer angemeldeten Benutzer gelten.

Der Unterschied zwischen diesen beiden Arten von Richtlinien wird an den Einstellungen für Windows-Einstellungen und Skripten deutlich. Sowohl die Benutzerkonfiguration einer Richtlinie als auch die Computerkonfiguration einer Richtlinie verfügen über Skripten. Die Computerkonfiguration hat jedoch kein Anmelde- und Abmeldeskript, da Computer sich weder an- noch abmelden. Statt dessen weist die Computerkonfiguration Skripten zum Starten und Herunterfahren auf. Diese Skripten werden erstellt, damit die Domäne beim Starten bzw. Herunterfahren auf dem im Container enthaltenen System bestimmte Befehle geben kann. Dies gilt insbesondere bei einem Standort.

Computer-Richtlinien werden synchron angewendet, d.h., sie werden angewendet, bevor der Benutzer

die Möglichkeit hat, sich anzumelden. Diese Einstellung kann geändert werden, sodass die Richtlinien asynchron angewendet werden. Das hat jedoch mehr Nachteile als Vorteile. Es wird nämlich sehr schwierig, Konflikte mit anderen Richtlinien vorherzusehen und zu korrigieren. Jede Richtlinie, die nach der Anmeldung ausgeführt werden soll, sollte einfach der Benutzerkonfiguration einer Richtlinie zugewiesen werden. Wenn Sie diese Änderung vornehmen möchten, geschieht dies in der Konsole **Gruppenrichtlinie** unter **Richtliniennamen, Computerkonfiguration, Administrative Vorlagen, System, Gruppenrichtlinie**.

Schließlich werden die Richtlinien auf dem Arbeitsplatzrechner kontinuierlich aktualisiert, sodass immer wieder im Laufe des Tages Änderungen vorgenommen und Benutzerfehler ohne Hilfe des Administrators korrigiert werden können. Diese Aktualisierung erfolgt standardmäßig alle eineinhalb Stunden. Das Aktualisierungsintervall sollte wenn möglich nicht geändert werden, da bei einer Änderung eine Kommunikation des Systems über das Netzwerk erforderlich und somit Netzwerkverkehr verursacht wird. Die Aktualisierung findet jedoch innerhalb des Standorts statt und sollte sich nicht auf den Verkehr im WAN auswirken.

Es kann von Nutzen sein, das Intervall zu kürzen, wenn dies für die Benutzergruppe voraussichtlich erforderlich sein wird. Wenn Sie diese Änderung vornehmen möchten, geschieht dies in der Konsole **Gruppenrichtlinie** unter **Richtliniennamen, Computer- bzw. konfiguration, Administrative Vorlagen, System, Gruppenrichtlinie, Gruppenrichtlinien-Aktualisierungsintervall für Benutzer bzw. Computer**.

12.3 Verwalten von Gruppenrichtlinien

Gruppenrichtlinienobjekte können von drei unterschiedlichen Stellen aus verwaltet werden: vom Gruppenrichtlinien-Snap-In (Microsoft Management Console = MMC), von der Konsole **Active Directory-Benutzer und -Computer** und von der Konsole **Active Directory-Standorte und -Dienste** aus. Der Grund dafür ist der, dass die Active Directory-Standorte und -Container sowie die Gruppenrichtlinien miteinander verwoben sind. Viele Administratoren arbeiten einfach mit dem Container und erstellen und verwalten die Richtlinie an einer Stelle. Andere finden es dagegen sinnvoller, Richtlinienobjekte von der MMC aus zu verwalten, um eine zentrale Stelle für die Verwaltung von Richtlinien zu haben.

In diesem Fall gibt es keine richtige oder falsche Vorgehensweise. Es ist nur wichtig, dass Sie daran denken, dass Sie immer ein Gruppenrichtlinienobjekt angeben müssen, wenn Sie mit einer Gruppenrichtlinie zu tun haben. Es ist vorstellbar, dass sämtliche Gruppenrichtlinien in einer MMC gespeichert werden, dass jedoch bereits ein Container in der Form der Konsole **Active Directory-Benutzer und -Computer** existiert. Wenn Sie mit der rechten Maustaste auf ein Containerobjekt klicken und die Option **Eigenschaften** wählen, erscheint die Registerkarte **Gruppenrichtlinie**.



Eine mögliche Lösung der Frage, wie man am besten zu den Gruppenrichtlinien gelangt, ist es, eine Organisationseinheit für die Gruppenrichtlinien zu erstellen. Wenn Sie die Organisationseinheit erstellt haben, erstellen Sie einfach sämtliche Gruppenrichtlinien in dieser Organisationseinheit und fügen Sie die Richtlinien von dieser Organisationseinheit aus zu anderen Containern hinzu. So können Sie von dieser einen Organisationseinheit aus alle Änderungen an der Gruppenrichtlinie vornehmen.

12.3.1 Erstellen und Zuweisen von Gruppenrichtlinienobjekten

Ein Gruppenrichtlinienobjekt kann nur über die Eigenschaften eines Containerobjekts erstellt werden. Das mag ein weiterer Grund dafür sein, warum es sinnvoll ist, Gruppenrichtlinien über die Konsole **Active Directory-Benutzer und -Computer** oder die Konsole **Active Directory-Standorte und -Dienste** zu verwalten. Weil diese nämlich von Anfang an Teil eines Standortes oder Containerobjekts sein müssen.

Das Erstellen eines Gruppenrichtlinienobjekts ist relativ einfach:

1. Öffnen Sie die Konsole **Active Directory-Benutzer und -Computer** oder die Konsole **Active Directory-Standorte und -Dienste** und klicken Sie mit der rechten Maustaste auf den Standort oder das Containerobjekt, in dem das Gruppenrichtlinienobjekt erstellt werden soll.
2. Wählen Sie die Option **Eigenschaften**.
3. Aktivieren Sie die Registerkarte **Gruppenrichtlinie** und klicken Sie auf die Schaltfläche **Neu** (siehe Abbildung 12.5).

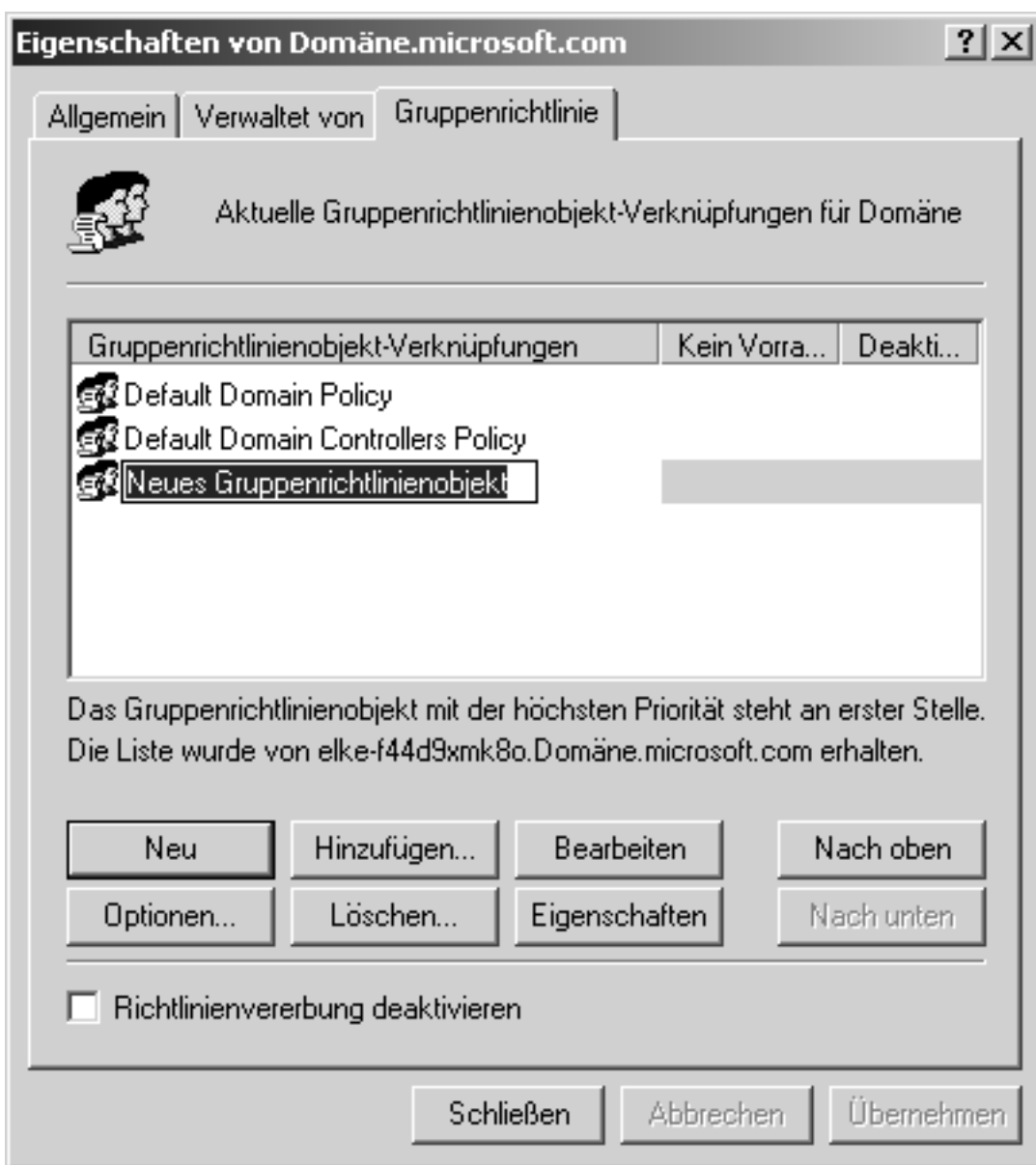


Abbildung 12.5: Erstellen eines neuen Gruppenrichtlinienobjekts

4. Es erscheint ein leeres Richtlinienobjekt mit einem Bereich, in dem Sie den neuen Namen eingeben können. Geben Sie einen anschaulichen Namen ein und drücken Sie auf die Eingabetaste.

Die Richtlinie ist nun erstellt und kann bearbeitet werden, um die gewünschten Einstellungen in der Registrierung vorzunehmen. Wenn die für den Container gewünschte Gruppenrichtlinie bereits für einen anderen Container erstellt worden ist, kann diese Richtlinie zu diesem Container hinzugefügt werden, wobei lediglich der Standort geändert werden muss. Gehen Sie dabei wie folgt vor:

1. Öffnen Sie die Konsole **Active Directory-Benutzer und -Computer** oder die Konsole **Active Directory-Standorte und -Dienste** und klicken Sie mit der rechten Maustaste auf den Standort oder das Containerobjekt, in dem das Gruppenrichtlinienobjekt erstellt werden soll.
2. Wählen Sie die Option **Eigenschaften** und klicken Sie dann auf die Schaltfläche **Hinzufügen**, um das in Abbildung 12.6 gezeigte Dialogfeld zu öffnen.

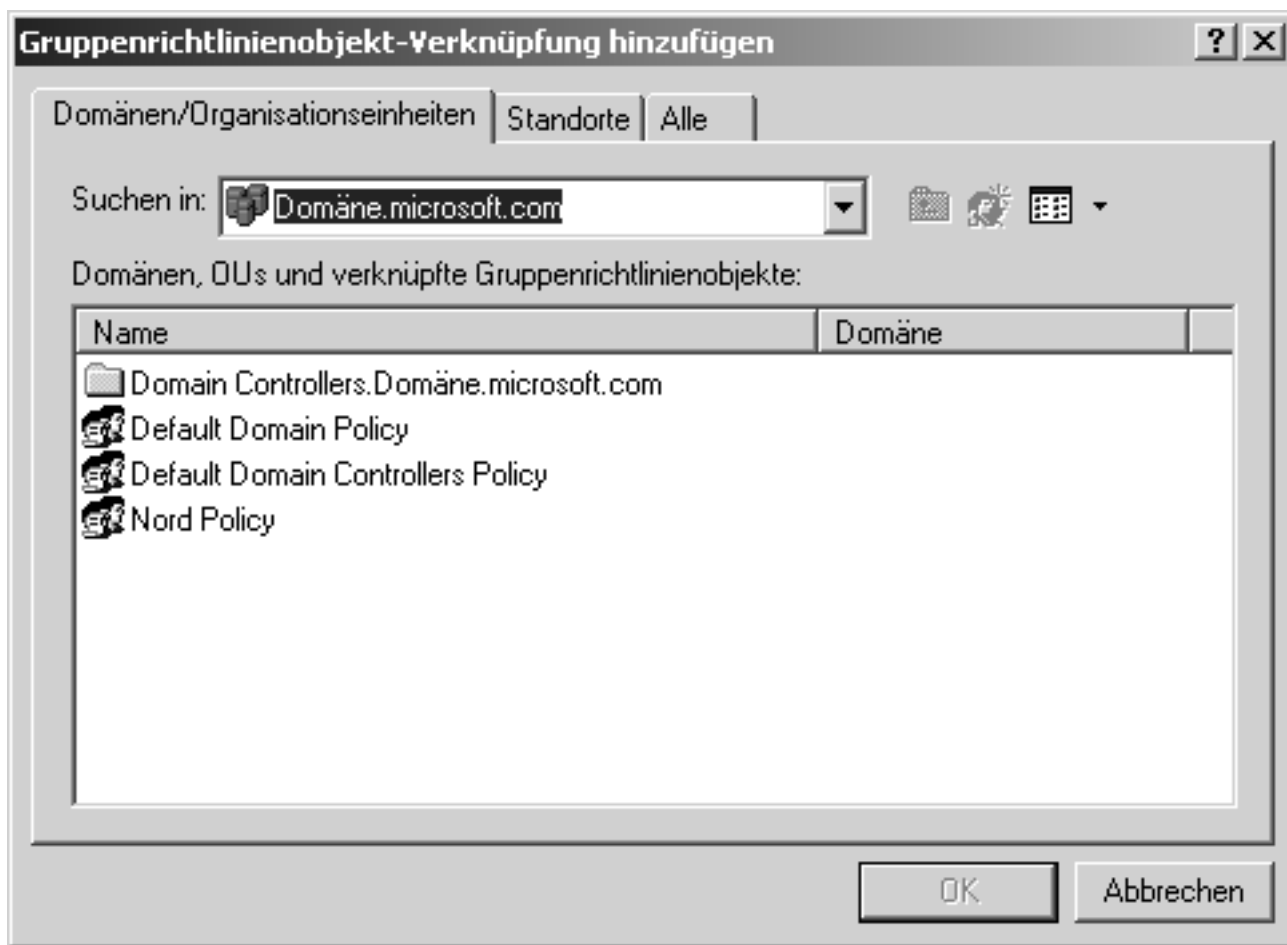


Abbildung 12.6: Hinzufügen eines Gruppenrichtlinienobjekts von einem anderen Container

3. Suchen Sie in der Explorer-Schnittstelle das Gruppenrichtlinienobjekt, das Sie anwenden möchten. Klicken Sie auf die Richtlinie und dann auf **OK**.

Wenn eine Richtlinie zu einem Containerobjekt hinzugefügt worden ist, können Verhaltens- und Steuereinstellungen definiert werden.

Vergessen Sie nicht, dass das Gruppenrichtlinienobjekt an sämtlichen Standorten geändert wird, wenn Sie dieses an einem Standort bearbeiten. Das bedeutet jedoch nicht, dass eine Änderung in einem Gruppenrichtlinienobjekt dieselbe Änderung in allen Gruppenrichtlinienobjekten zur Folge hat. Denken Sie daran, dass ein Gruppenrichtlinienobjekt, das in mehreren unterschiedlichen Containerobjekten verwendet wird, immer noch dasselbe Gruppenrichtlinienobjekt in allen Containerobjekten ist, in denen es existiert. Das ist der Grund dafür, weshalb eine Organisationseinheit für die Gruppenrichtlinien erstellt werden soll. Mit Hilfe einer solchen Organisationseinheit haben Sie eine bessere Kontrolle über die vorgenommenen Änderungen und deren möglichen universellen Auswirkungen.

Das Bearbeiten von Gruppenrichtlinienobjekten zu verstehen, ist sehr schwierig. Die Gruppenrichtlinien tatsächlich zu bearbeiten, ist dagegen einfach. Jeder kann Farbe auf eine Leinwand auftragen. Aber nicht jeder kommt dabei zu einem Ergebnis, das andere verstehen können und das anderen gefällt.

Aber lassen Sie uns am Anfang beginnen. Zunächst einmal müssen Sie einen Pinsel suchen. Und hier finden Sie Pinsel. Gehen Sie wie folgt vor, um eine Gruppenrichtlinie zu bearbeiten:

1. Öffnen Sie die Konsole **Active Directory-Benutzer und -Computer** oder die Konsole **Active Directory-Standorte und -Dienste** und klicken Sie mit der rechten Maustaste auf den Standort oder das

Containerobjekt, in dem das Gruppenrichtlinienobjekt erstellt werden soll.

2. Wählen Sie die Option **Eigenschaften**.

3. Aktivieren Sie die Registerkarte **Gruppenrichtlinie** und klicken Sie auf die Schaltfläche **Bearbeiten**, um das in Abbildung 12.7 gezeigte Bearbeitungsfenster zu öffnen.

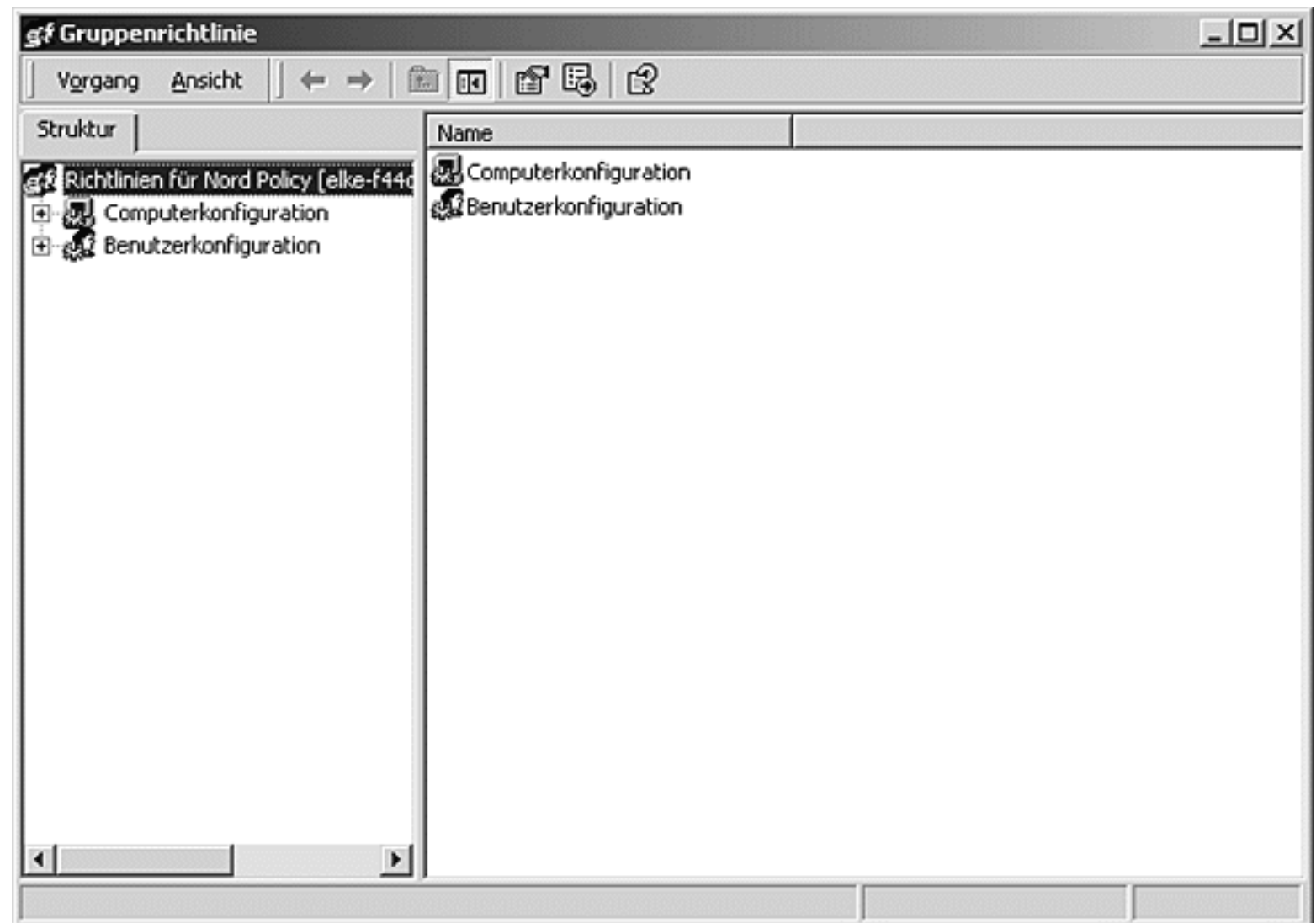


Abbildung 12.7: Fenster zum Bearbeiten eines Gruppenrichtlinienobjekts

4. Suchen Sie in der Explorer-Schnittstelle das Gruppenrichtlinienobjekt, das Sie ändern möchten.

Hier können Sie nicht nur festlegen, wo ein Gruppenrichtlinienobjekt zu einer Gruppe hinzugefügt wird, Sie können darüber hinaus auch einen Filter definieren, mit dem festgelegt wird, wie ein Benutzer bzw. eine Gruppe die Richtlinie nutzt. Gruppenrichtlinien werden so gefiltert, wie einer Datei Sicherheitsrechte zugewiesen werden. Für Benutzergruppen oder auch für einzelne Benutzer kann eine Richtlinie so geändert werden, dass diese in Bezug auf die durch die Richtlinie definierten Einstellungen anders behandelt werden.

Einige Benutzer oder Gruppen sind vielleicht in einem Container am besten aufgehoben, eignen sich aber für eine der Gruppenrichtlinien dieses Containers nicht. In diesem Fall ist es sinnvoll, diese Gruppe aus dem Bereich derer herauszufiltern, auf die sich diese Richtlinie auswirkt. Das ist genau so, wie es sinnvoll sein kann, einen Benutzer einer Gruppe zuzuordnen, ihm aber die Berechtigung für einen

bestimmten Ordner oder Drucker zu verweigern.

Und so filtern Sie ein Gruppenrichtlinienobjekt:

1. Öffnen Sie die Konsole **Active Directory-Benutzer und -Computer** oder die Konsole **Active Directory-Standorte und -Dienste**.
2. Klicken Sie mit der rechten Maustaste auf das Containerobjekt, das das zu bearbeitende Gruppenrichtlinienobjekt enthält, und wählen Sie die Option **Eigenschaften**.
3. Aktivieren Sie die Registerkarte **Gruppenrichtlinie**.
4. Wählen Sie das Gruppenrichtlinienobjekt aus und klicken Sie auf die Schaltfläche **Eigenschaften**. Aktivieren Sie die Registerkarte **Sicherheitseinstellungen** (siehe Abbildung 12.8).
5. Klicken Sie auf die Schaltfläche **Hinzufügen**, wählen Sie die zu ändernde Gruppe bzw. den zu ändernden Benutzer und klicken Sie dann auf **Hinzufügen**.
6. Wiederholen Sie diese Schritte, bis alle gewünschten Benutzer und Gruppen im unteren Teil des Dialogfeldes aufgeführt sind. Klicken Sie auf **OK**.
7. Wählen Sie den neu hinzugefügten Namen, ändern Sie die Einstellungen im Feld **Berechtigungen**, sodass diese der gewünschten Kombination entsprechen (siehe Tabelle 12.1). Klicken Sie auf **OK** und dann auf **Schliessen**.

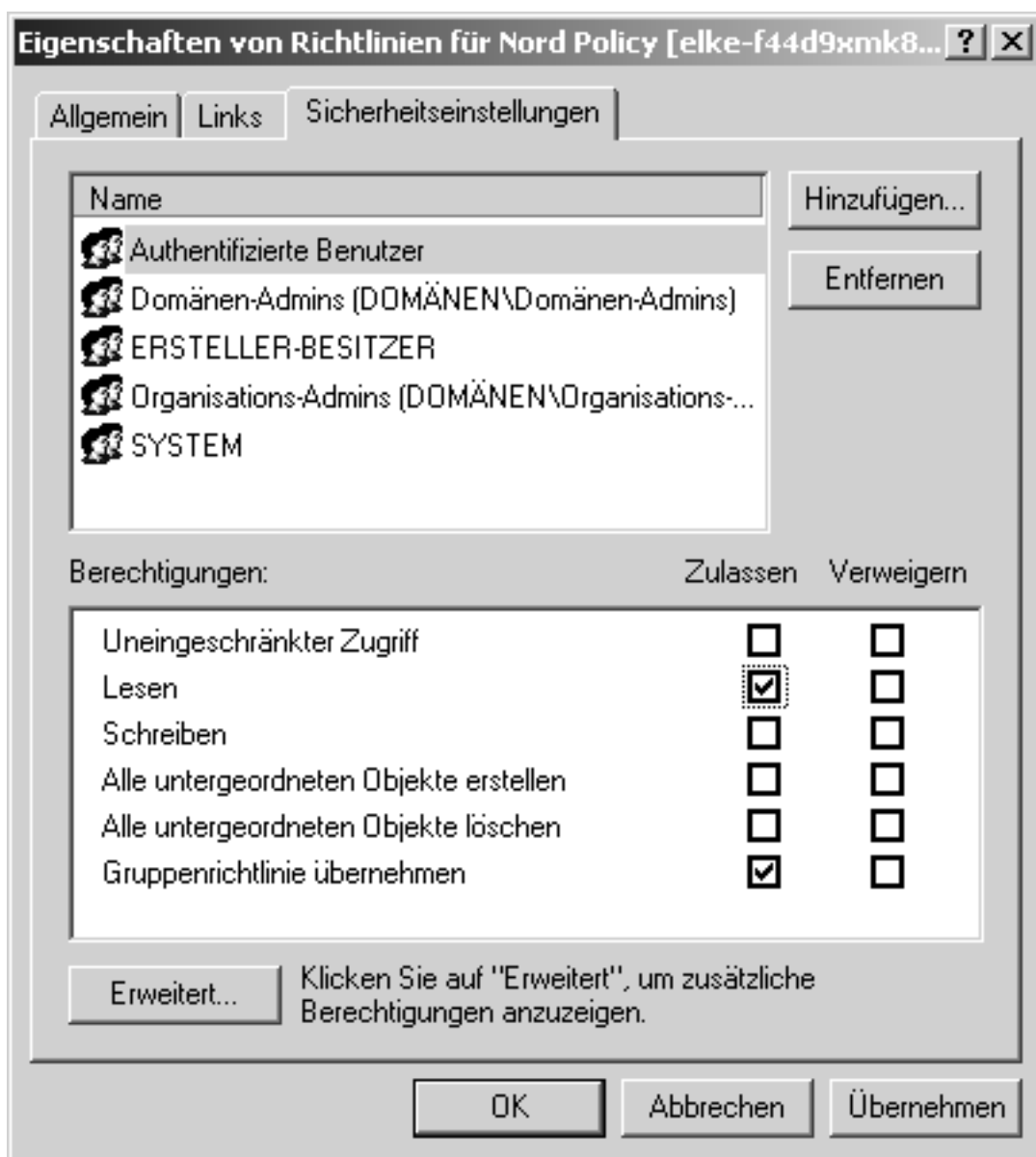


Abbildung 12.8: Das Feld Berechtigungen für Gruppenrichtlinien

Mit den oben in Schritt 7 erwähnten Berechtigungen wird die von Ihnen implementierte Steuermöglichkeit definiert. In der folgenden Tabelle sind die Berechtigungen aufgeführt, die zugewiesen werden können:

Berechtigung	Verwendung
Uneingeschränkter Zugriff	Ein Benutzer mit dieser Berechtigung verfügt über den uneingeschränkten Zugriff. Das ist dasselbe, als würde man dem Benutzer alle anderen Berechtigungen erteilen.
Lesen	Ausschließlich die Berechtigung zum Lesen und Verwenden des Gruppenrichtlinienobjekts zulassen oder verweigern.

Schreiben	Ausschließlich die Berechtigung zum Durchführen von Änderungen an der Richtlinie zulassen oder verweigern.
Alle untergeordneten Objekte erstellen	Ausschließlich die Berechtigung zum Erstellen von Objekten innerhalb der Richtlinie und zum Bearbeiten dieser Details zulassen oder verweigern.
Alle untergeordneten Objekte löschen	Ausschließlich die Berechtigung zum Löschen von Objekten innerhalb der Richtlinie zulassen oder verweigern.
Gruppenrichtlinien -übernehmen	Dieser Gruppe oder diesem Benutzer ausschließlich die Berechtigung zum Verwenden dieser Richtlinie zulassen oder verweigern. Wenn die Gruppe bzw. der Benutzer kein Mitglied des Containers des Gruppenrichtlinienobjekts ist, wird die Berechtigung automatisch verweigert.

Tabelle 12.1: Berechtigungen für Gruppenrichtlinienobjekte

12.3.2 Ändern der Richtlinie

Eine bestimmte Einstellung zu ändern ist der Teil des Verfahrens, der weitaus komplexer ist. Jede Einstellung sieht anders aus. Einige Einstellungen werden einfach aktiviert bzw. deaktiviert, andere wiederum sind sehr komplex und bieten die Möglichkeit, benutzerdefinierte Attribute des Betriebssystems und der Benutzersteuerung festzulegen. Das Betriebssystem ist zwar in keiner Weise »offen«, dennoch können Unternehmen aufgrund dieser Steuermöglichkeiten benutzerdefinierten Einstellungen und Verhalten Grenzen setzen.

12.3.3 Gruppenrichtlinien-Administratoren

Ebenso wie bei jedem anderen Bereich von Active Directory können neben den Administratoren auch andere Benutzer und Gruppen Gruppenrichtlinien verwalten und sogar erstellen. Die Steuerungsmöglichkeiten bei Gruppenrichtlinien reichen vom Erstellen und Zuweisen von Richtlinien bis einfach nur zum Lesen der Richtlinien.

Die Zuweisung dieser Richtlinien erfolgt innerhalb der Eigenschaften des Containers selbst oder über die Registerkarte **Sicherheit** der Gruppenrichtlinie. Je nach Vorgehensweise gibt es mehrere unterschiedliche Möglichkeiten, Berechtigungen zuzuweisen.

Wenn das gewünschte Ergebnis darin bestehen soll, dass der Benutzer nur bereits vorhandene Gruppenrichtlinien bearbeiten können soll, lassen sich diese Berechtigungen am einfachsten definieren, indem Sie den Benutzer zu einem Mitglied einer Gruppe machen, der mit Hilfe des Assistenten zum Zuweisen der Objektverwaltung die Verwaltung der Gruppenrichtlinien übertragen worden ist. Mit Hilfe dieses Assistenten kann die Verwaltung vieler Bereiche eines Containerobjekts übertragen werden. Im folgenden Beispiel wird die Verwaltung der Gruppenrichtlinie übertragen. Gehen Sie dabei wie folgt vor:

1. Klicken Sie im Snap-In **Active Directory-Benutzer und -Computer** mit der rechten Maustaste auf die Organisationseinheit, die Sie verwalten möchten, und wählen Sie dann die Option **Objektverwaltung zuweisen**.
2. Klicken Sie im Assistenten zum Zuweisen der Objektverwaltung auf **Weiter**, um zur nächsten Seite zu gelangen.
3. Sie werden aufgefordert, die Namen der Benutzer und Gruppen anzugeben, denen Sie die Aufgabe der Objektverwaltung zuweisen möchten.
4. Wählen Sie eine zuvor definierte Gruppe bzw. einen zuvor definierten Benutzer aus und klicken Sie dann auf **Weiter**.
5. Wählen Sie aus der Liste der vordefinierten Aufgaben die Option **Verwaltet Gruppenrichtlinien-Verknüpfungen** und klicken Sie dann auf **Weiter**. Klicken Sie auf **Fertig stellen**.

Wenn das gewünschte Ergebnis darin bestehen soll, dass der Benutzer bzw. die Gruppe Gruppenrichtlinienobjekte erstellen und verwalten können soll, gibt es mehrere Möglichkeiten, zu diesem Ziel zu gelangen. Eine Möglichkeit besteht darin, den Benutzer bzw. die Gruppe zu einem Mitglied der Gruppe Ersteller-Besitzer der Gruppenrichtlinie für diese Domäne zu machen. Das ist allerdings die Holzhammermethode.

Wenn Sie Rechte im Einzelnen zuweisen möchten, können Sie dies über das Dialogfeld **Eigenschaften** des Richtlinienobjekts (siehe Abbildung 12.8) tun. Wenn Sie auf die Schaltfläche **Hinzufügen** klicken und eine Gruppe auswählen, können Sie einzelne Eigenschaften für die Richtlinie hinzufügen (siehe Tabelle 12.1 und die Anweisungen für das Hinzufügen von Berechtigungen).

Wenn Sie für die Gruppenrichtlinie einzelne Berechtigungen definieren, haben Sie die beste Kontrolle darüber, wer das Recht hat, Objekte in der Gruppenrichtlinie zu erstellen und zu verwalten. Dies führt jedoch auch zu einem weniger gut vorhersehbaren Ergebnis. Seien Sie vorsichtig, wenn Sie beispielsweise einen Administrator hinzufügen möchten, der Gruppenrichtlinien nur prüfen können soll. Eine Gruppe, die nur über die Berechtigung Lesen verfügt, kann nicht einmal das Gruppenrichtlinien-Snap-In öffnen.

12.4 Windows Installer

Windows Installer ist eine Funktion zum Installieren und Deinstallieren von Anwendungen, mit deren Hilfe Sie für eine konsistente Anwendungslandschaft innerhalb der Domäne sorgen können. Das Konzept, das sich hinter Windows Installer verbirgt, gibt es als Teil unterschiedlicher Software-Produkte außerhalb des Betriebssystems Windows schon seit einiger Zeit. Mit Hilfe von Produkten wie Microsoft Systems Management Server (SMS) kann Software bereits seit einigen Jahren installiert werden. Bei Windows 2000 ist diese Funktion nun im Betriebssystem integriert.

Die Idee dabei ist die, dass Paketdateien (.msi) verwendet werden, die dem System mitteilen, welche Software-Komponenten auf dem System installiert sein sollten. Sie können dann je nach Bedarf einzelne Pakete hinzufügen oder entfernen, indem Sie diese Pakete miteinander vergleichen. Das ist nur möglich, weil das Betriebssystem von einer Registrierung verwaltet wird, in der jede Änderung an einer Anwendung oder am Betriebssystem aufgezeichnet wird. Dadurch, dass diese Änderungen aufgezeichnet werden, kann ein Programm die für die Verwaltung von Anwendungen erforderlichen Änderungen

suchen.

Das Basissystem wird dadurch erweitert, dass Windows Installer das Verwaltungssystem für das Hinzufügen, Entfernen und Ändern dieser Anwendungen steuert. Die Anwendungen können sich an unterschiedlichen Speicherorten befinden und ihnen können unterschiedliche Richtlinien zugewiesen werden, um ein robustes und fehlertolerantes System einzurichten.

Für dieses Programm gibt es viele Anwendungen, die einem vielleicht nicht sofort in den Sinn kommen. Im Folgenden finden Sie einige sehr nützliche Anwendungsmöglichkeiten:

- Wiederherstellen einer defekten Anwendung in einem System bzw. das vollständige Wiederherstellen sämtlicher Anwendungen in einem System
- Aktualisieren von Anwendungen und Anwendungs-Suiten auf neue Versionen
- Verhindern, dass Benutzer Parameter einer Anwendung so ändern, dass sie ihr System nicht mehr nutzen können
- Installieren neuer Arbeitsplatzrechner durch einfaches Anmelden an der Domäne
- Zuverlässiges Entfernen von Anwendungen, die aus der Liste der Standards des Unternehmens entfernt worden sind
- Striktes Einhalten von Software-Standards
- Kontrollieren der Anzahl der Installationen einer bestimmten Anwendung aus Lizenzberechtigungsgründen

Windows Installer ist eigentlich eine Kombination aus Winstall, dem *MSIEXEC*-Programm für die Verwendung von Paketen auf Seiten des Client, und dem Installationsmechanismus Active Directory.

12.4.1 WinInstaller

Der erste Schritt bei der Verteilung von Software besteht darin, die zu installierenden Anwendungspakete (.msi-Dateien) zu erstellen. Das Erstellen eines Pakets erscheint sehr arbeitsintensiv, wenn es richtig gemacht wird, aber es ist der Mühe wert.

Das größte Problem dürfte wohl sein, dass die Pakete auf einem Rechner erstellt werden sollten, der zumindest vorübergehend nur für das Erstellen dieser Pakete genutzt werden kann. Der Grund dafür ist der, dass die Pakete an viele unterschiedliche Rechner gesendet werden und sich auf diesen Rechnern unterschiedliche Anwendungen befinden. Es ist daher am besten, wenn der Rechner, auf dem die Pakete erstellt werden, keine verwirrenden Informationen enthält, die auf diesen Rechnern hinzugefügt würden.

Am besten verwenden Sie einen so genannten »sauberen Rechner«. Das ist ein Rechner, auf dem sich nur die Elemente befinden, die für die Installation und Ausführung der Anwendung erforderlich sind:

- das Betriebssystem Windows (2000, NT, 95/98 oder 3.x)
- die Treiber, die für die von der Anwendung in Anspruch genommene Hardware unbedingt erforderlich sind

Auf dem Rechner sollte nach Möglichkeit die Anwendung installiert sein, damit dieser nach jeder Erstellung eines neuen Pakets wieder seinen anfänglich sauberen Zustand einnehmen kann. Das Ganze kann man sich wie eine Whiteboard-Tafel vorstellen, die immer wieder neu beschrieben werden kann.

Wenn permanente Änderungen auf diesem Rechner gespeichert werden, können diese Änderungen in den Paketen erscheinen, die bei anderen Benutzern installiert werden. Laufwerkzuweisungen, Druckereinstellungen und andere Software-Einstellungen können Auswirkungen auf das Paket haben.



Das Ganze wird wesentlich einfacher, wenn Sie mit einem Programm zum Duplizieren von Festplatten wie z.B. Norton Ghost arbeiten. Wenn Sie ein Abbild des Rechners im sauberen Zustand erstellen und auf einer CD-ROM speichern, können Sie den Rechner unmittelbar nach dem Erstellen eines Pakets wieder in seinen ursprünglichen Zustand zurückversetzen. Andernfalls müssen Sie nach dem Erstellen eines Pakets das Betriebssystem, die Treiber und sämtliche Patches neu installieren, was sehr viel Zeit in Anspruch nimmt.

Wenn der saubere Rechner installiert und bereit ist, müssen als Nächstes »Vorher«- und »Nachher«-Snapshots erstellt werden. Snapshots werden in erster Linie deshalb vor und nach der Installation erstellt, weil das Betriebssystem eines Zielrechners entsprechend der Änderungen, die beim Vergleich der beiden Snapshots miteinander festgestellt werden, geändert wird.

Damit Ihr Rechner diese Snapshots erstellen kann, müssen Sie zunächst die Anwendung Veritas WinInstaller installieren. Die Installation dieser Anwendung ist sehr einfach. Eine eingeschränkte Version dieser Anwendung befindet sich auf der CD von Windows 2000 Server. Sie finden diese im Ordner *VALUEADD\3RDPARTY\MGMT\WINSTLE*. Um diese Anwendung zu installieren, doppelklicken Sie einfach auf die Datei *SWIADMLE.MSI*. Da es sich hierbei ebenfalls um ein WinInstaller-Paket handelt, haben Sie damit bereits Ihre erste WinInstaller-Installation ausgeführt.

Um einen »Vorher«-Snapshot zu erstellen, gehen Sie wie folgt vor:

1. Öffnen Sie das Startmenü von Windows 2000 und wählen Sie im Menü **Programme/VERITAS Software** den Eintrag **VERITAS Discover**, um das gleichnamige Programm zu starten (siehe Abbildung 12.9).



Abbildung 12.9: Das Dialogfeld von WinINSTALL Discover



Weisen Sie der WinINSTALL-Freigabe kein Laufwerk zu, um die Installation auszuführen. Diese Zuordnung kann als Teil des erstellten Pakets erscheinen oder einen Fehler im Paket verursachen.

2. Klicken Sie im Übersichtsfenster auf die Schaltfläche **Next**.
3. Geben Sie den Namen der Anwendung so ein, wie er erscheinen soll. Diese Eingabe wird als *Anwendungspaketname* bezeichnet. Erstellen Sie einen aussagekräftigen Namen mit bis zu maximal 40 Zeichen.
4. Geben Sie den Namen der Windows Installer-Datei (ohne Erweiterung) ein, in der die Informationen über die Installation gespeichert werden sollen. Die Datei wird dort gespeichert, wo Sie die Datei in der Baumstruktur speichern möchten.
5. Geben Sie an, ob die Anwendung für Windows 2000, Windows 3.x, Windows 95 oder Windows NT ausgeführt werden soll.
6. Klicken Sie auf die Schaltfläche **Next**, um das nächste Dialogfeld aufzurufen.
7. Klicken Sie in der daraufhin erscheinenden Dropdown-Liste auf das Laufwerk, in dem Discover seine temporären Arbeitsdateien speichern soll. Der Discover-Vorgang, bei dem Änderungen am System entdeckt (engl. discover) werden, wird wesentlich schneller ausgeführt, wenn Sie ein lokales Laufwerk wählen. Dieses Laufwerk sollte über mindestens 250 Mbyte freien Speicherplatz verfügen. Discover speichert die Dateien in einem temporären Arbeitsverzeichnis (*\\DISCOVER.wrk*) und löscht diese, nachdem der Vorgang abgeschlossen ist.
8. Klicken Sie auf die Schaltfläche **Next**, um das nächste Dialogfeld aufzurufen.
9. Wählen Sie mindestens ein Laufwerk aus der Liste **Available Drives**. Dabei ist es wichtig, dass Sie

nur das Laufwerk bzw. die Laufwerke auswählen, auf denen tatsächliche Anwendungsdateien installiert werden sollen.

10. Das Windows-Verzeichnis wird automatisch nach Änderungen in den Dateien *Win.ini* und *System.ini* durchsucht, auch wenn diese sich nicht auf dem ausgewählten Laufwerk befinden.

11. Klicken Sie auf die Schaltfläche **Add** oder auf die Schaltfläche **Add all**.

12. Klicken Sie auf die Schaltfläche **Next**, um das nächste Dialogfeld aufzurufen.

13. Klicken Sie auf die Schaltfläche **Files & Wildcard Entries**, wenn Sie Dateien oder Dateigruppen ausschließen möchten. Sämtliche hier ausgewählten Dateien erscheinen in der Liste **Directories & Files to Exclude**.



Die Anwendung WinINSTALL Discover verwendet Ausnahmedateien, mit deren Hilfe festgelegt wird, welche Bereiche der Systemkonfiguration von einer Überprüfung ausgeschlossen werden sollen. Diese Ausnahmedateien beruhen auf Standardausnahmedateien, die im Verzeichnis *WinINSTALL Administration Program* gespeichert werden. Die 32-Bit-Standard- Ausnahmedatei der Registrierung ist die Datei *Reg.xcp*. Der Name der 16-Bit-Datei lautet *Reg16.xcp*. Die Standardausnahmedatei heißt *Files.xcp*. Die Arbeitsausnahmedateien *Reg.xcp* bzw. *Reg16.xcp* und *xFiles.xcp* (wobei *x* der Name der einzelnen Ausnahmelauferke des Dateisystems ist) werden während des Discover-Vorgangs erstellt und im Arbeitsverzeichnis von Discover gespeichert.

In diesem Fenster können Sie Verzeichnisse und/oder Dateien auf beliebigen Laufwerken ausschließen. Wenn Sie die Überprüfung auf diese Art und Weise einschränken, wird die Verarbeitungszeit deutlich reduziert. Es ist sehr zu empfehlen, dass Sie die Standardausschlüsse verwenden. In der Regel ermöglichen die Standardeinstellungen die zuverlässigste Prüfung des Rechners. Das Windows-Verzeichnis sowie sämtliche Unterverzeichnisse dieses Verzeichnisses können nicht ausgeschlossen werden.

14. Klicken Sie auf eines oder mehrere Verzeichnisse in der Liste **All Directories**.

15. Klicken Sie auf die Schaltfläche **Add** oder auf die Schaltfläche **Add all**.

16. Klicken Sie auf die Schaltfläche **Next**.

Wenn der Discover-Vorgang abgeschlossen und die Anwendung installiert ist, müssen Sie ein »Nachher«-Snapshot erstellen. Damit kann das Programm die vorgenommenen Änderungen erkennen. Um ein »Nachher«-Snapshot zu erstellen, gehen Sie wie folgt vor:

1. Führen Sie vom Referenzrechner, von dem aus Sie das Verteilungspaket erstellen möchten, das Programm *DISCOZ.EXE* aus.

2. Klicken Sie auf die Schaltfläche **Next**. Discover erstellt den »Nachher«-Snapshot.

Wenn die Pakete erstellt sind, können Sie diese ändern. Dies geschieht über den Paket-Editor. Damit können Sie Elemente wie die INI-Dateien, die Komponenten sowie die Attribute der zu installierenden Anwendungen bearbeiten.

Dies ist jedoch nur dann zu empfehlen, wenn Sie sich mit der Anwendung und den Ergebnissen, die aus den Änderungen resultieren können, sehr gut auskennen. Am besten ist es, wenn Sie die gewünschten Änderungen am sauberen Rechner vornehmen, dort experimentieren und dann den »Nachher«-Snapshot

erstellen.

Wenn der »Nachher«-Snapshot erstellt ist, kann das Paket versendet und installiert werden.

12.4.2 Verteilen der Pakete

MSI-Pakete werden in der Welt von Windows 2000 über das Active Directory verteilt. Das Verbreiten der Software ist sowohl Teil der Benutzerkonfiguration als auch der Computerkonfiguration in der Snap-In-Konsole **Gruppenrichtlinie**. Damit ist es möglich, Software an Standorte, Domänen und Organisationseinheiten zu verteilen.

Bevor ein Paket ausgeliefert werden kann, muss der Client-Arbeitsplatzrechner das Paket interpretieren können. Dazu muss der Arbeitsplatzrechner das Programm *MSIEXEC.EXE* ausführen. Dieses Programm ist eine Komponente von Windows Installer. Es verwendet eine DLL-Datei (*MSI.DLL*), um die Paketdateien (*.msi*) zu lesen und Befehlszeilenoptionen zu integrieren.

Wenn Windows Installer auf einem Rechner installiert wird, werden die Dateiverknüpfungsfunktionen des Betriebssystems geändert, damit der MSI-Dateityp erkannt werden kann. Wenn Sie auf eine Datei mit der Erweiterung *MSI* doppelklicken, verknüpft das Betriebssystem diese MSI-Datei mit dem Windows Installer und führt die Anwendung *MSIEXEC.EXE* aus. Daher können Pakete auch über Anmeldeskripten verbreitet werden.

Pakete werden mit Hilfe des Active Directory über das Dialogfeld **Eigenschaften** des Gruppenrichtlinienobjekts verteilt (siehe Abbildung 12.10). Wenn Sie das Snap-In **Gruppenrichtlinien** für das Gruppenrichtlinienobjekt geöffnet haben, gehen Sie wie folgt vor, um ein Software-Paket hinzuzufügen:

1. Klicken Sie je nach dem Paket, das Sie installieren möchten, entweder auf das Pluszeichen neben **Computerkonfiguration** oder auf das Pluszeichen neben **Benutzerkonfiguration**.
2. Klicken Sie auf das Pluszeichen neben **Softwareeinstellungen** und dann auf **Softwareinstallation**.
3. Klicken Sie mit der rechten Maustaste auf **Softwareinstallation** und wählen Sie die Option **Neu** und dann die Option **Paket**.

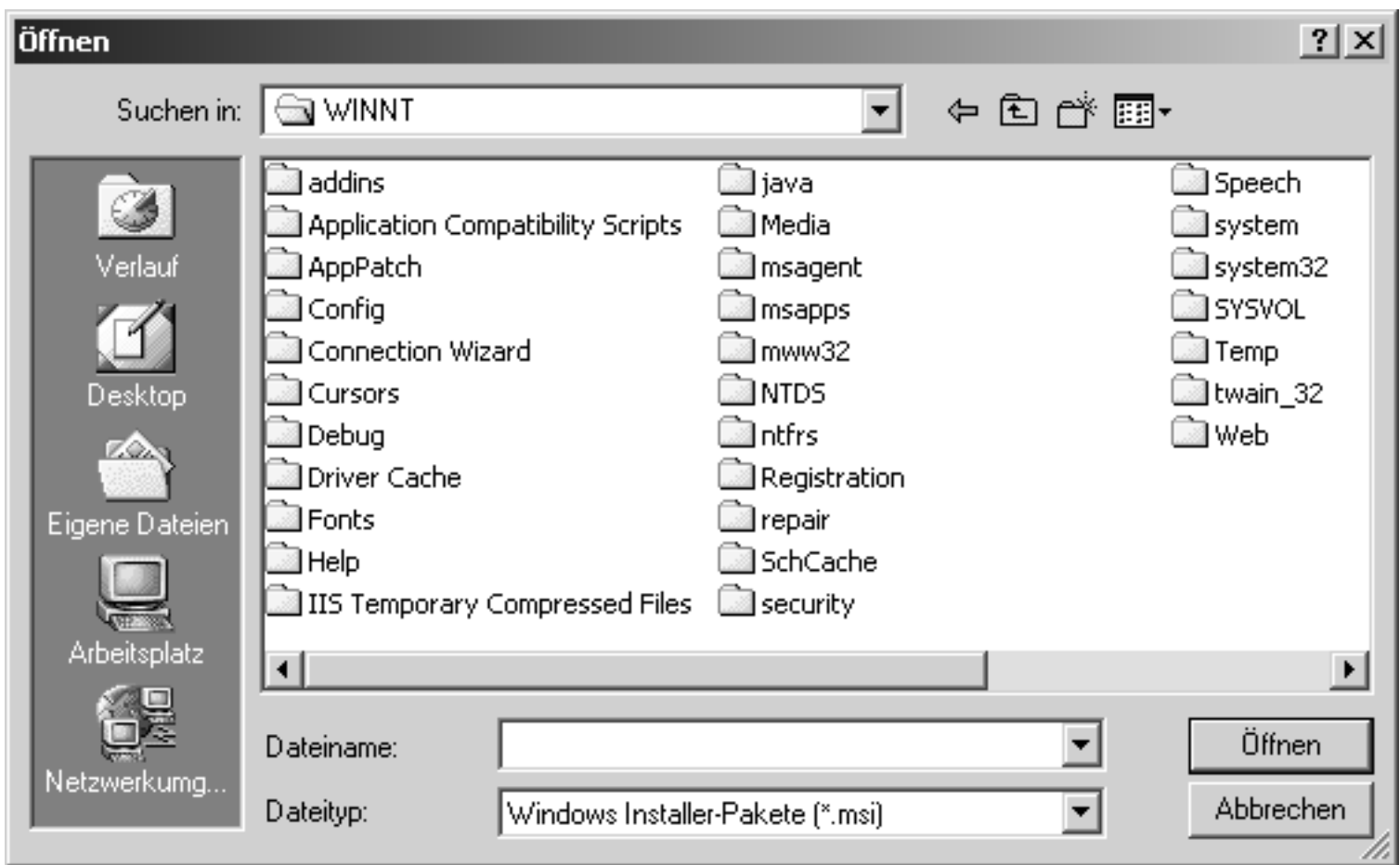


Abbildung 12.10: Das Dialogfeld Öffnen des Gruppenrichtlinienobjekts

4. Suchen Sie die zuvor erstellte *MSI*-Datei und wählen Sie die Option **Öffnen**.

12.5 Remoteinstallationsdienste

Der Remoteinstallationsdienst ist ein Dienst, mit dessen Hilfe Sie das Betriebssystem auf neuen Rechnern installieren oder deinstallieren können. Diese Installation erfolgt über eine beliebige Client-Festplatte mit Zugriff auf die Domäne.

Um eine Remotestartdiskette zu erstellen, verwenden Sie die Anwendung *RBFG.EXE*, die mit dem Remoteinstallationsdienst installiert wird. Sie können die Startdiskette nur auf Rechnern verwenden, die über unterstützte, PCI-basierte Netzwerkkadaper verfügen. Um eine Übersicht über die unterstützten Netzwerkkadaper anzuzeigen, starten Sie das Programm *RBFG . EXE* und klicken Sie auf die Option **Adapterliste**. Und so gehen Sie dabei vor:

1. Klicken Sie auf **Start** und dann auf **Ausführen**.
2. Geben Sie den UNC-Pfad des Programms *RBFG.EXE* ein und klicken Sie auf **OK**. Hier ein Beispiel:

```
\\Servername\RemoteInstall\Admin\I386\RBFG.exe
```

3. Legen Sie eine formatierte Diskette in das Laufwerk ein. Wählen Sie unter **Ziellaufwerk** das Ziellaufwerk aus und klicken Sie dann auf die Schaltfläche **Diskette erstellen**.

4. Klicken Sie auf die Schaltfläche **Schliessen**, wenn die Diskette erstellt ist. Nehmen Sie anschließend die Diskette aus dem Laufwerk.

Dieser Dienst wird nicht automatisch installiert. Um den Remoteinstallationsdienst zu installieren, gehen Sie wie folgt vor:

1. Öffnen Sie den Assistenten **Windows 2000 Server konfigurieren** (der Assistent, der zu Beginn automatisch gestartet wird). Klicken Sie auf **Start, Programme, Verwaltung, Konfiguration des Servers**.
2. Klicken Sie auf **Erweitert** und dann auf **Optionale Komponenten**.
3. Klicken Sie im Dialogfeld **Optionale Komponenten** auf **Starten**, um den Assistenten für Windows-Komponenten zu starten.
4. Wählen Sie aus der Liste der verfügbaren Optionen die Option **Remoteinstallationsdienste** und klicken Sie auf **Weiter**, um den Installationsvorgang zu starten.

Um diesen Vorgang manuell zu starten, gehen Sie wie folgt vor:

1. Klicken Sie auf **Start** und dann auf **Ausführen**.
2. Geben Sie **RISetup** ein und klicken Sie auf **OK**, um den Assistenten für die Konfiguration des Remoteinstallationsdienstes aufzurufen (siehe Abbildung 12.11).

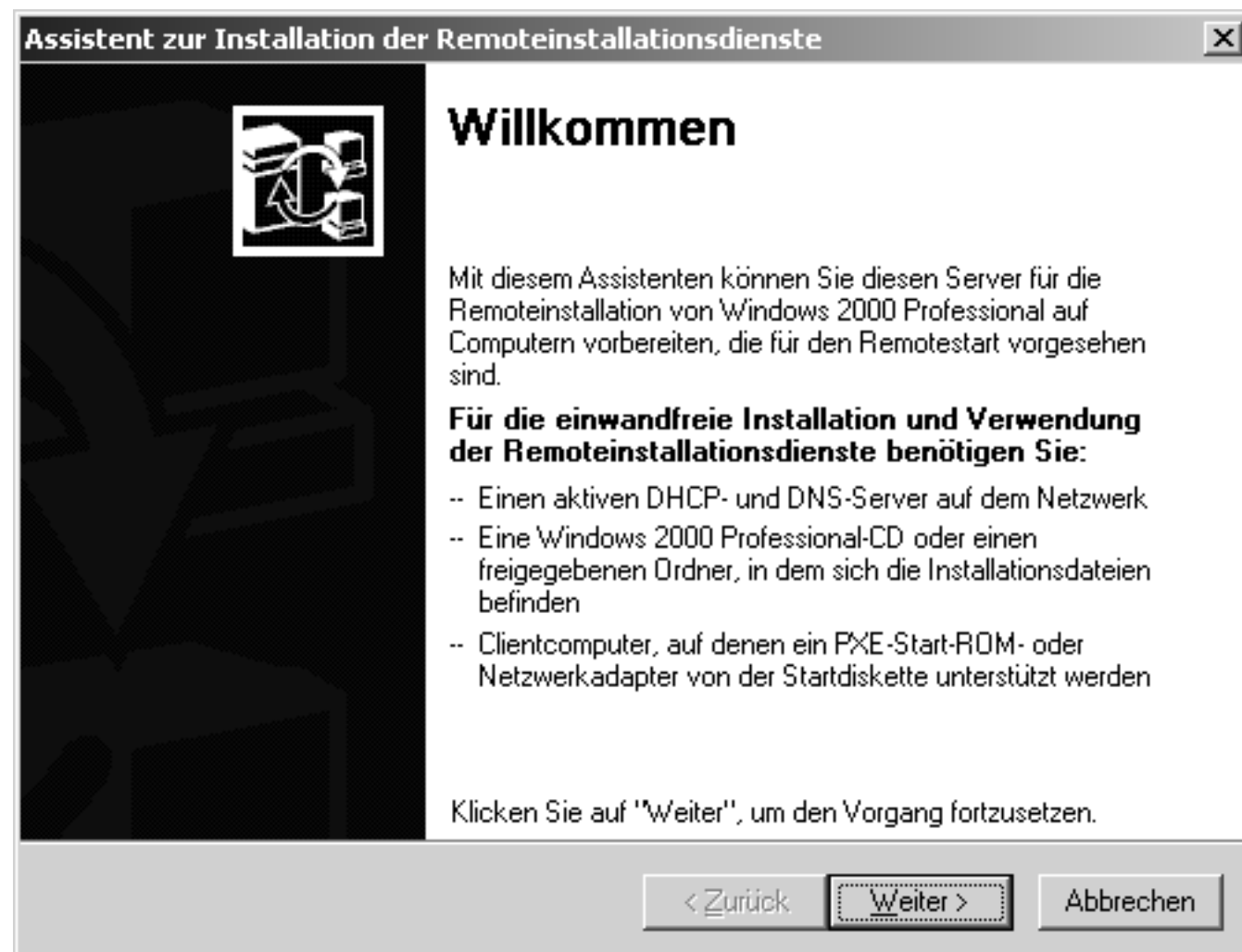


Abbildung 12.11: Der Assistent für die Remoteinstallation

3. Der Assistent zur Installation der Remoteinstallationsdienste fordert Sie auf, Folgendes anzugeben:

- *Laufwerk und Verzeichnis des Remoteinstallationsdienstes.* Geben Sie das Laufwerk und das Verzeichnis ein, in dem die Remoteinstallationsdienste installiert werden sollen. Das Laufwerk sollte ein für die Remoteinstallationsdienste reservierter Server sein, der über genügend Festplattenspeicher verfügen muss, um so viele Installationsabbilder unterstützen zu können, wie Sie mit diesem Server erstellen möchten. Der Server sollte mindestens über 4 Gbyte Speicherplatz verfügen.
- *Quellpfad des Arbeitsplatzrechners.* Geben Sie den Speicherort für die Windows 2000 Professional-Dateien an. Das kann entweder die Windows 2000 Professional-CD oder die Netzwerkfreigabe sein, die die Installationsdateien enthält.
- *Anschauliche Beschreibung und Hilfetext.* Geben Sie eine anschauliche Beschreibung für die Installation auf dem Arbeitsplatzrechner ein. Diese Beschreibung wird für die Benutzer bzw. Clients dieses Remoteinstallationsdienste-Servers angezeigt. Der Hilfetext dient als Beschreibung der Installationsoption des Betriebssystems für die Benutzer bzw. Clients dieses Remoteinstallationsdienste-Servers.

Wenn der Dienst installiert ist, muss er konfiguriert werden, um auf Client-Anforderungen reagieren zu können. Wenn Sie im Bereich **Active Directory-Benutzer und -Computer** mit der rechten Maustaste auf den Server klicken und dann die Option **Eigenschaften** wählen, sehen Sie die Registerkarte **Remoteinstallation**. Hier können Sie zwei Optionen ändern:

- **Client-Computern, die Dienst anfordern, antworten.** Wenn Sie diese Option wählen, werden die Remoteinstallationsdienste aktiviert. Diese Dienste antworten dann Client-Computern, die diesen Dienst anfordern. Wenn Sie diese Option nicht aktivieren, werden die Remoteinstallationsdienste angehalten. Dann antworten diese Dienste Client-Computern, die diesen Dienst anfordern, nicht.
- **Unbekannten Client-Computern nicht antworten.** Mit dieser Option wird festgelegt, ob der Remoteinstallationsdienste-Server unbekannten Client-Computern, die einen Remoteinstallationsdienste-Server anfordern, antwortet. Ein Client-Computer wird als bekannt betrachtet, wenn für diesen Computer im Active Directory ein Computerkontoobjekt erstellt worden ist. Sie sollten Client-Computer im Active Directory konfigurieren, bevor Sie diese Option aktivieren.

Wenn Sie diese Option wählen, antwortet der Remoteinstallationsdienste-Server unbekannten Client-Computern nicht. Diese Option sorgt für zusätzliche Systemsicherheit, indem nicht autorisierter Zugriff über unbekannte Computer verhindert wird.

Teil III

- 13. [Durchsuchen des Netzwerks](#)
- 14. [Remotezugriff - RAS](#)
- 15. [Multiprotokollumgebungen](#)
- 16. [Überlegungen zum Arbeitsplatzrechner](#)

Kapitel 13 Durchsuchen des Netzwerks

13.1 Grundlagen zum Konzept

Hinter dem Durchsuchen von Netzwerken verbirgt sich eigentlich ein recht einfaches Konzept. Im Prinzip durchsuchen Sie ein Netzwerk, wenn Sie sämtliche Geräte in der LAN/WAN-Umgebung Ihrer Organisation sehen möchten. Und das ist ganz einfach. Sie doppelklicken auf dem Desktop von Windows 2000 Server auf das Symbol **Netzwerkumgebung**, um das Fenster **Netzwerkumgebung** (siehe Abbildung 13.1) aufzurufen.

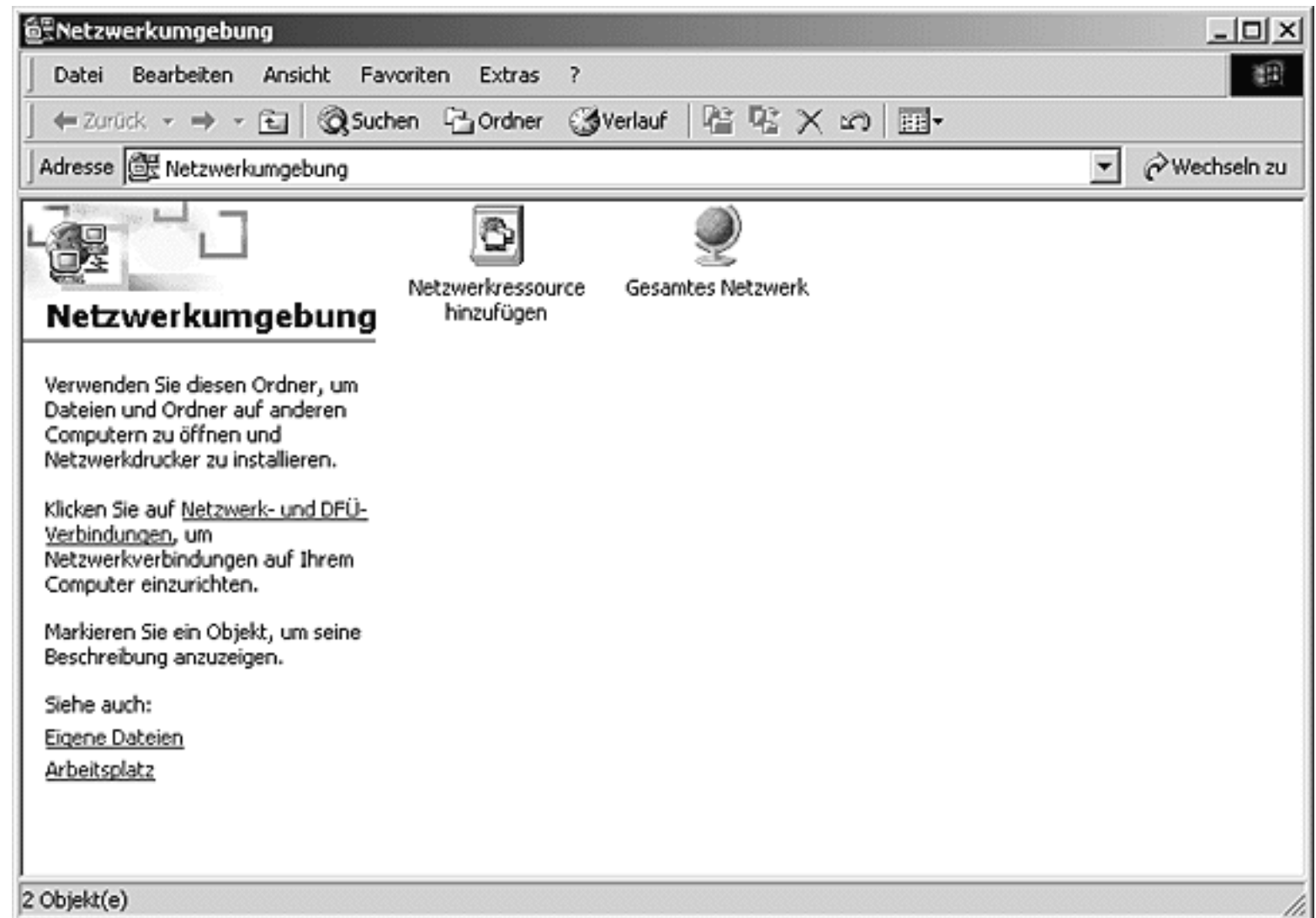


Abbildung 13.1: Das Fenster Netzwerkumgebung

In diesem Fenster stehen Ihnen einige Optionen zur Verfügung: Sie können mit Hilfe des Symbols **Benachbarte Computer** Ihr lokales Netzwerk oder mit Hilfe des Symbols **Gesamtes Netzwerk** Ihre WAN-Umgebung durchsuchen. Mit Hilfe des Symbols **Netzwerkressource hinzufügen** können Sie eine Verbindung zwischen Ihrem Windows 2000 Server-Rechner und freigegebenen Ordnern, Webordnern und/oder FTP-Sites innerhalb des Konnektivitätsbereiches Ihres Computers herstellen. Dazu gehören sowohl die Netzwerke Ihrer Organisation als auch das Internet. All diese Begriffe werden in diesem

Kapitel ausführlich erläutert.

Das Durchsuchen des Netzwerks innerhalb einer Windows 2000 Server-Umgebung hat sich von seinem Windows NT-Ursprung ausgehend immer weiter entwickelt. Der im Betriebssystem Windows 2000 Server integrierte Dienst Computerbrowser funktioniert im Wesentlichen wie der Computersuchdienst in der Windows NT 4.0 Server-Umgebung. Das bedeutet, dass er das Durchsuchen von Weitbereichsnetzen (WANs), die NetBIOS über TCP/IP verwenden, ebenso unterstützt wie das Durchsuchen von den Domänen, die immer noch von älteren Windows NT 4.0 Server-Betriebssystemen gesteuert werden. Darüber hinaus wird auch der Einsatz sowohl der WINS-Technologie (Windows Internet Name Service) von Windows NT 4.0 Server als auch die WINS 2000-Technologie (auf Windows 2000 Server basierender WINS) entsprechend unterstützt.

So wie Microsoft die Suchfunktionen beim Betriebssystem Windows 2000 weiterentwickelt hat, lässt sich das Durchsuchen am besten über die Veröffentlichung von Computerinformationen im Active Directory mittels *globaler Kataloge* bewerkstelligen. Ein globaler Katalog ist im Wesentlichen nichts anderes als ein Windows 2000-Dienst und Datenspeicher, der ein Replikat jedes Objekts, das in der Gesamtstruktur der Organisation im Active Directory bereits existiert, sowie einige der häufiger verwendeten Attribute enthält. Das bedeutet, dass das Computersystem eines Benutzers, der ein Windows 2000 Server-Netzwerk zu durchsuchen beginnt, auf den globalen Katalog (es gibt immer mindestens einen in jeder Gesamtstruktur) des Active Directory zugreift und einen bestimmten Computernamen schneller findet. Da die Attributliste eines globalen Katalogs nicht so lang ist wie die des Active Directory, erfolgt das Indizieren schneller, als wenn der Benutzer die Computerinformationen über die vollständige Attributliste des Active Directory beziehen müsste.



Es ist natürlich möglich, in einer Organisation mehr als eine Gesamtstruktur zu haben. Aufgrund der Probleme allerdings, die entstehen, wenn ein Benutzer versucht, Objekte und deren Attribute zwischen mehreren Windows 2000-Gesamtstrukturen zu replizieren, ist dies sehr unwahrscheinlich.

Natürlich wird nicht jede Organisation mit ihren Windows 2000-Servern eine Gesamtstruktur oder auch nur die Active Directory-Technologie nutzen. In diesen Fällen gibt es möglicherweise Windows NT 4.0-Server, die die Suchressourcen und Suchfunktionen des Netzwerks mittels WINS-Server (Windows Internet Name Service) verwalten. Darüber hinaus ist der gerade installierte Windows 2000-Server möglicherweise das erste Windows NT- oder Windows 2000 Server-System, das in dieser Organisation eingerichtet wurde. In diesem Fall gibt es nicht allzu viel, das durchsucht werden kann. Anders ausgedrückt: Wenn es nur einen Server gibt, sollte es eigentlich nicht allzu schwierig sein festzustellen, auf welchem Server sich die Druck- und Dateifreigaben des Netzwerks befinden.

Nun fragen Sie sich wahrscheinlich, wie das alles in der Windows 2000 Server-Umgebung funktioniert. Daher soll es hier nun ohne weitere Umschweife mit den drei wichtigsten Suchdienstbereichen weitergehen:

- Suchdienstfunktionen für Server
- Auswahlkriterien für den Suchdienst
- Suchdienstwahl

Wenn Sie diese drei Themen erst einmal verstanden haben, wird es wesentlich einfacher für Sie zu verstehen sein, wie die Suchumgebung einer Organisation konfiguriert und verwaltet wird.

13.1.1 Suchdienstfunktionen für Server

Wie bereits erwähnt, wird der Computersuchdienst Computerbrowser in Windows NT- und Windows 2000-Umgebungen ausgeführt und wird von allen Windows 3.11-, Windows 9x-, Windows NT-, Windows Consumer- (mit Codenamen *Millennium*) und Windows 2000-Computern in den einzelnen TCP/IP-Subnetzen innerhalb einer Organisation verwendet. Mit Hilfe des Computersuchdienstes kann festgelegt werden, welcher der Computer in einem bestimmten Subnetz als Suchdienst konfiguriert werden soll. Es ist wichtig zu wissen, dass nur Computer mit Windows ab der Version 9x aufwärts Suchlisten speichern können. Der Suchdienstcomputer ist derjenige, der die Suchlisten speichert und aktualisiert. Diese Suchlisten enthalten Informationen darüber, welche Computer, freigegebenen Ressourcen u.ä. über das Netzwerk verfügbar sind.

Um herauszufinden, welcher Computer die Suchliste enthält, müssen Sie zuerst einmal die fünf unterschiedlichen Funktionen kennen, die ein als Suchdienst konfigurierter Computer übernehmen kann. Bei Windows 2000 gibt es mehrere Suchdienstfunktionen, die hier in der Folge vom niederrangigen zum hochrangigen Suchdienst aufgeführt sind:

- nicht-Suchdienst
- potenzieller Suchdienst
- Sicherungssuchdienst
- Hauptsuchdienst
- Hauptsuchdienst der Domäne

Denken Sie jedoch daran, dass die meisten Computer im Netzwerk einer Organisation überhaupt keine Suchdienstfunktion übernehmen. Die meisten Computer zählen vielmehr zur Kategorie der Nicht-Suchdienste. Das trifft vor allem auf Unternehmensumgebungen, in denen es Tausende von potenziellen Suchdienstcomputern gibt, sowie auf kleine Unternehmen mit nur wenigen Computern zu. Da viele Computer auch als potenzielle Suchdienste im Netzwerk verfügbar sind, ist es wichtig, die Unterschiede zwischen den einzelnen Suchdienstfunktionen zu kennen. In Tabelle 13.1 sind die Suchdienstfunktionen in der Folge vom Suchdienst mit den wenigsten Funktionen (der Nicht-Suchdienst) bis hin zum Suchdienst mit den meisten Funktionen (der Hauptsuchdienst der Domäne) aufgeführt.

Suchdienstfunktion	Eigenschaft(en) der Suchdienstfunktion
Nicht-Suchdienst	Nicht-Suchdienste haben mit Suchlisten und deren Verwaltung nichts zu tun. Ein Nicht-Suchdienst kann auch so konfiguriert werden, dass er niemals potenzieller Suchdienst wird. Das bedeutet, er ist vor der zusätzlichen Netzwerklast sicher. Ein Nicht-Suchdienst fungiert in der Regel als ein Client-Suchdienst. D.h., er fordert Suchlisten von Suchdiensten in seinem eigenen Subnetz an.

Potenzieller Suchdienst	Ein potenzieller Suchdienst avanciert nur dann zum Sicherungssuchdienst, wenn der Hauptsuchdienst des Subnetzes dies anordnet. Ein potenzieller Suchdienst arbeitet unter normalen Bedingungen wie ein Nicht-Suchdienst, d.h., er hat mit der Verwaltung und Speicherung von Suchlisten nichts zu tun.
Sicherungssuchdienst	Ein Sicherungssuchdienst erhält seine Suchlisten vom Hauptsuchdienst, der sich im gleichen Subnetz wie er selbst befindet. Diese Suchliste beschränkt sich nur auf dieses eine Subnetz und bezieht sich nicht auf das gesamte Netzwerk. Auf Anforderung von anderen Windows-Computern verteilt der Sicherungssuchdienst die Suchliste an die entsprechenden Computer.
Hauptsuchdienst	Dieser Suchdienst ist dem Hauptsuchdienst der Domäne insofern sehr ähnlich, als er die in seinem Subnetz verfügbaren Novell NetWare-, Windows NT- und Windows 2000-Server in einer Liste sammelt. (UNIX-Server werden in der Liste nicht aufgeführt.) Der Hauptsuchdienst tauscht seine Liste der verfügbaren Server mit der Liste des Hauptsuchdienstes der Domäne aus, sodass diese beiden Suchdienste am ehesten in der Lage sind, eine aktuelle Suchliste für die Nutzung durch die restliche Netzwerkgemeinde zu verwalten. Eine weitere Aufgabe dieses Suchdienstes besteht darin, Kopien der Listen der in seinem Subnetz verfügbaren Netzwerk-Server an die Sicherungssuchdienste in seinem Subnetz zu verteilen, für den Fall, dass es zu Problemen im Netzwerk kommt (eine Art automatische Redundanz für sich selbst). Der Hauptsuchdienst kann darüber hinaus bei Bedarf auch als potenzielle Suchdienste konfigurierte Computer darüber informieren, dass diese die Aufgabe eines Sicherungssuchdienstes übernehmen sollen.
Hauptsuchdienst der Domäne	Dieser Suchdienst wird nur in Domänenumgebungen verwendet, d.h., mindestens ein Windows 2000-Server muss als Domänencontroller konfiguriert sein. Normalerweise wird der primäre Domänencontroller einer Domäne für diese Funktion eingesetzt. Dieser Suchdienst ist der Hauptsuchdienst der gesamten Domäne einschließlich all der TCP/IP-Subnetze in der Domäne, in der sich dieser Suchdienst befindet.

Tabelle 13.1: Suchdienstfunktionen und deren wichtigste Eigenschaften

Damit ein Computer eine andere Funktion übernehmen kann, muss ein bestimmtes Ereignis eintreten.

Dieses Ereignis kann sein, dass der Computer, der bisher eine bestimmte Suchdienstfunktion übernommen hat, aus dem Netzwerk genommen wird oder dass einer der als Suchdienst konfigurierten Computer Probleme mit der Hardware hat usw. Was letztlich den Ausfall eines Computers verursacht, ist nicht wichtig. Wichtig ist, was geschieht, wenn ein als Suchdienst konfigurierter Computer ersetzt werden muss. Der automatisch stattfindende Ersetzungsvorgang, der als *Suchdienstwahl* bezeichnet wird, wird in diesem Kapitel noch ausführlich beschrieben. Bevor wir uns darum kümmern, sollten Sie jedoch zunächst die Kriterien kennen, die eine Rolle spielen, wenn in der Windows-Netzwerkumgebung festgelegt wird, was jeder Client-Computer benötigt, um seine lokalen und Weitbereichsnetzwerke mit Hilfe dieser Suchlisten zu durchsuchen.

13.1.2 Kriterien für die Auswahl eines Suchdienstes

Zum Durchsuchen eines Netzwerks wird ein Windows-basierter Client-Computer in der Regel den Windows NT-Dienst WINS (Windows Internet Name Service) oder NetBIOS über TCP/IP (was von Microsoft aus unerfindlichen Gründen mit NetBT abgekürzt wird) verwenden. Wenn es einmal eine reine Windows 2000-Umgebung (d.h. alle Server und Clients arbeiten ausschließlich mit dem Betriebssystem Windows 2000 und verwenden das Windows 2000 Active Directory) geben wird, erfolgt dort die Namensauflösung mittels DNS (Domain Name System) von Microsoft. In den gemischten Umgebungen von heute, in denen es sowohl Windows NT- als auch Windows 2000-Server und Windows 9x-, Windows 3.x- und MS-DOS-Clients gibt, werden die meisten Computer LAN- und WAN-Netzwerke mittels WINS oder NetBT durchsuchen.

Wenn Sie auf dem Desktop von Windows auf das Symbol **Netzwerkumgebung** klicken, beginnen Sie bereits damit, das LAN bzw. WAN Ihrer Organisation zu durchsuchen. Ihr Client-PC meldet sich bei dem Computer, der im lokalen Subnetz als Hauptsuchdienst konfiguriert ist. Das muss nicht unbedingt ein Server-Computer sein. Es ist durchaus möglich, dass ein Windows 9x-Computer die Suchliste gespeichert hat. Dieser wird dann als *Sicherungssuchdienst* bezeichnet. Es ist jedoch wahrscheinlich, dass sich in jedem Subnetz Ihrer Organisation zumindest ein Windows NT- oder Windows 2000-Server befindet. (Sie werden das besser verstehen, wenn Sie den folgenden Abschnitt über die Suchdienstwahl gelesen haben.)

Wenn Ihr Computer das Netzwerk mittels einer Suchliste durchsucht, versucht er im Prinzip, den nett aussehenden Computernamen, den Sie im Fenster **Netzwerkumgebung** sehen können, in eine spezielle TCP/IP-Netzwerkadresse aufzulösen. Diese braucht er, damit er den Zielcomputer in den Netzwerken der Organisation oder im Internet überhaupt finden kann. Um das Ganze etwas einfacher zu machen, werden wir uns hier auf die Suche nach Computern in lokalen und Weitbereichsnetzen beschränken. Über die Suche nach Computern über das Internet erfahren Sie in Kapitel 8 und in dem Teil des Buches, in dem es um das DDNS (Dynamic Domain Name System) geht, mehr. Dieser Vorgang, bei dem ein Computernamen gesucht und in eine TCP/IP-Adresse (und umgekehrt) umgewandelt wird, wird als *Namensauflösung* bezeichnet. Es gibt zwei Windows NT 4.0- und Windows 2000-Dienste, die diesen Prozess unterstützen: WINS (Windows Internet Name Service) und DNS (Domain Name Service).



Bei Windows 2000 ist aus dem DNS ein *DDNS* geworden, da hier statt eines »statischen« Adressierungsschemas ein »dynamisches« verwendet wird. Da dies mit dem Thema dieses Kapitels jedoch wirklich nichts mehr zu tun hat, sollten Sie besser in Kapitel 8 weiter lesen, wenn Sie mehr über DDNS erfahren möchten.

WINS wird verwendet, um TCP/IP-Adressen NetBIOS-Namen zuzuordnen, während DNS schon immer von Microsoft-Betriebssystemen verwendet wird, um Hostnamen in TCP/IP-Adressen aufzulösen. Bei kleineren Netzwerken mit nur einer Subnetzmaske (d.h. mit weniger als 256 Computern) ist eigentlich keiner dieser Server-basierten Dienste erforderlich. Hier reicht ein einfaches NetBIOS über TCP/IP (NetBT) aus, um NetBIOS-basierte Computernamen zu suchen und den entsprechenden TCP/IP-Adressen zuzuordnen. Diese Information ist wichtig, da es, wenn Sie erst einmal verstanden haben, was weshalb geschieht, etwas einfacher wird, die Feinheiten der Suchdienste und der Suchlisten besser zu verstehen.

13.1.3 Suchdienstwahl

Die Suchdienstwahl ist ein sehr wichtiger Prozess, der in einer Umgebung mit Windows NT/2000-Hosts von Windows-basierten Computern automatisch in Gang gesetzt wird. Die Suchdienstwahl kann manuell insofern beeinflusst werden, als die Netzwerkadministratoren festlegen können, dass ein Windows 9x-, Windows NT- und/oder Windows 2000-Computer an der Verwaltung und Verteilung der Suchlisten nicht beteiligt wird. Der Systemadministrator kann bestimmen, dass einer dieser Computer vom restlichen Netzwerk als Nicht-Suchdienst betrachtet wird.

Die Suchdienstwahl ist ein Verfahren, bei dem ein Computer als neuer Hauptsuchdienst gewählt wird, wenn er die Voraussetzungen für diesen Suchdienst erfüllt. Neue Hauptsuchdienste werden nur gewählt, wenn eines der drei folgenden Ereignisse eintritt:

- Wenn ein Computer im Subnetz oder im WAN keinen Hauptsuchdienst finden kann.
- Wenn ein von Windows NT bzw. Windows 2000 bevorzugter Hauptsuchdienst plötzlich verfügbar wird (und damit eine »Wahl« zwischen sich und dem bisherigen Hauptsuchdienst provoziert).
- Wenn ein Windows NT-PDC (primärer Domänencontroller) oder Windows NT-BDC (Sicherungsdomänencontroller) oder ein Windows 2000-Domänencontroller im Subnetz oder im WAN neu gestartet wird.

Die Verfahrensweise bei diesen Wahlen ist recht einfach. Grundlage ist die Position der Suchdienstfunktion, die der jeweilige Computer zum Zeitpunkt der Wahl in der Domänenstruktur innehat. Computer nehmen aufgrund ihrer Suchdienstfunktion unterschiedliche Positionen in der Windows-Gemeinde ein. In einer gemischten Windows NT-/Windows 2000-Umgebung nimmt der PDC-Emulator (Emulator eines primären Domänencontrollers) in Bezug auf die Verwaltung der Suchlisten beispielsweise eine höhere Position ein als alle anderen Computer. Wenn hier jedoch Windows 2000 mit dem Active Directory eingesetzt wird, ist der Server mit dem globalen Katalog zuerst an der Reihe, was die Verwaltung der Suchlisten betrifft, dicht gefolgt von den Domänencontrollern. (Beachten Sie, dass in vielen kleineren Netzwerken der Server mit dem globalen Katalog und der Domänencontroller derselbe Computer sind.) Ebenso gibt es in der Domäne keinen PDC-Emulator, sondern nur Domänencontroller, wenn es sich um eine reine Windows 2000-Umgebung handelt.

Wie auch immer, die restlichen Suchlisten werden in der folgenden Reihenfolge verwaltet (wobei der wichtigste Suchdiensttyp zuerst, der am wenigsten wichtige Suchdiensttyp zuletzt aufgeführt wird):

- Der Suchdienst agiert momentan als Sicherungssuchdienst.
- Das `MaintainServerList`-Flag ist mit `Yes` definiert.
- Der Suchdienst agiert momentan als Hauptsuchdienst.

- Das System wird als der bevorzugte Hauptsuchdienst betrachtet.
- Der Computer ist ein WINS-Server.
- Der Computer ist ein primärer Domänencontroller (Windows NT 4.0) oder ein Domänencontroller (Windows 2000).
- Die Stufe der Kriterien der Vorgängerversion.
- Die Stufe der Wahlversion.
- Windows 2000 Server/Windows NT Server.
- Windows 2000 Professional/Windows NT 4.0 Workstation.
- Windows 9x oder Windows für Workgroups.
- Art des Betriebssystems.

Um eine Suchdienstwahl zu gewinnen, reicht es jedoch nicht einfach aus, der wichtigste Suchdiensttyp im Subnetz bzw. Netzwerk zu sein. Während der Suchdienstwahl wird ein Wahldatagramm von dem Computer, der diese Suchdienstwahl initiiert hat, an den PC gesendet, der die besten Chancen hat, zum Hauptsuchdienst gewählt zu werden. Abhängig von den Auswahlkriterien wird einer der am Senden und Empfangen des Wahldatagramms beteiligten Suchdienste die Wahl »gewinnen«. Dabei gelten folgende Kriterien:

- Wenn der Suchdienst, der das Wahldatagramm empfängt, eine höhere Position einnimmt als der Suchdienst, der das Datagramm gesendet hat, gewinnt der Suchdienst mit der höheren Position. Sind beide Suchdienste gleichrangig, wird das nächste Wahlkriterium herangezogen. Die Stufe des Wahlkriteriums ist ein statischer Wert, der nicht von der Version des Betriebssystems des Suchdienstcomputers abhängt.
- Wenn die Wahl in die zweite Runde geht, findet eine Bewertung der Wahlkriterien des empfangenden und des sendenden Suchdienstes statt. Wenn der empfangende Suchdienst eine höhere Position innehat, gewinnt er. Andernfalls geht die Wahl in die nächste Runde.
- Diese ist einfach zu verstehen. Einfach ausgedrückt: Wenn der empfangende Computer schon länger läuft als der sendende, dann gewinnt der empfangende Computer. Wenn er die Wahl nicht gewinnt, geht die Wahl in die letzte Runde.
- Wenn die Wahl bis jetzt noch auf keinen Computer gefallen ist, gewinnt derjenige mit dem »lexikalisch gesehen niedrigsten Namen«. Auf gut Deutsch heißt das, dass das System mit dem Namen gewinnt, der in der alphabetischen Reihenfolge (dabei sind Buchstaben und Zahlen eingeschlossen) am weitesten vorne steht. Ein System mit dem Computernamen *Apple* gewinnt die Wahl gegenüber einem System mit dem Computernamen *Microsoft*, weil A im Alphabet vor M kommt.

Auch wenn diese erste »Wahl« mit einem Gewinner endet, führt dies nicht dazu, dass dieser Gewinner sofort zum neuen Hauptsuchdienst ernannt wird. Wenn ein als Suchdienst konfigurierter Computer die Wahl gewonnen hat, tritt er in das *Stadium der Wahldurchführung*. In diesem Stadium sendet dieser Computer wiederholte Male Suchdienst-Wahldatagramme an die anderen in Frage kommenden Computer innerhalb der Domäne. Diese anderen Computer antworten mit unterschiedlichen Verzögerungszeiten, die von der Position der Computer in der Hierarchie der Domäne abhängen. Dies führt schließlich zum Gewinner der Suchdienstwahl. Danach wird der neue Hauptsuchdienst ernannt. Dieser beginnt den ganzen Prozess von Neuem, wenn er wieder zur Wahl eines Hauptsuchdienstes

herausgefordert wird.

13.2 Der Suchprozess

Der Suchprozess besteht aus drei Vorgängen:

- Sammeln von Suchdaten
- Verteilen von Suchdaten
- Bearbeiten von Suchanforderungen von Clients

Windows 2000 führt diese drei Aufgaben mit Hilfe der beiden Dienste Computerbrowser und TCP/IP-NetBIOS-Hilfsprogramm aus, die in der Computerverwaltung unter **Dienste** angezeigt werden (siehe Abbildung 13.2).

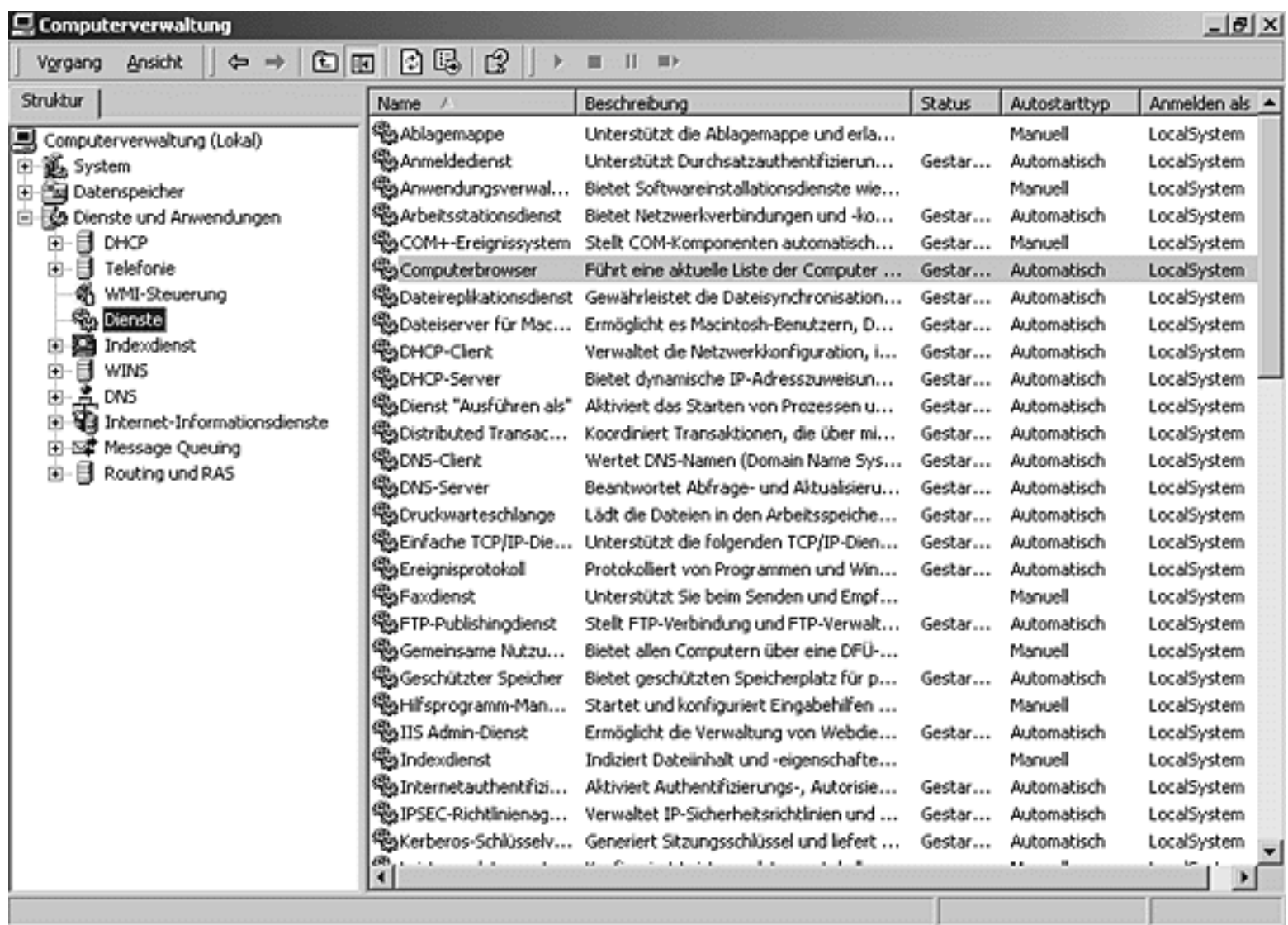


Abbildung 13.2: Dienste in Windows 2000



Falls Sie nicht mehr wissen, wie Sie die Computerverwaltung aufrufen können: Klicken Sie zuerst mit der rechten Maustaste auf dem Desktop von Windows 2000 auf das Symbol **Arbeitsplatz**. Klicken Sie in dem daraufhin erscheinenden Dropdown-Menü auf die Option **Verwaltung**.

Wenn einer der beiden Dienste auf Ihrem Windows 2000-Server nicht ausgeführt wird, klicken Sie auf den Dienst, um ihn zu markieren und klicken Sie dann auf die Schaltfläche **Start**, die sich oben im Fenster befindet und wie die Starttaste auf einem Kassettenrekorder aussieht, um den Dienst wieder zu starten. Wenn diese beiden Dienste ausgeführt werden, stellen diese ihre Fähigkeiten zur Verfügung, die für Ihre Windows 2000-Umgebung erforderlich sind.

Aus Sicht einer Domäne sind die Suchdienste in Windows 2000 Server-Umgebungen denen der alten Windows NT 4.0 Server-Umgebungen im Wesentlichen gleich. (Welche Auswirkungen die Konfiguration von Organisationseinheiten im Active Directory im Gegensatz zu einer Domänenstruktur auf das Durchsuchen hat, wird am Ende dieses Kapitels ausführlicher beschrieben.) Das Sammeln von Suchdaten funktioniert so, dass die unterschiedlichen Suchlisten, die der Hauptsuchdienst über Broadcasts an die einzelnen Netzwerksegmente (Subnetze) zusammengesammelt hat, zusammengeführt werden. Die Windows 2000-Server tun dies mit Hilfe der Dienste Computerbrowser und TCP/IP-NetBIOS-Hilfsprogramm, während Windows NT-Server dazu ihren Serverdienst verwenden.

Diese Serverdienste erstellen die Suchlisten mit Hilfe von Hostankündigungen. Diese Hostankündigungen werden vom Hauptsuchdienst jedes Subnetzes im Netzwerk gesammelt. In einer reinen Windows 2000 Server-Umgebung sind diese Ankündigungen TCP/IP-basiert. Wenn es im Netzwerk ältere Windows NT Server-Domänencontroller gibt, werden die Ankündigungen mit Hilfe der Netzwerkprotokolle NetBEUI oder IPX/SPX übertragen. Wenn der Hauptsuchdienst die Ankündigungen empfängt, vergleicht er den Computernamen des übertragenden Computers mit dem in seiner Suchliste. Wenn der Computernamen in der Liste des Hauptsuchdienstes nicht vorhanden ist, wird er hinzugefügt. Wenn der Name in der Liste enthalten ist, wird er, falls erforderlich, aktualisiert.

Wenn die Suchliste vollständig ist, muss sie an sämtliche Sicherungssuchdienste im Subnetz verteilt werden. Außerdem kündigt sich der Hauptsuchdienst ebenfalls bei allen Computern im lokalen Subnetz an, sodass jeder Server und Client »weiß«, welcher Computer als Hauptsuchdienst konfiguriert ist und wo sich dieser Computer befindet. Wenn der Hauptsuchdienst nicht in regelmäßigen Zeitabständen (etwa alle 15 Minuten) eine aktualisierte Suchliste sendet, erkennt der Sicherungssuchdienst, dass der Hauptsuchdienst offline ist. Wenn dies der Fall ist, wird ein neuer Hauptsuchdienst gewählt und anschließend konfiguriert.

Zu den wichtigsten Aufgaben eines als Suchdienst und insbesondere des als Hauptsuchdienst konfigurierten Computers gehört es, Suchanforderungen von Netzwerk-Clients zu bearbeiten. Es gibt eine Reihe unterschiedlicher Suchanforderungen. Dazu gehört auch die erste Anforderung, die von einem Client gesendet wird, wenn er zum ersten Mal in einem bestimmten Subnetz hochgefahren wird. Andere Anforderungen dienen dazu, die Computernamen der Sicherungssuchdienste aufzulösen, die sich im gleichen Subnetz wie der Client befinden sollen. Der Client bekommt beim Hochfahren im Subnetz vom Hauptsuchdienst eine kurze Liste mit den Sicherungssuchdiensten.

13.2.1 Suchdienstankündigungen

Suchdienstankündigungen werden von den einzelnen Computern im Netzwerk verwendet, um die Suchlisten, die von den unterschiedlichen Hauptsuchdiensten (Hauptsuchdienst der Domäne, Hauptsuchdienst und Sicherungssuchdienst) in einer Netzwerkumgebung mit Windows NT/2000-Domänen erstellt und verwaltet werden, aktuell zu halten. Als Hauptsuchdienst konfigurierte Computer empfangen diese Ankündigungen in regelmäßigen Zeitabständen von folgenden

Arten von Clients:

- Windows NT 3.1 (Beachten Sie, dass es bei dieser ersten Version von Windows NT noch keine »Workstation«-Version gegeben hat.)
- Windows NT 3.1 Advanced Server
- Windows für Workgroups 3.1 und 3.11
- Windows 95 (sowohl die A- als auch die B-Version)
- Windows 98 und Windows 98 Second Edition
- Windows Millennium (Consumer Windows)
- Windows NT Workstation 3.5, 3.51 und 4.0
- Windows NT Server 3.5, 3.51 und 4.0
- Windows 2000 Professional
- Windows 2000 Server, Advanced Server und Datacenter
- Auf LAN Manager basierende Systeme

Reine MS-DOS-Clients und Clients, die die grafische Benutzeroberfläche von Windows 3.1 bzw. 3.11 (nicht die Windows für Workgroups-Version) ausführen, können keine Suchdienstankündigungen erzeugen.

Wie Sie in Abbildung 13.3 sehen können, sind die Zeitabstände, in denen die Clients diese Suchdienstankündigungen senden müssen, relativ kurz.

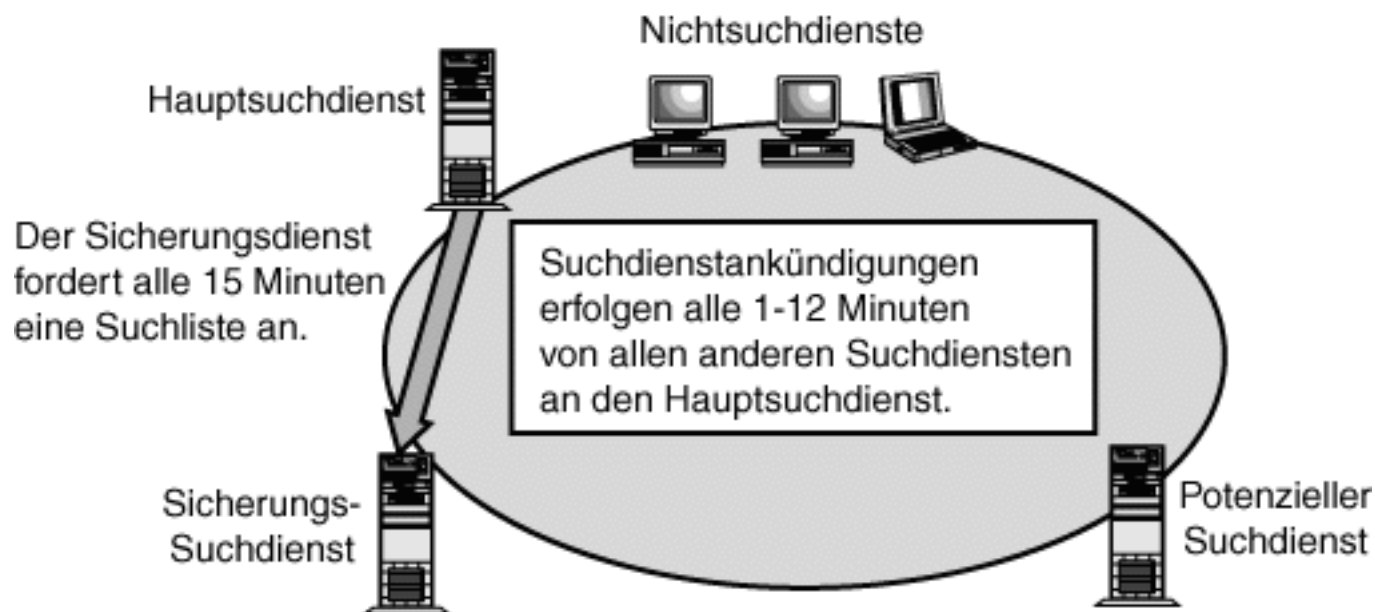


Abbildung 13.3: Suchdienstankündigungen und der dazu gehörende Zeitplan.

Darüber hinaus erhalten die Sicherungssuchdienste alle 15 Minuten eine Kopie der neuen bzw. aktualisierten Suchliste. Die dafür verantwortlichen Computer sind (wie Sie der folgenden Liste entnehmen können) im Wesentlichen dieselben wie jene, die die Suchdienstankündigungen senden:

- Windows NT 3.1 (beachten Sie, dass es bei dieser ersten Version von Windows NT noch keine »Workstation«-Version gegeben hat)
- Windows NT 3.1 Advanced Server

- Windows für Workgroups 3.1 und 3.11
- Windows 95 (sowohl die A- als auch die B-Version)
- Windows 98 and Windows 98 Second Edition
- Windows Millennium (Consumer Windows)
- Windows NT Workstation 3.5, 3.51 und 4.0
- Windows NT Server 3.5, 3.51 und 4.0
- Windows 2000 Professional
- Windows 2000 Server, Advanced Server und Datacenter

13.2.2 Der Hauptsuchdienst

Der als Hauptsuchdienst konfigurierte Computer ist der Computer, der für das Sammeln der Informationen verantwortlich ist, die für das Erstellen der Suchliste für die Domäne erforderlich sind. Diese Suchliste enthält die aufgelösten Computernamen sämtlicher Server, die sich in der Arbeitsgruppe bzw. in der Domäne (vorausgesetzt, diese erstreckt sich nicht über mehrere Subnetze) des Hauptsuchdienstes befinden, sowie eine Liste der Domänen und Netzwerke des gesamten Netzwerks der Organisation. Diese Domänen- und Netzwerklisten enthalten natürlich möglicherweise nicht alle Nicht-Microsoft-Domänen, -Strukturen und -Arbeitsgruppen, wie die, die von Novell NetWare-Servern, UNIX-Servern usw. erstellt worden sind. Wenn Sie sich die Suchliste Ihrer Arbeitsgruppe ansehen möchten, klicken Sie auf dem Desktop von Windows 2000 auf das Symbol **Netzwerkumgebung**. Doppelklicken Sie dann auf das Symbol **Benachbarte Computer**, um solch eine Liste aufzurufen.

Wenn sich eine Domäne über mehr als ein Subnetz im Netzwerk der Organisation erstreckt, kann der Hauptsuchdienst keine Suchliste für die gesamte Domäne verwalten. Dazu ist ein neuer Suchdienst, nämlich der *Hauptsuchdienst der Domäne* erforderlich. Der Hauptsuchdienst der Domäne koordiniert die Ergebnisse der Hauptsuchdienste, die Informationen für das Erstellen und Verwalten von Suchlisten für die einzelnen Subnetze sammeln.

Es gibt einige wichtige Eigenschaften des Hauptsuchdienstes der Domäne, die Sie kennen sollten. Der Hauptsuchdienst der Domäne befindet sich immer im PDC-Emulator (Emulator des primären Domänencontrollers) der gesamten Windows 2000-Umgebung. Ein PDC-Emulator wird in einem gemischten Netzwerk verwendet. Wenn es in keinem der Subnetze Windows NT 3.51- oder 4.0-Server gibt, sollten Sie im einheitlichen Modus arbeiten. Das bedeutet, dass es im ganzen Netzwerk nur Windows 2000-Domänencontroller und keinen PDC-Emulator gibt. Voraussetzung dafür ist, dass Active Directory sowie DNS bzw. DDNS im Netzwerk nicht verwendet werden.

13.2.3 Die Suchliste

Eine *Suchliste* enthält einfach die in einem bestimmten Netzwerk verfügbaren Windows NT- und Windows 2000-Domänen und -Server. Die Liste wird vom Windows 2000 Server-Computerbrowser verwaltet. Dieser Dienst arbeitet mit jedem der Suchdiensttypen (Hauptsuchdienst der Domäne, Hauptsuchdienst, Sicherungssuchdienst usw.). Sie können die Liste des Computerbrowser-Dienstes über die Netzwerkumgebung aufrufen (indem Sie auf dem Desktop von Windows 2000 auf das Symbol **Netzwerkumgebung** doppelklicken). Hier ist die Liste in zwei Bereiche unterteilt: **Benachbarte**

Computer und **Gesamtes Netzwerk**. Wenn Sie auf **Gesamtes Netzwerk** doppelklicken, werden sämtliche Computer, Drucker, freigegebene Dateien und Ordner sowie Personen im Windows 2000-Netzwerk angezeigt. Wenn Sie auf **Benachbarte Computer** doppelklicken, werden nur die Computer angezeigt, die sich in Ihrer lokalen Arbeitsgruppe bzw. Domäne befinden.

13.2.4 Überlegungen zum Durchsuchen mehrerer Domänen und WANs

Wenn sich das Netzwerk Ihrer Organisation über mehrere Subnetze und Domänen erstreckt, müssen Sie einige Dinge beachten. Das Ganze wird noch komplexer und verwickelter, wenn dabei noch Microsoft DNS und Active Directory verwendet werden. Daher wird ein Teil dieses Themenbereichs erst gegen Ende dieses Kapitels ausführlicher beschrieben. Um das Ganze etwas zu vereinfachen, konzentrieren wir uns in diesem Abschnitt darauf, wie das Durchsuchen von Weitbereichsnetzen (WANs) mit Hilfe des Netzwerkprotokolls TCP/IP funktioniert, sowie darauf, wie das Alles funktioniert, wenn Domänencontroller mit Hilfe von NetBIOS über TCP/IP (NetBT) gesucht werden.

Zunächst einmal müssen Sie bestimmen, ob eine Technologie, die als *WINS (Windows Internet Name Service)* bezeichnet wird, verwendet werden soll. In einer reinen Windows 2000-Umgebung, in der alle Server mit Windows 2000 Server und alle Clients mit Windows 2000 Professional arbeiten, ist NetBIOS über TCP/IP nicht erforderlich. Bevor Sie NetBIOS deaktivieren, sollten Sie auf jeden Fall sehr genau prüfen, ob sich nicht doch noch ein älteres Windows-System (Windows 3.x, Windows 9x, Windows NT oder Windows Millennium) irgendwo in Ihrem Netzwerk befindet. Denken Sie daran, dass Windows 2000 das erste Windows-basierte Betriebssystem ist, das ohne NetBIOS über TCP/IP auskommt. Sie müssen sich also ganz sicher sein, bevor Sie eine Technologie deaktivieren, die für alle anderen Versionen von Microsoft Windows lebenswichtig ist.

Als Nächstes müssen Sie herausfinden, ob alle Clients und Server in den Netzwerken Ihrer Organisation so konfiguriert werden können, dass sie den Einsatz eines alternativen Schemas zur Auflösung von Computernamen in IP-Adressen wie z.B. Microsoft DNS (dabei handelt es sich eigentlich um die dynamische Version des DNS, die bei Windows 2000 als DDNS bezeichnet wird) unterstützen. Die Namensauflösung wird bei Windows 2000-Servern und -Clients standardmäßig so konfiguriert, dass diese mit Hilfe von DDNS erfolgt. Darüber hinaus werden sämtliche WINS-Clients in einer Windows 2000-Domäne ebenfalls standardmäßig auf den Microsoft DDNS-Server für die Auflösung von Computernamen verweisen, die mehr als 15 Zeichen umfassen oder einen Punkt enthalten. Bei Computernamen, die bis zu 15 Zeichen umfassen, werden WINS-Clients zunächst versuchen, diese mit Hilfe der WINS-Methode aufzulösen und DDNS nur dann verwenden, wenn die WINS-Methode nicht funktioniert. Daher ist es erforderlich, einen WINS-Server für die Unterstützung der Suchdienste einzusetzen, um eine Suche im WAN einer Organisation effektiv durchzuführen, vorausgesetzt, in diesem WAN wird weder Active Directory noch Microsoft DNS verwendet.

Denken Sie jedoch daran, dass Sie ohne WINS bzw. DDNS auskommen, auch wenn sich Ihr kleines Netzwerk über mehrere Domänen, nicht jedoch über mehrere Subnetze erstreckt. Wenn sich im Netzwerk der Organisation mehr als 50 Clients befinden, wird der Einsatz von WINS bzw. DDNS jedoch zu einem Muss.

Wenn Sie sich einmal entschieden haben, dass Sie nur mit WINS arbeiten möchten (vorausgesetzt, Sie verwenden weder Active Directory noch Microsoft DNS), müssen Sie noch einige weitere Dinge

berücksichtigen. Wenn Sie für das Durchsuchen der WANs der Organisation den WINS-Dienst konfigurieren, stellen Sie im Prinzip ein Medium für die Auflösung von NetBIOS-Namen in IP-Adressen zur Verfügung. WINS ermöglicht keine Auflösung von Host-Namen in IP-Adressen. Das bedeutet, dass keiner der UNIX-Clients in Ihrem WAN diese Funktion nutzen kann, da DDNS auf einem offeneren und nicht auf Microsofts eigenem Standard beruht und daher beim Durchsuchen des Netzwerks auch Nicht-Microsoft-Clients erreicht. Eine andere Möglichkeit besteht darin, bei Nicht-Microsoft-Clients und Microsoft NetBIOS-Clients jeweils die Dateien `Hosts` bzw. `Lmhosts` zu verwenden. Da diese beiden Dateien statische Dateien sind und auf jedem Server bzw. Client vorhanden sein müssen, ist es recht mühselig, diese Dateien bei jeder Änderung im Netzwerk zu aktualisieren. Oder anders ausgedrückt: Es ist praktisch nicht möglich, derartige Dateien für ein WAN zu verwalten.

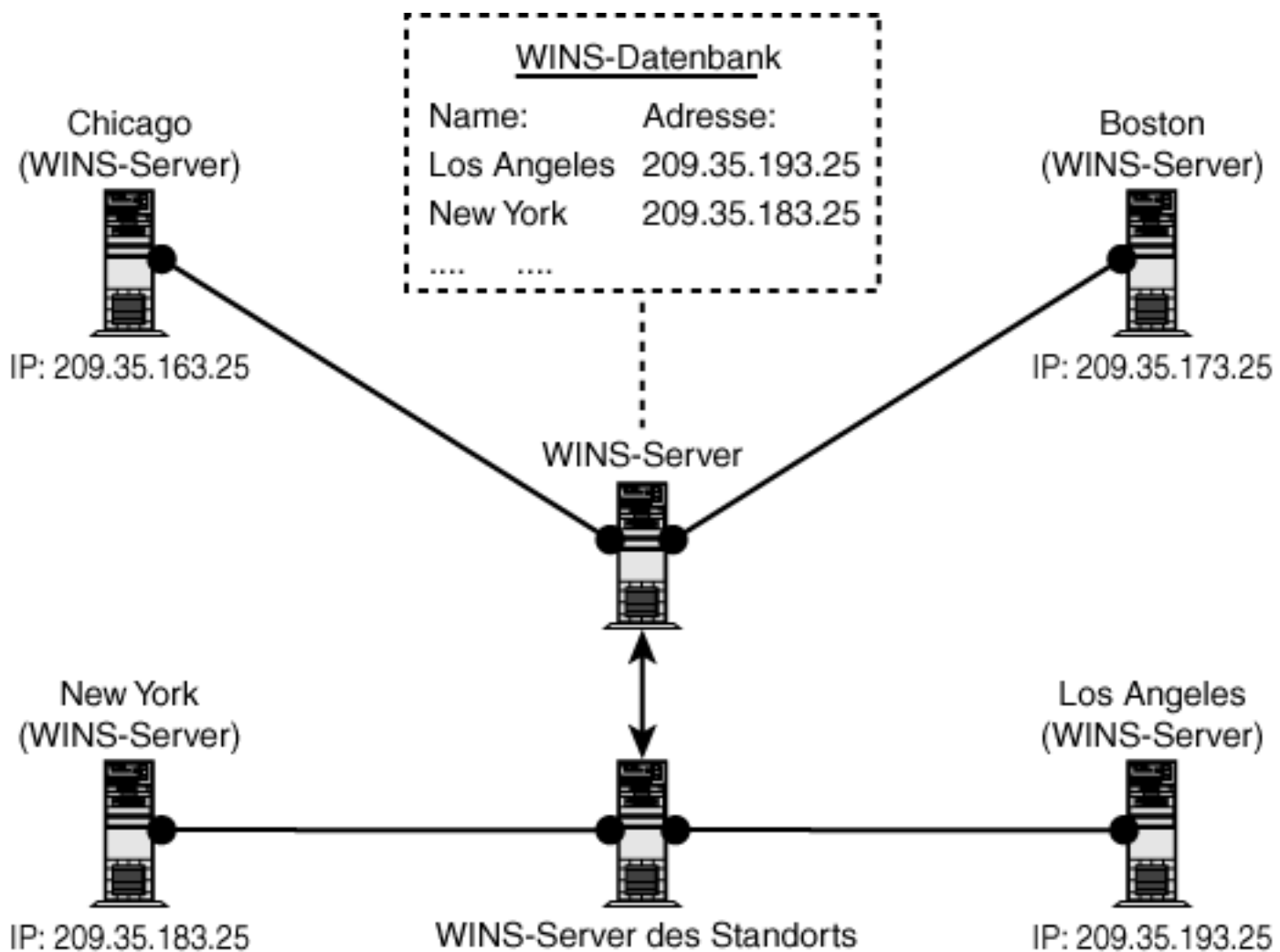
Wenn die Organisation jedoch entscheidet, WINS-Server einzusetzen (in Kapitel 8 erfahren Sie mehr darüber, wie Sie die WINS-Technologie im Netzwerk Ihrer Organisation implementieren), haben Sie einige Möglichkeiten, den Suchprozess für ein Weitbereichsnetz zu fördern:

- Da WINS als eine Art Ersatzverzeichnisdienst für die Auflösung von NetBIOS-Namen in IP-Adressen (und umgekehrt) dient, werden die Suchfähigkeiten des Hauptsuchdienstes der Domäne weiter verbessert, wenn dieser Hauptsuchdienst ein WINS-aktivierter Client ist, denn der Hauptsuchdienst der Domäne wird vier- bis fünfmal pro Stunde vom WINS-Server eine aktualisierte Liste mit den Servern in der Domäne erhalten.
- Jeder WINS-aktivierte Client kann unabhängig davon, ob er als Suchdienst konfiguriert ist oder nicht, einen WINS-Server nach Änderungen in der Liste der NetBIOS-Namen abfragen.
- WINS-aktivierte Clients sind besser ausgerüstet, um über Subnetze hinweg »sehen« zu können, da die normalerweise remote gespeicherten Listen der Namen sämtlicher Domänen auf deren lokalem WINS-Server gespeichert (und regelmäßig an andere WINS-Server im WAN repliziert) werden.

Vielleicht ist es einfacher zu verstehen, weshalb WINS für den Suchprozess so vorteilhaft ist, wenn Sie sich die Funktionsweise von WINS einmal grafisch vor Augen führen. In Abbildung 13.4 sehen Sie beispielsweise vier voneinander unabhängige Domänen (was darauf schließen lässt, dass weder Active Directory noch Microsoft DNS verwendet wird) eines fiktiven Unternehmens, die sich jeweils in einer anderen Stadt befinden: Chicago, Boston, New York und Los Angeles.

Jede Niederlassung in diesen Städten verfügt über ihr eigenes Windows 2000-Domänennetzwerk. Alle arbeiten im gemischten Modus, wobei PDC-Emulatoren die WINS-Server-Dienste für die jeweilige Umgebung übernehmen. Sämtliche Clients innerhalb der einzelnen Domänen sind WINS-fähig. Somit hat jeder die für Suchzwecke erforderlichen besten Voraussetzungen. Wenn die unterschiedlichen PDC-Emulatoren in ihren jeweiligen Netzwerken zu arbeiten beginnen, registrieren sie den Namen ihrer Domäne beim bevorzugten WINS-Server jedes Standorts.

Aufgrund der Replikation der WINS-Datenbank erhält jeder der WINS-Server, die eine Verbindung zwischen den unterschiedlichen Unternehmensstandorten (die beiden WINS-Server in der Mitte des Diagramms) herstellen, nach und nach sämtliche Computernamen und IP-Adressen der Domänen auf beiden Seiten der WAN-Verbindung. Diese sind dann ihrerseits in der Lage, diese Informationen an die anderen WINS-Server innerhalb des von ihnen weitergeleiteten Netzwerks weiterzugeben. Dieser ganze Vorgang ist es, mit dem das Durchsuchen von WANs in einer gemischten Umgebung am besten funktioniert.



Die WINS-Server befinden sich auf dem PDC-Emulator (PDCE) für jeden Domäne, und jeder PDCE ist gleichzeitig der Hauptsuchdienst der eigenen Domäne.

Abbildung 13.4: Durchsuchen eines WAN mit Hilfe von WINS

Es gibt einige Dinge, an die Sie denken sollten, wenn Sie im gemischten Modus ohne Active Directory arbeiten:

- Zuerst einmal dürfen die Versionen des Betriebssystems der Hauptsuchdienste der Domäne, die nicht Windows 2000-Server sind, nicht älter als Version 3.5 sein (d.h., es können keine Windows NT 3.1 Advanced Server eingesetzt werden). Das kommt ganz einfach daher, weil Windows NT 3.1 mit der WINS-Technologie noch nichts anzufangen weiß (diese war damals noch nicht erfunden).
- Dann müssen sämtliche Clients in der Arbeitsgruppe WINS-fähig sein. Oder anders ausgedrückt: Sämtliche Clients in der Arbeitsgruppe müssen den WINS-Dienst unterstützen. Wie gesagt, bei Windows für Workgroups-, Windows 9x-, Windows NT- (ab Version 3.5) und Windows 2000-Clients ist das kein Problem. Aber seien Sie vorsichtig, wenn Sie eine große Anzahl an Macintosh-, UNIX- oder DOS-Clients haben.
- Seien Sie schließlich auch bei der Verwendung von statischen Domännennamen und IP-Adressen auf Nicht-WINS-Servern vorsichtig, da diese zu veralteten Einträgen in der WINS-Suchliste

führen können, wenn ein Computernamen oder eine IP-Adresse im Netzwerk geändert oder gelöscht wird.

Das andere Verfahren, mit dessen Hilfe ein Windows 2000- oder ein älterer Windows-Client (Windows für Workgroups, Windows 9x, Windows NT) einen Domänencontroller finden kann, ist eine Technik, die unter der Bezeichnung *NetBIOS über TCP/IP (NetBT)* bekannt ist. Das Suchen und Auffinden von Domänencontrollern ist in der Welt der Windows 2000-Netzwerke sehr wichtig, da der Domänencontroller den Zugriff auf das Netzwerk steuert. Wenn ein Client in einem Netzwerk nicht authentifiziert werden kann, kann er den Suchprozess niemals beginnen. Da Windows 2000-Domänen mit Hilfe der Active Directory-Technologie erstellt und gesteuert werden, beruht der Suchprozess einzig und allein auf DNS-Abfragen zur Auflösung von Namen und Standorten von Windows 2000-Domänencontrollern. Innerhalb von Windows 2000-Arbeitsgruppen, in denen es keinen Domänencontroller gibt, hängt die Authentifizierung für die Ressourcen der Arbeitsgruppe (vorausgesetzt, die Clients werden von einem Windows 2000-Server in dieser Arbeitsgruppe kontrolliert) davon ab, ob die Clients den entsprechenden Windows 2000-Server finden.

In der Welt von NetBT geschieht dies durch den Einsatz von NetBIOS über TCP/IP-Meldungen, die im Subnetz und/oder weitergeleiteten Netzwerk unter Verwendung der UDP-Anschlussnummer 137 (User Datagram Protocol) verteilt werden. Bei einer Vielzahl von weitergeleiteten Netzwerken wird die Verwendung des UDP-Anschlusses 137 auf Routerebene blockiert, da dies eine häufige Fehlerquelle ist, die zu massenhaften Broadcasts im Netzwerk führt. Wenn ein weitergeleitetes Netzwerk diesen Rahmentyp jedoch nicht blockiert, erscheint das Netzwerk für den suchenden Client als ein einziges, gigantisches Netzwerksegment. Damit kann ein kleines bis mittelgroßes Netzwerk ohne DNS- oder WINS-Server durchsucht werden, wobei der Suchprozess immer länger dauert, je größer das Netzwerk wird.

Zurück zu Positiverem: Es ist nun möglich, gänzlich ohne die beiden wichtigsten Suchtechniken - NetBIOS über TCP/IP- sowie WINS-Server - auszukommen und sich statt dessen der von Microsoft geprägten Zukunft des DNS (Domain Name System) zuzuwenden. DNS ist ein Dienst für die Auflösung von Internet- und TCP/IP-Namen, mit dessen Hilfe Clients Computernamen registrieren und auflösen können. Die Windows 2000-Implementierung von DNS unterscheidet sich jedoch von den Implementierungen der Vergangenheit dadurch, dass DNS nun Computernamen und IP-Adressen dynamisch aktualisiert, speichert und abrufen. Diese neue Version wird häufig als *DDNS (Dynamic Domain Name System)* bezeichnet.

Damit NetBT- bzw. WINS-Implementierungen in den Windows 2000 Server-Netzwerken Ihrer Organisation vollständig überflüssig werden, muss in Ihrer Organisation eine Migration sämtlicher WINS-Server (falls vorhanden) durchgeführt werden, sodass eine reine Microsoft DNS-Umgebung gegeben ist. Darüber hinaus muss in der Organisation die Verwendung der Technologie NetBIOS über TCP/IP unterbunden werden, sodass keiner der Clients Namen mit Hilfe von auf NetBIOS basierenden Namensabfragen und UDP-Anschluss 137 auflöst. Es wird geschätzt, dass in der Vergangenheit nahezu 80 % der Sicherheitsprobleme bei Windows NT direkt auf die unbefugte Verwendung von NetBIOS zurückzuführen waren. Dieses Feature bei Windows 2000 zu deaktivieren, ist also aus Gründen der Sicherheit für Ihre Organisation von Vorteil. Bevor Ihre Organisation einen dieser beiden Migrationsschritte durchführt, sollten Sie sämtliche Server und Netzwerke Ihrer Organisation prüfen um sicherzugehen, dass sich keine älteren Windows-Clients in der Organisation befinden, die die Dienste WINS oder NetBT beanspruchen.

Sie sollten damit beginnen, sämtliche WINS-Server zu Windows 2000-DNS-Servern zu migrieren. Dieser Prozess beginnt mit der Installation der erforderlichen Anzahl an DNS-Servern. Danach müssen sämtliche Clients im Netzwerk so konfiguriert werden, dass sie statt WINS DNS für die Namensauflösung verwenden. Wenn dies abgeschlossen ist, können die WINS-Server selbst migriert werden, sodass letztlich im Unternehmen nur noch DNS-Server zum Durchsuchen des Netzwerks verwendet werden.

13.2.5 Ausfälle von Suchdiensten

Es gibt mehrere Arten von Ausfällen, die bei Suchdiensten in einem Windows 2000 Server-Netzwerk auftreten können: das Herunterfahren eines Nicht-Suchdienstes, der Ausfall eines Sicherungssuchdienstes, der Verlust eines Hauptsuchdienstes und das Beenden eines Hauptsuchdienstes der Domäne. Beachten Sie, dass Ausfälle von Suchdiensten in Clustern nur bei Windows 2000 Advanced Server auftreten können und daher in diesem Buch nicht behandelt werden. Beim Herunterfahren eines Suchdienstes geschieht Folgendes:

- Wenn es sich bei dem Suchdienst, der heruntergefahren wird, um einen Sicherungssuchdienst handelt, informiert dieser den Hauptsuchdienst mittels Ankündigungen über diesen Vorgang. Dies geschieht dadurch, dass der Sicherungssuchdienst die Ankündigung so ändert, dass der Computerbrowser und das TCP/IP-NetBIOS-Hilfsprogramm in seiner Liste der ausgeführten Serverdienste nicht mehr enthalten sind.
- Wenn es sich bei dem Suchdienst, der heruntergefahren wird, um den Hauptsuchdienst des Subnetzes handelt und das Herunterfahren beabsichtigt (und also kein Systemabsturz) ist, erzwingt der Hauptsuchdienst eine Suchdienstwahl.

Wenn der Hauptsuchdienst der Domäne, der Hauptsuchdienst, ein Sicherungsdienst oder ein Nicht-Suchdienst unbeabsichtigt heruntergefahren wird, wird das Ganze etwas schwieriger. Bei dieser Art des Herunterfahrens spricht man vom *Ausfall eines Suchdienstes*. Dieses Problem wird je nach Art des ausfallenden oder ausgefallenen Suchdienstes unterschiedlich gehandhabt.

Wenn der Hauptsuchdienst einer Domäne ausfällt, muss ein neuer Hauptsuchdienst der Domäne durch den Ersatz des Windows 2000 PDC-Emulators oder durch den Ersatz des neuen Windows 2000-Domänencontrollers erstellt werden. Bis der Hauptsuchdienst der Domäne ersetzt worden ist, werden die Hauptsuchdienste der einzelnen Subnetze ihre Subnetze bedienen, wobei die Netzwerkumgebung mit Informationen etwas kurz gehalten wird. Clients können allerdings dennoch auf Geräte in anderen Subnetzen zugreifen, vorausgesetzt, der vollständige UNC-Name (Universal Name Convention) für das entsprechende Gerät ist bekannt. Wenn beispielsweise der Pfad `\\servername\freigabename\verzeichnis\dateiname` (das ist der vollständige Windows 2000-Name einer Ressource im Netzwerk) vom Client eingegeben werden kann, wird der Zielrechner auch gefunden.

Wenn ein Hauptsuchdienst ausfällt, wird einer der vielen Sicherungssuchdienste dies innerhalb von 15 Minuten feststellen. Wenn der Verlust eines Hauptsuchdienstes erkannt wurde, initiiert der Sicherungssuchdienst, der den Verlust entdeckt hat, eine Suchdienstwahl, damit ein neuer Hauptsuchdienst konfiguriert wird.

Wenn ein Sicherungssuchdienst ausfällt, kann es bis zu einer Stunde dauern, bis dieser Verlust bemerkt und der Sicherungssuchdienst vom Hauptsuchdienst aus der Liste der Suchdienste entfernt wird. Der

Verlust eines Sicherungssuchdienstes ist nicht von so großer Bedeutung, da der Client, der die Suchliste von diesem einen Sicherungssuchdienst angefordert hat, nun einfach eine Anforderung an einen anderen, als Sicherungssuchdienst konfigurierten Computer sendet. Wenn der Client keinen berechtigten Sicherungssuchdienst findet, der ihm die angeforderte Suchliste zur Verfügung stellen kann, fordert der Client diese Liste beim Hauptsuchdienst an. Wenn er keinen funktionierenden Hauptsuchdienst findet, wird die Suchdienstwahl in Gang gesetzt, um einen neuen Hauptsuchdienst zu finden.

Wenn ein Nicht-Suchdienst ausfällt, hat das kaum Auswirkungen auf das Durchsuchen. Nach einer variablen Zeitdauer - üblicherweise zwischen 3 und 51 Minuten - löscht der Hauptsuchdienst den Nicht-Suchdienst aus der Suchliste. Der Grund für eine solch unterschiedliche Zeitdauer liegt in den regelmäßigen Zeitrahmen der Suchdienstankündigungen für Nicht-Suchdienste sowie in den Verzögerungen zwischen der Aktualisierung von Suchlisten zwischen dem Hauptsuchdienst und den Sicherungssuchdiensten begründet. Abgesehen von einem durch Suchdienstankündigungen verursachten, leicht erhöhten Netzwerkverkehr, die durch den Ausfall eines Nicht-Suchdienstes verursacht werden, hat der Ausfall eines Nicht-Suchdienstes praktisch keine Auswirkungen auf den Suchvorgang.

13.2.6 Einen Windows 2000-Server so konfigurieren, dass er nie als Suchdienst eingesetzt wird

Es ist nicht allzu schwierig, dafür zu sorgen, dass ein Windows NT-Server bzw. ein Windows NT Workstation-Rechner, ein Windows Advanced Server oder ein Datacenter-Computer nicht als Suchdienst eingesetzt wird. Dazu müssen Sie den Registrierungseditor des Betriebssystems Windows 2000 Server aufrufen. Klicken Sie dazu auf **Start, Ausführen** und geben Sie dann einen der Registrierungseditorbefehle (`Regedit.exe` oder `Regedt32.exe`) ein. Drücken Sie anschließend die Eingabetaste, um den Registrierungseditor zu starten. Daraufhin öffnet sich das Fenster des Registrierungseditors. Um dies so einfach wie möglich zu machen, ist in Abbildung 13.5 der ältere Registrierungseditor *Reedit.exe* dargestellt.

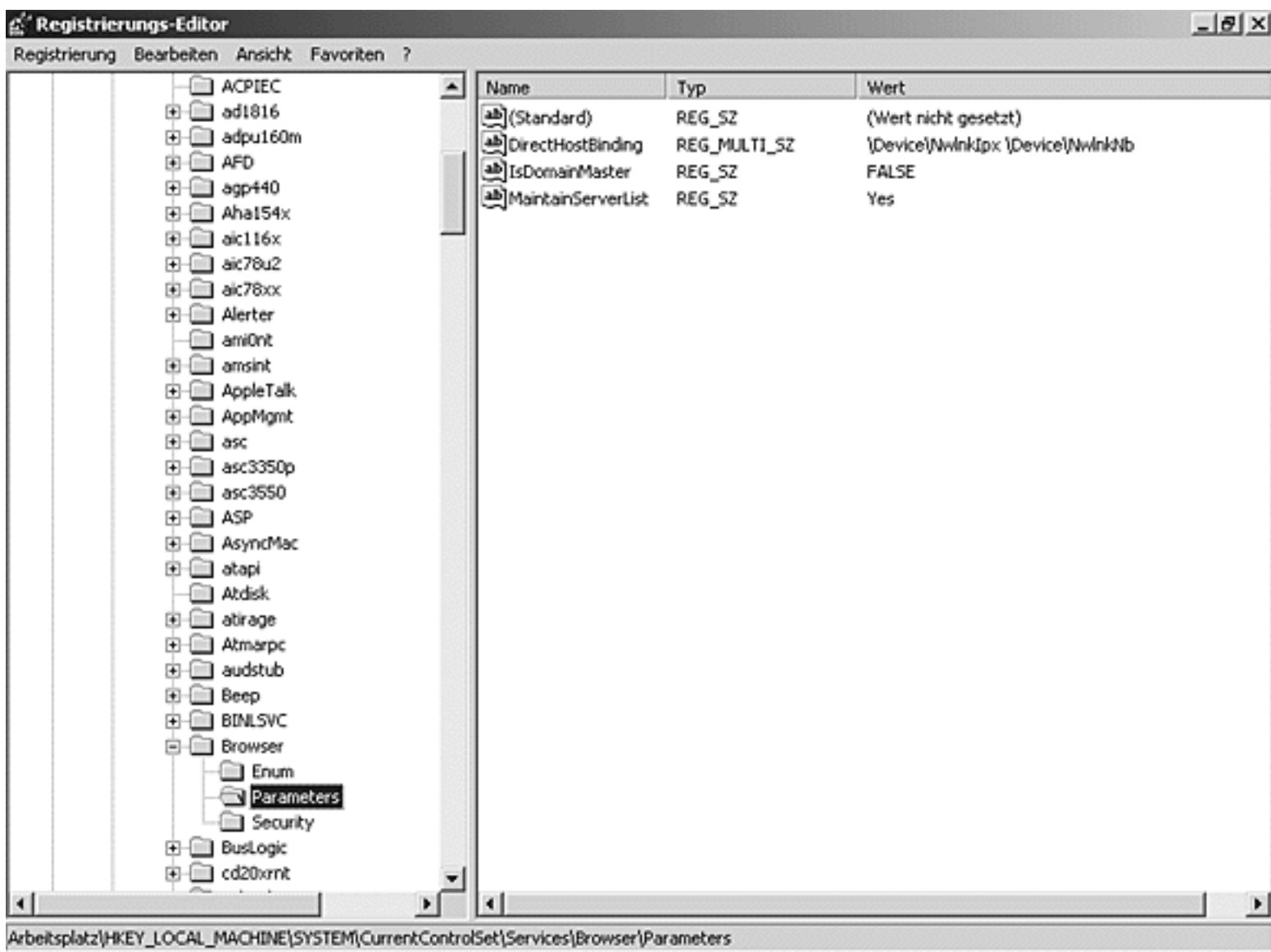


Abbildung 13.5: Der Registrierungseditor von Windows 2000

Bei Windows 2000 gibt es nach wie vor wie auch bei Windows NT Server 4.0 zwei unterschiedliche Versionen des Registrierungseditors. Mit dem Befehl `Regedit.exe` rufen Sie die ältere Version des Registrierungseditors auf, die Sie bestimmt von Windows NT her gut kennen. Dieser Editor besteht aus einem einzelnen großen Fenster, das Sie nach oben und nach unten verschieben können, um den Inhalt aller fünf Zweige der Registrierung anzuzeigen, zu bearbeiten oder zu löschen.

Mit dem Befehl `Regedt32.exe` rufen Sie die 32-Bit-Version des Registrierungseditors auf. Hier werden die fünf Zweige der Registrierung in übereinander liegenden Fenstern dargestellt, wobei in jedem Fenster ein Zweig der Registrierung angezeigt wird. Das Gute an dieser Version ist, dass Sie die Windows 2000-Registrierung in einem schreibgeschützten Modus öffnen können. Damit wird verhindert, dass Sie Einträge versehentlich löschen, was dazu führen kann, dass Ihr gesamtes System abstürzt. Der Nachteil dieser Version ist der, dass Microsoft »vergessen« hat, die vollständige Suchfunktion zu implementieren. Diese finden Sie nur in der älteren *Regedit.exe*-Version des Windows 2000-Registrierungseditors.

Wenn Sie den Registrierungseditor geöffnet haben, klicken Sie (wie in diesem Beispiel) unter *HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Parameters* auf den Ordner *Parameters*, um diesen zu markieren. Sehen Sie sich nun den Parameternamen *MaintainServerList* an. Hier sind aller Wahrscheinlichkeit nach als Typ *REG_SZ* und als Wert *Yes* angegeben. Um diesen Computer vor der Suchliste zu verbergen, müssen Sie diesen Datenwert einfach in *No* umändern. Klicken Sie dazu mit der rechten Maustaste auf den Parameternamen *MaintainServerList*. Daraufhin erscheint ein Dropdown-Menü. Klicken Sie in diesem Menü auf die obere Option **Ändern**. Daraufhin erscheint das Dialogfeld **Zeichenfolge bearbeiten** (siehe Abbildung 13.6).



Abbildung 13.6: Ändern eines Registrierungsparameters

Geben Sie im Feld **Wert** *No* ein und klicken Sie dann auf **OK**, um Ihre Änderung in der Registrierung zu speichern. Beachten Sie, dass es die Funktion **Rückgängig** hier nicht gibt. Wenn Sie eine Änderung in der Registrierung vorgenommen haben, ist diese von Dauer. Es ist daher ratsam, dass Sie eine Sicherungskopie erstellen, bevor Sie Änderungen an der Registrierung vornehmen, nur für den Fall, dass etwas schief geht.

Ein weiterer Parameter, den Sie vielleicht kennen sollten, ist der Suchparameter *IsDomainMaster*. Wenn Sie diesen Eintrag in *True* ändern, wird dieser Windows 2000-Server ein bevorzugter Hauptsuchdienst. Das bedeutet, dass dieser Server automatisch eine Suchdienstwahl erzwingt, sobald Sie ihn in einem Subnetz des Netzwerks starten. Und da dieser Server ein bevorzugter Hauptsuchdienst ist, wird er die Suchdienstwahl aller Wahrscheinlichkeit nach auch gewinnen, da ein Computer mit dieser Ernennung bei jeder Suchdienstwahl Priorität gegenüber anderen Computersystemen hat.

13.2.7 Überlegungen zum Suchdienst im Hinblick auf das Active Directory

Mit der neuen Windows 2000-Technologie, unter der Bezeichnung Active Directory bekannt, ändert sich alles, was Sie über die Funktionsweise, das Verwalten und die Verwendung von Suchdiensten in der Netzwerkumgebung einer Organisation wissen. Active Directory ist ein Verzeichnisdienst, der lose auf dem X.500-Verzeichnisdienst sowie auf dem LDAP-Protokoll (Lightweight Directory Access Protocol) beruht und die Grundlage für sämtliche ernsthaften Netzwerkaktivitäten in der Welt der Windows 2000-Computersysteme darstellt. Sie können sich das Active Directory als eine Informationsquelle vorstellen, die verwendet wird, um Informationen über wichtige Objekte zu speichern. Ihr persönliches Adressbuch ist beispielsweise ein Verzeichnis, in dem Informationen über Freunde, deren Adressen, Telefonnummern, E-Mail-Adressen u.ä. gespeichert werden. Ihre Organisation kann das Active

Directory von Windows 2000 verwenden, um Informationen dieser Art und mehr zu speichern und dann die vielen Vorteile und Tools zu nutzen, mit der Microsoft die Active Directory-Technologie ausgestattet hat.

Das Durchsuchen des Active Directory von Windows 2000 ist aus Sicht des Systemadministrators weitaus schwieriger zu kontrollieren und zu konfigurieren, jedoch aus der Sicht des Benutzers einfacher zu handhaben. Einer der Gründe für den höheren Grad an Komplexität ist die bloße Anzahl an Diensten, die für die unterschiedlichen Funktionen des Active Directory, von dem nur ein kleiner Teil für den Suchvorgang verwendet wird, eingesetzt werden muss. So ist beispielsweise ein Index erforderlich, damit das Unternehmensverzeichnis der Active Directory-Technologie richtig funktioniert. Dieser Index, als *globaler Katalog* für eine Windows 2000-Netzwerkumgebung bekannt, besteht aus einem Teilreplikat sämtlicher Objekte in der Active Directory-Datenbank. Wenn Sie die Netzwerkumgebung (sowohl **Benachbarten Computer** als auch **Gesamtes Netzwerk**) von Windows 2000 durchsuchen, durchsuchen Sie eigentlich einen Teil des Active Directory. Diese Suchvorgänge sowie die Domänenanmeldungen basieren auf den im globalen Katalog enthaltenen Objekten.

Der andere größere Bereich, bei dem sich in Bezug auf das Durchsuchen etwas getan hat, ist der gesamte Bereich dessen, was eine *Domäne* ist. In der Welt von Windows NT war die Domäne das Herz des Netzwerks. Hier wurden sämtliche Anmeldeinformationen gespeichert und die Benutzergemeinde sowie die im Windows NT-Netzwerk verfügbaren Ressourcen kontrolliert. Bei Windows 2000 Server gelangten Domänen und Domänencontroller zu einer völlig neuen Bedeutung. Wie Sie sich vielleicht noch an Kapitel 1 erinnern können, gibt es keine primären Domänencontroller und Sicherungsdomänencontroller mehr. Diese wurden einfach durch *Domänencontroller* (DCs) ersetzt. Um das Ganze noch etwas komplizierter zu machen, gibt es noch einen Domänencontroller, der als *PDC-Emulator* bezeichnet wird, und der von Windows 2000-Servern in einer Umgebung im gemischten Modus (d.h. in einer Umgebung, in der noch ältere Windows NT 4.0-Sicherungsdomänencontrollern verwendet werden) verwendet wird. Der PDC-Emulator verschwindet erst dann, wenn alle Domänencontroller in den LANs bzw. WANs der Organisation zu Windows 2000-Domänencontrollern migriert worden sind.

Um das Ganze also etwas einfacher zu machen, können Sie sich die Windows 2000-Domäne als eine einzelne Sicherheitsgrenze der Windows 2000-Netzwerkumgebung und das Active Directory als eine Ansammlung von einer oder mehreren Domänen vorstellen. Nun wissen Sie ja, dass eine Domäne aus nur einem einzelnen Computer (was das Durchsuchen sehr einfach macht) oder aus mehreren physikalischen Standorten (siehe Abbildung 13.4 und stellen Sie sich vor, alle vier Städte wären zu einer einzigen Windows 2000 Server-Domäne zusammengefasst) bestehen kann. Es ist beim Einsatz von Active Directory sehr wahrscheinlich, dass viele Domänen über Vertrauensstellungen miteinander verbunden sind, die viele Ressourcen, darunter auch den globalen Katalog, gemeinsam nutzen. Ist eine Domäne in dieser Art aufgebaut, spricht man von einer *Domänenstruktur*. Viele miteinander verbundene Domänenstrukturen bilden die *Gesamtstruktur* der Domäne. Verwirrt? Machen Sie sich keine Sorgen. Der Knoten wird auch bei Ihnen irgendwann platzen. (Lesen Sie doch einfach in Teil III nach, wenn Sie sich nicht mehr an all die Unterschiede und Bedeutungen dieser Begriffe erinnern können.)

Kapitel 14 Remotezugriff - RAS

14.1 Routing und RAS verstehen

Microsoft hat beim neuen Betriebssystem Windows 2000 Server die RAS- und DFÜ-Fähigkeiten, die es bei Windows NT 3.5x und 4.0 Server zum ersten Mal gab, aktualisiert und erheblich verbessert. In dieser aktualisierten Welt von Windows 2000 hat sich die Terminologie nur wenig, die Schnittstelle jedoch deutlich verändert. Um diese Technologie zu nutzen, rufen Sie **Routing und RAS** über die Menüoption **Verwaltung** auf. Routing und RAS bietet nicht nur Multiprotokollrouting-, Remote-Zugriff- und VPN-Funktionalität, sondern macht darüber hinaus auch das Hinzufügen, Entfernen, Überwachen und Verwalten von RAS-Benutzern so leicht wie nie zuvor. Sie werden im Laufe dieses Kapitels die vielen Änderungen zu schätzen lernen, die Microsoft an seinem neuesten, für die größten Organisationen entwickelten Betriebssystem vorgenommen hat.

In Tabelle 14.1 sind die wichtigsten Eigenschaften des Routing- und RAS-Dienstes von Windows 2000 Server aufgeführt.

Windows 2000 Server-Funktion	Beschreibung
Integration in die Active Directory-Struktur von Windows 2000	Attribute von RAS-Benutzern können direkt in der Datenbank des Active Directory gespeichert werden, wodurch das Suchen nach Informationen einfacher wird.
Microsoft CHAP 2.0	Diese neue Version des CHAP-Protokolls (Challenge Handshake Authentication Protocol) wurde speziell dafür entwickelt, VPN-Verbindungen (Virtual Private Network) sicherer als bisher zu machen.
EAP-Protokoll (Extensible Authentication Protocol)	Das EAP-Protokoll dient dazu, Nicht-Microsoft-Anbietern das Erstellen von Windows 2000-RAS-Plugins für PPP-Implementierungen (Point-to-Point-Protocol) zu ermöglichen. Das ist für Organisationen ganz praktisch, die Smartcards in ihren IT-Strukturen einsetzen möchten.
L2TP-Protokoll (Layer 2 Tunneling Protocol)	Mit Hilfe des L2TP-Protokolls können Organisationen die neue Funktion IPsec (IP Security) von Windows 2000 besser nutzen und so ein höheres Maß an Routing- und RAS-Sicherheit bieten.

Unterstützung für IP-Multicast

Nun ist das Weiterleiten von IP-Multicastverkehr zwischen Clients und dem Internet oder einem Unternehmensnetzwerk möglich. Darüber hinaus unterstützt IP-Multicast von Windows 2000 Server die zweite Version des IGMP-Protokolls (Internet Group Management Protocol).

Tabelle 14.1: Bedeutende Verbesserungen des Routing- und RAS-Dienstes bei Windows 2000 Server

14.2 Protokollunterstützung

Routing und RAS von Windows 2000 Server bietet viele neue Facetten des Routing- und RAS-Zugriffs, die es bei den bisherigen Versionen von Windows NT nicht gab. So ist es nun beispielsweise möglich, mit Windows 2000 Server ein echtes virtuelles privates Netzwerk (VPN) einzurichten, während in der Vergangenheit Add-On-Tools und -Utilities (teilweise von Drittanbietern) verwendet werden mussten, um eine sichere Verbindung über ein virtuelles privates Netzwerk für Windows NT einzurichten. Systemadministratoren, die sich mit Routingprotokollen und Routingdiensten wie TCP/IP (Transmission Control Protocol/Internet Protocol), IPX (Internetwork Packet Exchange) und AppleTalk auskennen, können Windows 2000 Server-Routing genau für diese Dienste nutzen. Jedes dieser Protokolle wird in diesem Kapitel etwas ausführlicher beschrieben, damit Sie selbst entscheiden können, welches Protokoll unter welchen Umständen verwendet werden kann und sollte.

14.2.1 TCP/IP

TCP/IP ist nicht nur für Windows 2000 Server, sondern auch für das Internet das wichtigste Netzwerkprotokoll. TCP/IP war nicht von Anfang an das Netzwerkprotokoll, das sich Microsoft für die Windows NT-Familie ausgesucht hat, als Windows NT 1993 auf den Markt kam (Microsoft hat sich damals für NetBEUI entschieden). Aber dieses Protokoll hat seit damals eine weite Wegstrecke hinter sich gebracht. TCP/IP besteht eigentlich aus einer Reihe von Protokollen und ist das Netzwerkprotokoll, das standardmäßig im Betriebssystem Windows 2000 Server installiert wird.

Sowohl für LANs und WANs als auch für die Welt des RRAS bietet das TCP/IP-Protokoll eine weite Bandbreite von Windows 2000 Server-Funktionalitäten. TCP/IP ist aufgrund der Tatsache, dass es das wohl am häufigsten geroutete Protokoll ist, das durch den Einsatz von IPSec gesichert werden kann, bei Systemadministratoren so beliebt.

Die TCP/IP-Protokollsuite besteht aus vielen Protokollen, wie z.B. TCP, IP und IGMP, die in Kapitel 8 ausführlicher beschrieben werden. An dieser Stelle hier ist es jedoch recht hilfreich, etwas mehr über das IGMP-Protokoll zu erfahren. Mit Hilfe dieses Protokolls können Host-Computer in einem Netzwerk Mitglied in einer Multicastgruppe werden. Zum IGMP-Protokoll gibt es zwei Schnittstellen:

- *IGMP-Proxy*, dessen Funktion darin besteht, den Multicastverkehr aus dem Internet zu trennen und direkt an den IGMP-Router weiterzuleiten.
- *IGMP-Router*, dessen Funktion darin besteht, den Multicastverkehr an einen Client-Computer, der Mitglied der Multicastgruppe ist, weiterzuleiten.

TCP/IP-Adressen können in der Welt von Windows 2000 Server auf zwei unterschiedliche Arten aufgelöst werden: mit Hilfe von DNS (Domain Name System) oder mittels WINS (Windows Internet Name Service). Routing und RAS unterstützt beide Möglichkeiten. Die Windows 2000 Server-Version von DNS ist jedoch zu bevorzugen, da diese neue dynamische Version von DNS die Zuordnung von IP-Adressen zu einem Computernamen erleichtert.

14.2.2 AppleTalk

AppleTalk ist das Netzwerkprotokoll, das Sie implementieren müssen, um Macintosh-Clients in Ihrer Organisation zu unterstützen, die auf Ressourcen zugreifen müssen, die sich auf einem Windows 2000-Server befinden. Dieses Protokoll muss auf jedem Windows 2000-Server installiert werden, auf dem Macintosh-Benutzer Dateien speichern, auf dessen Dateien Macintosh-Benutzer zugreifen oder dessen Dateien Macintosh-Benutzer drucken möchten. Dieses Protokoll installieren Sie mit Hilfe des **Assistenten für die optionalen Windows-Netzwerkkomponenten**. Damit konfigurieren Sie Ihren Windows 2000-Server für den Einsatz von Datei- und/oder Druckdiensten für Macintosh-Computer (Näheres dazu können Sie in Kapitel 16 nachlesen). AppleTalk ist eines der vielen Protokolle, die von Routing und RAS im Rahmen der Multiprotokollfunktionalität unterstützt werden.

14.2.3 NWLink IPX/SPX/NetBIOS-kompatibles Transportprotokoll

Das NWLink IPX/SPX/NetBIOS-kompatible Transportprotokoll wird gelegentlich auch einfach nur als IPX/SPX bezeichnet. Mit Hilfe dieses Protokolls können Windows NT-, Windows 9x- und Windows 2000-Benutzer auf Ressourcen und Informationen auf Novell NetWare-Systemen zugreifen. IPX (Internetwork Packet Exchange) ist das Protokoll, das direkt auf den Novell-Netzwerken verwendet wird. Es ist ein routingfähiges Protokoll wie TCP/IP auch.

Windows 2000 Server bietet Novell-Clients insbesondere im Bereich Routing und RAS eine Vielzahl von Diensten. Wenn ein RAS-Client, der Windows 2000 ausführt, auf einen NetWare-Server zugreifen möchte, muss auf diesem Client ein NetWare-Redirector ausgeführt werden. Dieser Redirector wird als Gateway Service für NetWare bezeichnet. Der RAS-Server fungiert als IPX-Router, der die unterschiedlichen Arten von Netzwerkverkehr, darunter RIP (Routing Information Protocol), SAP (Service Advertising Protocol) und NetBIOS über IPX, zwischen dem RAS-Server und dem RAS-Client steuert.

Der RAS-Server weist RAS-Clients für die Verbindung mit einem IPX-Netzwerk immer automatisch eine IPX-Netzwerknummer zu. Diese Netzwerknummer stammt entweder aus einem Pool statischer Adressen oder wird durch den RAS-Administrator dynamisch zugewiesen. Denken Sie daran, dass das NWLink IPX/SPX/NetBIOS-kompatible Transportprotokoll auf dem RAS-Server installiert werden muss, um Remotezugriff für NetWare-Clients zur Verfügung zu stellen.

14.2.4 NetBEUI

NetBEUI war in der ersten Version von Windows NT enthalten. Es wurde für die Peer-to-Peer-Netzwerkklücke konzipiert, die mit der Windows NT-Servergruppe gefüllt werden sollte. NetBEUI ist ein sehr gutes und schnelles Netzwerkprotokoll, das sich am besten für kleine LANs und private Arbeitsgruppen eignet. Die gute Leistung, die erzielt werden kann, wenn NetBEUI als

DFÜ-Protokoll gewählt wird, sollte nicht übersehen werden. NetBEUI wurde aber dennoch für Peer-to-Peer-Verbindungen entwickelt. Das bedeutet, dass Sie für einen DFÜ-Client, der auf Daten auf einem einzelnen Server oder einer kleinen Gruppe von Servern im gleichen lokalen Netzwerk zugreifen möchte, NetBEUI verwenden sollten. Da NetBEUI nicht routingfähig ist, kann dieses Protokoll nur in Netzwerken mit Brücken, nicht jedoch in Netzwerken mit Routern verwendet werden. Das ist ein gewaltiger Nachteil für NetBEUI in der heutigen Welt der Netzwerke und des Internet.

Aus Sicht des Administrators ist NetBEUI ebenfalls ein hervorragendes Protokoll: Es erfordert neben der Auswahl eines Computernamens, der aus bis zu 15 alphanummerischen Zeichen bestehen soll, kaum Verwaltung. Damit ist NetBEUI weitaus einfacher zu konfigurieren als TCP/IP, das die Angabe einer Reihe von Segmenten, Subnetzen und anderen Einstellungen erfordert.

NetBEUI hat jedoch auch einige Nachteile: Es kann nicht geroutet werden. Das bedeutet, der Zugriff auf ein WAN ist nicht möglich. NetBEUI ist zu TCP/IP insofern nicht kompatibel, als dass es keine Datenpakete direkt von einem NetBEUI-basierten LAN ins Internet weiterleiten kann. Und NetBEUI eignet sich nicht bei einer großen Anzahl von Computern. Denn es entsteht zu viel Netzwerkverkehr, wenn das Netzwerk mehr als 50 Computer umfasst und NetBEUI verwendet wird.

14.3 Sicherheit beim Remotezugriff

Windows 2000 Server unterstützt mit seiner Implementierung von Routing und RAS die Protokolle L2TP, MS-CHAP 2.0 (Microsoft Handshake Authentication Protocol), EAP (Extensible Authentication Protocol) und Smartcards. Die Sicherheit für die Implementierung von Routing und RAS innerhalb des Betriebssystems Windows 2000 Server wurde seit der ersten Verwendung von Routing und RAS bei Windows NT Server 4.0 (einer Service Pack-Release) deutlich verbessert. Es ist nun möglich, eine sichere Verbindung über ein virtuelles privates Netzwerk ohne zusätzliche Programme von Drittanbietern (Smartcards und Geräte mit Sicherheits-IDs ausgenommen) allein mit der von Windows 2000 Server zur Verfügung gestellten Software einzurichten.

EAP eignet sich für Gruppen, in deren Organisationen Smartcards eingesetzt werden. Um die entsprechenden Einstellungen an Ihrem Computer vorzunehmen, rufen Sie im Fenster **Routing und RAS** über das Symbol **RAS-Richtlinien** das Dialogfeld **Einwählprofil bearbeiten** auf. Wie Sie dabei im Einzelnen vorgehen, wird weiter hinten in diesem Kapitel ausführlicher beschrieben.

Mit Hilfe des Protokolls L2TP (Layer 2 Tunneling Protocol) können Sie in Ihrer Organisation IPSec verwenden. L2TP bietet Ihrer Organisation ein wesentlich höheres Maß an Sicherheit für Routing- und RAS-Zugriffe. Denken Sie jedoch daran, dass die Microsoft-Implementierung von IPSec in Windows 2000 Server negative Auswirkungen auf die Netzwerkleistung haben kann. Die Leistung kann dabei um bis zu 40 % abfallen. Aus diesem Grund sollten Sie IPSec nur dann im internen LAN oder WAN Ihrer Organisation einsetzen, wenn Sie wirklich gute Gründe haben, die dafür sprechen. Darüber hinaus sollten Sie, wenn Sie L2TP als Basis Ihres virtuellen privaten Netzwerks verwenden, darauf achten, dass Sie das strengste Authentifizierungsschema anwenden, wobei bei den DFÜ-Clients MS-CHAP 2.0 verwendet wird. Vermeiden Sie jegliche Art der LAN Manager-Authentifizierung Ihrer RAS- bzw. lokalen Benutzer.

Nachdem Sie Routing und RAS installiert haben, sollten Sie diesen Dienst so konfigurieren, dass Richtlinien für die Daten- und Netzwerkverschlüsselung implementiert und erzwungen werden.

Zusätzlich sollten Sie die unterschiedlichen Anmeldefunktionen aktivieren, sodass Sie die Verwendung des Routing- und RAS-Dienstes in Ihrer Organisation und deren komplexe Netzwerkstrukturen und Server entsprechend überwachen können. Denken Sie daran, dass RAS nur die üblichen verfügbaren Windows 2000 Server-Benutzerkonten nutzt. Versuchen Sie also gar nicht erst, die Einstellungen zu ändern.

Um eine RAS-Verbindung zu einem RAS-Server herzustellen und Daten an den RAS-Server zu senden bzw. von diesem Daten zu empfangen, muss ein RAS-Client eine Reihe von Schritten durchlaufen. Der RAS-Client greift auf den RAS-Server über eine analoge oder digitale Verbindung, über eine Einwähl- oder eine Standleitung zu. Wenn die Verbindung hergestellt ist, sendet der RAS-Server eine Herausforderung an den RAS-Client. Dieser antwortet dem Server mit einer verschlüsselten Antwort, die den Benutzernamen, den Domännennamen und das Benutzerkennwort enthält. Der RAS-Server vergleicht dann die Antwort des RAS-Clients mit der Benutzerkontendatenbank oder der Windows 2000 Active Directory-Struktur um festzustellen, ob die Antwort gültig ist. Wenn die Antwort gültig ist, legt der RAS-Server fest, welche RAS-Richtlinien für dieses Benutzerkonto gelten sollen und wendet diese entsprechend an. Wenn ein Rückruf erforderlich ist, initiiert der RAS-Server diesen, bevor er den Aushandlungsprozess für die Verbindung abschließt.

Wenn die Verbindung vom RAS-Server zum RAS-Client hergestellt ist, verfügt der RAS-Benutzer nur über die Rechte, die er auch hätte, wenn er nicht kilometerweit vom Server weg wäre, sondern sich direkt neben dem Server befände. Der RAS-Client muss nach der Anmeldung am Windows 2000-Server in einem gesonderten Schritt authentifiziert werden, um auf eine lokale Ressource zugreifen oder auch nur Verkehr im Netzwerk der Organisation erzeugen zu können. Die gesamten Authentifizierungs- und Berechtigungsprozesse können vom Windows 2000-RAS-Server vollständig verschlüsselt werden. Es ist wichtig, dass sämtlicher Daten- und Netzwerkverkehr, der der Außenwelt ausgesetzt wird (wenn beispielsweise Daten über das Internet übertragen werden), durch den Einsatz von RAS-Richtlinien und mit Hilfe der Möglichkeiten zur Verschlüsselung, die in Windows 2000 Server zur Verfügung stehen, privat gehalten wird.

14.4 Installieren von Routing und RAS

Die Installation von Routing und RAS ist relativ einfach. Wenn Sie Windows 2000 Server installieren, wird der Routing- und RAS-Dienst als Teil der normalen Windows 2000-Installationsroutine automatisch installiert. Etwas, das vielleicht nicht gleich offensichtlich ist, ist die Tatsache, dass der Dienst in einem deaktivierten Modus installiert wird. Das bedeutet, dass Sie diesen Dienst zuerst aktivieren und dann konfigurieren müssen, um ihn überhaupt nutzen zu können. Das ist eigentlich der einfache Teil, vorausgesetzt, Sie können das Konfigurationsfenster der Verwaltungskonsolle von Microsoft (MMC = Microsoft Management Console) über die Menüoption **Routing und RAS** aufrufen.

Um festzustellen, ob die Menüoption **Routing und RAS** verfügbar ist, klicken Sie auf die Schaltfläche **Start**, dann auf **Programme** und anschließend auf **Verwaltung**. Suchen Sie in dem nun erscheinenden Dropdown-Menü das Bild eines kleinen Computers mit zwei Netzkabeln und der Bezeichnung **Routing und RAS**.

Wenn die Menüoption **Routing und RAS** auf Ihrem Bildschirm nicht erscheint, haben Sie natürlich ein kleines Problem. Das bedeutet, dass Sie, obwohl der Dienst bereits auf Ihrem Server installiert ist, keine

Administratorrechte für die Verwendung oder Konfiguration dieses Dienstes haben. Diese Rechte haben Sie nur, wenn Sie sich am Windows 2000-Server als Mitglied der Gruppe der Administratoren angemeldet haben. Wenn Sie bei dem Windows 2000-Server, an dem Sie arbeiten, nicht über diese Rechte verfügen, dann setzen Sie sich mit Ihrem Netzwerkadministrator in Verbindung, damit er Ihnen diese Rechte zuweist, sodass Sie den Routing- und RAS-Dienst konfigurieren können.

Nachdem Sie den Software-Teil der Konfiguration abgeschlossen haben, müssen Sie dafür sorgen, dass Ihr Windows 2000-Server den Hardware-Anforderungen für die Unterstützung von Routing und RAS entspricht. Sie benötigen mindestens eine analoge Telefonleitung wie z.B. eine offene Faxleitung oder eine Direktleitung (achten Sie darauf, dass Sie nicht eines der vielen über die Hauptschalttafel angeschlossenen Telefone Ihres Unternehmens verwenden, das funktioniert nämlich nicht). Vielleicht möchten Sie aber auch besser eine digitale Leitung wie z.B. eine ISDN- (Integrated Services Digital Network) oder eine T1-Datenleitung verwenden. Darüber hinaus benötigen Sie einen COM-Anschluss (ein Multiportadapter eignet sich hierfür hervorragend) und einen möglichst NDIS-fähigen (Network Driver Interface Specification) Netzwerkadapter für bessere Netzwerkverbindungen. Es gibt buchstäblich Hunderte von unterschiedlichen Kombinationen von Hardware-Komponenten, die zusammen mit Windows 2000 Server verwendet werden können. Es ist daher am besten, wenn Sie anhand der Microsoft Windows 2000-Hardwarekompatibilitätsliste feststellen, ob Ihre Hardware-Komponenten zum Betriebssystem Windows 2000 Server kompatibel sind. Die Hardwarekompatibilitätsliste können Sie auf unterschiedliche Art und Weise einsehen:

- Wenn Sie ein Microsoft TechNet-Abonnent sind, finden Sie die Windows 2000-Hardwarekompatibilitätsliste auf einer der CDs.
- Wenn Sie ein MSDN-Abonnent (Microsoft Developer Network) sind, finden Sie die Windows 2000-Hardwarekompatibilitätsliste auf Ihrer MSDN-CD.
- Wenn Sie ein Modem oder einen Internet-Anschluss haben, finden Sie die Windows 2000-Hardwarekompatibilitätsliste auf der Microsoft-Website (www.microsoft.com).

14.4.1 Konfigurieren des RAS-Servers

Um mit der Konfiguration von Routing und RAS zu beginnen, klicken Sie auf die Schaltfläche **Start**, dann auf die Menüoption **Programme**, anschließend auf **Verwaltung** und schließlich auf die Option **Routing und RAS**. Daraufhin erscheint das in Abbildung 14.1 dargestellte Fenster.

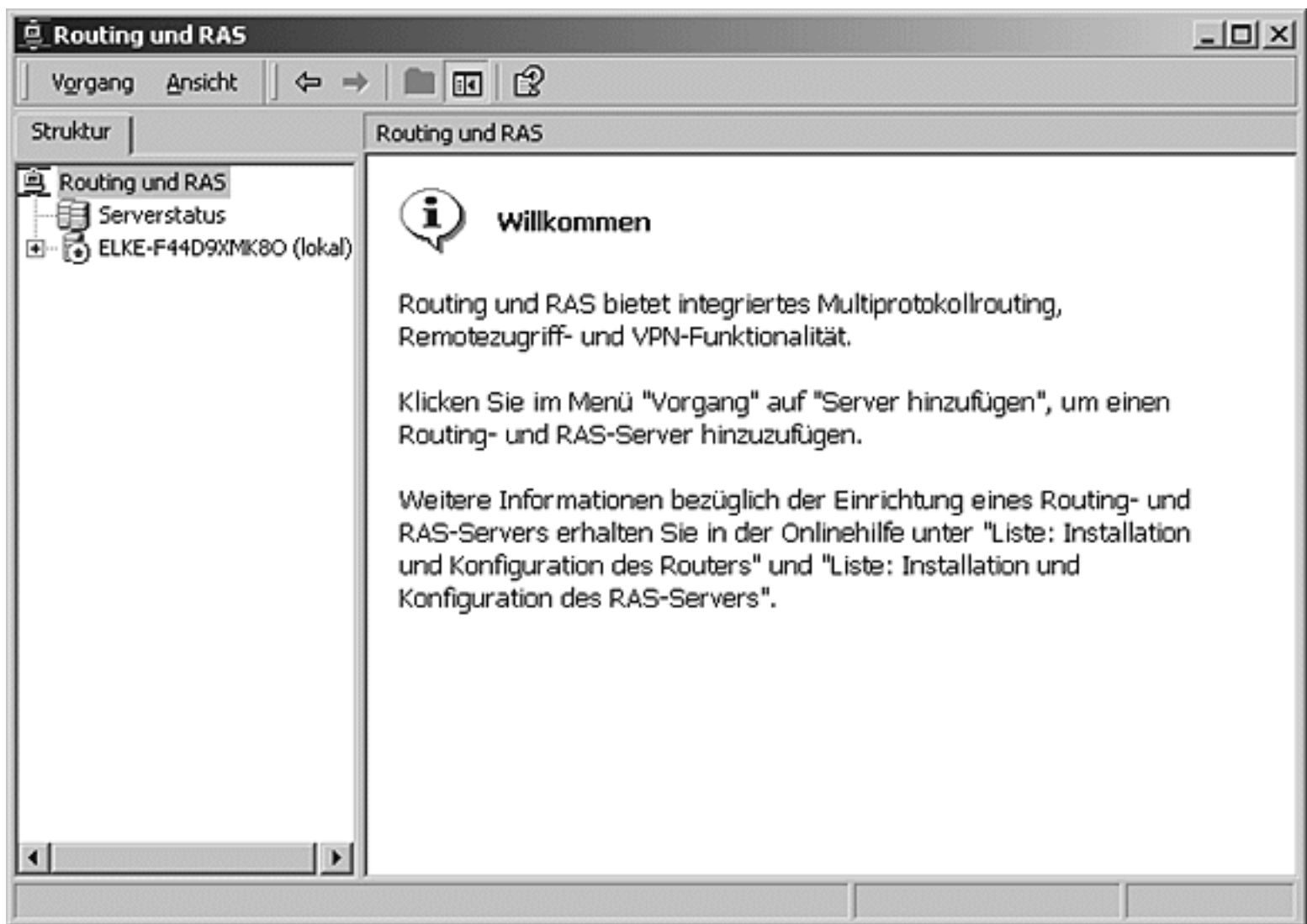


Abbildung 14.1: Das Fenster Routing und RAS

Denken Sie daran, dass Ihnen der Routing- und RAS-Dienst mehr Möglichkeiten als nur die Dienste für eine DFÜ-Verbindung zu Ihrem Windows 2000-Server bietet. Die Routing- und RAS-Dienste bieten darüber hinaus auch Routingdienste für virtuelle private Netzwerke unter Verwendung mehrerer Protokolle, LAN-zu-LAN- und LAN-zu-WAN-Verbindungen sowie Netzwerkadressübersetzung (NAT). Das bedeutet, dass Sie sich zuerst überlegen sollten, welche Art der Verbindung Sie konfigurieren möchten, bevor Sie mit der Implementierung dieser Technologie beginnen. Ansonsten kann es dazu führen, dass Sie eine sinnlose Technologie unsicher oder gar nutzlos implementieren. Was ich damit sagen möchte: Vermeiden Sie es, eine RAS-Lösung zu kompliziert zu machen. Verwenden Sie kein virtuelles privates Netzwerk für eine LAN-zu-LAN-Lösung, wenn Sie eigentlich nur eine einfache WAN-Architektur benötigen. RAS-Technologien sind in der Regel nicht so kompliziert, wie sie sich viele Leute vorstellen, die von der Sache nichts verstehen. Vermeiden Sie also unnötig komplizierte Lösungen mit Elementen, die Sie nicht wirklich verstehen.

Sehen Sie sich als Nächstes noch einmal das in Abbildung 14.1 dargestellte Fenster **Routing und RAS** an. Links in diesem Fenster sehen Sie eine Baumstruktur, in der sich das Symbol für **Routing und RAS** ganz oben befindet. Darunter sind mindestens zwei weitere Symbole zu sehen: Das eine ist mit der Bezeichnung **Serverstatus** gekennzeichnet, das andere mit dem Computernamen Ihres Servers. Neben dem mit dem Computernamen Ihres Servers bezeichneten Symbol befindet sich ein Pluszeichen. Das

bedeutet, dass sich dahinter noch mehr Informationen verbergen. Wenn Sie herausfinden möchten, welche Geheimnisse dieses Symbol für Sie bereit hält, kann klicken Sie auf dieses Pluszeichen. Der Name Ihres Computers ist nun mit einem roten Kreis gekennzeichnet. Das bedeutet, dass der Routing- und RAS-Dienst auf Ihrem Server momentan nicht gestartet ist. Um den Status zu prüfen, klicken Sie auf das Symbol **Serverstatus** direkt über dem mit dem Namen Ihres Computers bezeichneten Symbol (siehe Abbildung 14.2).

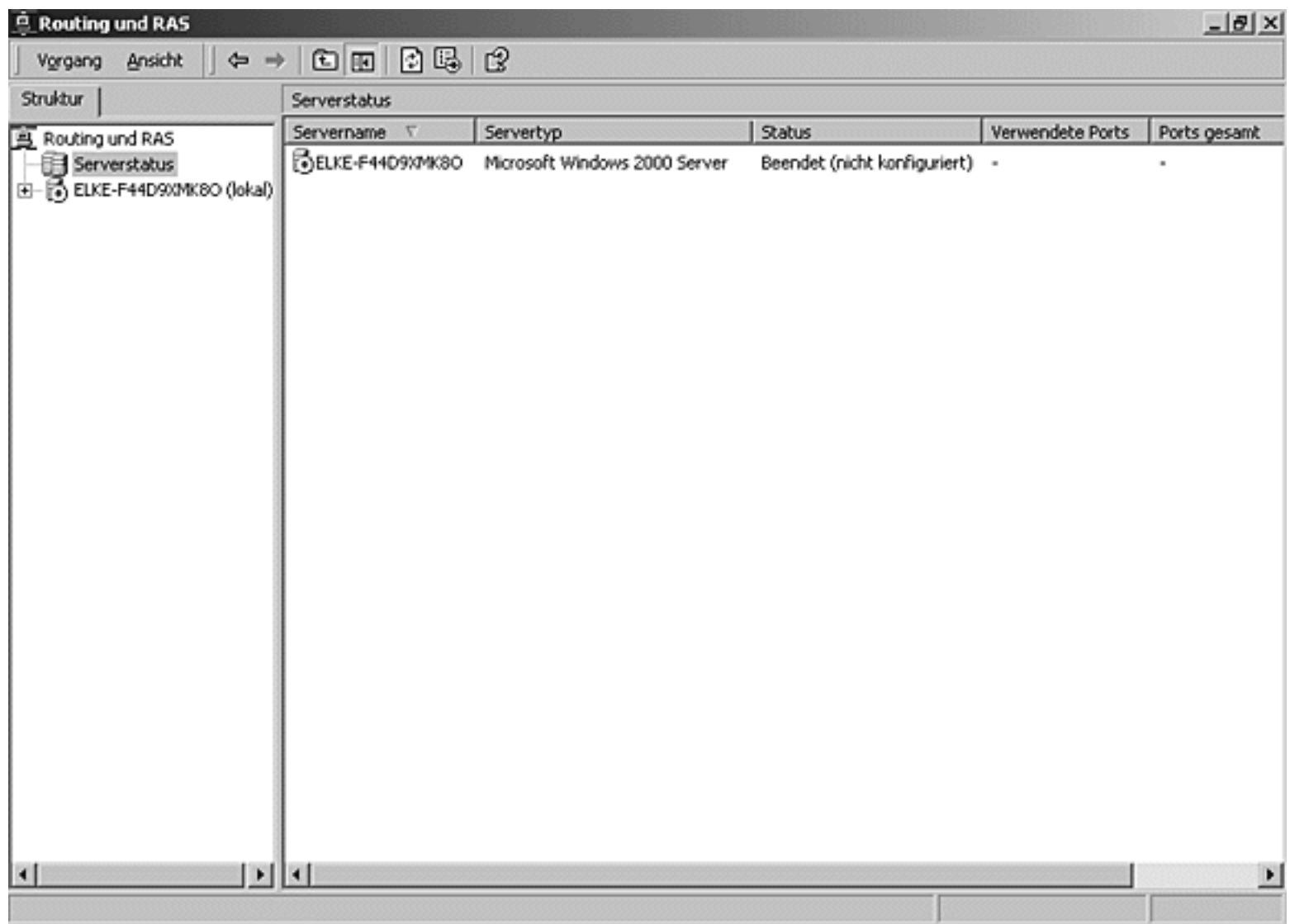


Abbildung 14.2: Prüfen Sie den Status Ihres Servers

Nun wird auf der rechten Seite des Fensters der Status Ihres Computers angezeigt. In Abbildung 14.2 können Sie beispielsweise sehen, dass der Status **Beendet (nicht konfiguriert)** angezeigt wird, d.h. der Routing- und RAS-Dienst wurde für diesen Server beendet und ist noch nicht konfiguriert. Um den Routing- und RAS-Dienst für diesen Windows 2000 Server zu konfigurieren, gehen Sie wie folgt vor:

1. Klicken Sie (entweder auf der rechten oder auf der linken Seite des Fensters) mit der rechten Maustaste auf den Namen des Servers und wählen Sie dann die Menüoption **Routing und RAS konfigurieren und aktivieren** (die Option ganz oben in dem kleinen Menü). Daraufhin öffnet sich das erste Fenster des Setup-Assistenten für den Routing- und RAS-Server (siehe Abbildung 14.3).

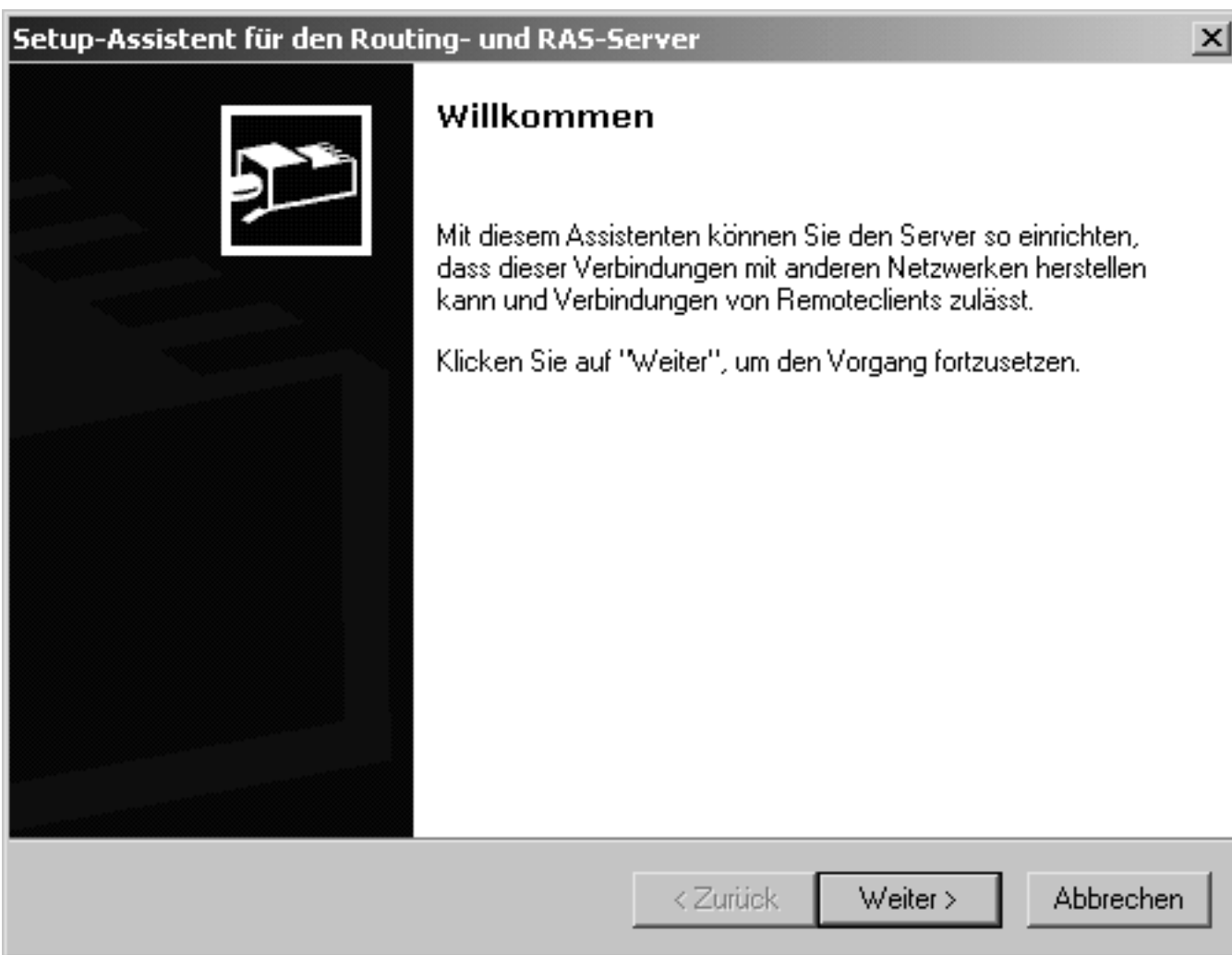


Abbildung 14.3: Willkommensfenster des Setup-Assistenten

2. Um die Konfiguration mit dem Assistenten zu beginnen, klicken Sie auf die Schaltfläche **Weiter**. Daraufhin erscheint das in Abbildung 14.4 dargestellte Fenster.



Abbildung 14.4: Aktivieren Sie Ihren Server nur für den Remotezugriff

3. In diesem Fenster des Assistenten legen Sie die Art der Konfiguration fest. Da wir in diesem Beispiel einen RAS-Server konfigurieren möchten, aktivieren Sie das Optionsfeld **RAS-Server**, um Remotecomputern das Einwählen in dieses Netzwerk zu ermöglichen. Klicken Sie anschließend auf die Schaltfläche **Weiter**, um das nächste Fenster des Assistenten aufzurufen (siehe Abbildung 14.5).

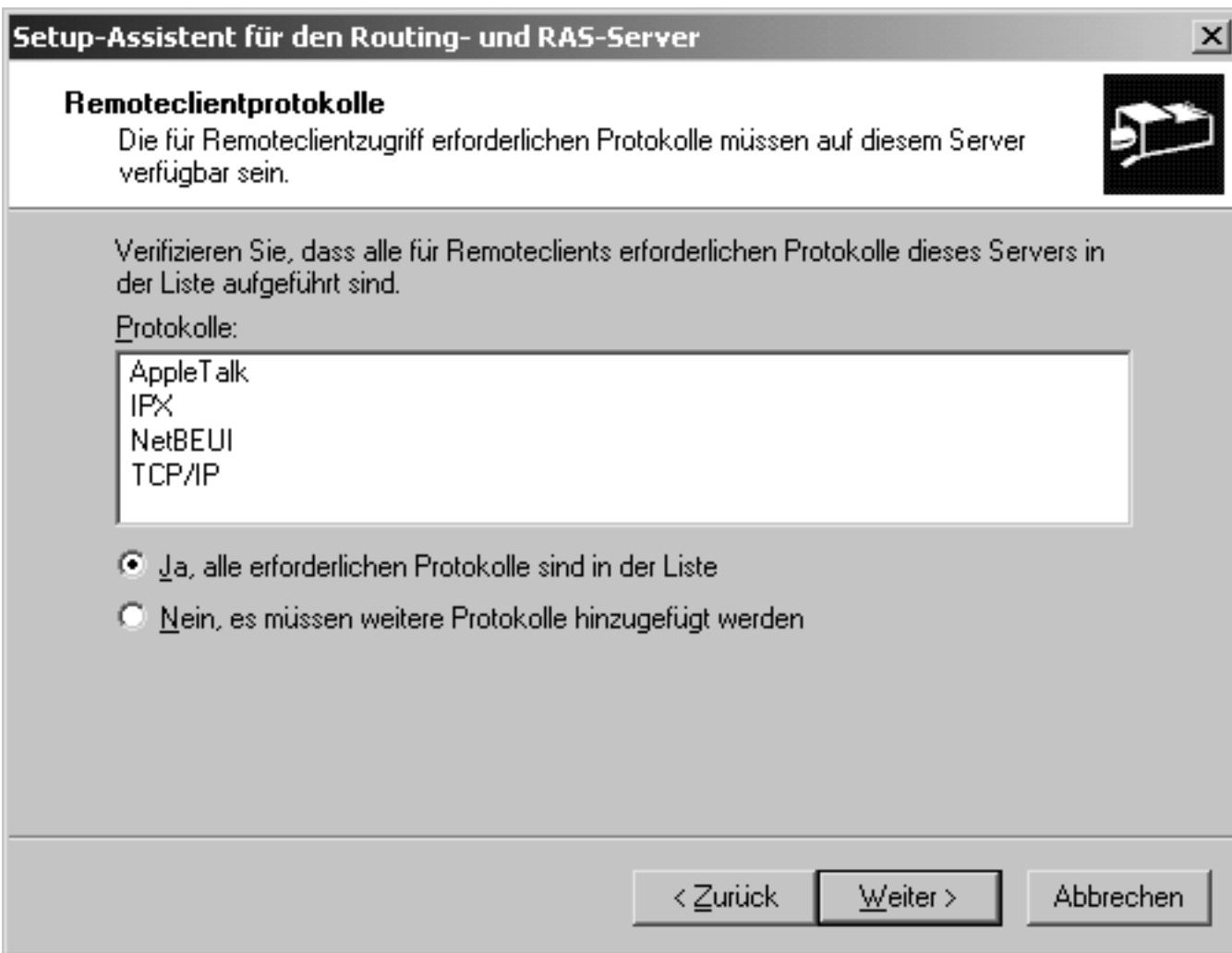


Abbildung 14.5: Prüfen, ob alle erforderlichen Protokolle vorhanden sind

4. Hier können Sie prüfen, ob alle für den Zugriff auf diesen Server erforderlichen Protokolle verfügbar sind. Wenn nicht alle erforderlichen Protokolle vorhanden sind, klicken Sie auf das Optionsfeld **Nein, es müssen weitere Protokolle hinzugefügt werden**. Wenn alle erforderlichen Protokolle vorhanden sind, klicken Sie auf das Optionsfeld **Ja, alle erforderlichen Protokolle sind in der Liste**. Klicken Sie anschließend auf die Schaltfläche **Weiter**, um zum nächsten Fenster des Assistenten zu gelangen (siehe Abbildung 14.6).

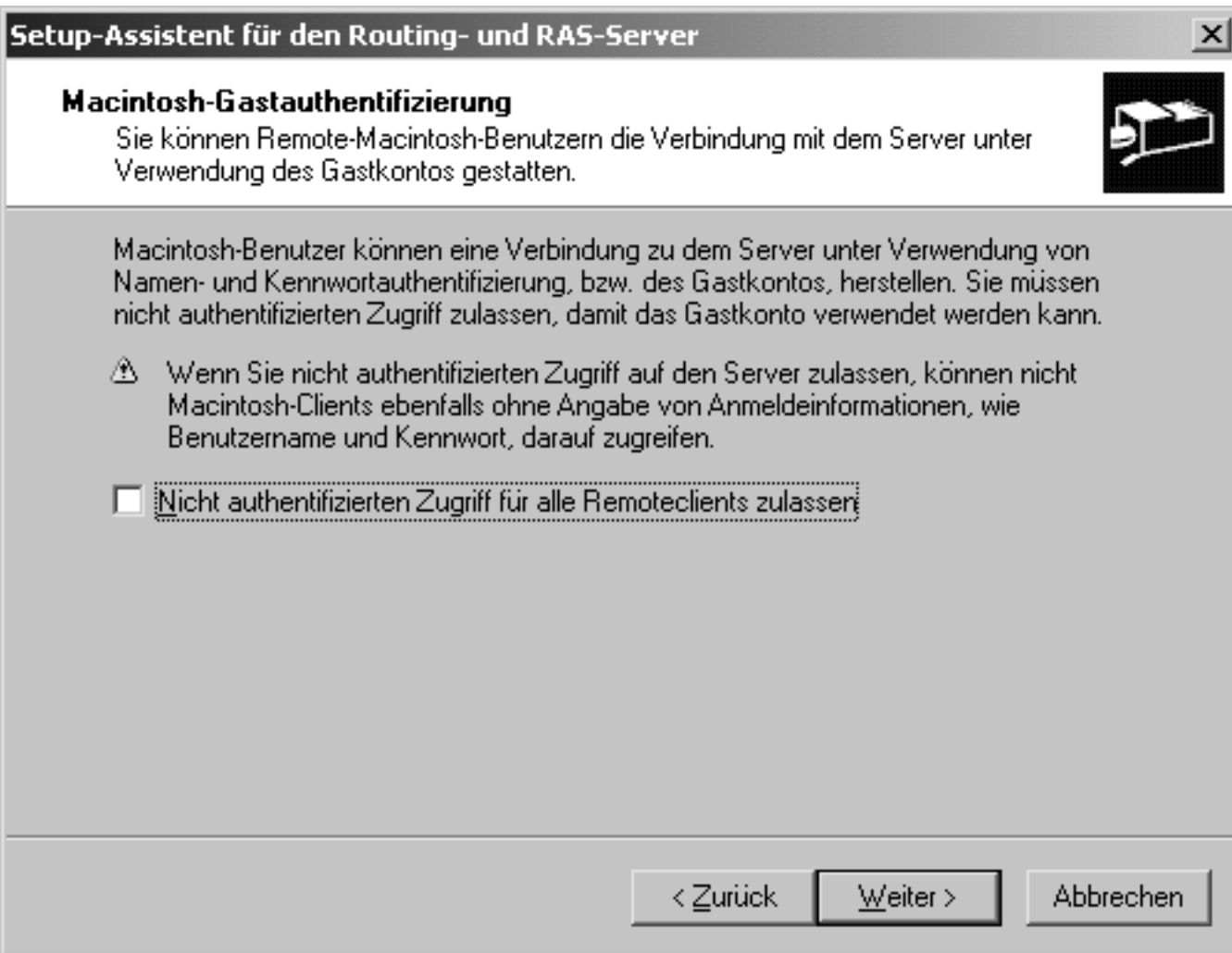


Abbildung 14.6: Einrichten eines Gastkontos für Macintosh-Benutzer

5. Hier können Sie Remote-Macintosh-Benutzern den Zugriff auf den Server ermöglichen, indem Sie für diese Benutzer ein Gastkonto einrichten. Damit das Gastkonto verwendet werden kann, müssen Sie den nicht authentifizierten Zugriff auf den Server zulassen. Um dies zu tun, aktivieren Sie das Kontrollkästchen **Nicht authentifizierten Zugriff für alle Remoteclients zulassen**. Nehmen Sie die gewünschten Einstellungen vor und klicken Sie anschließend auf die Schaltfläche **Weiter**, um das nächste Fenster des Assistenten aufzurufen (siehe Abbildung 14.7).

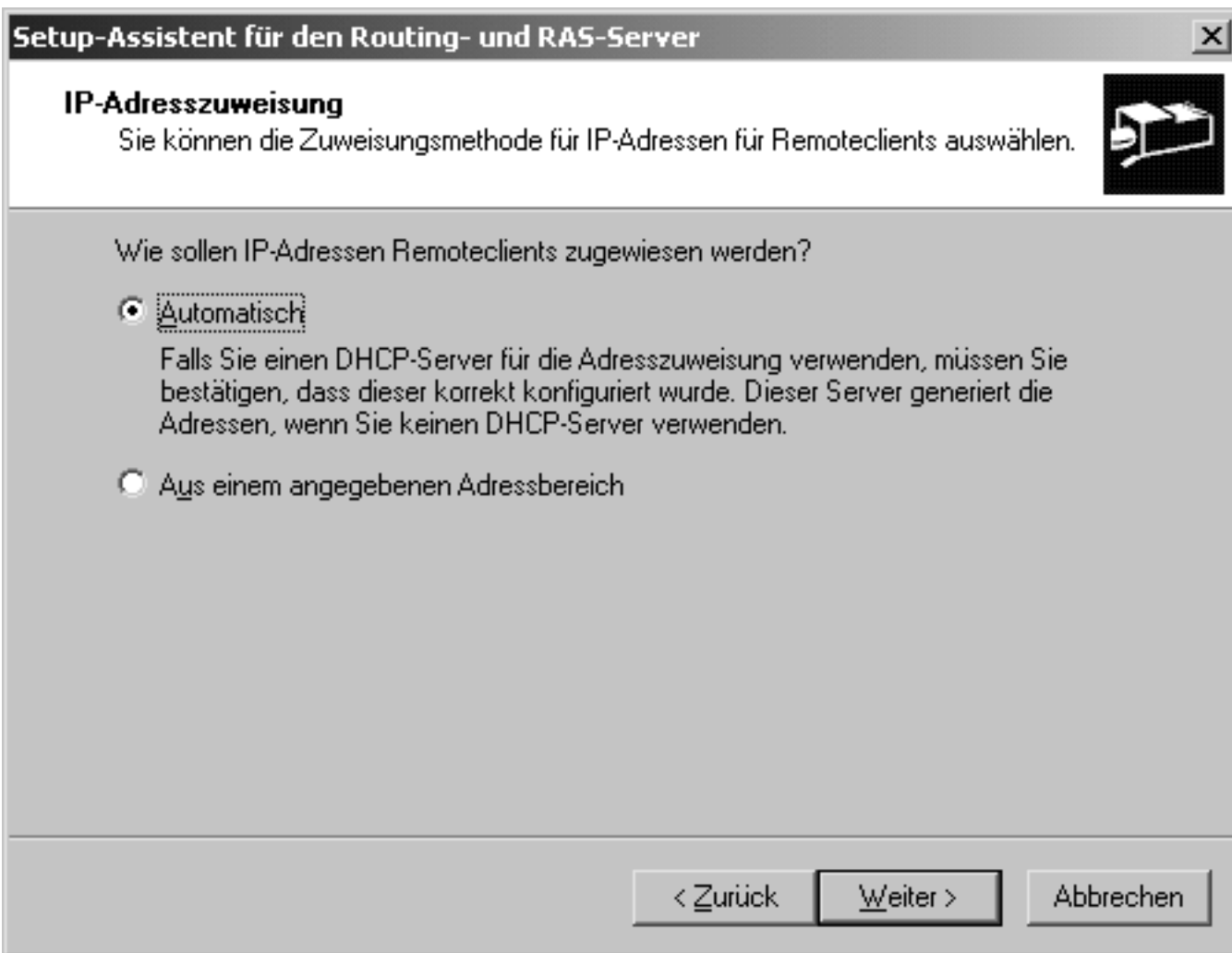


Abbildung 14.7: Auswahl der Zuweisungsmethode für IP-Adressen

6. In diesem Fenster können Sie festlegen, ob Remoteclients IP-Adressen automatisch oder aus einem angegebenen Adressbereich zugewiesen werden sollen. Nehmen Sie die gewünschten Einstellungen vor und klicken Sie anschließend auf die Schaltfläche **Weiter**, um das nächste Fenster des Assistenten aufzurufen (siehe Abbildung 14.8).

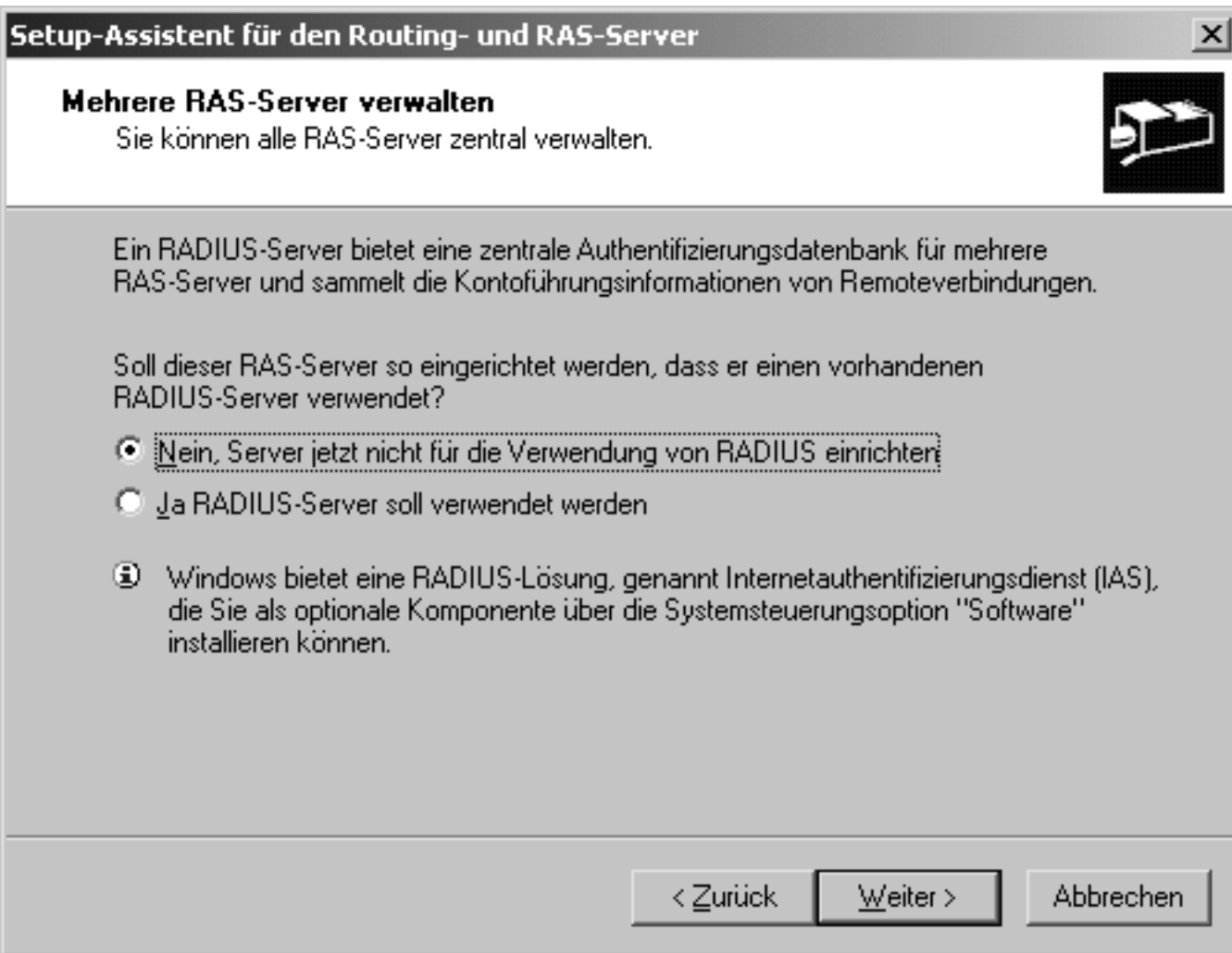


Abbildung 14.8: Verwalten mehrerer RAS-Server

7. Sie haben die Möglichkeit, alle RAS-Server von zentraler Stelle aus zu verwalten. Dazu können Sie den RAS-Server, den Sie gerade konfigurieren, so einrichten, dass er einen RADIUS-Server verwendet. Dieser bietet eine zentrale Datenbank für die Authentifizierung und sammelt Informationen über die Kontoführung von Remoteverbindungen. Nehmen Sie die gewünschten Einstellungen vor und klicken Sie anschließend auf die Schaltfläche **Weiter**, um zum letzten Fenster des Assistenten zu gelangen (siehe Abbildung 14.9).



Abbildung 14.9: Fertigstellen des Assistenten

8. Dieses Fenster zeigt an, dass der Server als RAS-Server konfiguriert worden ist. Um den Vorgang abzuschließen, klicken Sie auf die Schaltfläche **Fertig stellen**.

Abhängig von der Geschwindigkeit Ihres Windows 2000-Servers und dem verfügbaren Speicher sowie der Taktfrequenz des Prozessors kann dieser Vorgang wenige Sekunden bis hin zu einer Minute und länger dauern. Haben Sie also etwas Geduld. Wenn der Dienst startet, werden Sie im Fenster **Routing und RAS** ein Symbol mit einem grünen Pfeil in einem weißen Kreis neben dem Namen Ihres Computers bemerken.

Dieses Symbol ist ein Hinweis darauf, dass der Routing- und RAS-Dienst gestartet ist. Auf der rechten Seite des Fensters können Sie erkennen, wie viele Ports insgesamt verfügbar sind und wie viele Ports verwendet werden. In der Spalte **Status** wird nun der Status **Gestartet** angezeigt.

14.4.2 Erweiterte Konfiguration des RAS-Servers

Nun, da wir zum detaillierteren Teil der Konfiguration gelangt sind, sollen hier nun die bekannteren, im RAS-Bereich des Routing- und RAS-Dienstes zur Verfügung stehenden Optionen beschrieben werden. Im Anschluss daran soll der Routing-Bereich des Routing- und RAS-Dienstes ebenfalls erläutert werden. Dies trägt dazu bei, dass Sie besser verstehen, was notwendig ist, damit Sie mit Ihrer Windows 2000 Server-Installation RAS-Benutzer unterstützen können.

Wenn Sie sich noch einmal das Fenster **Routing und RAS** ansehen, werden Sie erkennen, dass der RAS-Dienst Ihres Computers gestartet ist und ausgeführt wird. Wenn Sie nun auf das Pluszeichen neben dem mit dem Namen Ihres Computers gekennzeichneten Symbol klicken, werden eine Reihe neuer Optionen und Einstellungen angezeigt (siehe Abbildung 14.10).

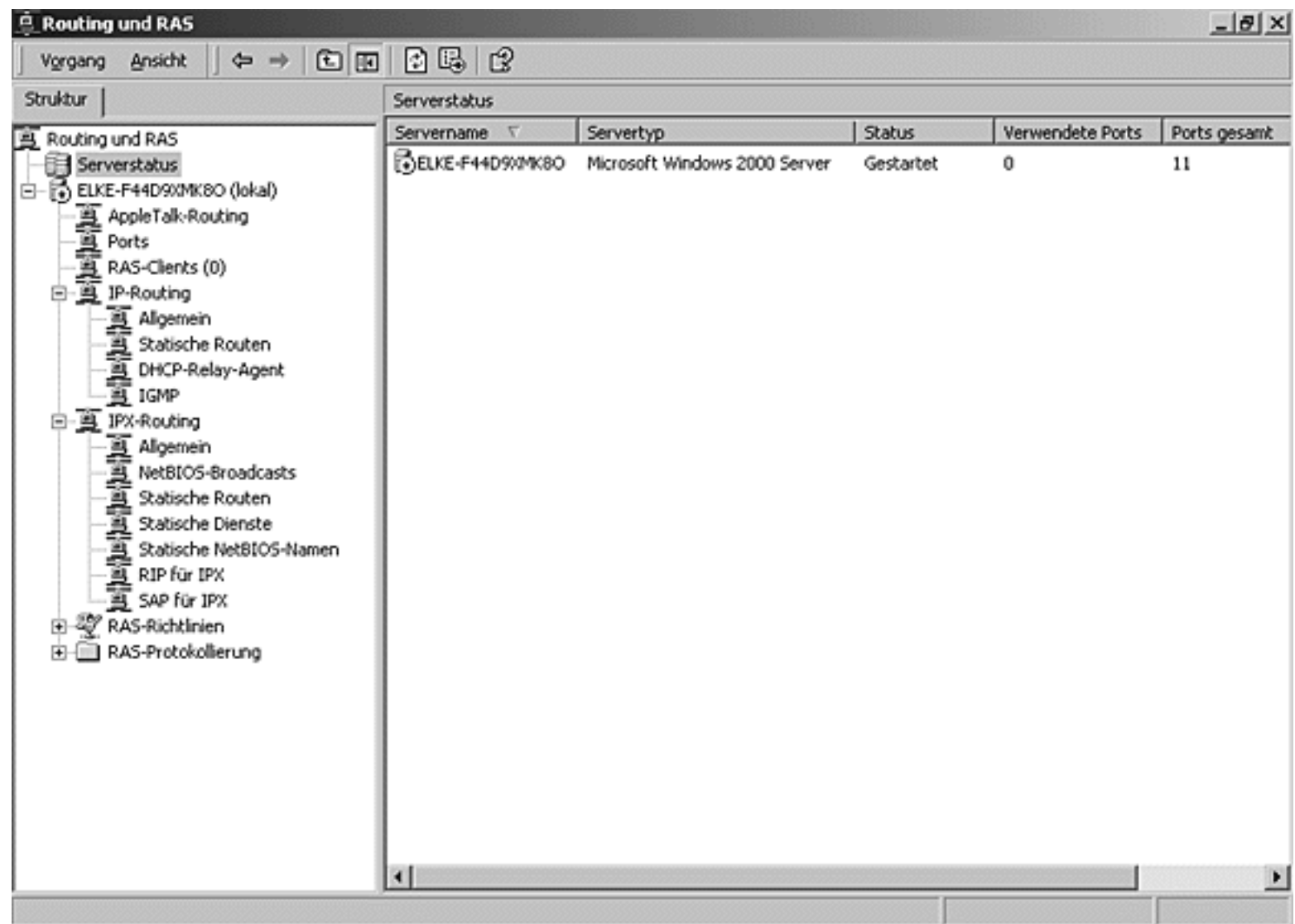


Abbildung 14.10: Anzeige der IPX- und IP-Routingmethoden

In diesem Fenster werden all die unterschiedlichen Verbindungsmöglichkeiten angezeigt, die innerhalb der Implementierung von Routing und RAS möglich sind. Dazu gehören auch die beiden Routingprotokolle IP und IPX, die wir auf diesem Beispiel-Server noch nicht konfiguriert haben. Zunächst einmal möchten wir uns jedoch auf die vier Bereiche im linken Teil des Fensters konzentrieren, die zu einer detaillierteren Konfiguration von RAS für Windows 2000 Server führen:

- RAS-Clients
- Ports
- RAS-Richtlinien
- RAS-Protokollierung

RAS-Clients

Als Erstes werden wir uns den Bereich **RAS-Clients** näher ansehen. In unserem Beispiel sind null Clients mit dem Server verbunden.



Die Zahl in Klammern neben **RAS-Clients** gibt an, wie viele RAS-Clients momentan eine Verbindung zum RAS-Server hergestellt haben. Diese Zahl ändert sich und kann theoretisch bis 256 gehen, wenn ein zusätzlicher COM-Anschluss verwendet wird.

Ein Systemadministrator wird diesen Bereich des Routing- und RAS-Dienstes verwenden, um die RAS-Clients, die momentan eine Verbindung zum RAS-Server hergestellt haben, zu überwachen. Sehr hilfreich dabei ist die Möglichkeit, dass Sie in diesem Fenster weitere Server hinzufügen und somit mehrere Server gleichzeitig überwachen können. (Das setzt natürlich voraus, dass Sie über die entsprechenden Rechte verfügen, um die Routing- und RAS-Informationen der anderen Server einzusehen.) Um einen weiteren Server hinzuzufügen, klicken Sie mit der rechten Maustaste ganz oben in der Struktur auf das Symbol **Routing und RAS**. Daraufhin erscheint ein Kontextmenü. Klicken Sie hier auf die Option **Server hinzufügen**. Nun öffnet sich das Dialogfeld **Server hinzufügen** (siehe Abbildung 14.11).

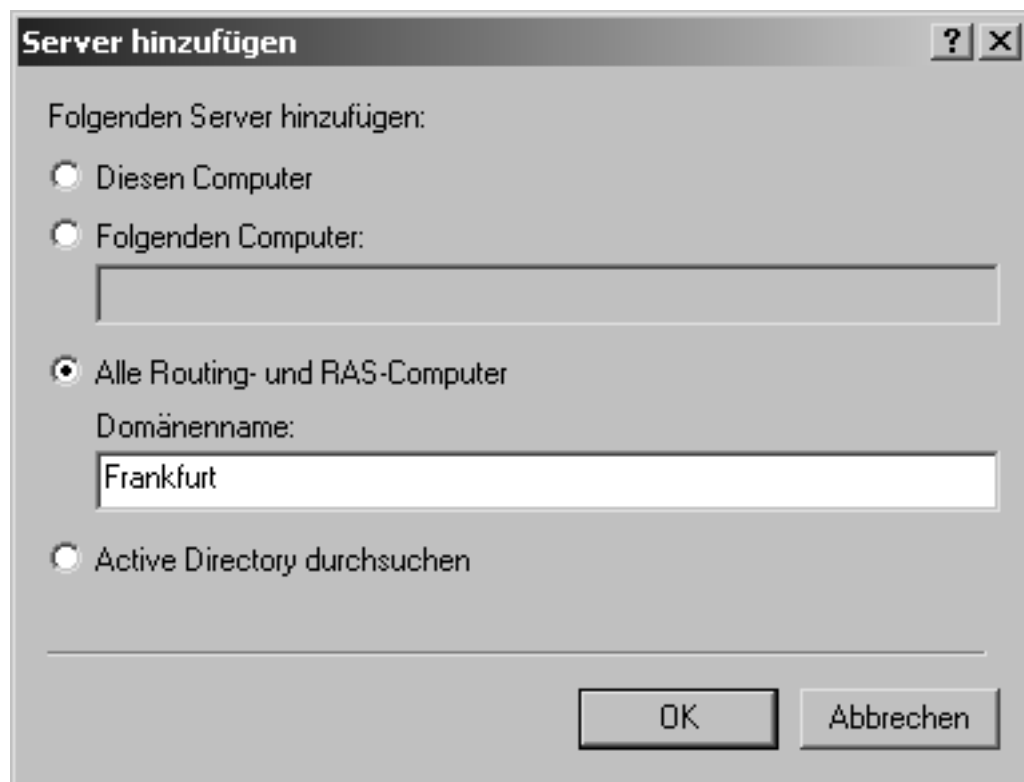


Abbildung 14.11: Das Dialogfeld Server hinzufügen

Die Optionen in diesem Dialogfeld erklären sich mit Ausnahme der unteren von selbst. Die untere Option, **Active Directory durchsuchen**, wird nur im Zusammenhang mit der Option **Alle Routing- und RAS-Computer** verwendet. Damit kann der RAS-Administrator die Active Directory-Struktur seiner Organisation durchsuchen und all die verfügbaren Routing- und RAS-Computer finden, die er überwachen kann. (Wie bereits erwähnt, kann der Routing- und RAS-Administrator ohne entsprechende Berechtigungen die verfügbare Liste noch nicht einmal aufrufen, geschweige denn einen Server überwachen.) Die oberste Option, **Diesen Computer**, bedeutet, dass damit Ihr lokaler Routing- und RAS-Server hinzugefügt wird. Wenn Sie die Option **Folgenden Computer** aktivieren, müssen Sie den

UNC-Namen (Universal Naming Convention) für den Computer eingeben, den Sie überwachen möchten, vorausgesetzt, Sie kennen den vollständigen UNC-Namen dieses Windows 2000-Servers. Nachdem Sie Ihre Wahl getroffen haben, klicken Sie auf die Schaltfläche **OK**, um zum Hauptfenster **Routing und RAS** zurückzukehren.

Ports

Als Nächstes soll die Option **Ports** erläutert werden. Allgemeine Informationen dieser Option sind in Abbildung 14.12 dargestellt.

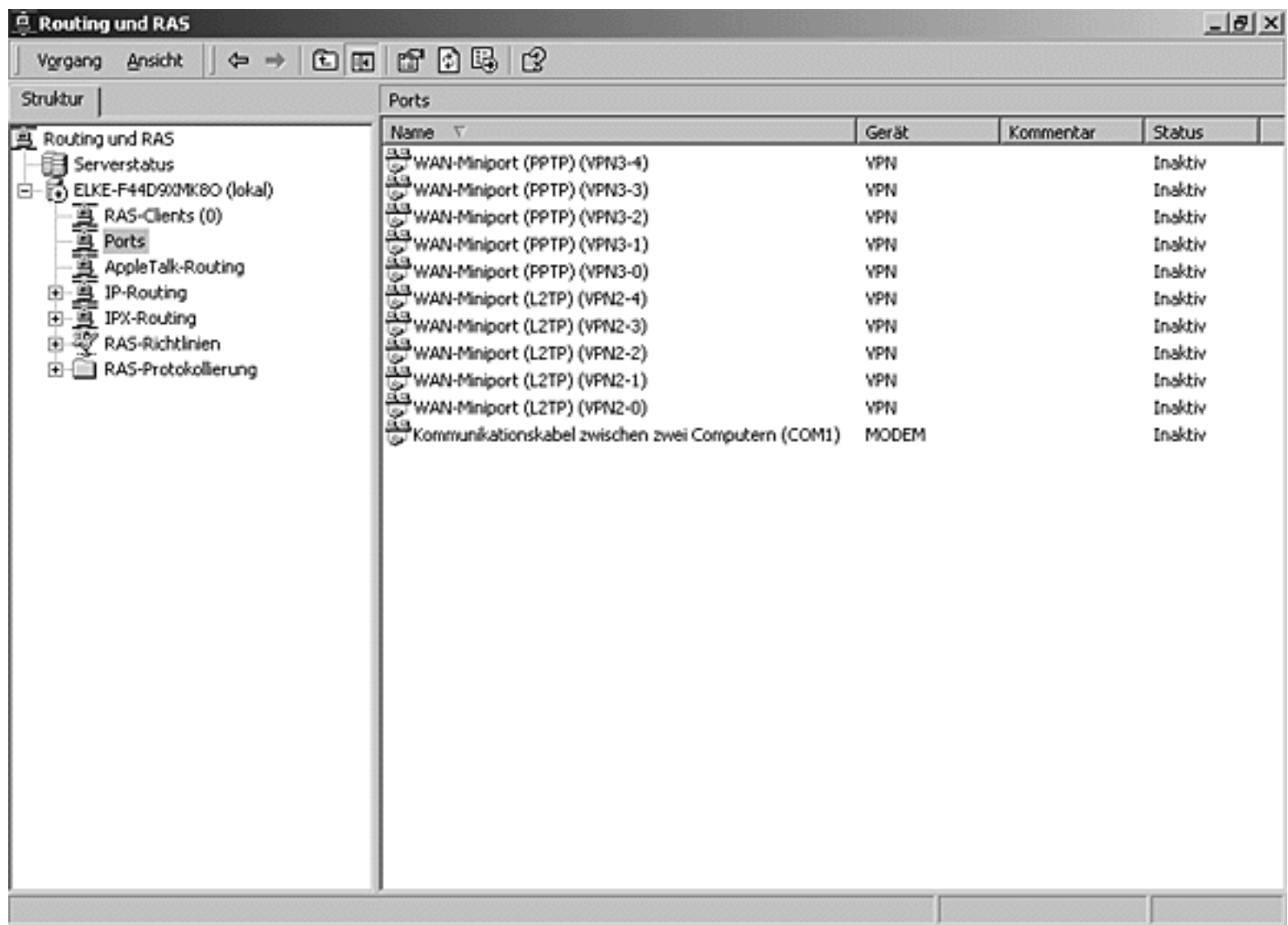


Abbildung 14.12: Verfügbare Routing- und RAS-Ports

Der Sinn und Zweck dieser Option ist offensichtlich: Es soll eine vollständige Liste aller DFÜ- und WAN-Anschlüsse angezeigt werden, die der Administrator für diesen Routing- und RAS-Server verwenden kann. Anschlüsse, die mit dem Gerätetyp VPN angezeigt sind, sind Anschlüsse, die die für ein virtuelles privates Netzwerk erforderlichen Verschlüsselungstechnologien unterstützen.

So unterstützen beispielsweise die ersten fünf WAN-Anschlüsse in Abbildung 14.12 (VPN3-4 bis VPN3-0) das Protokoll PPTP (Point-to-Point Tunneling Protocol). Die nächsten fünf in diesem Fenster aufgeführten WAN-Anschlüsse (VPN2-4 bis VPN2-0) unterstützen das Protokoll L2TP.

Das letzte Gerät (**MODEM**) in dieser Liste ist das Modem, das auf dem Windows 2000-Server in unserem Beispiel installiert ist. Modems und übrigens auch Infrarotgeräte werden üblicherweise zwar nicht für virtuelle private Netzwerke verwendet. Technisch gesehen können sie jedoch auch für diesen Zweck eingesetzt werden. Der Hauptgrund dafür, warum diese Geräte nicht für das virtuelle private Netzwerk einer Organisation verwendet werden, hat in erster Linie mit der Bandbreite zu tun. Ein Infrarotanschluss ermöglicht einen Datendurchsatz von 115 Kbit/s. Ein normales analoges Modem hat dagegen schon Probleme, 56 Kbit/s zu schaffen. Der Faktor Bandbreite reicht in der Regel schon aus, um einen Administrator vor einer VPN-Lösung seiner Sicherheitsprobleme abzuschrecken.

Wenn Sie im linken Bereich des Fensters mit der rechten Maustaste auf das Symbol **Ports** und im daraufhin erscheinenden Dropdown-Menü auf die Option **Eigenschaften** klicken, erscheint das in Abbildung 14.13 dargestellte Dialogfeld **Eigenschaften von Ports**.

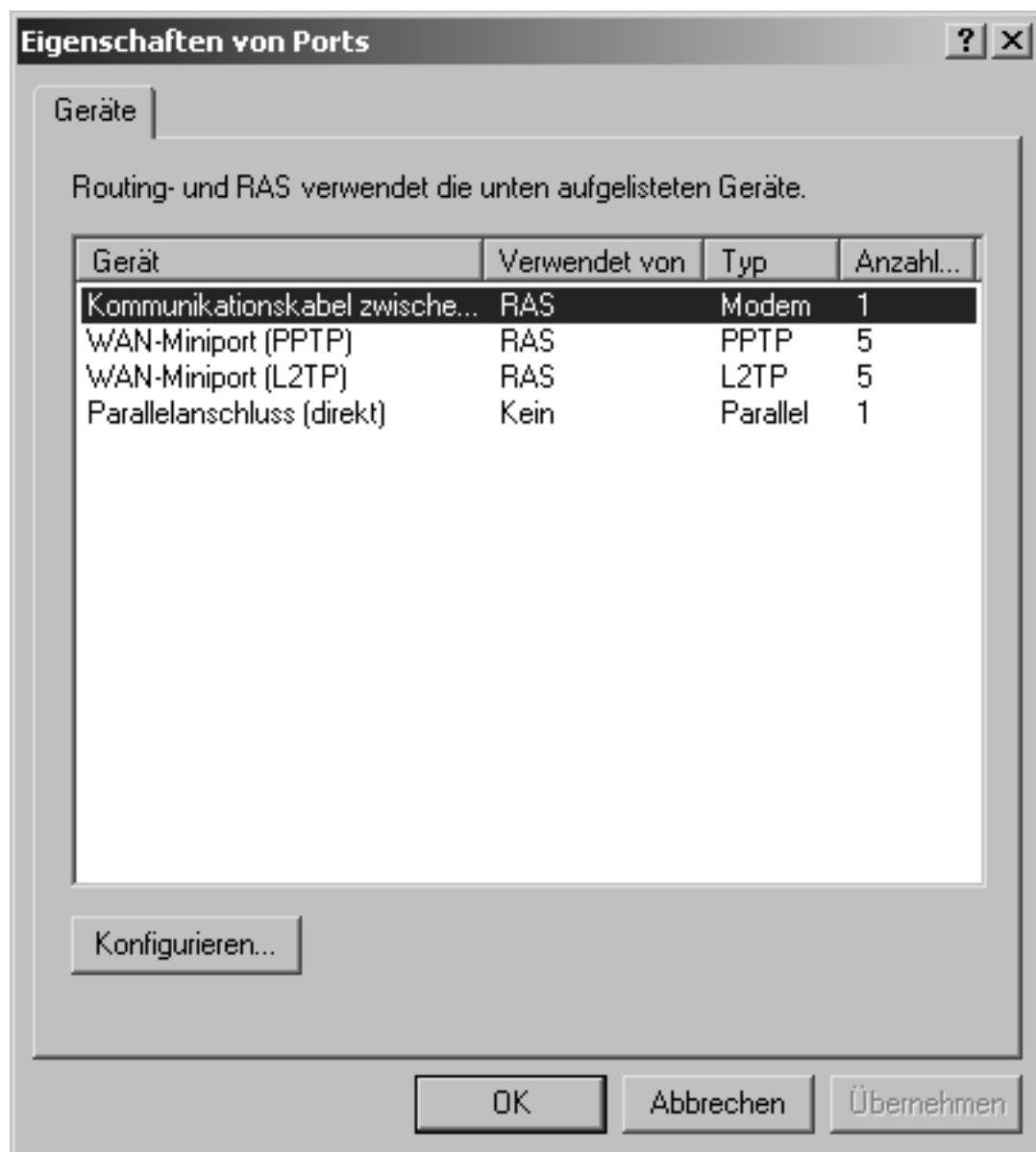


Abbildung 14.13: Verfügbare Routing- und RAS-Geräte

Das Dialogfeld **Eigenschaften von Ports** dient in erster Linie dazu, eine vollständige Liste der auf dem Routing- und RAS-Server verfügbaren Anschlüsse anzuzeigen. Darüber hinaus kann der Administrator mit Hilfe dieses Dialogfelds die unterschiedlichen RAS-Konfigurationen und RAS-Richtlinien

konfigurieren und verwalten. Wenn Sie beispielsweise, wie in Abbildung 14.13 dargestellt, auf **Kommunikationskabel zwischen zwei Computern** und dann auf die Schaltfläche **Konfigurieren** klicken, erscheint das in Abbildung 14.14 dargestellte Dialogfeld **Gerät konfigurieren**.



Abbildung 14.14: Konfigurieren eines RAS-Gerätes

Das Dialogfeld **Gerät konfigurieren** erfüllt im Wesentlichen zwei Funktionen: Hier kann festgelegt werden, ob ein bestimmtes Gerät nur beim Windows 2000-Server eingehende RAS-Verbindungen und/oder ob es sowohl ein- als auch ausgehende, bei Bedarf herzustellende Routingverbindungen unterstützen soll. Um eine dieser Optionen zu aktivieren, müssen Sie lediglich auf das entsprechende Kontrollkästchen klicken. Das Feld **Rufnummer dieses Geräts** hat eine größere Bedeutung, als Sie vielleicht vermuten. Sie verwenden dieses Feld für die vom Benutzer gewählte Rufnummer und mit BAP-aktivierte Verbindungen (Bandwidth Allocation Protocol).

RAS-Richtlinien

Die letzte Option in diesem Dialogfeld wird im Zusammenhang mit den RAS-Geräten verwendet, die mehrere Anschlüsse unterstützen können, wie z.B. ISDN- oder andere WAN-Geräte. Nachdem Sie die

von Ihnen gewünschten Optionen gewählt haben, klicken Sie auf **OK**, um zum Dialogfeld **Eigenschaften von Ports** zurückzukehren. Um all Ihre Einstellungen zu speichern und zum Hauptfenster **Routing und RAS** zurückzukehren, klicken Sie im Dialogfeld **Eigenschaften von Ports** auf die Schaltfläche **OK**.

Klicken Sie als Nächstes im linken Bereich des Fensters **Routing und RAS** auf das Symbol **RAS-Richtlinien**.

Daraufhin werden im rechten Bereich des Fensters nur noch zwei Spalten angezeigt: **Name** und **Reihenfolge**. In der Spalte **Name** wird ein mehr oder weniger anschaulicher Name für die auf Ihrem Routing- und RAS-Computer installierte RAS-Richtlinie angezeigt. Die Spalte **Reihenfolge** spielt dann eine Rolle, wenn mehr als eine Richtlinie angewendet wird. Die Funktion **Reihenfolge** ist wichtig, da diese die genaue Reihenfolge angibt, in der mehrere RAS-Richtlinien innerhalb Ihrer Organisation angewendet werden. In der Regel gibt es nur eine Richtlinie: **Zugriff zulassen, wenn Einwählrechte erteilt worden sind**. Das ist die Standardrichtlinie, die von Windows 2000 bei der Installation des Routing- und RAS-Dienstes automatisch implementiert wird. Wenn Sie auf eine Richtlinie doppelklicken, erscheint das Dialogfeld **Eigenschaften** für diese Richtlinie (siehe Abbildung 14.15).

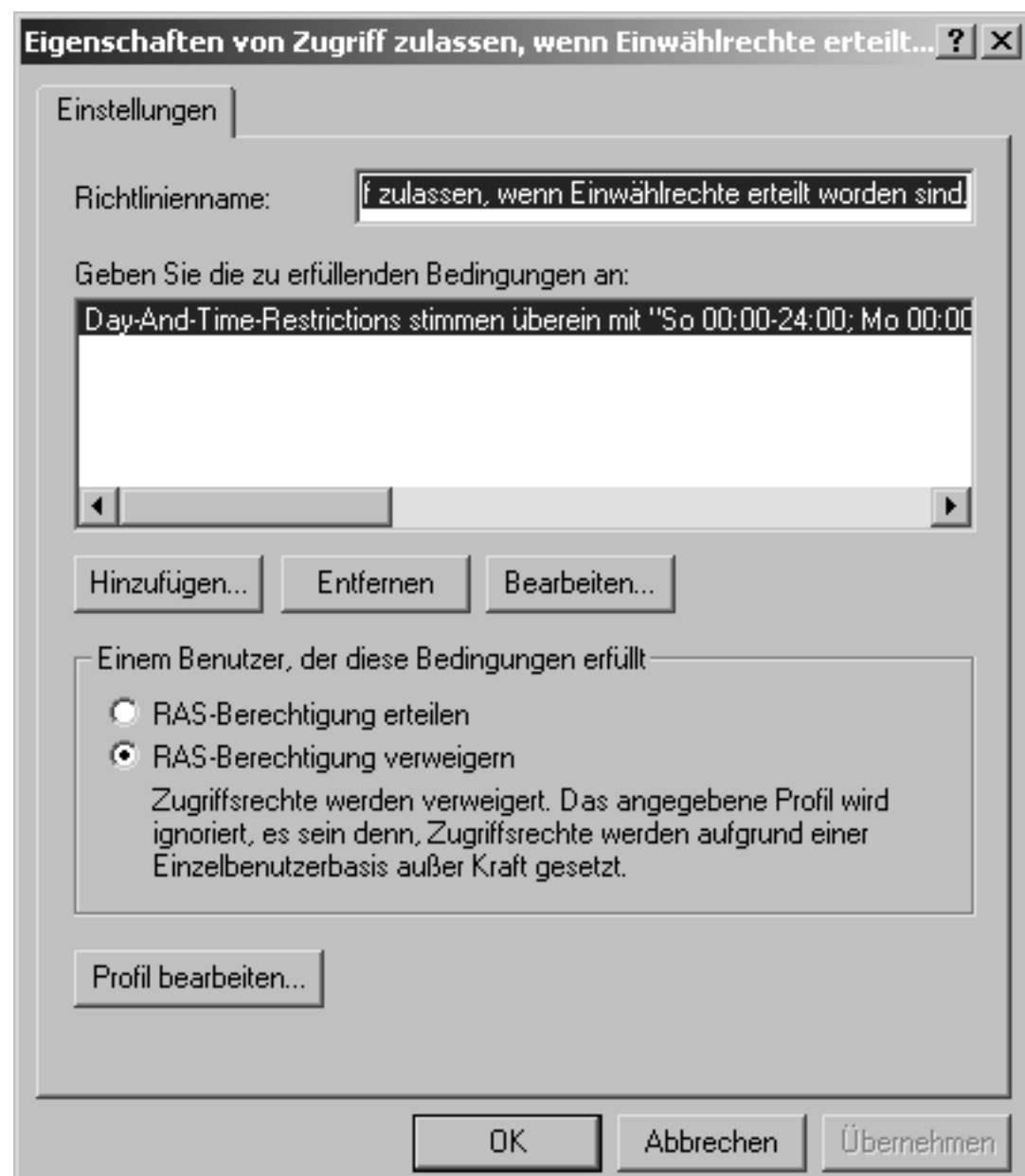


Abbildung 14.15: Das Dialogfeld Eigenschaften einer RAS-Richtlinie

Im Feld **Richtliniennamen** erscheint eine Beschreibung der RAS-Richtlinie, die Sie ändern können. Im Feld **Geben Sie die zu erfüllenden Bedingungen an** können Sie festlegen, unter welchen Bedingungen die RAS-Richtlinie in Ihrer Organisation angewendet werden soll. Der Bereich **Einem Benutzer, der diese Bedingungen erfüllt** wird verwendet, um den Benutzern, die die oben angegebene Richtlinie erfüllen, RAS-Berechtigungen zu erteilen oder zu verweigern. Diese Berechtigung ist eine globale Berechtigung, die nur durch Zugriffsrechte aufgrund einer Einzelbenutzerbasis außer Kraft gesetzt werden kann. Wenn Sie eine RAS-Richtlinie ändern möchten, doppelklicken Sie einfach im Hauptfenster **Routing und RAS** auf die entsprechende Richtlinie. Daraufhin erscheint das Dialogfeld **Eigenschaften** für diese Richtlinie. Klicken Sie hier auf die Schaltfläche **Bearbeiten**, um das in Abbildung 14.16 dargestellte Dialogfeld aufzurufen.

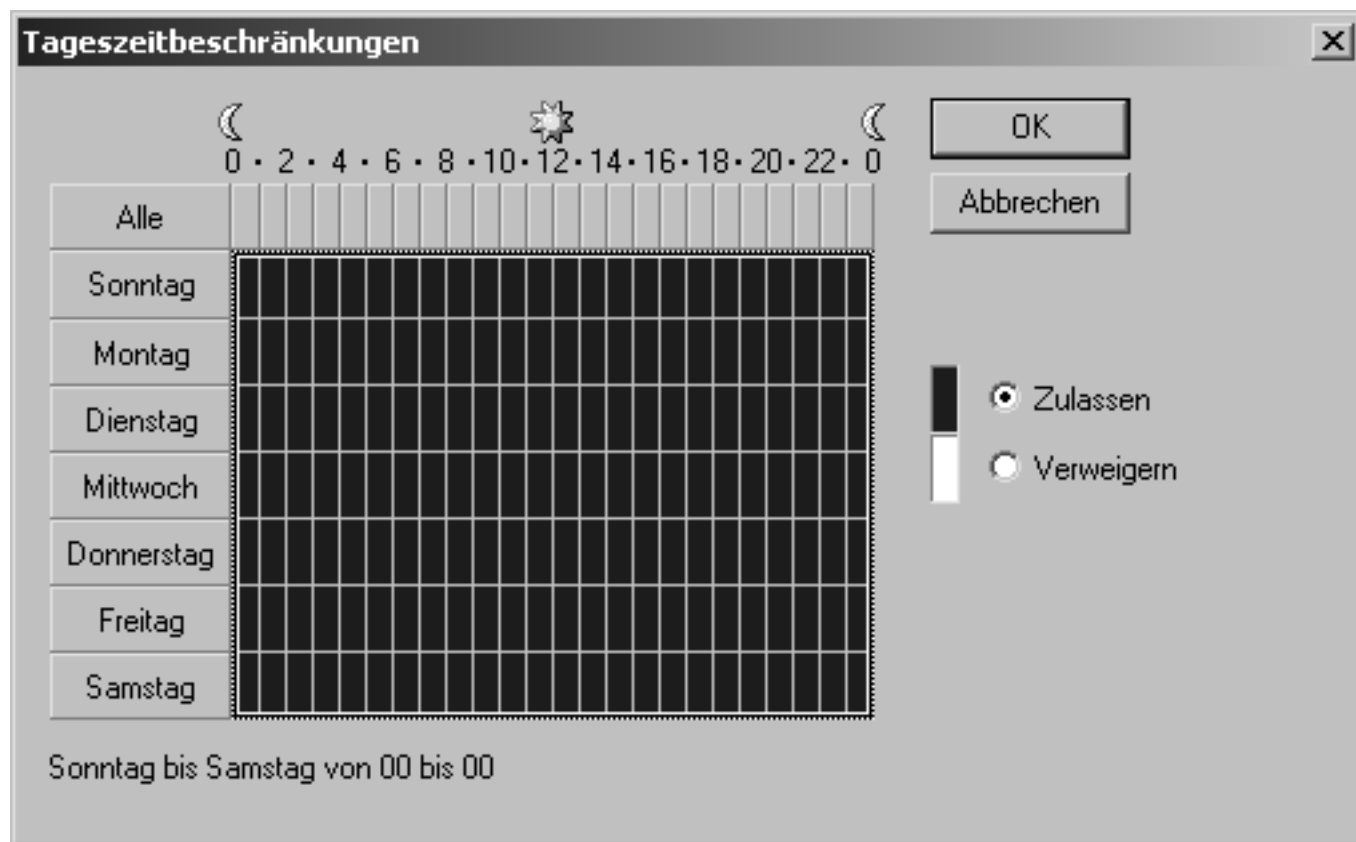


Abbildung 14.16: Festlegen von Tageszeitbeschränkungen

Das Dialogfeld **Tageszeitbeschränkungen** erscheint, weil die zu ändernde RAS-Richtlinie die Tageszeiten betrifft. Um Änderungen vorzunehmen, klicken Sie auf eines oder mehrere der Wochentag- und Uhrzeitkästchen in der Mitte dieses Dialogfelds. Ziehen Sie den Mauszeiger, wenn Sie mehrere Kästchen gleichzeitig markieren möchten. Klicken Sie anschließend entweder auf **Zulassen** oder **Verweigern**, um die Berechtigungen für die markierten Wochentag- bzw. Uhrzeitkästchen zu ändern. Klicken Sie nun auf die Schaltfläche **OK**, um wieder zum Dialogfeld **Eigenschaften** zurückzukehren.

Klicken Sie im Dialogfeld **Eigenschaften** links unten auf die Schaltfläche **Profil bearbeiten**, um weitere Änderungen am Einwählprofil für diese RAS-Richtlinie vorzunehmen. Sie sehen nun das Dialogfeld **Einwählprofil bearbeiten** auf Ihrem Bildschirm (siehe Abbildung 14.17).

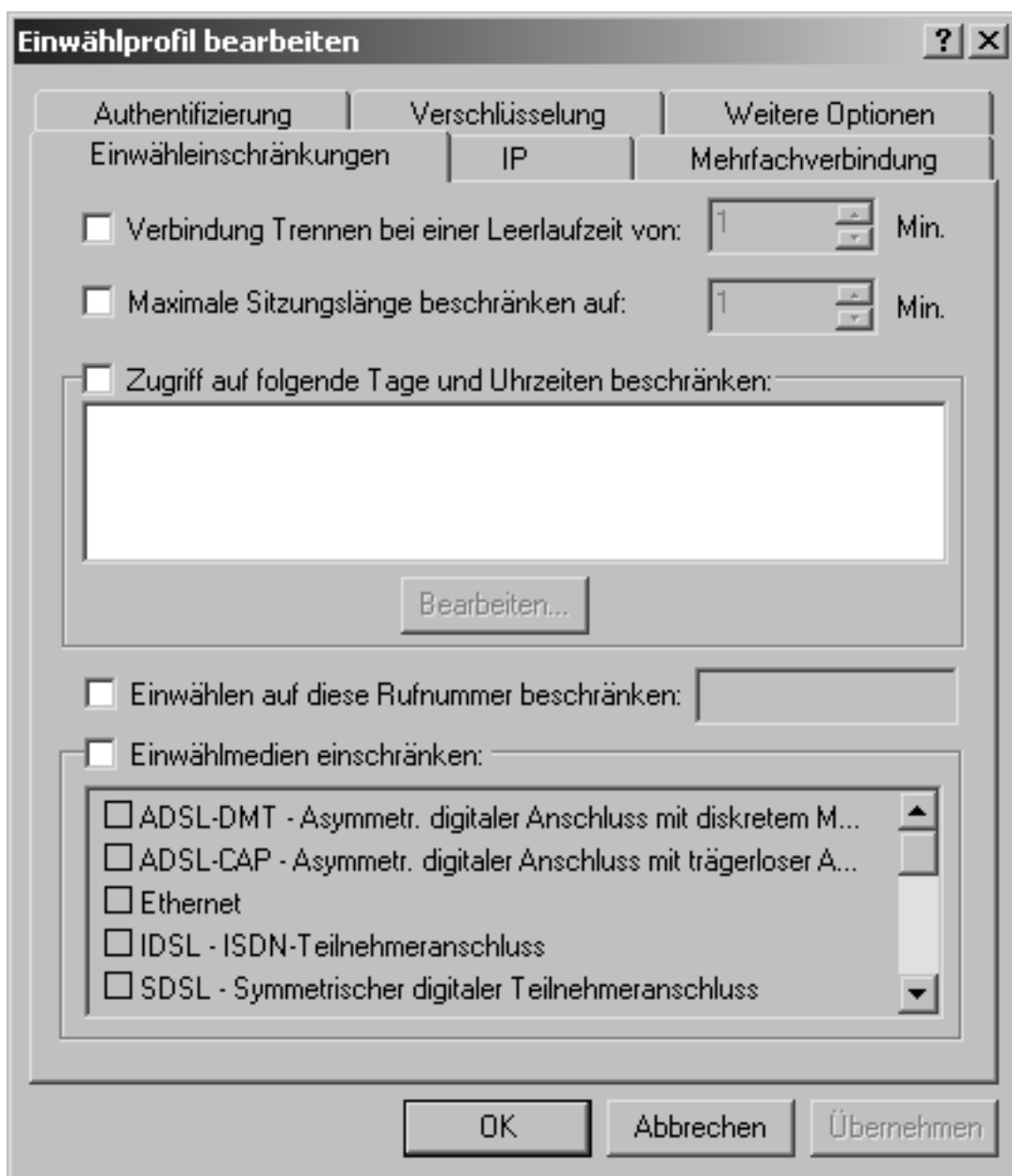


Abbildung 14.17: Festlegen von Einwähleinschränkungen für ein Einwählprofil

Wie Sie sehen, verfügt das Dialogfeld **Einwählprofil bearbeiten** über sechs Registerkarten:

- Einwähleinschränkungen
- IP
- Mehrfachverbindung
- Authentifizierung
- Verschlüsselung
- Weitere Optionen

Einwähleinschränkungen

Das Dialogfeld öffnet sich immer so, dass die Registerkarte **Einwähleinschränkungen** oben liegt (siehe Abbildung 14.17). Eine der angenehmen Eigenschaften von Windows 2000 ist es, dass Sie nun die RAS-Benutzer, die ihre RAS-Sitzungen für eine lange Zeitdauer aufrecht erhalten und dabei

beispielsweise in die Mittagspause gehen, besser steuern können. Diese Tage sind für diese Benutzer nun gezählt, da Sie nun eine maximale Sitzungslänge definieren oder Verbindungen nach einer bestimmten Leerlaufzeit einfach trennen können. Sie können darüber hinaus auch den Zugriff durch bestimmte Benutzer auf bestimmte Tage und Uhrzeiten beschränken, indem Sie das Kontrollkästchen **Zugriff auf folgende Tage und Uhrzeiten beschränken** aktivieren. Klicken Sie, nachdem Sie dieses Kontrollkästchen aktiviert haben, auf die Schaltfläche **Bearbeiten**, sodass Sie die Uhrzeiten und Wochentage für diesen Bereich der Richtlinie auswählen können. Wenn Sie nun also auf die Schaltfläche **Bearbeiten** klicken, erscheint das Dialogfeld **Tageszeitbeschränkungen** (siehe Abbildung 14.16). Nehmen Sie die erforderlichen Änderungen vor und klicken Sie dann auf **OK**, um diese Änderungen zu übernehmen. Klicken Sie auf die Schaltfläche **Abbrechen**, wenn Sie alles so belassen möchten, wie es war. Sie befinden sich nun wieder bei der Registerkarte **Einwähleinschränkungen**.

Die nächste Option auf dieser Registerkarte ist die Option **Einwählen auf diese Rufnummer beschränken**. Wenn Sie diese Option aktivieren, können Sie in das Textfeld rechts neben der Option eine Telefonnummer eingeben. Das bedeutet, dass RAS-Benutzer diese Telefonnummer wählen müssen, um auf Ihren Windows 2000-Server zugreifen zu können. Diese Funktion ist ganz praktisch, wenn Sie den RAS-Dienst für die Fernverwaltung Ihres Windows 2000-Servers, und nicht für die gesamten Heerscharen an Verkäufern verwenden möchten.

Als Nächstes folgt der Bereich **Einwählmedien einschränken**. Hier können Sie die Einwählmedien auf die in diesem Feld markierten Medien beschränken. Um diese Art der Einschränkung zu aktivieren, müssen Sie zunächst das Kontrollkästchen **Einwählmedien einschränken** aktivieren. Erst dann können Sie aus den in diesem Feld angezeigten Medien beliebige Medien wählen. Von den sechs in diesem Feld angezeigten Medien wird wohl die ISDN-Leitung am häufigsten gewählt.

Mit Hilfe dieser Optionen können Sie verhindern, dass Unbefugte auf Ihren Windows 2000-Server und vielleicht sogar auf das übrige Netzwerk zugreifen. Unbefugte müssten dazu nicht nur Telefonnummer, Benutzer-ID und Kennwortschema kennen, sondern müssten auch über genau die angegebene Hardware verfügen, was sehr unwahrscheinlich ist.

IP

Klicken Sie als Nächstes auf den Reiter der in Abbildung 14.18 dargestellten Registerkarte **IP**.

Diese Registerkarte ist in zwei Bereiche unterteilt: Der Bereich für die zu verwendende IP-Adresszuweisungsrichtlinie und der Bereich für die IP-Paketfilter, die für die RAS-Verbindung verwendet werden sollen. Der Bereich **IP-Adresszuweisungsrichtlinie** erklärt sich von selbst. Sie lassen entweder den Windows 2000-Server die Richtlinie mit Hilfe seiner eigenen Netzwerkeinstellungen selbst definieren oder Sie legen fest, dass entweder der Client eine bestimmte IP-Adresse anfordern kann oder dass der Server jedem RAS-Client eine IP-Adresse zuteilt. Klicken Sie auf das Optionsfeld der von Ihnen gewünschten Option.

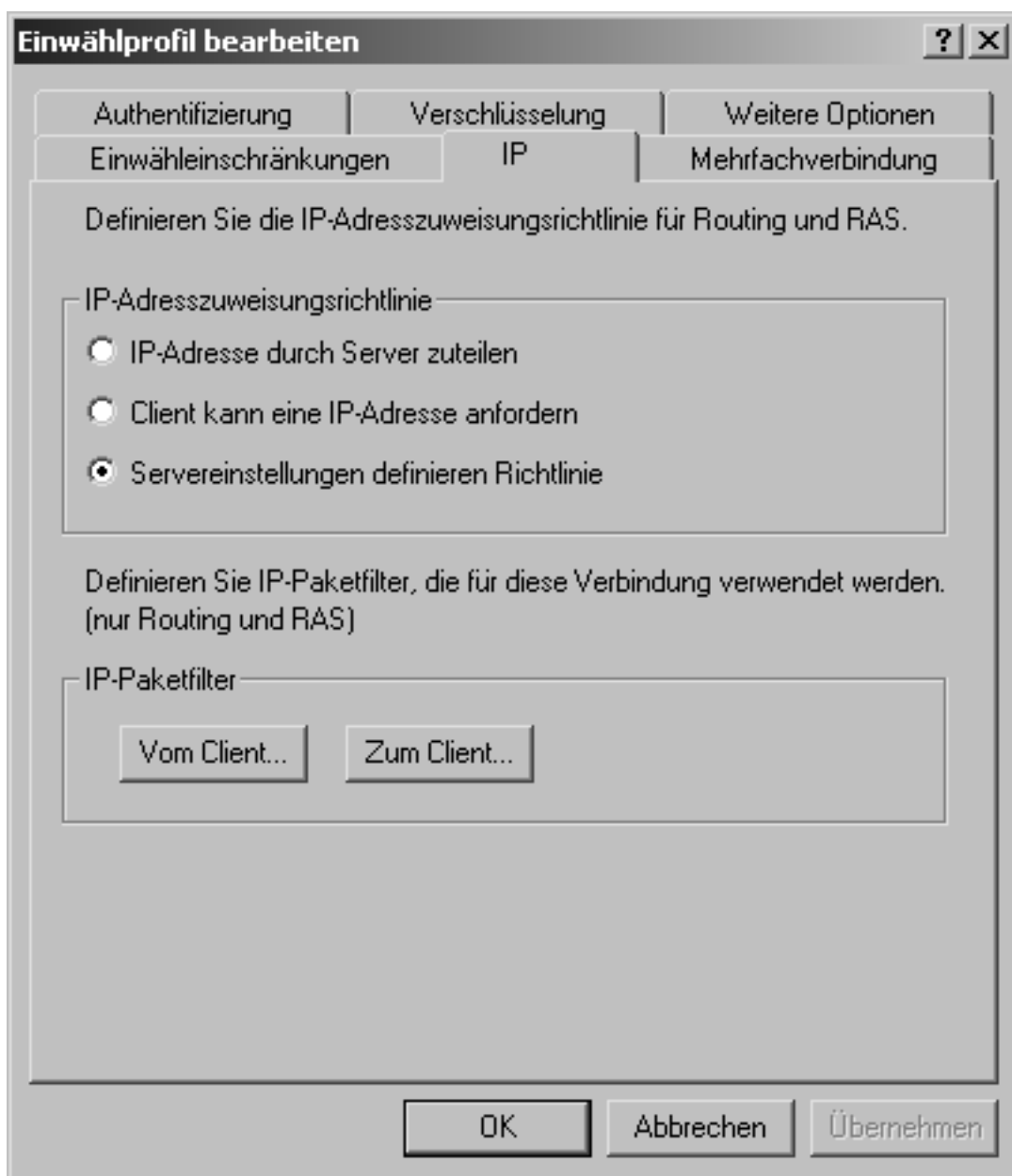


Abbildung 14.18: Definieren von IP-Adresszuweisungen

Im unteren Bereich dieser Registerkarte werden die für Routing und RAS verwendeten IP-Paketfilter definiert, die während des Bestehens einer Verbindung von einem RAS-Benutzer zu einem Windows 2000-Server verwendet werden sollen. Obwohl es sich dabei weniger um eine Frage des RAS, als vielmehr um eine Frage des Routing handelt, sollten Sie sich diesen Bereich dennoch etwas genauer ansehen. Wenn Sie die erforderlichen Änderungen vorgenommen haben, klicken Sie auf den Reiter der in Abbildung 14.19 dargestellten Registerkarte **Mehrfachverbindung**.

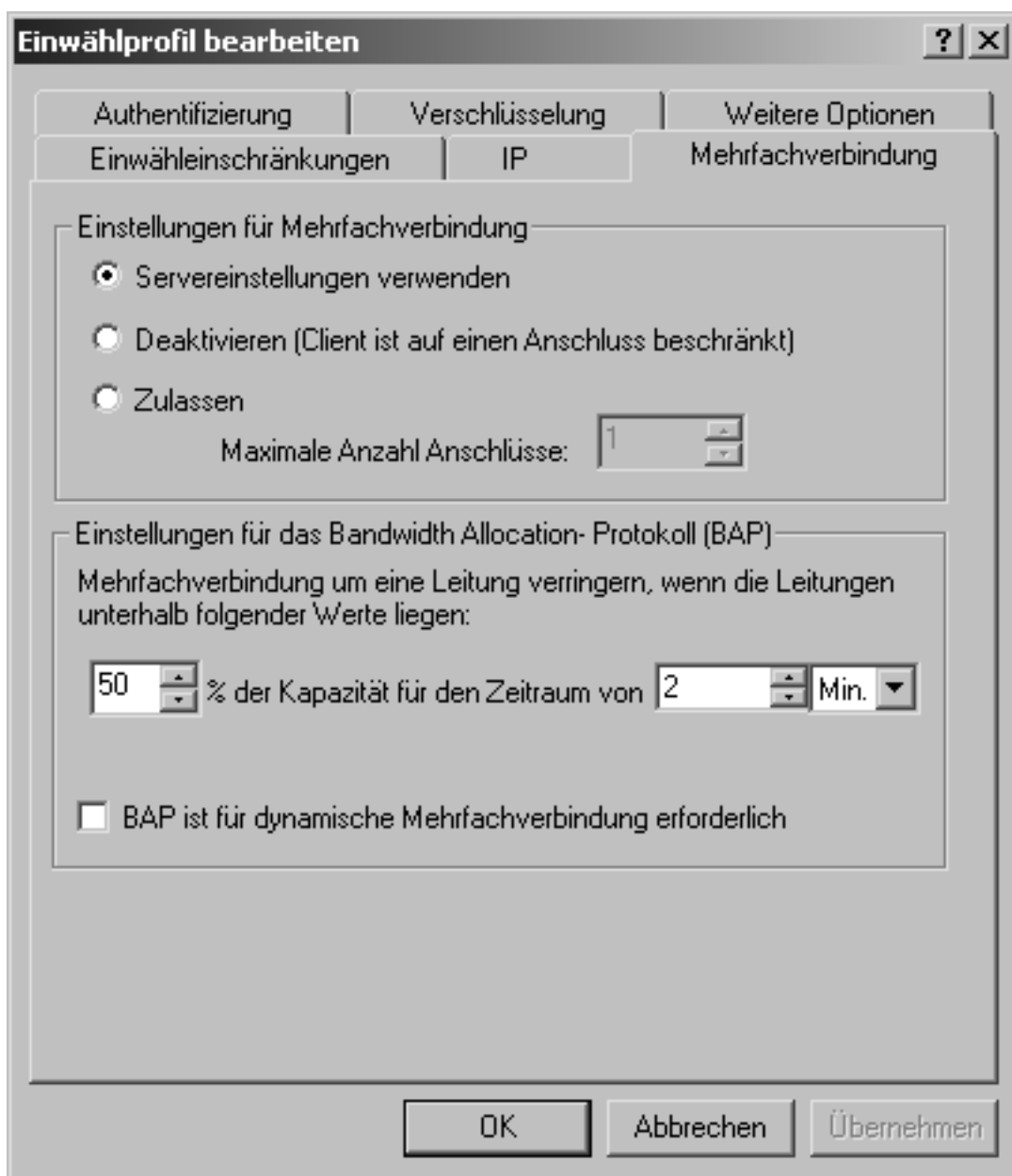


Abbildung 14.19: Konfigurieren der Einstellungen für Mehrfachverbindungen und für das BAP-Protokoll

Mehrfachverbindung

Die Registerkarte **Mehrfachverbindung** dient in erster Linie dazu, den RAS-Benutzern mit einem einzigen analogen oder digitalen Modem wie z.B. einem ISDN-Modem eine höhere Bandbreite als sonst möglich zur Verfügung zu stellen. Das Wesentliche an der Technologie der Mehrfachverbindungen ist, dass zwei oder mehrere Modems zu einer RAS-Verbindung gebündelt werden können. Wenn Sie beispielsweise zwei 56-Kbit/s-Modems bündeln, resultiert daraus eine Bandbreite von insgesamt etwa 112 Kbit/s (denken Sie jedoch daran, dass die Bandbreite je nachdem, wie gut das Modem des Servers mit dem des Clients zusammenarbeitet, variieren kann). Die obere Hälfte der Registerkarte **Mehrfachverbindung** wurde dafür konzipiert, um dieses Arrangement zu ermöglichen, um nämlich die Bandbreite mehrerer Modems für eine Verbindung zwischen dem RAS-Client und dem Windows 2000-Server zu bündeln.

Mit Hilfe der Registerkarte **Mehrfachverbindung** können Sie darüber hinaus auch die Qualität der Mehrfachverbindung durch die Verwendung des BAP-Protokolls (Bandwidth Allocation Protocol) verbessern. BAP ist bei Mehrfachverbindungen sehr nützlich, da es ermöglicht, dass sich die Anzahl der für eine einzige Verbindung zusammengefassten Modems je nach erforderlicher Bandbreite ändert. Diese dynamische Änderung der Bandbreite für eine bestimmte RAS-Verbindung bedeutet für den RAS-Benutzer eine deutlich erhöhte Produktivität. Um diese Routing- und RAS-Funktion zu aktivieren, klicken Sie auf die nach oben bzw. nach unten zeigenden Pfeile neben der Prozentangabe, um die Kapazität festzulegen, bei der BAP ausgelöst werden soll. Klicken Sie auf die nach oben bzw. nach unten zeigenden Pfeile neben dem Feld für die Zeitangabe, um einen Zeitraum anzugeben, nach dem BAP ausgelöst werden soll. Das Kontrollkästchen **BAP ist für dynamische Mehrfachverbindung erforderlich** wird verwendet um anzugeben, ob BAP für weitere Mehrfachverbindungssitzungen aktiviert werden soll. Klicken Sie, nachdem Sie Ihre Wahl getroffen haben, auf den Reiter der in Abbildung 14.20 dargestellten Registerkarte **Authentifizierung**.

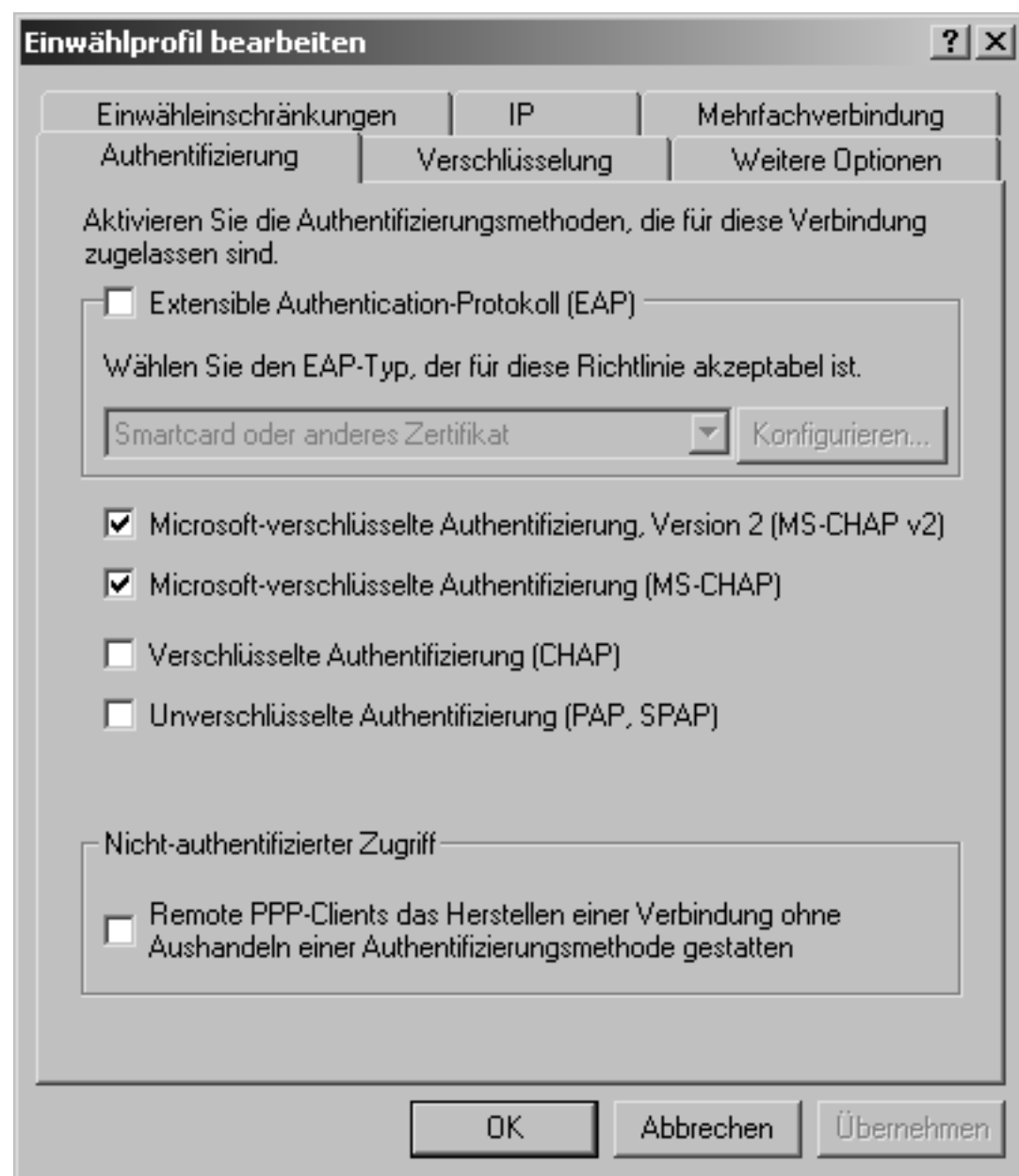


Abbildung 14.20: Auswahl von Authentifizierungsoptionen

Authentifizierung

Mit Hilfe der Registerkarte **Authentifizierung** definieren Sie die Authentifizierungsmethoden für Ihre RAS-Verbindungen. Die meisten der Optionen auf dieser Registerkarte beziehen sich zwar direkt auf die Verschlüsselung, diese kann jedoch nur mit Hilfe der Registerkarte **Verschlüsselung** aktiviert bzw. deaktiviert werden. Wenn Sie auf das Kontrollkästchen **Extensible Authentication-Protokoll (EAP)** klicken, wird diese Funktion aktiviert. Das bedeutet, dass ein weiterer Bereich von Authentifizierungsmethoden wie Authentifizierung durch öffentliche Schlüssel mit Hilfe von Smartcards, einmalige Kennwörter, Tokenkarten u.ä. unterstützt wird. Sie müssen die HEAP-Funktion aktivieren, damit Sie den HEAP-Typ für die Richtlinie aus der unterhalb des Kontrollkästchens **Extensible Authentication-Protokoll (EAP)** erscheinenden Dropdown-Liste wählen können. Die Schaltfläche **Konfigurieren** neben dem Dropdown-Listenfeld ist nur dann verfügbar, wenn EAP die verfügbaren Optionen ändern kann. MD5-Challenge EAP verfügt beispielsweise über keine konfigurierbaren Optionen. Für die Authentifizierung durch öffentliche Schlüssel mit Hilfe von Smartcards gibt es dagegen sehr wohl konfigurierbare Optionen.



Der Ausdruck MD5 hat eigentlich keine wirkliche Bedeutung. Die Buchstaben MD stehen allerdings für Message Digest (engl. Nachrichtenverarbeitung). MD5 wurde 1994 als ein einseitiger Hash-Algorithmus entwickelt, der eine beliebige Datenlänge annimmt und einen 128-Bit-»Fingerabdruck« für diese Daten erstellt. Dieser Fingerabdruck wird als Message Digest bezeichnet und kann nicht in seine ursprüngliche Form zurückverwandelt werden. Das bedeutet, dass es für jemand anderen nicht möglich ist, den eigentlichen Inhalt Ihrer Daten nur allein aufgrund des MD5-Fingerabdrucks zu ermitteln.

Mit Hilfe des mittleren Bereichs der Registerkarte **Authentifizierung** kann der RAS-Administrator die unterschiedlichen Arten der CHAP- und SPAP/PAP-Authentifizierungsmethoden (Shiva Password Authentication Protocol/Password Authentication Protocol) aktivieren bzw. deaktivieren, indem er auf die entsprechenden Kontrollkästchen klickt:

- Microsoft-verschlüsselte Authentifizierung, Version 2 (MS-CHAP v2)
- Microsoft-verschlüsselte Authentifizierung (MS-CHAP)
- verschlüsselte Authentifizierung (CHAP)
- unverschlüsselte Authentifizierung (PAP, SPAP)



Denken Sie daran, dass der Einsatz unverschlüsselter Authentifizierung nicht unbedingt schlecht ist, vor allem dann nicht, wenn Nicht-Microsoft-Clients als Gast auf Ihre Windows 2000 Server-Umgebung zugreifen müssen.

Die letzte Option auf dieser Registerkarte, **Nicht-authentifizierter Zugriff**, verwenden Sie, wenn ein entfernter PPP-Client auf Ihren Windows 2000-Server zugreifen können soll, ohne eine Authentifizierungsmethode aushandeln zu müssen. Das ist für Gast- oder Macintosh-Benutzer ebenso wie für RAS-Benutzer recht praktisch, deren Telefonnummer als Ersatzauthentifizierungsmethode verwendet wird (wenn Sie beispielsweise das ANI-Schema (Automatic Number Identifier) oder eine andere Art der Identifikation der Anrufer-ID verwenden). Nachdem Sie auf dieser Registerkarte die gewünschten Optionen gewählt haben, klicken Sie auf den Reiter der in Abbildung 14.21 dargestellten Registerkarte **Verschlüsselung**.

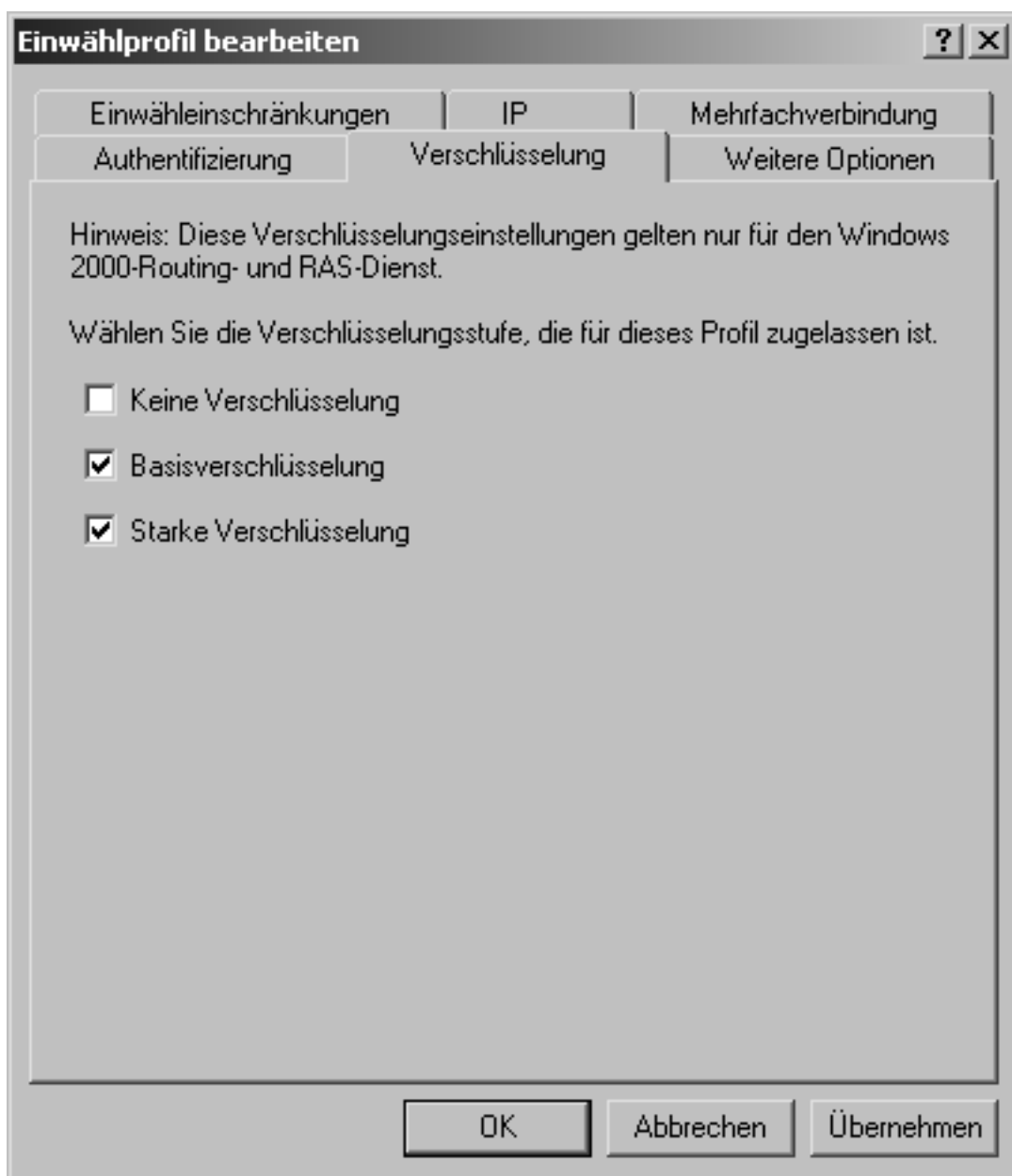


Abbildung 14.21: Wahl der Verschlüsselungsstufe

Verschlüsselung

Die Angaben auf der Registerkarte **Verschlüsselung** sind relativ einfach zu verstehen und zu implementieren. Kurz gesagt: Wenn Sie mit Ihren Remote- und RAS-Clients keinerlei Verschlüsselung verwenden möchten, dann wählen Sie das obere Kontrollkästchen **Keine Verschlüsselung**. Wenn Sie das mittlere Kontrollkästchen, **Basisverschlüsselung**, aktivieren, bedeutet das, dass Ihre Organisation ihre RAS-Clients dazu bringt, einen 40-Bit-Chiffrierschlüssel nach DES (Digital Encryption Standard) zu verwenden, der international eingesetzt werden kann. Die dritte Option, **Starke Verschlüsselung**, bewirkt, dass ein 56-Bit-Schlüssel nach DES verwendet wird. Wenn Sie die gewünschten Optionen aktiviert haben, klicken Sie auf den Reiter der in Abbildung 14.22 dargestellten Registerkarte **Weitere Optionen**.

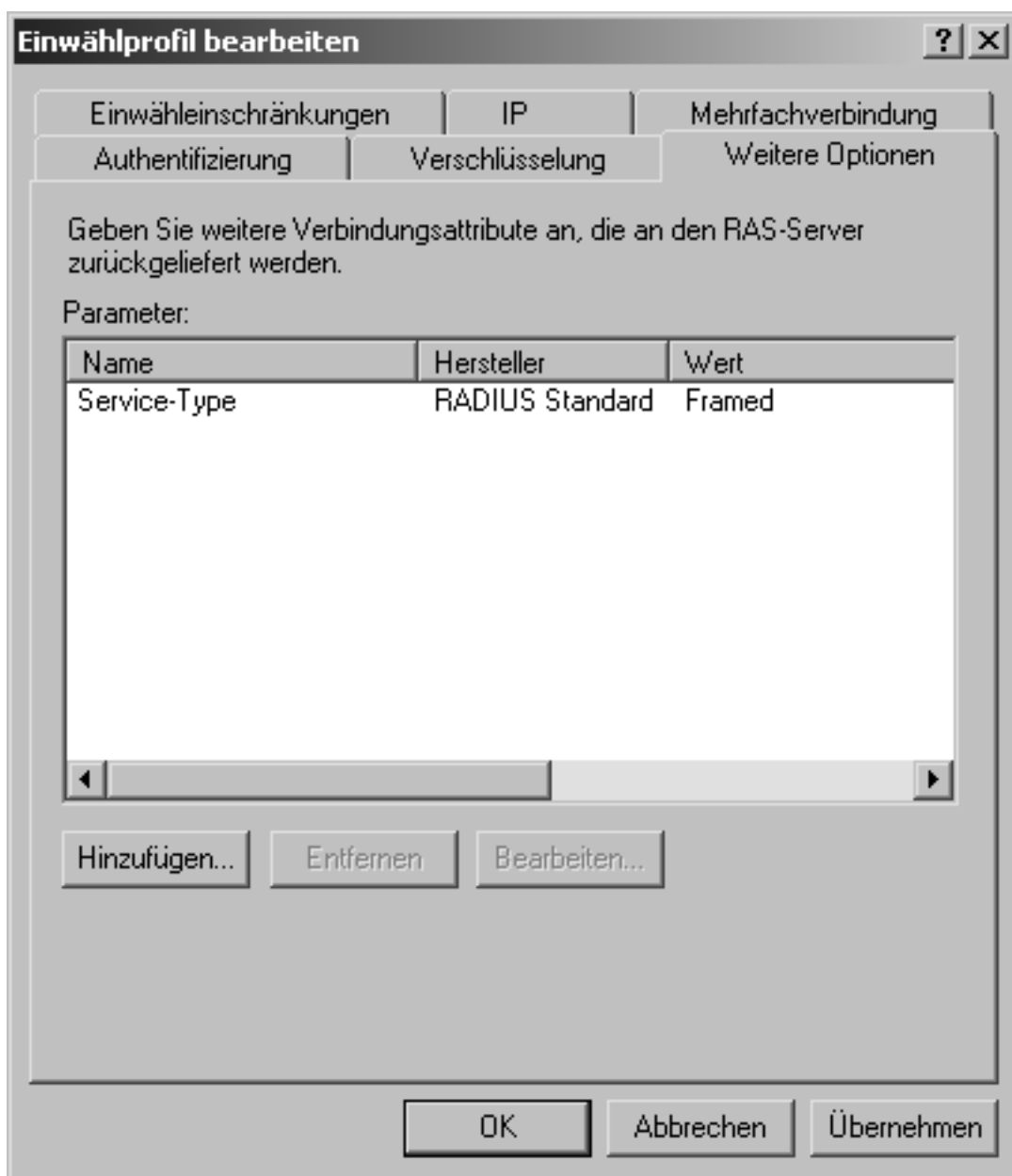


Abbildung 14.22: Auswahl weiterer Optionen

Weitere Optionen

Mit Hilfe der Registerkarte **Weitere Optionen** können Sie Ihre Routing- und RAS-Implementierung so konfigurieren, dass weitere Verbindungsattribute verwendet werden, die beim Zugriff auf den RAS-Server an diesen zurückgeliefert werden. Das ist Teil der RADIUS-Technologie (Remote Authentication Dial-In User Service), bei der es sich um einen Industriestandard handelt, der auf den RFCs 2138 und 2139 beruht. RADIUS dient dazu, Authentifizierungs-, Autorisierungs- und Kontoführungsdienste für verteilte DFÜ-Netzwerke zur Verfügung zu stellen. Ein RADIUS-Client kann der Computer eines Endbenutzers sein. Viel wahrscheinlicher ist es jedoch, dass es sich bei einem RADIUS-Client um einen DFÜ-Server handelt, der von einem Internetdienstanbieter zusammen mit den RAS-Benutzern Ihrer Organisation verwendet wird. Die Windows 2000-Implementierung unterstützt gegenwärtig vier Hersteller: Ascend Communications, Cisco, die RADIUS-Standards (von Microsoft) und US Robotics. Um einen dieser RADIUS-Dienste hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen**. Daraufhin erscheint das in Abbildung 14.23 dargestellte Dialogfeld **Attribute hinzufügen**.

Im Dialogfeld **Attribute hinzufügen** wählen Sie die RADIUS-Attribute, die Sie für Ihr RAS-Netzwerk benötigen. In unserem Beispiel haben wir das Attribut Tunnel-Type gewählt. Dabei handelt es sich um einen Attributtyp des Herstellers RADIUS Standard. Wenn Sie das zu verwendende Attribut (verschieben Sie dazu die relativ lange Liste entsprechend nach oben bzw. unten) gefunden haben, klicken Sie auf die Schaltfläche **Hinzufügen**. Daraufhin erscheint das in Abbildung 14.24 dargestellte Dialogfeld **Mehrwertige Attributinformationen**.

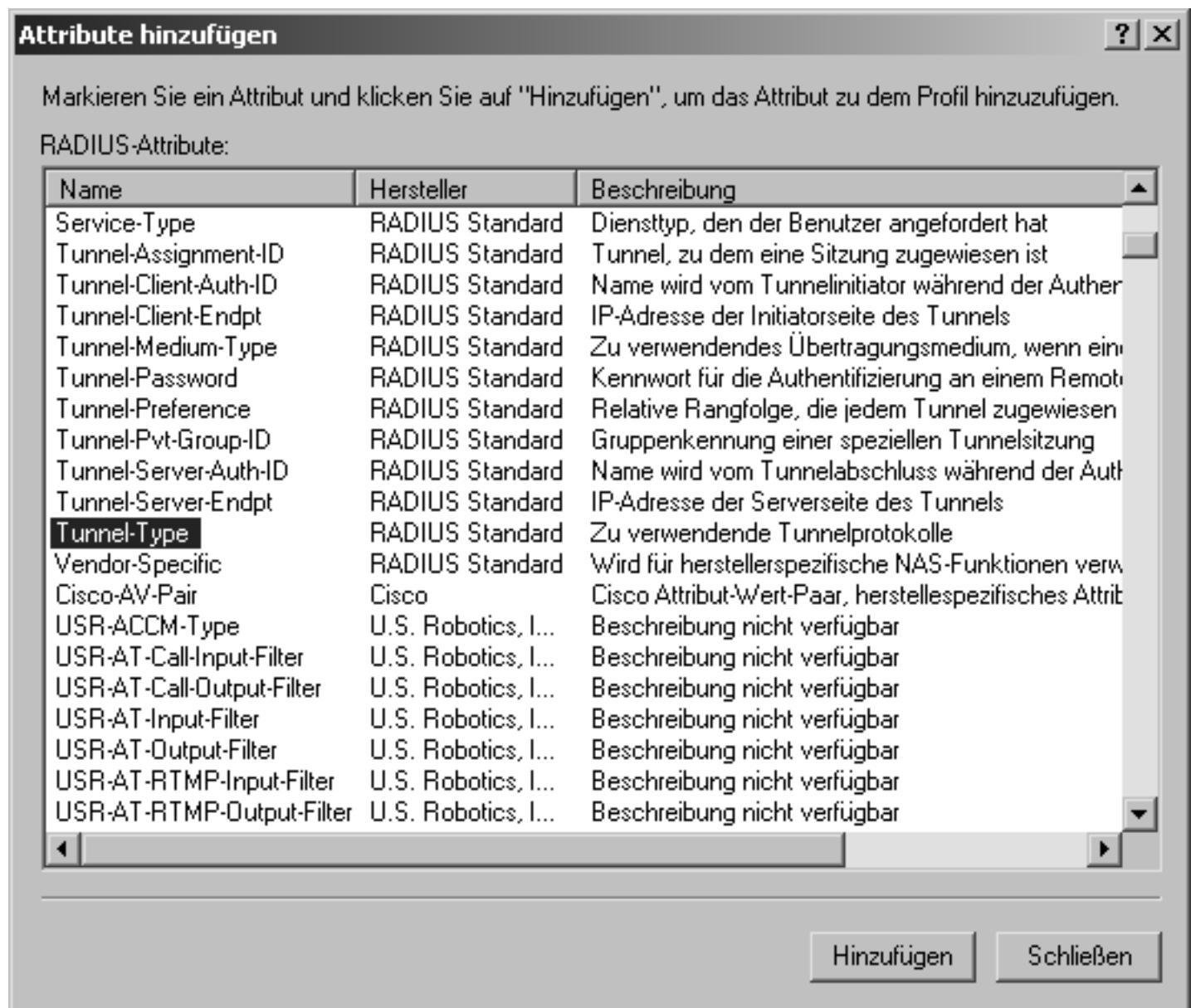


Abbildung 14.23: Auswahl eines RADIUS-Attributs

Mehrwertige Attributinformationen [?] [X]

Attributname:
Tunnel-Type

Attributnummer:
64

Attributformat:
Enumerator

Attributwert:

Hersteller	Wert

Nach oben
Nach unten
Hinzufügen
Entfernen
Bearbeiten

OK Abbrechen

Abbildung 14.24: Das Dialogfeld Mehrwertige Attributinformationen

Mit dem Dialogfeld **Mehrwertige Attributinformationen** schließen Sie die Konfiguration der Hersteller- und Attributinformationen ab. Klicken Sie dazu auf die Schaltfläche **Hinzufügen**. Daraufhin erscheint das in Abbildung 14.25 dargestellte Dialogfeld **Auflistbare Attributinformationen**.

Im unteren Bereich dieses Dialogfelds befindet sich eine Dropdown-Liste mit den unterschiedlichen auflistbaren Attributen. Wenn Sie die von Ihnen gewünschten Attribute gewählt haben, klicken Sie auf die Schaltfläche **OK**, um zum Dialogfeld **Mehrwertige Attributinformationen** zurückzukehren.

In diesem Dialogfeld klicken Sie ebenfalls auf die Schaltfläche **OK**, um zum Dialogfeld **Attribute hinzufügen** zurückzukehren. Hier klicken Sie auf die Schaltfläche **Schliessen**, um zum Dialogfeld **Einwählprofil bearbeiten** mit der Registerkarte **Weitere Optionen** zurückzukehren. Klicken Sie nun noch einmal auf die Schaltfläche **OK** und schon befinden Sie sich wieder im Hauptfenster **Routing und RAS**.

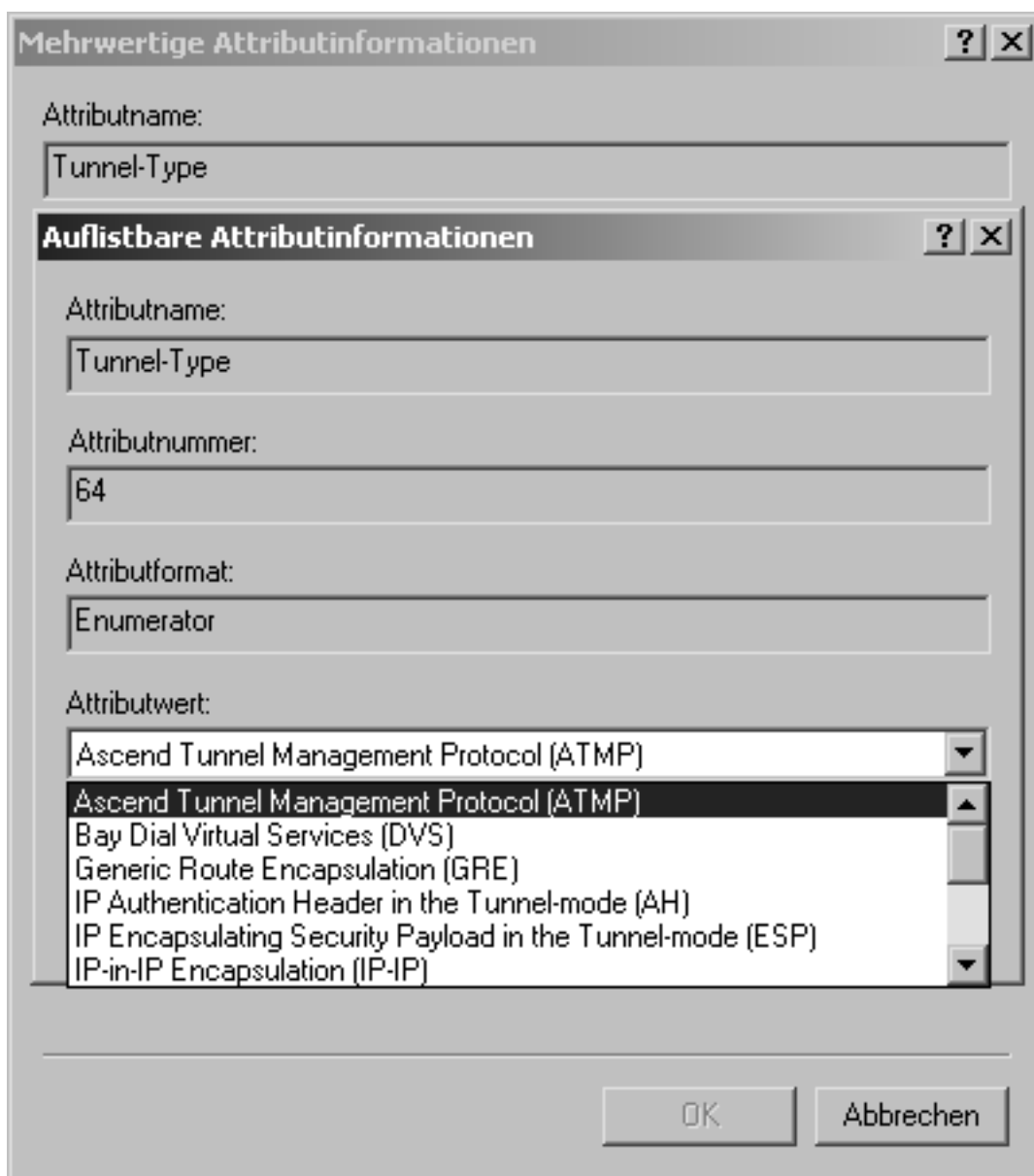


Abbildung 14.25: Auswahl eines Attributwerts

RAS-Richtlinien

Ein weiterer Aspekt von RAS, den Sie beachten sollten, ist der, dass über das Fenster **Routing und RAS** unendlich viele RAS-Richtlinien implementiert werden können. Um eine neue RAS-Richtlinie hinzuzufügen, klicken Sie im linken Bereich des Fensters mit der rechten Maustaste auf das Symbol **RAS-Richtlinie**. Klicken Sie in dem daraufhin erscheinenden Menü auf die Option **Neu**. Daraufhin erscheint ein Menü zur Auswahl einer RAS-Richtlinie.

Als Nächstes öffnet sich das in Abbildung 14.26 dargestellte Dialogfeld **RAS-Richtlinie hinzufügen**.

RAS-Richtlinie hinzufügen

Richtlinienname
Geben Sie einen Namen für die Richtlinie an.

Eine RAS-Richtlinie ist ein Satz von Vorgängen, die auf eine Gruppe von Benutzern, die bestimmte Bedingungen erfüllen, angewendet werden können.

So wie Sie Regeln für eingehende Mail in einer Mailanwendung bestimmen können, können Sie Bedingungen festlegen, die für die RAS-Richtlinie angewendet werden müssen. Außerdem können Sie Vorgänge festlegen, die ausgeführt werden müssen, wenn die Bedingungen erfüllt sind.

Angezeigter Richtlinienname:

Musterrichtlinie

< Zurück Weiter > Abbrechen

Abbildung 14.26: Geben Sie einen eindeutigen Namen für Ihre neue RAS-Richtlinie ein

In diesem Dialogfeld geben Sie einen anschaulichen Namen für die neue RAS-Richtlinie, die Sie gerade erstellen, ein. Sie sollten einen möglichst aussagekräftigen Namen verwenden. Denn wenn Sie zig Richtlinien erstellt haben, ist es schwierig, die einzelnen Richtlinien auseinander halten zu können. Klicken Sie auf die Schaltfläche **Weiter**, um das in Abbildung 14.27 dargestellte Dialogfeld **Attribut auswählen** zu öffnen.



Abbildung 14.27: Auswahl eines Attributs

Nun müssen Sie ein RAS-Richtlinienattribut wählen, das Sie auf diese neue Richtlinie anwenden möchten. Um ein Attribut auszuwählen, markieren Sie den Namen des entsprechenden Attributs und klicken dann auf die Schaltfläche **Hinzufügen**. Daraufhin erscheint das in Abbildung 14.28 dargestellte Dialogfeld für die Auswahl von speziellen Attributen für das gewählte Attribut.

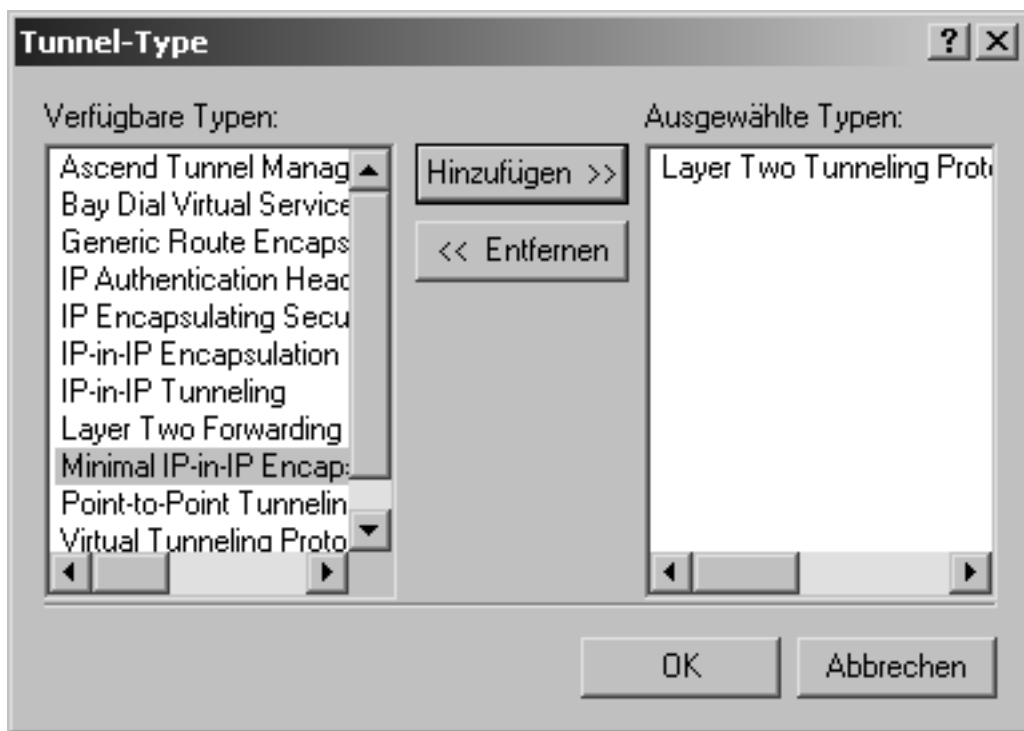


Abbildung 14.28: Wählen Sie ein spezielles Attribut für das Attribut Tunnel-Type.

Im Dialogfeld **Tunnel-Type** (beachten Sie, dass dieses Dialogfeld anders aussieht, je nachdem, welchen Attributtyp Sie im vorhergehenden Dialogfeld gewählt haben) müssen Sie den Typen der einzuschränkenden Richtlinie für das Tunnelprotokoll angeben. Klicken Sie dazu auf eine der Optionen im Feld **Verfügbare Typen** und dann auf die Schaltfläche **Hinzufügen**, um diese Option in das Feld **Ausgewählte Typen** zu verschieben (wie das in Abbildung 14.28 dargestellt ist). Wenn Sie Ihre Wahl getroffen haben, klicken Sie auf die Schaltfläche OK, um wieder zum Dialogfeld **RAS-Richtlinie hinzufügen** zu gelangen. Hier wird nun Ihr neu gewähltes Attribut angezeigt (siehe Abbildung 14.29).

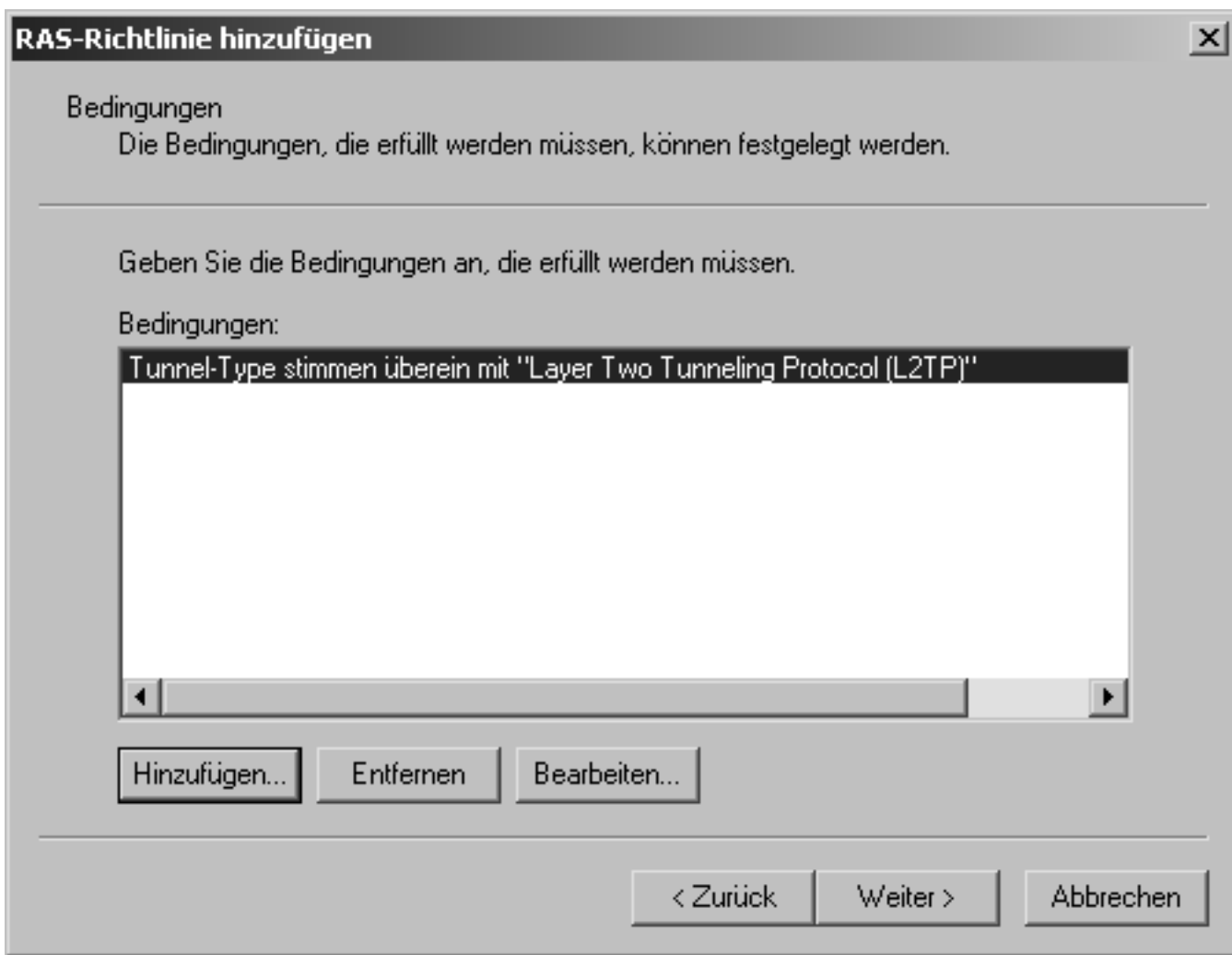


Abbildung 14.29: Festlegen von Bedingungen für die RAS-Richtlinie

Mit den Schritten, die Sie eben ausgeführt haben, legen Sie fest, welche Bedingungen erfüllt werden müssen, damit die RAS-Richtlinie in Kraft tritt. Sie können beliebig viele Bedingungen auswählen, indem Sie auf die Schaltfläche **Hinzufügen** klicken und diese letzten Schritte entsprechend oft wiederholen. Wenn Sie mit Ihrer Auswahl zufrieden sind, klicken Sie auf die Schaltfläche **Weiter**. Daraufhin erscheint das in Abbildung 14.30 dargestellte Dialogfeld für die Definition von Berechtigungen.



Abbildung 14.30: RAS-Berechtigung erteilen oder verweigern

In diesem Dialogfeld legen Sie fest, ob Sie den RAS-Zugriff auf Ihren Windows 2000-Server aufgrund der im vorhergehenden Dialogfeld definierten Bedingungen erteilen oder verweigern. Sie müssen eine der beiden Optionen wählen. Klicken Sie dann auf die Schaltfläche **Weiter**. Nun erscheint das in Abbildung 14.31 dargestellte Dialogfeld für die Festlegung des Benutzerprofils.

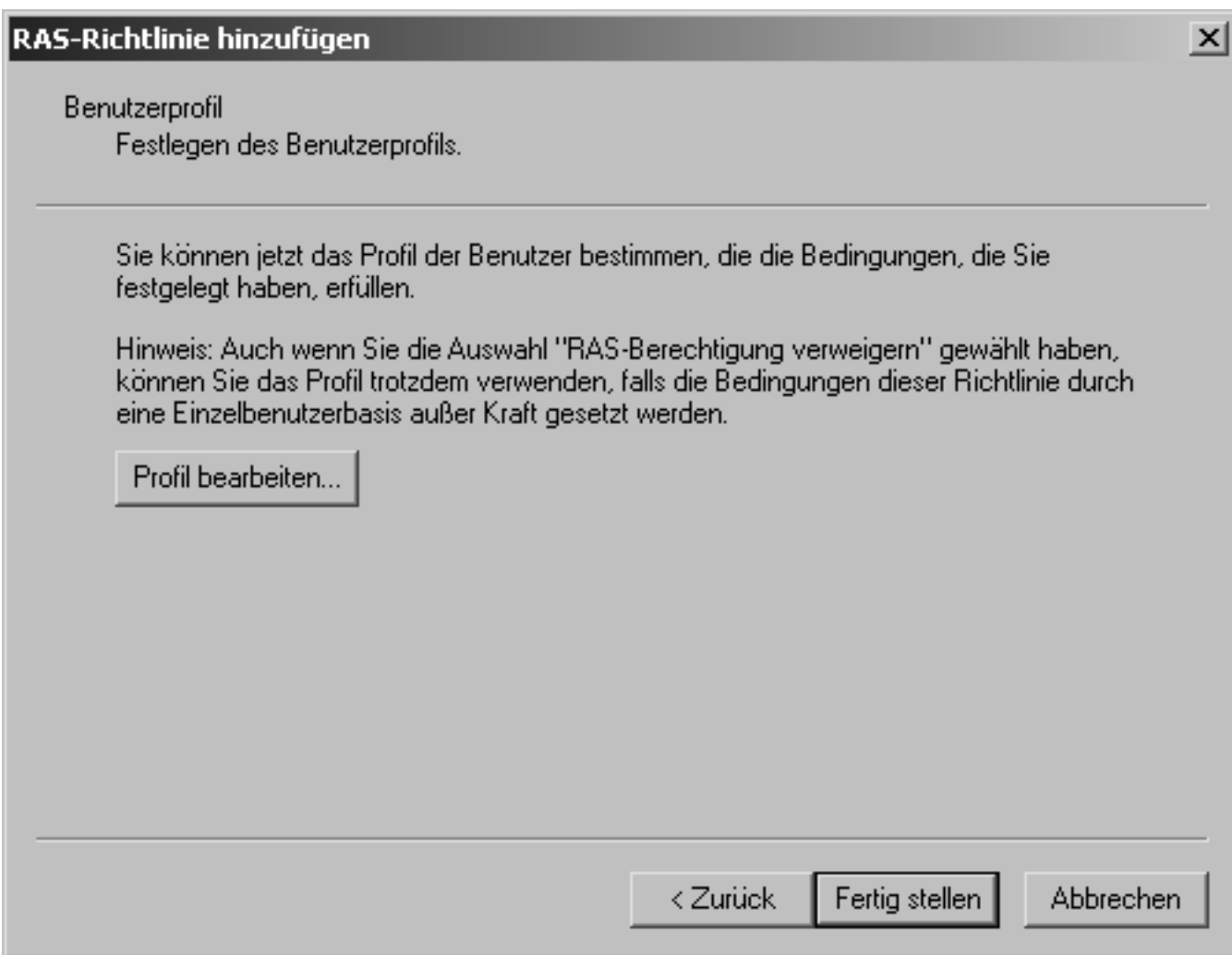


Abbildung 14.31: Entscheiden Sie, ob Sie das Benutzerprofil bearbeiten möchten.

Jetzt müssen Sie festlegen, ob es sich bei dieser RAS-Richtlinie um eine selektive Richtlinie handeln soll. Wenn Sie möchten, dass diese Richtlinie auf jeden angewendet wird, dann brauchen Sie in diesem Dialogfeld nichts zu tun. Denken Sie jedoch daran, dass das Profil immer noch außer Kraft gesetzt werden kann, wenn durch die Bedingungen dieser neuen RAS-Richtlinie die Richtlinienentscheidungen einer höheren Autorität geändert werden. Wenn Sie mit Ihrer Entscheidung zufrieden sind, klicken Sie auf die Schaltfläche **Fertig stellen**, um diesen Teil der Konfiguration abzuschließen. Daraufhin erscheint wieder das Fenster **Routing und RAS**. Nun wird Ihre neu definierte Richtlinie im rechten Bereich des Fensters angezeigt (siehe Abbildung 14.32).

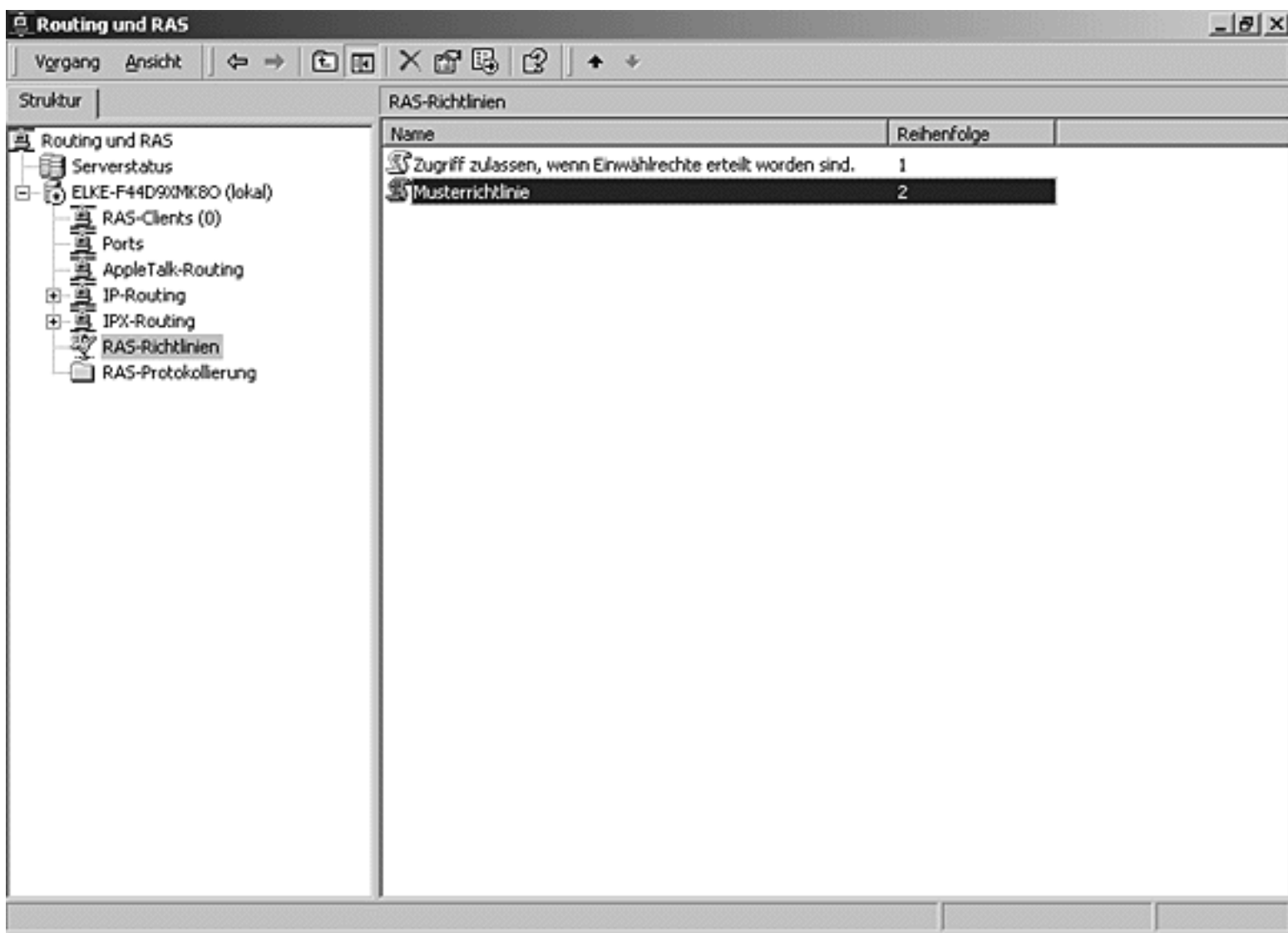


Abbildung 14.32: Ihre neu erstellte RAS-Richtlinie

RAS-Richtlinien werden in der Reihenfolge, in der sie erstellt wurden, angezeigt. Um die RAS-Richtlinien im Fenster **Routing und RAS** neu anzuordnen, klicken Sie mit der rechten Maustaste auf die Richtlinie, deren Position Sie verändern möchten, und wählen Sie aus dem daraufhin erscheinenden Dropdown-Menü eine neue Position.

Die Option **Nach oben** bewirkt genau das, was Sie denken: Wenn Sie auf diese Option klicken, wird die markierte Richtlinie um eine Position nach oben verschoben. Wenn Sie auf die Option **Nach unten** klicken, geschieht das Gegenteil. Wenn Sie eine bestimmte Richtlinie löschen möchten, markieren Sie diese Richtlinie, klicken mit der rechten Maustaste auf diese Richtlinie und wählen aus dem daraufhin erscheinenden Dropdown-Menü die Option **Löschen**. Über die Option **Eigenschaften** können Sie jeden Aspekt der Konfiguration der RAS-Richtlinie ändern, den Sie im oben beschriebenen Konfigurationsprozess definiert haben.

RAS-Protokollierung

Klicken Sie als Nächstes im Fenster **Routing und RAS** auf das Symbol **RAS-Protokollierung**. Daraufhin wird der Ordner **RAS-Protokollierung** geöffnet und dessen Inhalt im rechten Teil des Fensters angezeigt (siehe Abbildung 14.33).

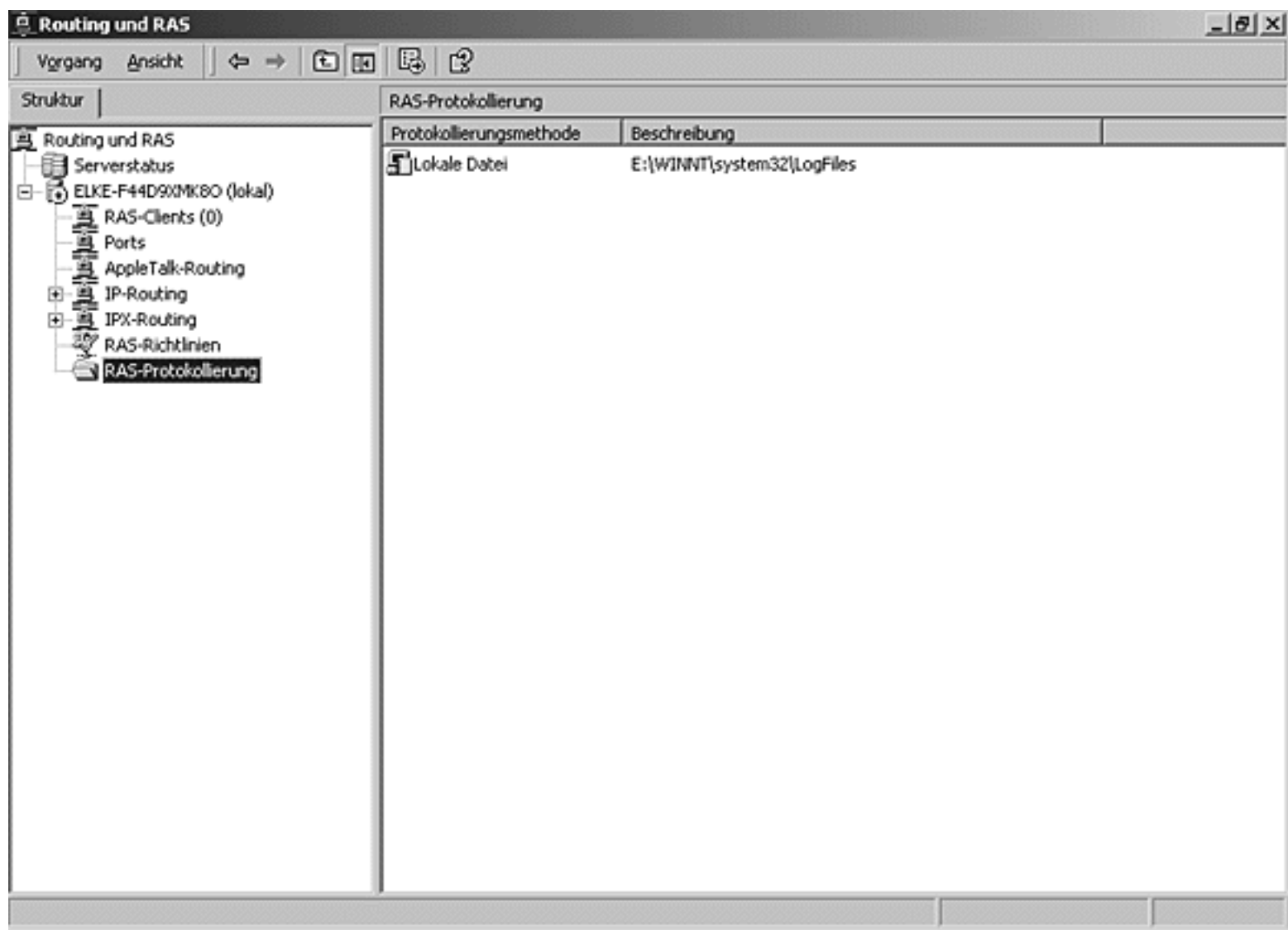


Abbildung 14.33: RAS-Protokollierung

Im rechten Bereich des Fensters wird die Protokollierungsmethode und eine Beschreibung der Protokolle angezeigt. Dabei handelt es sich meistens um die Angabe des Speicherorts der Protokolldatei. Wenn Sie mit der rechten Maustaste auf eine der Protokollierungsmethoden klicken (in unserem Beispiel wird nur eine Protokollierungsmethode angezeigt), erscheint ein Menü mit den beiden Optionen **Eigenschaften** und **Hilfedatei anzeigen**. Wenn Sie auf **Hilfedatei anzeigen** klicken, wird die Hilfedatei aufgerufen. Wenn Sie auf **Eigenschaften** klicken, erscheint das in Abbildung 14.34 dargestellte Dialogfeld **Eigenschaften von Lokale Datei**.

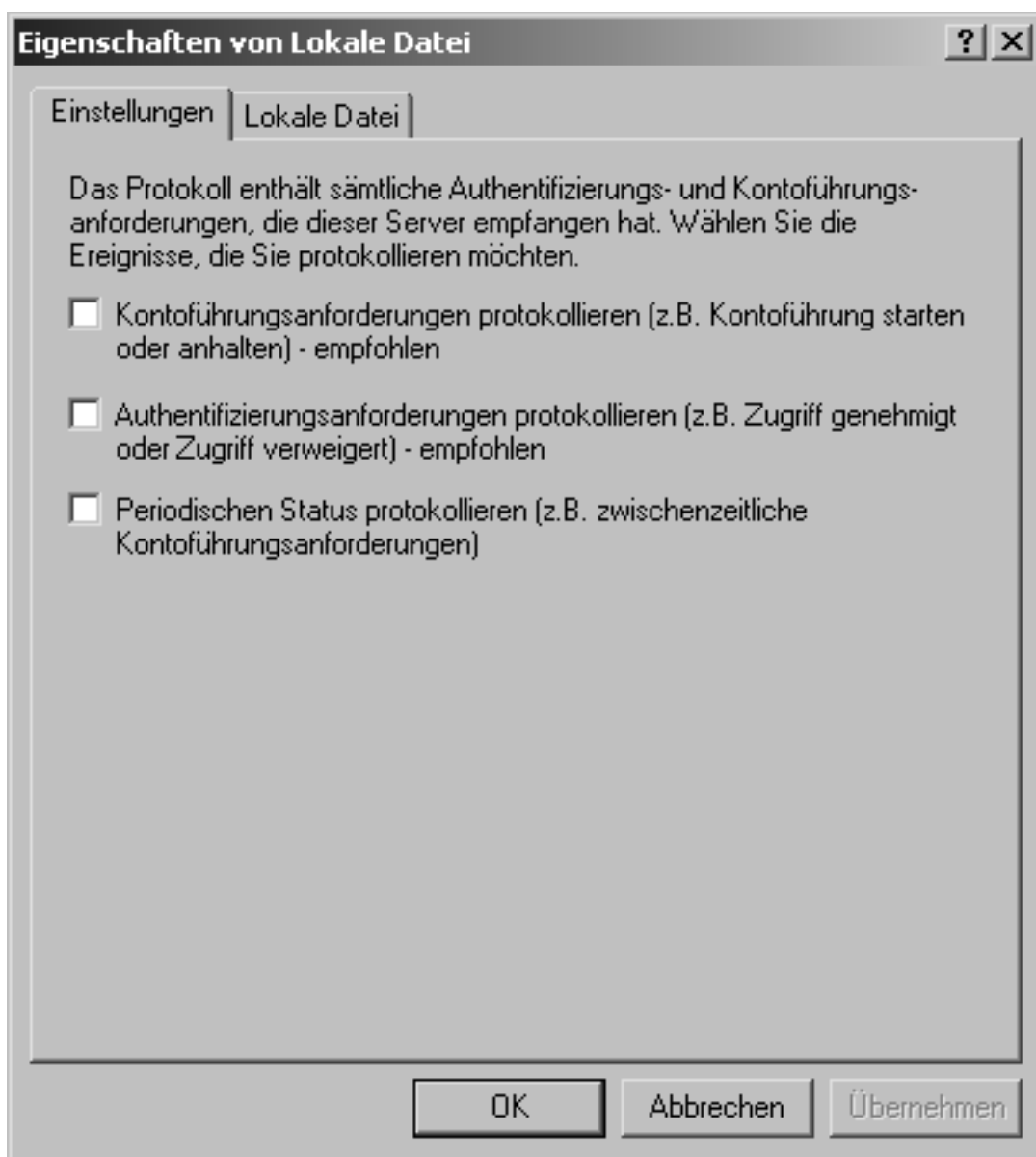


Abbildung 14.34: Definieren von Eigenschaften der lokalen Datei für die RAS-Protokollierung

In Abbildung 14.34 sind die drei möglichen Protokollierungsoptionen für den RAS-Server dargestellt. Um eine dieser Optionen zu aktivieren, klicken Sie auf das Kontrollkästchen neben der jeweiligen Option. Klicken Sie anschließend auf den Reiter der in Abbildung 14.35 dargestellten Registerkarte **Lokale Datei**.

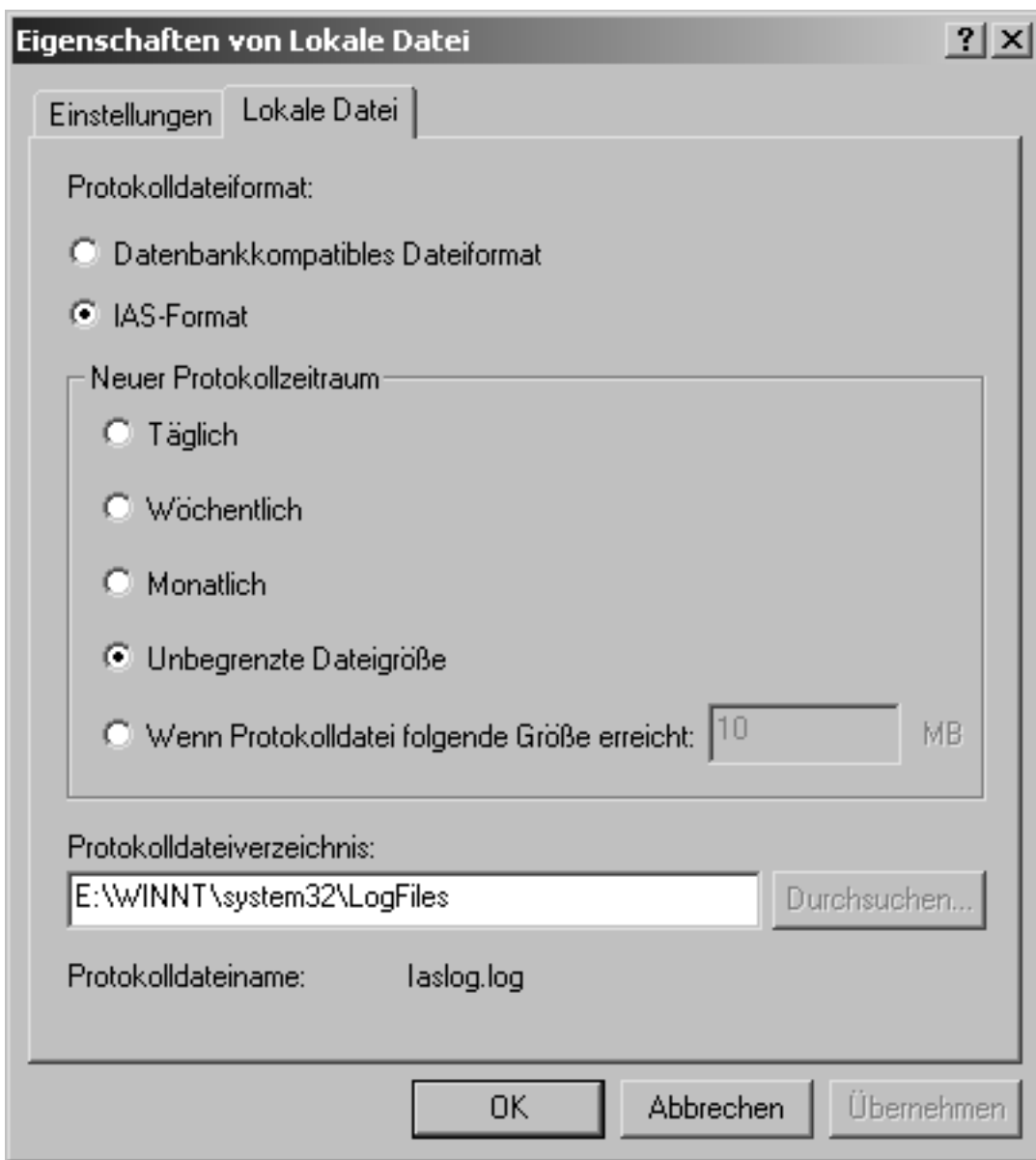


Abbildung 14.35: Auswahl von Protokolldateioptionen

Mit Hilfe der Registerkarte **Lokale Datei** können Sie als RAS-Administrator bestimmte Optionen für die Protokollierung wie z.B. das Format der Protokolle, den vom Protokoll erfassten Zeitraum, den Speicherort sowie den Namen des Protokolls festlegen. Eine der wichtigsten Entscheidungen, die Sie auf dieser Registerkarte fällen müssen, ist die, ob das Protokoll in einem ODBC-kompatiblen (Open Database Connectivity) oder in einem IAS-Format (Internet Authentication Service) gespeichert werden soll. Wenn das Protokoll in einem ODBC-kompatiblen Format gespeichert wird, kann es in einer ODBC-kompatiblen Datenbank gespeichert werden. Das IAS-Format ist dagegen ein textbasiertes Format, das auch von anderen (auch von nicht von Microsoft stammenden) Protokollierungsprogrammen gelesen werden. Die in den beiden Bereichen **Neuer Protokollzeitraum** und **Protokolldateiformat** zur Verfügung stehenden Optionen erklären sich von selbst. Wenn Sie Ihre Wahl getroffen haben, klicken Sie auf die Schaltfläche **OK**, um Ihre Änderungen zu speichern und zum Hauptfenster **Routing und RAS** zurückzugelangen.

14.4.3 Konfigurieren des Routing

Um das Routing konfigurieren zu können, müssen Sie auf Ihrem Windows 2000-Server das Fenster **Routing und RAS** öffnen. Wenn Sie dieses Fenster noch nicht geöffnet haben, klicken Sie auf die Schaltfläche **Start**, wählen die Option **Programme**, dann die Option **Verwaltung** und klicken anschließend auf **Routing und RAS**. Daraufhin öffnet sich das Fenster **Routing und RAS**.

Da wir den Windows 2000-Server bereits als RAS-Server konfiguriert haben, erscheint der Name Ihres Computers bereits im linken Bereich des Fensters unterhalb des Symbols **Serverstatus**. Die mit **Routing** gekennzeichneten Symbole werden für die Konfiguration des Routing verwendet. Ein Bereich der RAS-Konfiguration sorgt dafür, dass sämtliche auf Ihrem Computer bereits installierten Protokolle hier als mögliche Routingoptionen erscheinen. Wie Sie sehen, gibt es hier beispielsweise Einträge für das IP-Routing sowie für das IPX-Routing. Diese Einträge werden bei den Servern angezeigt, auf denen sowohl die TCP/IP-Protokollsuite als auch das NWLink IPX/SPX/NetBIOS-kompatible Transportprotokoll bereits vor den ersten, im vorhergehenden Abschnitt dieses Kapitels beschriebenen Schritten der Konfiguration von Routing und RAS installiert sind.

Wenn Sie mehrere Computer gleichzeitig verwalten möchten, können Sie dies tun, indem Sie mit der rechten Maustaste ganz oben in der Struktur auf das Symbol **Routing und RAS** klicken. Daraufhin erscheint ein Dropdown-Menü.

Dieses Menü bietet Ihnen die Möglichkeit, einen neuen Server hinzuzufügen. Dazu benötigen Sie natürlich für diesen anderen Computer die entsprechenden Rechte als Administrator. Auf diesem Server muss ebenfalls der Routing- und RAS-Dienst ausgeführt werden, bevor Sie den Server hinzufügen können. Um einen neuen Server hinzuzufügen, klicken Sie auf die Option **Server hinzufügen**. Nun öffnet sich das Dialogfeld **Server hinzufügen** (siehe Abbildung 14.36).

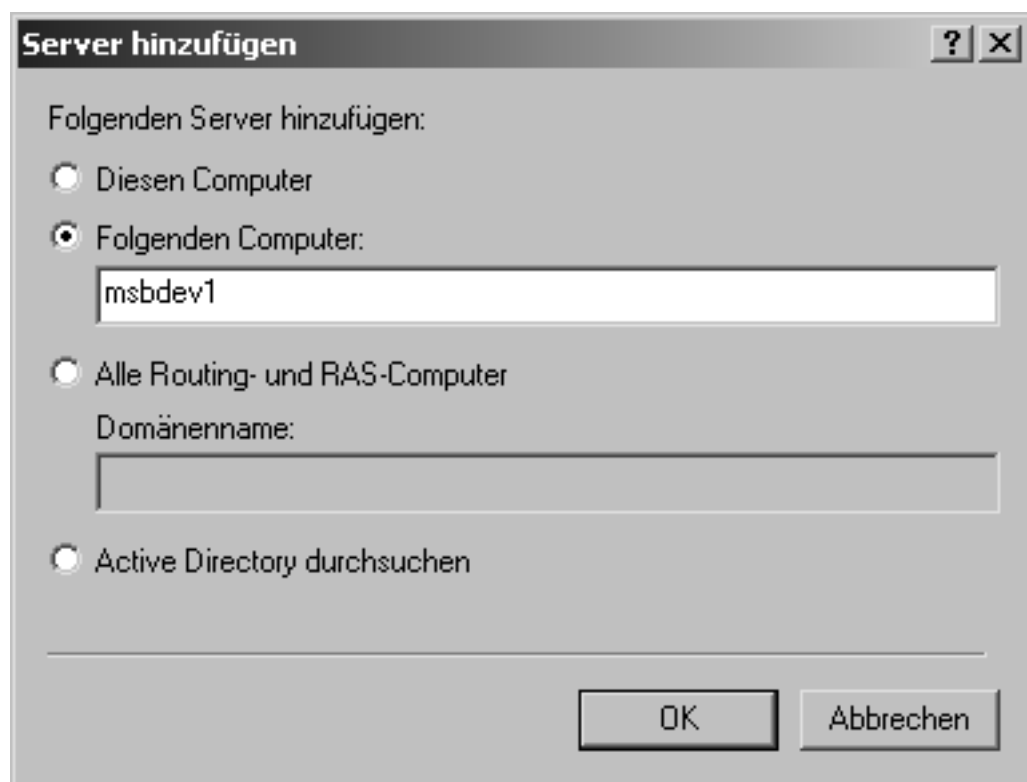


Abbildung 14.36: Hinzufügen eines neuen Servers

Im Dialogfeld **Server hinzufügen** stehen Ihnen einige Optionen zur Verfügung:

- **Diesen Computer:** Wählen Sie diese Option, wenn Sie den RAS-Dienst noch nicht konfiguriert haben.
- **Folgenden Computer:** Geben Sie den Computernamen des anderen Systems ein, das Sie verwalten möchten, vorausgesetzt, es besteht eine schnelle LAN- oder WAN-Verbindung zu diesem Computer. (Langsame DFÜ-Verbindungen zu anderen Computern eignen sich nicht für Routing- und RAS-Verwaltungsaufgaben.)
- **Alle Routing- und RAS-Computer:** Wenn Sie hier den Namen der Domäne eingeben, in der sämtliche von Ihnen gewünschten Routing- und RAS-Computer enthalten sind, erscheint jeder dieser Computer automatisch in Ihrer Verwaltungsliste. (Das ist wesentlich einfacher, als die Computer einzeln über die Option **Diesen Computer** auszuwählen.)
- **Active Directory durchsuchen:** Sie sollten diese Option wählen, wenn die Active Directory-Technologie für Ihre Umgebung bereits installiert und konfiguriert ist und Sie über die erforderlichen Rechte verfügen, um das Active Directory nach Informationen durchsuchen zu können. Wie bei der Option **Folgenden Computer** können Sie auch hier im Active Directory nach einem bestimmten Computernamen suchen und dann nur diesen einen Computer angeben.

Wenn Sie den neuen Computer, den Sie verwalten möchten, gefunden haben, klicken Sie auf die Schaltfläche **OK**, um Ihre Wahl zu bestätigen. Damit gelangen Sie wieder zum Hauptfenster **Routing und RAS**. Im linken Bereich dieses Fensters wird nun der neue Computer angezeigt (siehe Abbildung 14.37).

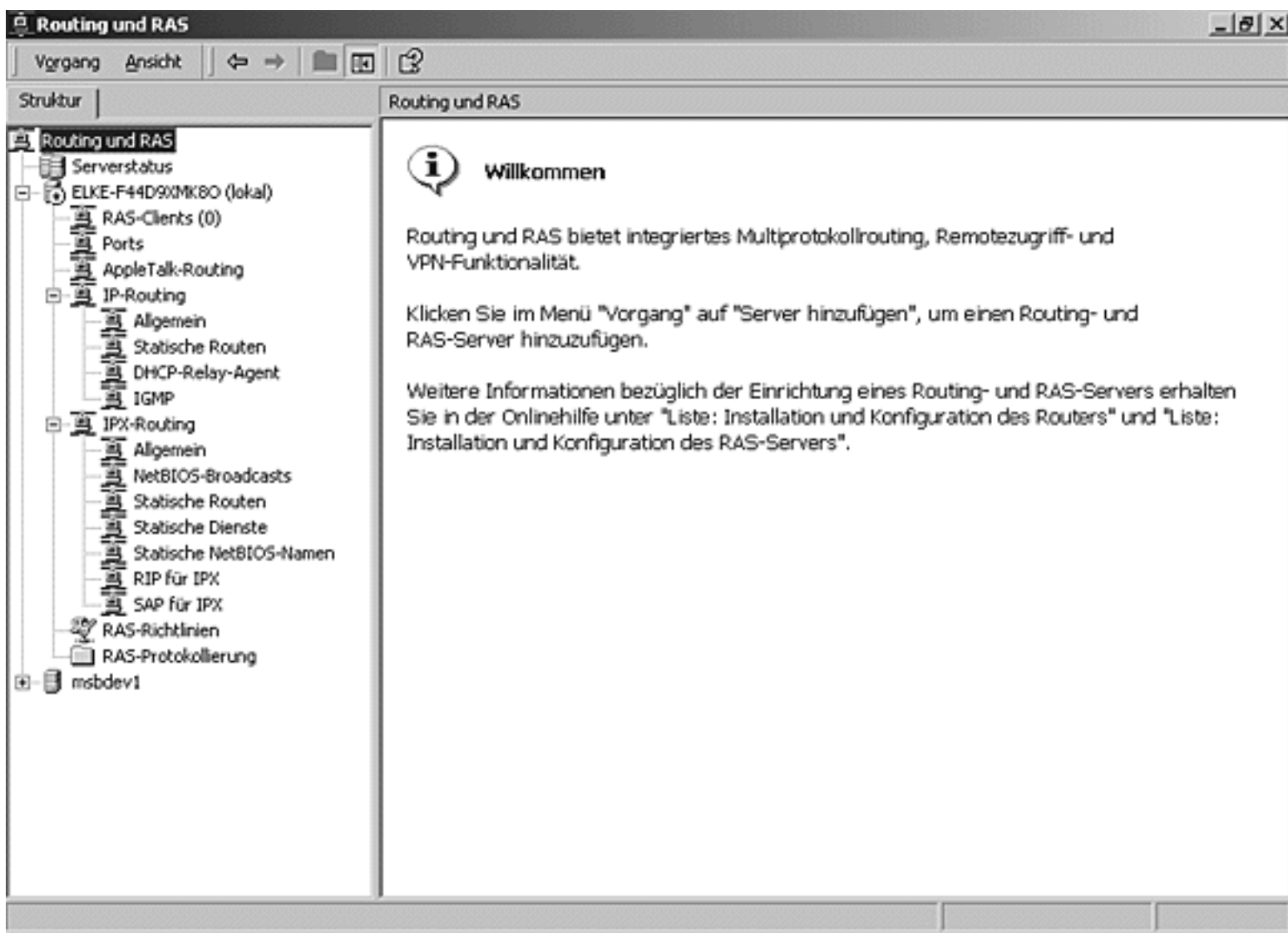


Abbildung 14.37: Anzeige aller für die Verwaltung verfügbaren Routing- und RAS-Server



Damit es einfacher ist, diesem Beispiel zu folgen, werden wir nur den lokalen Server für das Routing konfigurieren. Ein Remote-Server wird auf dieselbe Art und Weise konfiguriert. Aufgrund der Tatsache, dass der lokale Server bereits bekannt ist, sollte es einfacher sein, diesen Beispielen hier zu folgen.

Klicken Sie auf das in der Baumstruktur direkt unterhalb des Symbols **IP-Routing** befindliche Symbol **Allgemein** (siehe Abbildung 14.38).

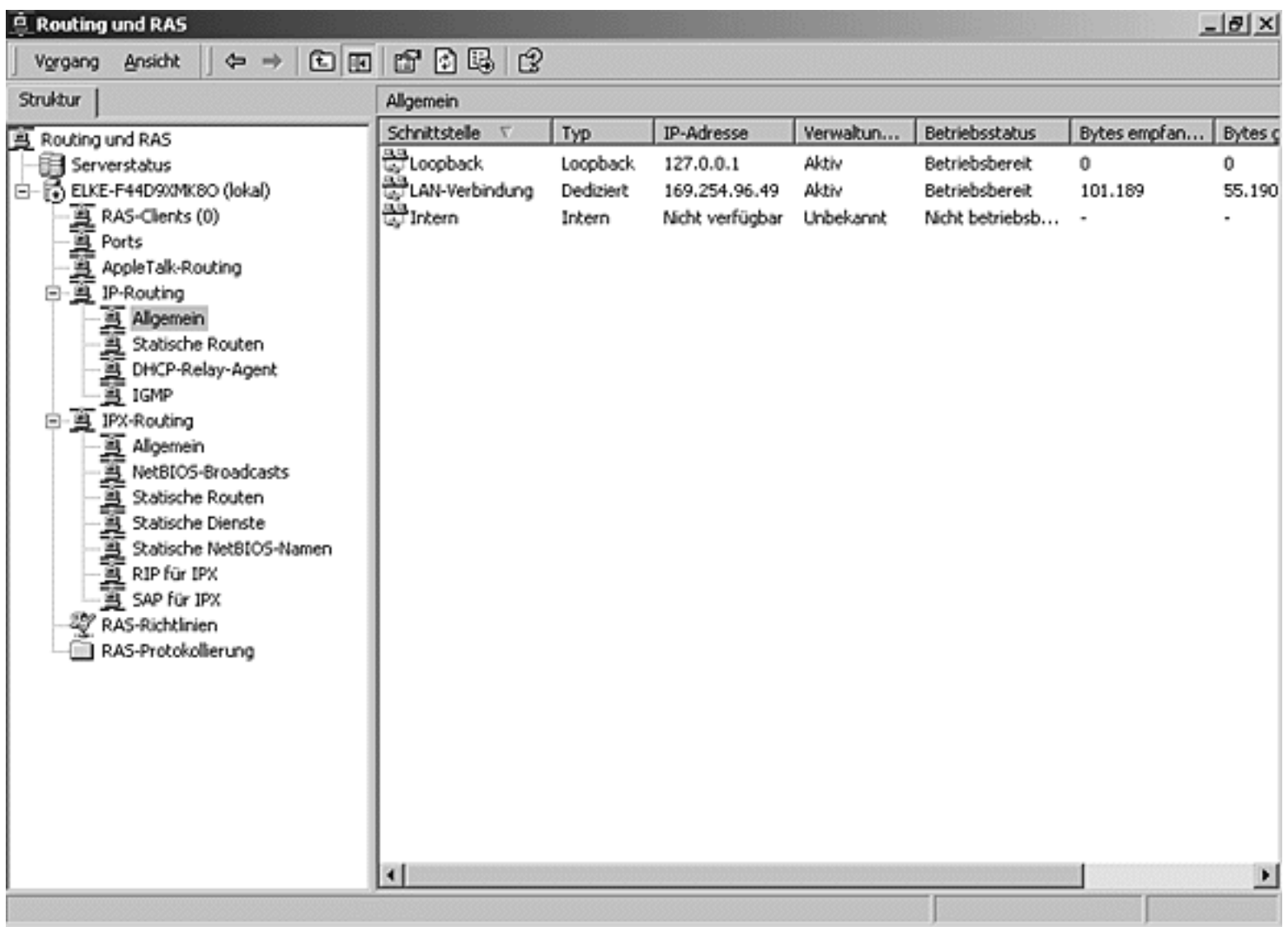


Abbildung 14.38: Allgemeine Angaben zum IP-Routing

Wenn Sie auf das Symbol **Allgemein** klicken, werden im rechten Bereich des Fensters unter der Spalte **Schnittstelle** einige Schnittstellen angegeben:

- Loopback
- LAN-Verbindung
- Intern

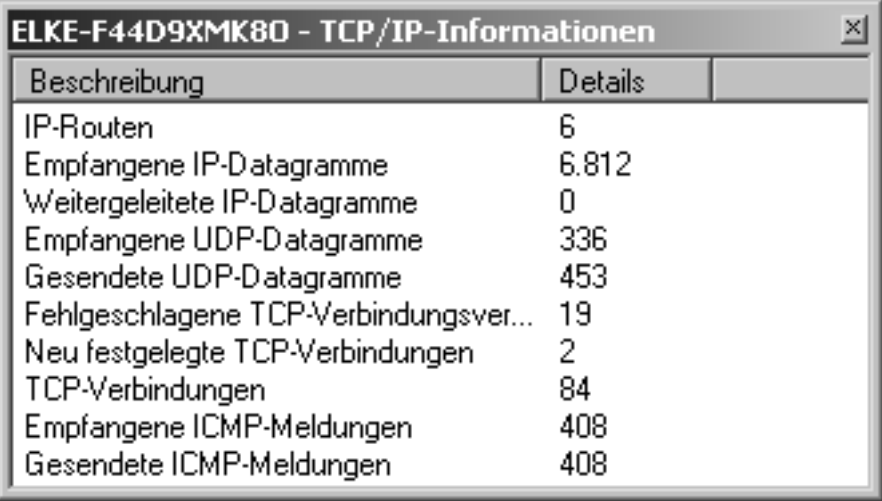
Diese Schnittstellen sind die in Ihrem Windows 2000-Server definierten Schnittstellen, die für das Routing konfiguriert werden können. Es ist zwar möglich, eine oder mehrere dieser Schnittstellen zu löschen. Dies sollten Sie jedoch nicht tun, wenn Sie beabsichtigen, die Routingfunktionen von Windows 2000 zu nutzen. Wenn Sie dennoch eine der Schnittstellen löschen möchten, klicken Sie mit der rechten Maustaste auf die entsprechende Schnittstelle. Daraufhin erscheint ein Dropdown-Menü, in dem Sie die Option **Löschen** wählen.

Wenn Sie mit der rechten Maustaste auf das Symbol **Allgemein** klicken, erscheint ein Menü mit mehreren Optionen:

- Neue Schnittstelle
- Neues Routingprotokoll

- TCP/IP-Informationen anzeigen
- Multicast-Weiterleitungstabelle anzeigen
- Multicast-Statistik anzeigen
- Ansicht
- Aktualisieren
- Liste exportieren
- Eigenschaften
- Hilfedatei anzeigen

Die meisten dieser Optionen erklären sich von selbst, einige bedürfen dagegen einer Erläuterung. Wenn Sie beispielsweise auf die Option **TCP/IP-Informationen anzeigen** geklickt haben, erscheint das in Abbildung 14.39 dargestellte Fenster.



Beschreibung	Details
IP-Routen	6
Empfangene IP-Datagramme	6.812
Weitergeleitete IP-Datagramme	0
Empfangene UDP-Datagramme	336
Gesendete UDP-Datagramme	453
Fehlgeschlagene TCP-Verbindungsver...	19
Neu festgelegte TCP-Verbindungen	2
TCP-Verbindungen	84
Empfangene ICMP-Meldungen	408
Gesendete ICMP-Meldungen	408

Abbildung 14.39: TCP/ IP-Informationen für den Computer ELKE-F44D9XMK80

In der Spalte **Beschreibung** werden Informationen über die unterschiedlichen Komponenten der TCP/IP-Protokollsuite wie z.B. TCP, IP und ICMP angezeigt. Sie verwenden ein Fenster wie dieses wie eine Art vorbeugende Maßnahme (Sie stellen vielleicht ein Problem fest, dass z.B. immer mehr TCP-Zugriffsversuche fehlschlagen) oder um ein mögliches Routingproblem mit Ihrem Windows 2000-Server zu diagnostizieren.

Wenn Sie andere Optionen wie z.B. die Option **Multicast-Weiterleitungstabelle anzeigen** wählen, erscheint ein leeres Fenster.

Das geschieht deshalb, weil das Multicastrouting auf Ihrem Windows 2000-Server noch nicht installiert bzw. konfiguriert worden ist. Das Fehlen von Statistiken ist kein Grund zur Sorge, außer Sie haben das Multicastrouting für Ihren Windows 2000-Server bereits konfiguriert. Wenn dies der Fall ist, dann machen Sie sich zu Recht Sorgen: Dann haben Sie ein Problem.

Wenn Sie die Option **Eigenschaften** wählen, öffnet sich das Dialogfeld **Eigenschaften von Allgemein** für das IP-Routing auf Ihrem Server, von wo aus Sie mit der Konfiguration beginnen. Wenn sich das Dialogfeld öffnet, liegt die Registerkarte **Allgemein** ganz oben (siehe Abbildung 14.40).



Abbildung 14.40: Optionen für die Ereignisprotokollierung für das IP-Routing

Auf der Registerkarte **Allgemein** können Sie die unterschiedlichen Optionen für das auf Ihrem Server ausgeführte IP-Routing definieren. Nachdem Sie eine Protokollierungsstufe für den betreffenden Server festgelegt haben, klicken Sie auf den Reiter der Registerkarte **Vorrangsstufen**, um die in Abbildung 14.41 dargestellte Registerkarte aufzurufen.

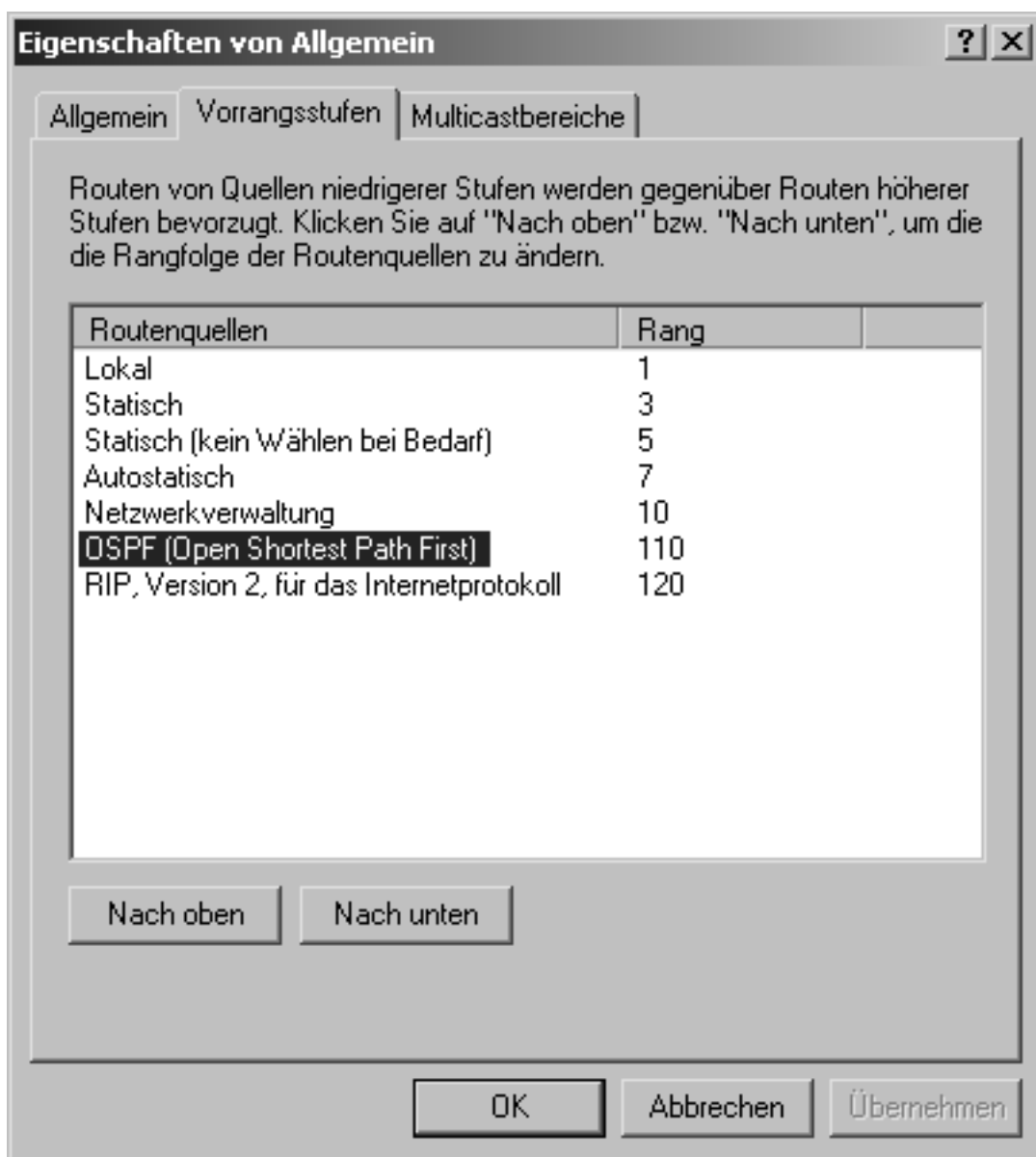


Abbildung 14.41: Festlegen der Vorrangstufe

Die Registerkarte **Vorrangstufen** wird verwendet, um die Rangfolge der unterschiedlichen, für Ihren Server möglichen Routen festzulegen. Um die Rangfolge für eine bestimmte Routenquelle zu ändern, klicken Sie zuerst auf die entsprechende Routenquelle und dann entweder auf die Schaltfläche **Nach oben** oder auf die Schaltfläche **Nach unten**.

Dadurch wird die entsprechende Routenquelle in der Rangfolge um eine Position nach oben bzw. nach unten verschoben. Klicken Sie auf den Reiter der in Abbildung 14.42 dargestellten Registerkarte **Multicastbereiche**, um diese Registerkarte aufzurufen.



Abbildung 14.42: Die Registerkarte Multicastbereiche

Wenn Sie diese Registerkarte zum ersten Mal aufrufen, ist sie noch leer. Um in der Konfiguration des IP-Routing Multicastbereiche hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen**. Daraufhin erscheint das in Abbildung 14.43 dargestellte Dialogfeld **Bereichsgrenze hinzufügen**.

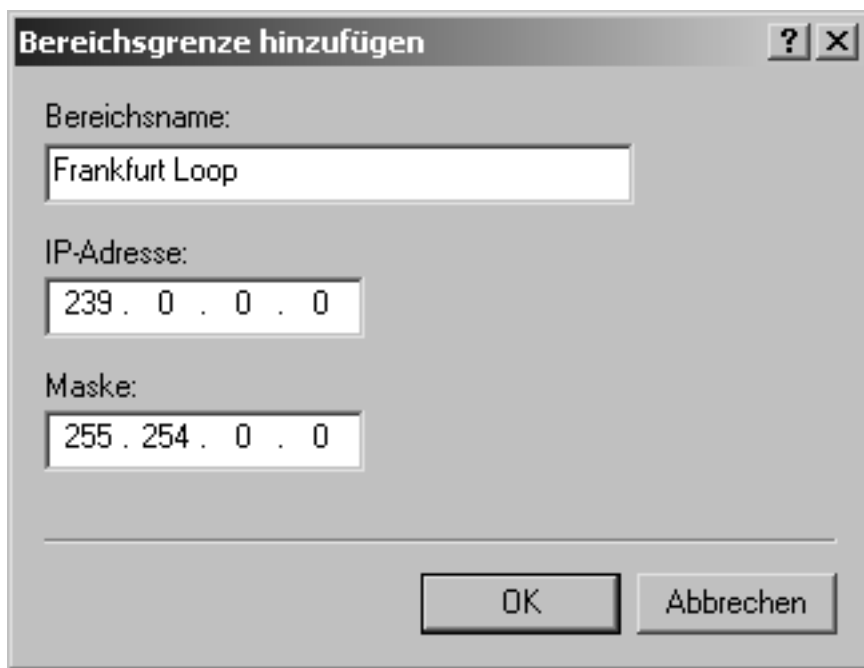


Abbildung 14.43: Hinzufügen einer Bereichsgrenze

Im Dialogfeld **Bereichsgrenze hinzufügen** müssen Sie drei Eintragungen vornehmen:

- Bereichsname
- IP-Adresse
- Maske

Diese Einträge sind für Ihre Bereichsgrenze erforderlich, die eine gültige IP-Adresse und Subnetzmaske für den TCP/IP-Adressbereich für Ihren Computer enthalten muss (versuchen Sie beispielsweise nicht, eine Adresse und eine Maske zu verwenden, die unterhalb der hier angezeigten Adresse bzw. Maske liegen, wenn Ihr Computer eine IP-Adresse der Klasse A haben soll).



Wenn Sie nicht wissen, wie ein Bereich von TCP/IP-Adressen mit den dazugehörigen Subnetzmasken richtig erstellt wird, sollten Sie in diesem Bereich von Windows 2000 Server keine Experimente wagen.

Klicken Sie auf die Schaltfläche OK, um wieder zur Registerkarte **Multicastbereiche** zurückzukehren (siehe Abbildung 14.44).



Abbildung 14.44: Ihr neu erstellter Multicastbereich wird angezeigt.

Sie sollten nun auf dieser Registerkarte den neu erstellen Multicastbereich sehen. Wenn nicht, dann sollte eine Fehlermeldung erschienen sein, die Ihnen mitgeteilt hat, was Sie falsch gemacht haben (sehr wahrscheinlich haben Sie eine falsche Bereichsadresse eingegeben). Wenn Sie alle Bereiche erstellt und die Einstellungen auf den anderen Registerkarten vorgenommen haben, klicken Sie auf **OK**, um die Einstellungen zu speichern und zum Hauptfenster **Routing und RAS** zurückzukehren.

Hinzufügen eines neuen Routingprotokolls

Als Nächstes möchten Sie vielleicht ein neues Routingprotokoll zu Ihrer Routing- und RAS-Konfiguration hinzufügen. Klicken Sie dazu auf die Option **Neues Routingprotokoll**.

Im Dialogfeld **Neues Routingprotokoll** können Sie ein neues Routingprotokoll hinzufügen, indem Sie zuerst auf das Protokoll, das Sie hinzufügen möchten, und dann auf die Schaltfläche **OK** klicken. Daraufhin erscheint wieder das Hauptfenster **Routing und RAS** mit dem neuen Protokoll. Von hier aus können Sie das Dialogfeld **Eigenschaften** für die einzelnen Protokolle aufrufen und gegebenenfalls Änderungen an der Konfiguration dieser Protokolle vornehmen.

Klicken Sie als Nächstes auf das Symbol **Statische Routen**. Daraufhin erscheint das in Abbildung 14.45 dargestellte Fenster.

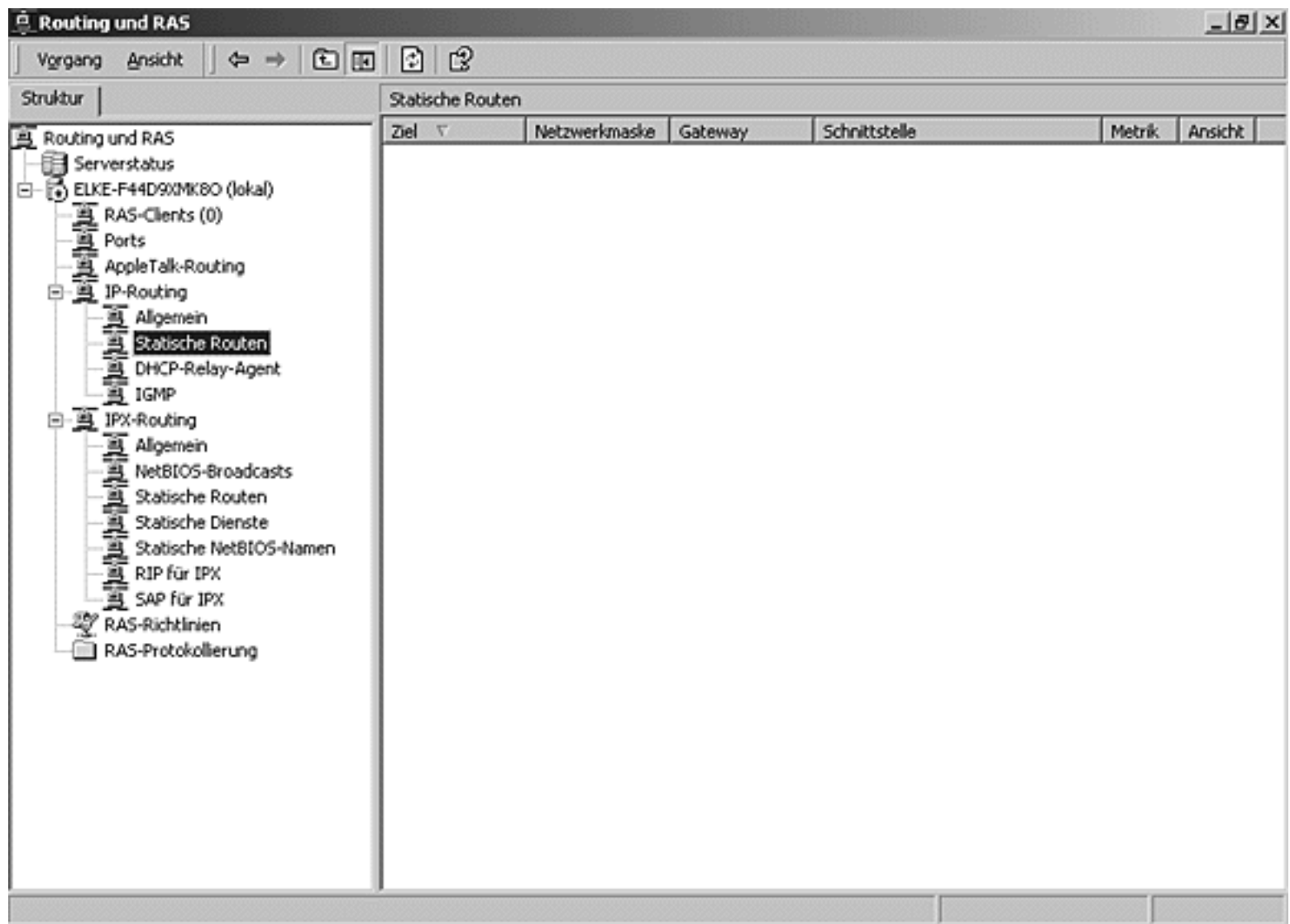


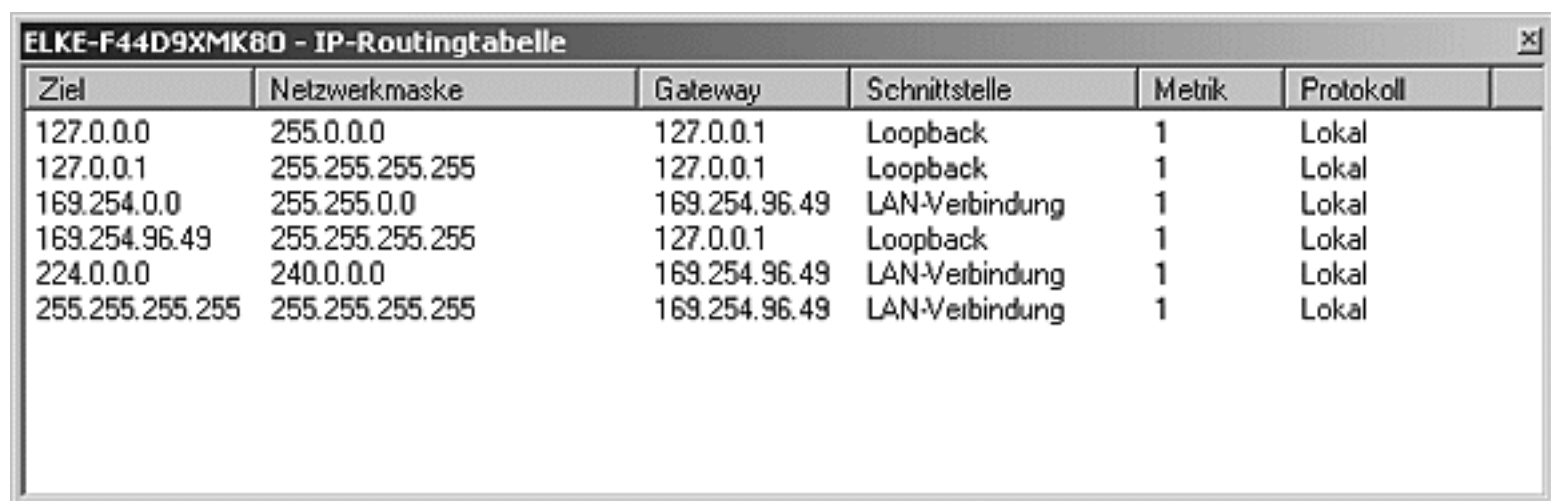
Abbildung 14.45: Anzeige von statischen Routen (falls vorhanden)

Wie Sie feststellen werden, sind für Ihren Computer keine statischen Routen konfiguriert. Sie können rasch eine statische Route hinzufügen, indem Sie mit der rechten Maustaste auf das Symbol **Statische Routen** klicken. Klicken Sie in dem daraufhin erscheinenden Dropdown-Menü auf die Option **Neue Statische Route**. Daraufhin erscheint das Dialogfeld **Statische Route**.

Sie verwenden das Dialogfeld **Statische Route**, um zur Routing- und RAS-Umgebung Ihres Servers eine neue statische IP-Route hinzuzufügen. Sie müssen die Zielinformationen, eine Netzwerkmaske, die TCP/IP-Adresse des Gateway und die zu verwendende Stufe der Metrik eingeben. Möglicherweise können Sie auch festlegen, ob diese neue Route für bei Bedarf herzustellende Wählverbindungen verwendet werden soll. Wenn Sie das Kontrollkästchen **Bei Bedarf herzustellende Wählverbindungen über diese Route initiieren** aktivieren bzw. deaktivieren können, dann aktivieren bzw. deaktivieren Sie dieses Kontrollkästchen entsprechend der Anforderungen Ihrer Routingumgebung. Im Feld **Ziel** geben Sie den Host bzw. die IP- oder Subnetzadresse oder aber Informationen über die Standardroute ein. Die Netzwerkmaske muss zur Adresse Ihres Ziels passen, d.h. wenn Sie beispielsweise als Zieladresse

255 . 255 . 255 . 255 angeben, dann muss die Netzwerkmaske 0 . 0 . 0 . 0 sein. Eine IP-Adresse für das Gateway muss dann angegeben werden, wenn es sich um eine LAN-basierte Routingschnittstelle handelt. Beim Routing für Wählen bei Bedarf bleibt das Feld **Gateway** dagegen leer. Im Feld **Metrik** geben Sie die Anzahl der Hops ein, die zwischen dem Server und dem Ziel liegen. Diese Einstellung wird für die Metrik verwendet, mit der die beste Route festgelegt wird. Sie können eine Zahl eingeben, indem Sie auf den nach unten bzw. auf den nach oben zeigenden Pfeil neben diesem Feld klicken. Klicken Sie anschließend auf die Schaltfläche **OK**, um die neue Route zu speichern und zum Hauptfenster **Routing und RAS** zurückzukehren.

Die andere Option, die sich auf statische Routen bezieht und in dem Menü aufgeführt wird, das erscheint, wenn Sie mit der rechten Maustaste auf das Symbol **Statische Routen** klicken, ist die Option **IP-Routingtabelle anzeigen**. Wenn Sie auf diese Option klicken, erscheint das in Abbildung 14.46 dargestellte Fenster.



Ziel	Netzwerkmaske	Gateway	Schnittstelle	Metrik	Protokoll
127.0.0.0	255.0.0.0	127.0.0.1	Loopback	1	Lokal
127.0.0.1	255.255.255.255	127.0.0.1	Loopback	1	Lokal
169.254.0.0	255.255.0.0	169.254.96.49	LAN-Verbindung	1	Lokal
169.254.96.49	255.255.255.255	127.0.0.1	Loopback	1	Lokal
224.0.0.0	240.0.0.0	169.254.96.49	LAN-Verbindung	1	Lokal
255.255.255.255	255.255.255.255	169.254.96.49	LAN-Verbindung	1	Lokal

Abbildung 14.46: Die IP-Routingtabelle für den Server ELKE-F44D9XMK80

Die hier angezeigten Informationen sollten Ihnen bekannt vorkommen, da sie den Informationen sehr ähnlich sind, die angezeigt werden, wenn Sie bei der Eingabeaufforderung von Windows 2000 den Befehl `Print Route` eingeben.

Das nächste IP-Routingprotokoll, das im linken Bereich des Fensters angezeigt wird, ist das Protokoll IGMP. Das Routingprotokoll IGMP (Internet Group Management Protocol) wird verwendet, um Gruppeninformationen zwischen potenziellen Gruppenmitgliedern innerhalb des IP-Adressenbereichs der Klasse D (d.h. Multicastziele) zu übertragen. Es wird hier als ein Beispiel dafür verwendet, um Ihnen zu zeigen, wo die unterschiedlichen Routingprotokolle erscheinen, wenn Sie diese in der IP-Routingstruktur hinzufügen, nämlich direkt unterhalb des Symbols **Statische Routen**.

Wenn Sie mit der rechten Maustaste auf das Symbol **Allgemein** klicken und dann die Option **Neue Schnittstelle** wählen, kann es vorkommen, dass eine Fehlermeldung erscheint (siehe Abbildung 14.47).



Abbildung 14.47: Eine IP-Routing-Fehlermeldung

Fehlermeldungen wie diese erscheinen immer dann, wenn Sie versuchen, eine Routingfunktion auszuführen, die die Möglichkeiten der Windows 2000 Server-Umgebung übersteigt. Das bedeutet nicht, dass das immer so ist. Es kann jedoch vorkommen, wenn Sie eine Änderung in Ihrer Computerumgebung vorgenommen haben. Aus diesem Grund sollten Sie jede Änderung statt auf Ihren Produktionssystemen zuerst in einer simulierten Entwicklungsumgebung testen.



Routingkonfigurationen bilden die Basis jedes Netzwerks innerhalb einer Organisation sowie zwischen Organisationen (wie z.B. bei Internetverbindungen). Aus diesem Grund sollten Sie wirklich jede Änderung an der Konfiguration in einer reinen Testumgebung und nicht in einer Produktionsumgebung testen. Wenn Sie dies nicht tun, kann es zum Verlust von Daten, einem Absinken der Produktivität und zu einer Vergeudung von Ressourcen kommen, von der Möglichkeit des Ausfalls eines (.com-)Unternehmens ganz zu schweigen.

Wenn Sie unterschiedliche Arten von Informationen bezüglich Ihrer Routingschnittstellen wie z.B. die allgemeinen Loopback- und LAN-Verbindungen sowie sämtliche statischen Routen anzeigen möchten, müssen Sie lediglich mit der rechten Maustaste im rechten Bereich des Fensters auf die entsprechende Option klicken. Daraufhin erscheint das in Abbildung 14.48 dargestellte Menü.

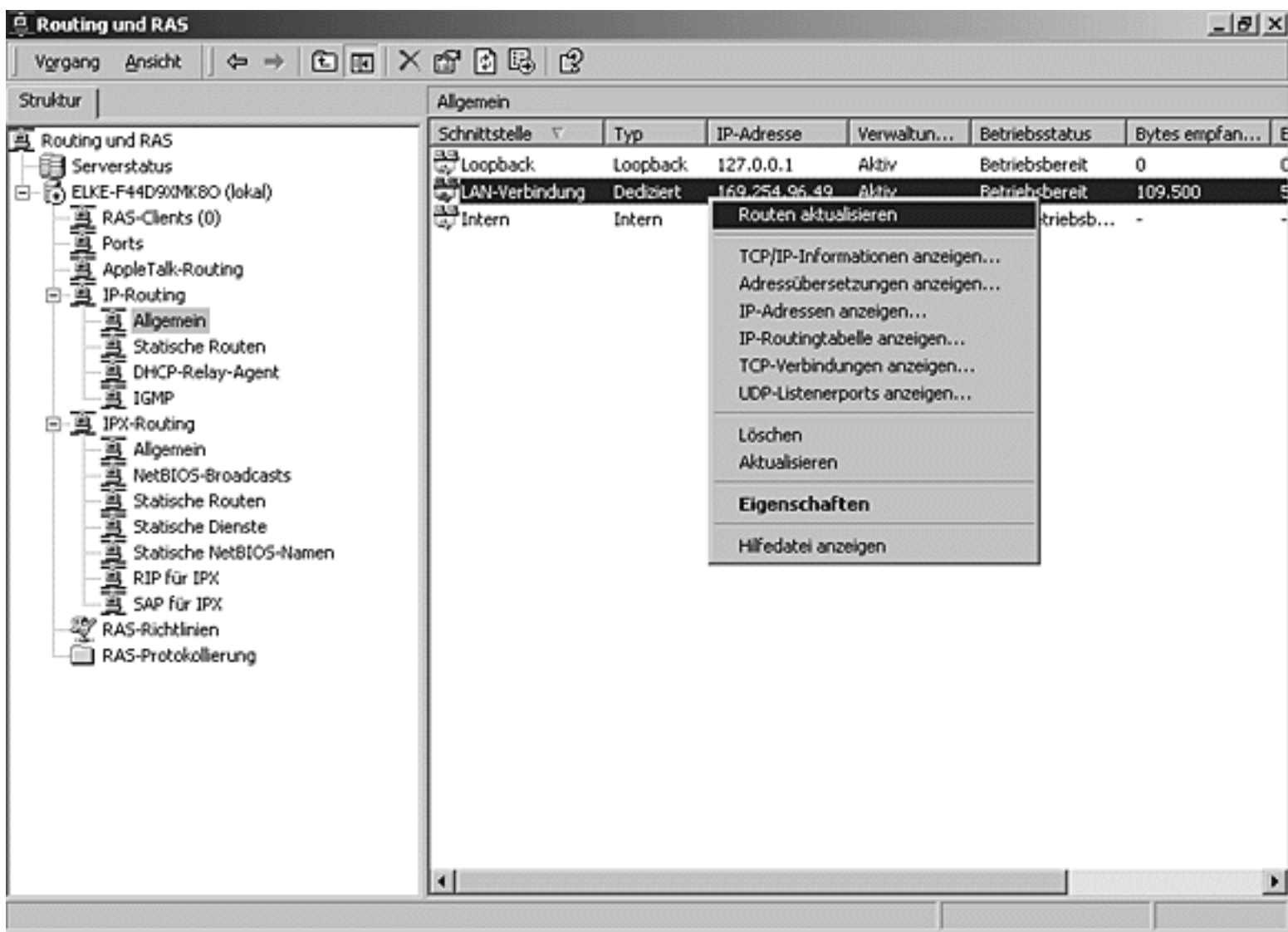


Abbildung 14.48: Potenzielle Informationen über die Konfiguration des IP-Routing

Darüber hinaus können Sie bei einigen der im rechten Bereich des Fensters angezeigten Routingschnittstellen die unterschiedlichen Eigenschaften aktualisieren oder ändern. Die Dialogfelder für die Konfiguration der Routingprotokolle sind bei allen Protokollen ähnlich. Sehen Sie sich beispielsweise den in Abbildung 14.49 dargestellten Bereich für das IPX-Routing an.

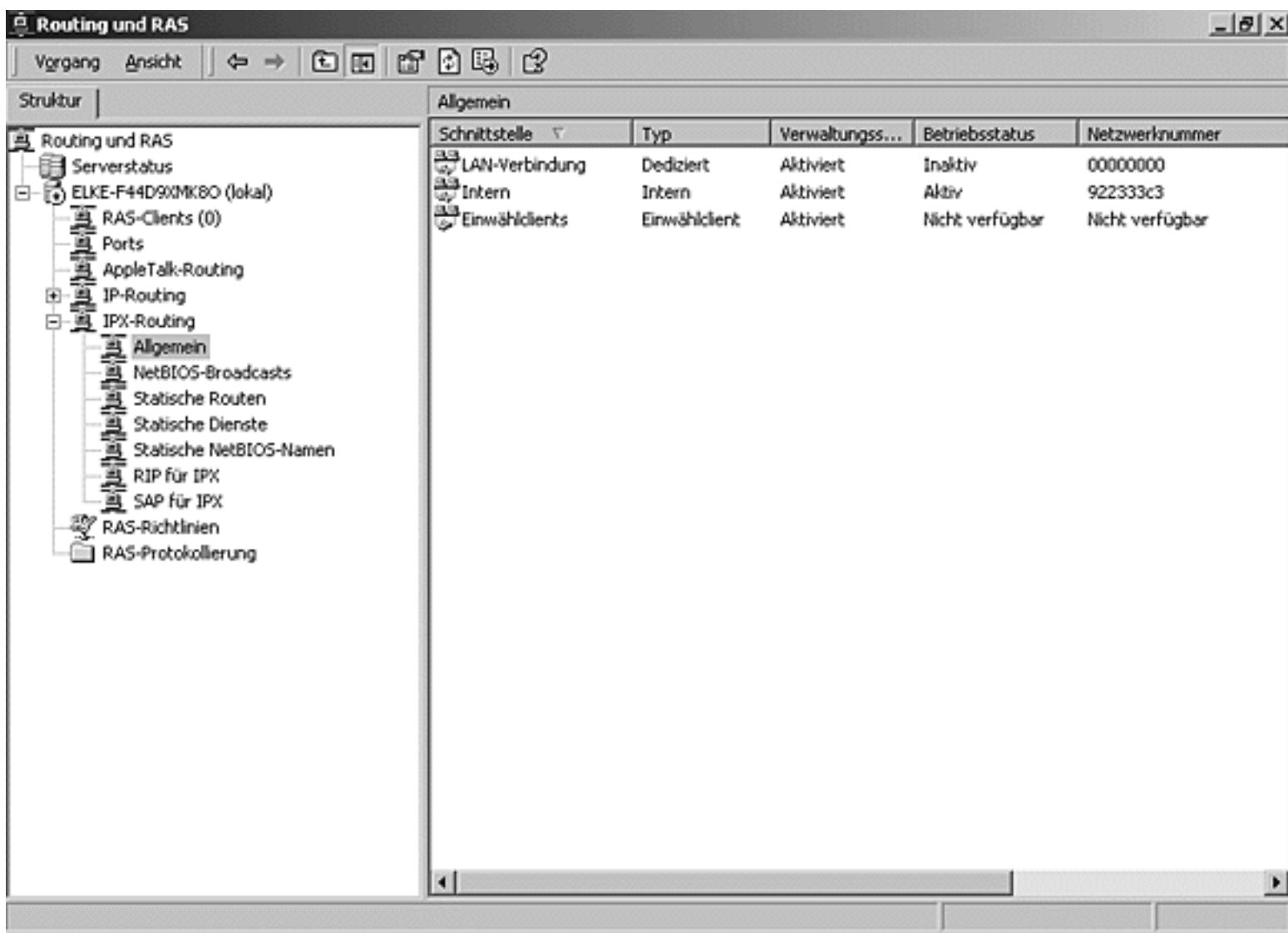


Abbildung 14.49: Allgemeine Informationen über das IPX-Routing

Wie Sie sehen, wird in der Struktur unterhalb des Symbols **IPX-Routing** als Erstes das Symbol **Allgemein** angezeigt. Diesem Symbol folgen die Symbole **NetBIOS-Broadcasts** sowie die unterschiedlichen Symbole für die statischen Routen. Diese Struktur unterscheidet sich also kaum von der des IP-Routing.

Es gibt jedoch leider Tausende von unterschiedlichen Routingkonfigurationen. Es würde den Rahmen dieses Buches bei weitem sprengen, wenn diese hier alle erläutert würden. Es soll hier lediglich darauf hingewiesen werden, wo und wie diese Einstellungen konfiguriert werden können. Wenn Sie sich nur an Routing und RAS erinnern, haben Sie schon die halbe Miete.

14.4.4 Protokollunterstützung

Routing und RAS unterstützt viele Protokolle. Das ermöglicht ein Multiprotokollrouting. Was in Organisationen recht praktisch ist, in denen mit mehreren Protokollen gleichzeitig gearbeitet wird. Mit Hilfe der Multiprotokollunterstützung von Windows 2000 Server können Sie Server so konfigurieren, dass diese eine große Vielzahl von Netzwerkprotokollen wie z.B. TCP/IP, NetBEUI, IPX/SPX und AppleTalk unterstützen. Routing- und RAS-Server, die diese vielen Protokolle unterstützen, können

innerhalb der entmilitarisierten Zone der Organisation installiert werden. Dadurch kann sichergestellt werden, dass ein Netzwerkprotokoll innerhalb des Unternehmens und ein anderes Protokoll außerhalb des Unternehmens verwendet wird (das war früher ein Schutzmechanismus für Netzwerke, der in der heutigen Internet-fähigen Welt nur noch für kleine Arbeitsgruppen empfohlen werden kann).

Eine weitere Eigenschaft der Protokollunterstützung ist unter der Bezeichnung *Multihoming* bekannt. Dabei geht es darum, einen Windows 2000-Server so zu konfigurieren, dass er über mehrere TCP/IP-Adressen verfügt. Multihoming wird innerhalb von Windows 2000 Server auf unterschiedliche Arten unterstützt. Die am weitesten verbreitete Art und Weise besteht in der Zuweisung mehrerer IP-Adressen für eine einzelne Netzwerkkarte. Der Grund dafür, warum das für Sie als Netzwerkadministrator nützlich sein kann, ist der, dass Sie damit statische Routen konfigurieren können, um so Netzwerke miteinander zu verbinden, die Sie sonst nicht miteinander verbinden könnten. Wenn Sie beispielsweise einige ungleiche Netzwerke haben, die Sie miteinander verbinden möchten, können Sie dies tun, wenn Sie die Unterstützung des Multihoming von Windows 2000 Server nutzen.

14.4.5 Modem

Windows 2000 Server unterstützt zwar viele unterschiedliche Modems, sowohl digitale als auch analoge, aber es ist wichtig, dass Sie darauf achten, dass die Geräte vollständig kompatibel zur Windows 2000 Server-Umgebung sind. Wie in diesem Kapitel bereits erwähnt, sollten Sie in der Hardwarekompatibilitätsliste von Microsoft nachsehen, ob Ihr Gerät geeignet ist. Wenn Sie Ihre Hardware prüfen, bevor Sie sie installieren, können Sie Probleme vermeiden, die Sie ansonsten mit Sicherheit bekommen werden.

Wenn Sie beabsichtigen, für Ihre RAS-Benutzer einen Modempool einzurichten, sollten Sie sich für eine Erweiterungsausrüstung für COM-Anschlüsse von einem namhaften Hersteller entscheiden. Damit ist es einfacher, diese Anschlüsse über den RAS-Bereich von Windows 2000 Server zu konfigurieren. Wenn Sie für Ihre RAS-Verbindungen Smartcards verwenden, sollten Sie vor dem Kauf der Ausrüstung, die Sie verwenden möchten, ebenfalls darauf achten, dass diese vollständig zu Windows 2000 Server kompatibel ist.

Auf der Seite der Software sollten Sie darauf achten, dass Sie sämtliche Einwähl- und RAS-Richtlinien sowie die Optionen für die RAS-Protokollierung richtig konfiguriert haben. Damit können Sie Ihre RAS-Implementierungen, insbesondere die, die nationale oder gar internationale Grenzen überschreiten, besser überwachen.

14.4.6 Unterstützen von WANs

Weitbereichsnetze werden von einem Windows 2000-Server auf viele unterschiedliche Arten unterstützt. Der Routing- und RAS-Dienst von Windows 2000 bietet Routingdienste für virtuelle private Netzwerke unter Verwendung mehrerer Protokolle, LAN-zu-LAN- und LAN-zu-WAN-Verbindungen sowie Netzwerkadressübersetzung (NAT). All diese Dienste können entweder lokal über das Fenster **Routing und RAS** oder im WAN über dasselbe Fenster konfiguriert werden. Darüber hinaus können mit Windows 2000 Server die verwendeten Protokolle wie z.B. TCP/IP, IPX/SPX und AppleTalk problemlos hinzugefügt, geändert und gelöscht werden. Des Weiteren kann ein Windows 2000-Server, auf dem der RAS-Dienst aktiviert ist, in einer SNMP-Umgebung (Simple Network Management Protocol) als SNMP-Agent teilnehmen.

Eine weitere nützliche Eigenschaft der Unterstützung von WANs durch Windows 2000 Server ist die der Verbindungsfreigabe. Mit Hilfe der Verbindungsfreigabe kann in einem kleineren Netzwerk eine einzelne WAN-Verbindung, üblicherweise zum Internet, freigegeben und gemeinsam genutzt werden. Ein Windows 2000-Server, der eine freigegebene WAN-Verbindung zur Verfügung stellt, fungiert als NAT (Netzwerkadressübersetzer), ein vereinfachter DHCP-Server, und als ein Microsoft DNS- und/oder WINS-Server, wodurch die Kosten für derartige Verbindungen gesenkt werden. Wenn Sie die Funktion der Verbindungsfreigabe für Ihre LAN- bzw. WAN-Umgebung nutzen möchten, stehen Ihnen zwei Arten der Verbindung zur Verfügung:

- Übersetzt: Das übersetzte Verfahren ist das bei weitem beste Verfahren, da es dem Netzwerk aufgrund der Fähigkeit, dieses vom Internet oder dem anderen WAN mit Hilfe von NAT abzusichern, eine zusätzliche Sicherheitsstufe bietet.
- Geroutet: Mit dem gerouteten Verfahren werden lediglich Datenpakete von Ihrem Netzwerk zum anderen WAN oder zum Internet geroutet. Das bedeutet, Ihr Netzwerk ist nicht besonders sicher.

Unabhängig davon, welche Art der Verbindung Sie wählen, sollten Sie daran denken, dass sich die Technologie der Verbindungsfreigabe nur dafür eignet, ein kleines internes Netzwerk mit einem größeren WAN wie z.B. dem Internet zu verbinden. Diese Technologie funktioniert zwischen zwei WANs nicht.

14.5 Authentifizierung

Die von Windows 2000 Server unterstützte Routing- und RAS-Authentifizierung wurde gegenüber der älteren von Windows NT Server 4 unterstützten RAS-Authentifizierung deutlich verbessert. Neben den Bereichen der einfachen Authentifizierung von Benutzername und Benutzerkennwort gab es nur wenig, das ein Netzwerkadministrator tun konnte, um den Horden der unberechtigten Benutzer, die versuchten, ein Netzwerk zu infiltrieren, Einhalt zu gebieten. Bei Windows 2000 Server stehen Ihnen nun mehrere Möglichkeiten, darunter die Authentifizierungsmethoden CHAP und SPAP/PAP zur Verfügung.

Erinnern Sie sich daran, als wir im Zusammenhang mit der Installation und Konfiguration des Routing- und RAS-Dienstes beschrieben haben, wie die für einen bestimmten Server verfügbaren Eigenschaften verwendet werden können und dann über die Registerkarte **Sicherheit** zum Bereich der Authentifizierungsmethoden gelangt sind? In diesem Bereich werden die unterschiedlichen Authentifizierungsmethoden für den Routing- und RAS-Dienst definiert. In demselben Bereich können Sie den Authentifizierungsanbieter für Ihre Routing- und RAS-Konfiguration angeben: entweder die Windows-Authentifizierung oder die RADIUS-Authentifizierung. Diese Authentifizierungsmethoden werden vom Routing- und RAS-Dienst verwendet, um festzulegen, wie die RAS- bzw. DFÜ-Authentifizierung geführt wird. Für die Windows-Authentifizierung werden die integrierten Sicherheitsfunktionen von Windows 2000 Server und/oder die Windows NT-Datenbank SAM (Security Accounts Manager) verwendet, um den Zugriff auf die Ressourcen Ihres Netzwerks zu überwachen. RADIUS-Authentifizierung bedeutet, dass der RAS-Dienst mit Hilfe eines RADIUS-Servers die Methode festlegt, mittels derer Router für Wählen bei Bedarf und der Remotezugriff Clients am Netzwerk authentifizieren.

Einer der wichtigsten Aspekte der Authentifizierung, den Sie nicht vergessen sollten, ist der, dass die Auswirkungen auf die Clients umso größer werden, je mehr Stufen der Authentifizierung Sie Ihren Benutzern auferlegen. Wenn Sie beispielsweise IPsec auf all Ihre RAS-Benutzer anwenden würden,

würden Sie einen sofortigen Anstieg der Netzwerklast um etwa 40 % für diese RAS-Benutzer feststellen können. Es gibt aber natürlich auch eine zweite Seite der Medaille. Je weniger Authentifizierungsstufen Sie implementieren und beispielsweise auf die Verwendung jeglicher Verschlüsselung verzichten und Kennwörter in Klartext zulassen, umso offener ist Ihr Netzwerk für nicht autorisierte Benutzer. Es geht darum, den goldenen Mittelweg für Ihre Organisation zu finden, um in diesen sich rasch ändernden Zeiten in einer ökonomischen Welt des Internet zu überleben.

14.6 Fehlersuche

Das Verfahren, mit dem eine RAS-Verbindung auf Fehler überprüft wird, ist theoretisch einfach, die Umsetzung in die Praxis ist dagegen ziemlich schwierig. Gleichgültig, für welches Verfahren Sie sich entscheiden, es sollte eines sein, das unabhängig von der jeweiligen Situation immer wiederholt wird. Der Grund dafür, warum Sie immer nur eine Fehlersuchmethode anwenden sollten, ist einfach: Der Prozess funktioniert besser, da Sie in der Lage sind, Fehler schneller zu finden (denn viele Fehler haben ähnliche Symptome und Ursachen). Die Strategie zur Fehlersuche und die Vorgehensweise sollten einfach zu befolgen sein und mindestens diese Schritte in dieser Reihenfolge beinhalten:

1. Dokumentieren Sie alles. Beginnen Sie eine Fehlersuche niemals ohne aufzuschreiben, was alles versucht wird, um das Problem zu beheben, da Sie sonst nach einer Weile beginnen, sich im Kreis zu drehen, ohne dies zu merken.
2. Diskutieren Sie den Fehler mit der Person, die den Fehler als Erste bemerkt hat, auch wenn diese Person keine technischen Kenntnisse hat. Hören Sie dieser Person sehr genau zu. Wenn Sie den Fehler entdeckt haben, dann schreiben Sie ausführlich auf, was Sie beobachtet haben, und lesen Sie dann nach, was Sie aufgeschrieben haben. Vielleicht fällt Ihnen etwas auf, das Sie nicht bemerkt haben, als Sie über den Fehler nachgedacht haben.
3. Achten Sie darauf, ob der Fehler reproduzierbar ist. Wenn er nicht reproduzierbar ist, dokumentieren Sie das Problem und verbuchen es unter der Kategorie »Ungelöst«. Vergeuden Sie keine Zeit und kostbare Unternehmensressourcen damit herumzuraten, was wohl schief gelaufen sein mag. Wenn ein Fehler nicht reproduzierbar ist, kann er nicht behoben werden.
4. Notieren Sie jeden einzelnen Schritt, der erforderlich ist, um den Fehler zu reproduzieren. Fertigen Sie (falls es welche gibt) von jeder Fehlermeldung eine Bildschirmabbildung und von den Dateien der Ereignisprotokolle von Dr. Watson und Windows 2000 eine Kopie an.
5. Sie sollten auf jeden Fall genau wissen, wann der Fehler zum ersten Mal aufgetreten ist und wie lange er schon vorliegt. Sie sollten außerdem wissen, was der Systemadministrator oder der Benutzer tat, als der Fehler zum ersten Mal auftrat (vorausgesetzt, es war ein Mensch, der den Fehler als Erster bemerkt hat, und nicht eine der Anmeldeeinheiten von Windows 2000).
6. Nachdem der Fehler behoben ist, sollten Sie in allen Einzelheiten aufschreiben, was getan wurde, um das Problem zu beheben und vielleicht was getan werden kann, damit das Problem in Zukunft nicht mehr auftritt. Speichern Sie dieses Dokument in elektronischer Form in einer Art Online-Datenbank oder auf einer Seite im Intranet, sodass andere Netzwerkadministratoren, auf derselben oder auf einer höheren Autoritätsstufe von den Problemen anderer in der Organisation lernen können.

Wenn Sie sich eine Strategie für die Fehlersuche zurecht gelegt haben, ist es an der Zeit, mit der eigentlichen Fehlersuche zu beginnen. Am besten beginnen Sie mit dem Ereignisprotokoll von Windows 2000, da hier sämtliche Warnmeldungen, Fehlermeldungen und allgemeine Daten bezüglich Ihrer

RAS-Umgebung, die über den Routing- und RAS-Dienst installiert und konfiguriert wurde, protokolliert werden. Eine weitere hervorragende Informationsquelle ist die PPP-Verfolgungsoption. Diese stellt eine Liste der Programmiermeldungen und PPP-Steuermeldungen zur Verfügung, die während einer PPP-Verbindung erstellt werden. Wenn etwas schief geht, ist es hilfreich, zumindest die Ereignisse direkt vor und während des Auftretens des jeweiligen Fehlers nachvollziehen zu können. Diese Protokolldatei finden Sie im Ordner %systemroot% Ihres Windows 2000-Servers. Um die PPP-Verfolgungsfunktion auf Konsolenebene zu aktivieren, müssen Sie Ihre Windows 2000 Server-Registrierung ändern, indem Sie den Wert des Eintrags *EnableConsoleTracing* in der Registrierung mit 1 definieren. Denken Sie daran, dass Sie diesen Eintrag vornehmen müssen, bevor Sie den Router starten. D.h. hierbei handelt es sich vielmehr um eine Vorbeugemaßnahme als um eine Fehlersuche. Nehmen Sie die entsprechende Änderung in der Windows 2000 Server-Registrierung im Bereich *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing* (z.B. *EnableConsoleTracing* REG_DWORD 1) vor.

Eine weitere hervorragende Möglichkeit, Problemen mit Routing- und RAS-Verbindungen auf die Spur zu kommen, stellt der Netzwerkmonitor dar. Mit diesem Programm können Sie den eigentlichen RAS-Verkehr analysieren. Das bedeutet, dass Sie vielleicht eine Lösung oder zumindest eine Möglichkeit finden können, wie das Problem umgangen werden kann. Denken Sie jedoch daran, dass der Netzwerkmonitor die Leistung Ihres Netzwerks erheblich beeinträchtigen kann. Überbeanspruchen Sie den Gebrauch des Netzwerkmonitors daher nicht und geben Sie auch nicht jedem die Möglichkeit, dieses Programm zu nutzen, da dies ein ernsthaftes Sicherheitsrisiko für Ihre Windows-Anwendungen darstellen kann. Wenn Sie mehr über dieses Programm wissen möchten, dann finden Sie im Windows 2000 Resource Kit nähere Informationen. Sie können aber auch jemanden fragen, der Erfahrung mit dem Microsoft Systems Management Server (SMS) hat. Eine vollständige Version des Netzwerkmonitors ist im BackOffice SMS-Produkt enthalten. Mit dieser Version können Sie nicht nur einen einzelnen Server, sondern das gesamte WAN »sehen«.

Kapitel 15 Multiprotokollumgebungen

Würde man sich bezüglich der Wahl unter den Protokollen für LAN-Verbindungen streiten, würde TCP/IP auf jeden Fall gewinnen. Es ist jedoch so, dass manchmal auch Verlierer ihre Existenzberechtigung haben. Kommunikationsprotokolle für LAN- und WAN-Verbindungen haben ihre Stärken und Schwächen wie alles andere beim Computer auch. IPX/SPX ist beispielsweise nicht weniger tot als der Macintosh-Computer. Beide werden jedoch immer weniger verwendet.

In diesem Kapitel soll nun nicht jedes einzelne Protokoll beschrieben werden. TCP/IP ist bei weitem mehr als ein »Standard«-Protokoll. Es ist nahe daran, ein »erforderliches« Protokoll zu sein. Jeder, der behauptet, Windows 2000 könne ohne TCP/IP ausgeführt werden, braucht sich nur die Verzweigungen von DNS und DHCP im Active Directory vor Augen zu führen.

Dieses Kapitel bietet eine kurze Beschreibung der in Windows 2000 integrierten Kommunikationsprotokolle sowie der technischen Gründe, die für deren Einsatz sprechen.

15.1 Protokolle, die Windows 2000 unterstützt

Windows 2000 unterstützt die Mehrzahl der Kommunikationsprotokolle nach Industriestandard. Nach über 20 Jahren der Computer-Netzwerke hat sich der Bereich der Protokolle etwas beruhigt. Von all den vielen Protokollen und Anbietern haben sich insgesamt fünf durchgesetzt.

Und das sind sie:

- *TCP/IP*. Transmission Control Protocol/Internet Protocol, vom amerikanischen Verteidigungsministerium für LAN/WAN-Verbindungen im ARPANET entwickelt.
- *IPX/SPX*. Internet Packet Exchange/Sequential Packet Exchange, von Novell für NetWare entwickelt.
- *AppleTalk*. Das von Apple entwickelte Protokoll für Verbindungen zwischen Macintosh-Computern und Apple-Peripheriegeräten.
- *DLC*. Data Link Control von Hewlett-Packard.
- *NetBEUI*. Der frühe Versuch eines auf NetBIOS (Network Basic Input/Output System) basierenden LAN-Protokolls von IBM und Microsoft.

15.1.1 Installieren eines neuen Protokolls

Alle hier aufgeführten Protokolle können in der Systemsteuerung über die Option **Netzwerk- und DFÜ-Verbindungen** (siehe Abbildung 15.1) installiert und konfiguriert werden. Eine großartige neue Funktion von Windows 2000 ist, dass neue Protokolle hinzugefügt und entfernt werden können, während der Server läuft. Das hört sich zunächst nicht besonders genial an. Wenn aber für eine Migration oder eine Übertragung vorübergehend ein anderes Protokoll verwendet werden soll, kann diese neue Funktion ein Segen sein.



Abbildung 15.1: Systemsteuerungsoption Netzwerk

Die Technologie, mit deren Hilfe Protokolle hinzugefügt, entfernt, beendet, gestartet oder gewechselt werden können, während der Server läuft, ist insbesondere bei der Fehlersuche sehr nützlich (siehe Abbildung 15.2). Es ist sehr schwierig, einem Problem mit einer Verbindung auf den Grund zu gehen, wenn man das System jedes Mal neu starten muss, sobald ein Protokoll hinzugefügt oder ein anderes Protokoll verwendet wird. Wenn der Server jede beliebige umfangreiche Anwendung ausführt, kann dies nahezu unmöglich sein. Ein Exchange- oder SQL Server-Rechner kann bis zu einer halben Stunde brauchen, um neu zu starten.

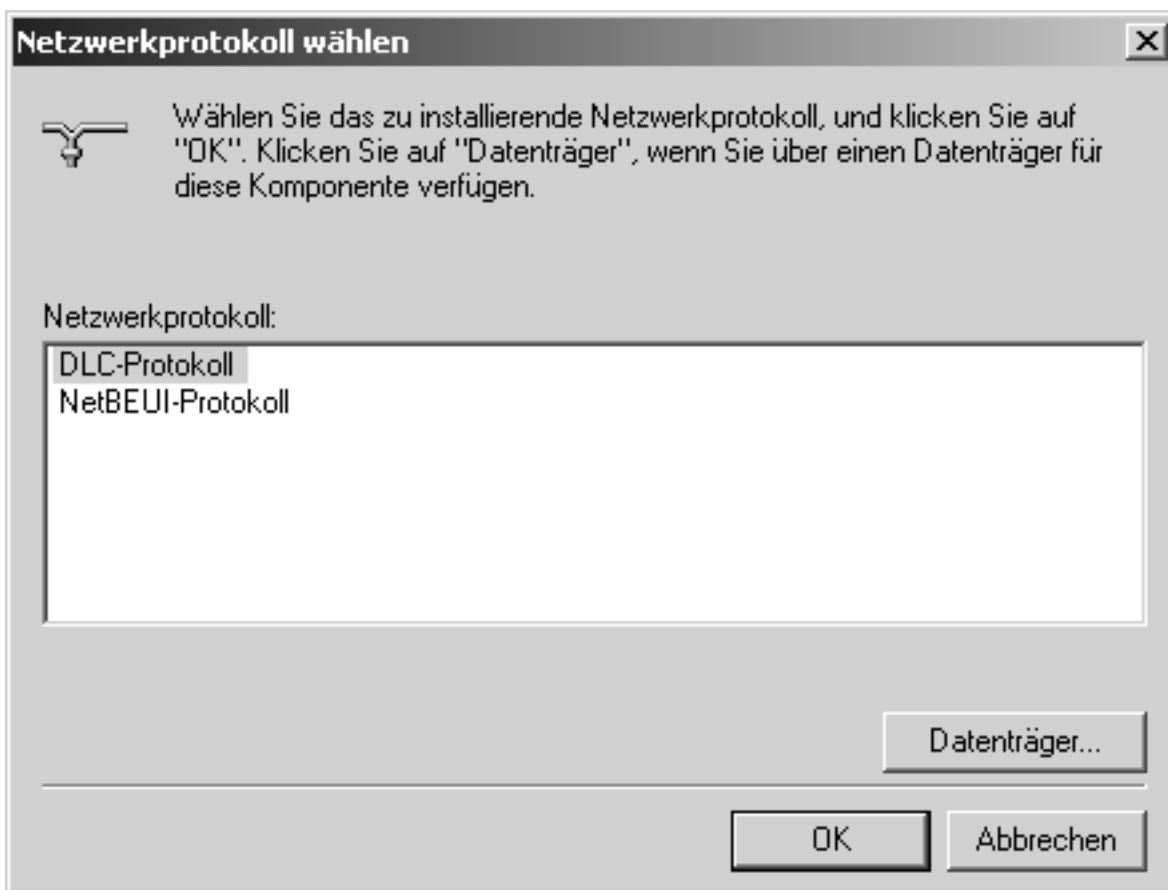


Abbildung 15.2: Das Dialogfeld für die Auswahl des Protokolls

Um ein neues Protokoll hinzuzufügen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Systemsteuerung die Option **Netzwerk- und DFÜ-Verbindungen**. Sie haben zwei Möglichkeiten, dies zu tun. Sie können entweder auf **Start/Einstellungen/Systemsteuerung** klicken und dann auf **Netzwerk- und DFÜ-Verbindungen** doppelklicken. Am einfachsten ist es aber, wenn Sie mit der rechten Maustaste auf **Netzwerkumgebung** klicken und dann die Option **Eigenschaften** wählen.
2. Klicken Sie anschließend mit der rechten Maustaste auf das Symbol der Netzwerkverbindung und wählen Sie im Kontextmenü die Option **Eigenschaften**.
3. Klicken Sie auf **Installieren**.
4. Klicken Sie auf **Protokoll** und dann auf **Hinzufügen**.



Wenn Ihnen diese Schnittstelle bekannt vorkommt, dann weil sie bekannt ist. Sie wurde entwickelt, um Windows ein einheitlicheres Aussehen zu geben, sodass man immer weiß, dass man sich in Windows befindet. Die neue Schnittstelle bei Windows 2000 sieht der alten von Windows 95/98 sehr ähnlich. Man wollte dadurch deren Verwendung vereinfachen.

5. Es wird die Liste der verfügbaren Protokolle angezeigt. Wenn Sie eines dieser Protokolle verwenden möchten, dann klicken Sie auf dieses Protokoll und dann auf **OK**. Wenn das Protokoll, das Sie verwenden möchten, in dieser Liste nicht aufgeführt ist, dann klicken Sie auf **Datenträger** und geben für das Betriebssystem den Pfad der Protokolldatei an.
6. Nun erscheint das Protokoll in einem Fenster. Um den Vorgang abzuschließen, klicken Sie auf **Schliessen**. Wenn das System für die Verwendung des Protokolls weitere Angaben benötigt (wie z.B.

Netzwerknummer, Hostadresse usw.), werden Sie aufgefordert, diese Informationen nun einzugeben.

Wenn Sie ein Protokoll entfernen möchten, befolgen Sie einfach Schritt 1 und klicken in Schritt 2 auf **Deinstallieren**. Wenn Sie Ihre Wahl bestätigt haben, ist die Option aktiviert.

15.1.2 Lade sie alle!

Da es so einfach ist, Protokolle hinzuzufügen, ist die Versuchung groß, einfach jedes Protokoll, das man bekommen kann, hinzuzufügen. Wenn es gut ist, zwei Sprachen zu sprechen, dann muss es großartig sein, fünf zu sprechen. Sie müssen jedoch bedenken, dass das System durch die Installation eines Protokolls nicht einfach nur die Fähigkeit, eine neue Sprache zu sprechen, erworben hat, sondern sich vielmehr *einverstanden erklärt*, diese Sprache praktisch jedes Mal, wenn es spricht, auch zu sprechen. Das ist ein bisschen so wie bei einem Dolmetscher bei der UN, der fünf Sprachen spricht und immer alles in allen fünf Sprachen sagen muss.

Die Belastung eines Servers und des Netzwerks wächst proportional mit jedem Protokoll, das hinzugefügt wird. Das bedeutet nicht, dass jedes Protokoll dieselbe Menge Verkehr erzeugt. Jedes Protokoll muss jedoch bei jeder Meldung, die der Server versenden möchte, berücksichtigt werden. Die einzige Erleichterung besteht darin, dass es protokollspezifische Anforderungen gibt, die nicht für alle Protokolle erforderlich sind.

Wenn man also im Chinesischen 13 Wörter braucht, um einen Satz auszudrücken, und 14 Wörter im Englischen, entsteht ein Verkehr von 27 Wörtern. Das sind 13 Wörter mehr als erforderlich wären, wenn jeder Englisch sprechen würde.

Nur weil es möglich ist, bedeutet das nicht, dass es getan werden *muss*. Am besten ist es, so wenig Protokolle wie möglich auf dem Server zu installieren. Darin unterscheidet sich dieser Bereich nicht von anderen Bereichen des Servers. Das ist nicht wie bei einem Arbeitsplatzrechner, der gelegentlich abstürzt, weil er so viele Anwendungen ausführt. Server sind zu wichtig, da sie freigegebene Ressourcen sind.

15.1.3 Art der Verbindung

Ein Protokoll kommuniziert über die Netzwirkabel mit Peers entweder *verbindungsorientiert* oder *verbindungslos*. Das ist aufgrund des Unterschieds bei der Bandbreite und der Qualität der Verbindungen eine wichtige Unterscheidung.

In der Welt von TCP/IP ist das TCP-Protokoll beispielsweise ein *verbindungsorientiertes Protokoll*. Das bedeutet, dass zunächst eine Verbindung aufgebaut werden muss und erst danach kommuniziert werden kann. Bei diesen Protokollen ist außerdem eine Bestätigung der Verbindung erforderlich. Das ist so ähnlich wie bei einem Einschreibebrief. Der Brief wird versendet und die Transaktion wird erst als erfolgreich betrachtet, wenn der Empfänger bestätigt, dass er den Brief erhalten hat. SPX von IPX/SPX ist ebenfalls ein verbindungsorientiertes Protokoll.

Das Gegenteil davon wird als *verbindungsloses Protokoll* bezeichnet. Das bedeutet nicht, dass es hier keine Verbindung gibt. Vielmehr ist damit gemeint, dass das Protokoll an der Bestätigung der Verbindung nicht beteiligt ist. Das ist als würde man einen Brief ganz normal versenden: Ein Brief wird in den Briefkasten geworfen. Es wird erwartet, dass er ankommt. Aber wenn er nicht ankommt, weiß der

Absender das nicht. Ein verbindungsloses Protokoll versendet einfach die Pakete und kümmert sich nicht darum, ob diese ankommen. IPX und UDP (von der TCP/IP-Protokollsuite) sind Beispiele für verbindungslose Protokolle.

15.1.4 TCP/IP

TCP/IP wurde aus vielen einleuchtenden Gründen zum Standardprotokoll für viele Betriebssysteme. Meiner Meinung nach ist der wichtigste Grund der, dass es ein öffentlich zugängliches Protokoll ist. Dieses Protokoll gehört nicht einem einzelnen Unternehmen, denn es wurde vom amerikanischen Verteidigungsministerium entwickelt. Das bedeutet, dass es sich um ein freies Protokoll handelt.

Als das Internet entstand, wurden TCP und IP neben vielen anderen Protokollen vom amerikanischen Verteidigungsministerium für die Kommunikation zwischen den Standorten des Ministeriums entwickelt. Viele dieser Protokolle sind heute Teil dessen, was unter der Bezeichnung *TCP/IP-Suite* bekannt ist.

Ein Kommunikationsverfahren innerhalb des Verteidigungsministeriums zu entwickeln, hatte seine Vorteile. Das Protokoll ist sehr stabil und umgeht langsame oder fehlende Bereiche des Netzwerks. Das Produkt wurde unter anderem öffentlich zugänglich gemacht, weil die amerikanische Öffentlichkeit für dessen Entwicklung bezahlt hat und somit Eigentümer des Protokolls ist.

Dies LAN ist Ihr LAN

Dieses Protokoll gehört im wahrsten Sinne des Wortes der Öffentlichkeit. Es ist ein öffentlicher Standard. Die US-amerikanische Regierung sorgte dafür und setzte eine Gruppe, die so genannte Internet Engineering Task Force (IETF), ein, die für die Wartung und Verwaltung der Protokollsuite verantwortlich ist.

Änderungen, die an diesem Protokoll vorgenommen werden, werden über *RFCs* (Requests for Comment) veröffentlicht. Wenn ein Anbieter Änderungen an TCP/IP vornimmt, wird in der Regel die mit der Änderung verbundene RFC-Nummer angegeben. Microsoft hat bei der Entwicklung von Windows 2000 eine ganze Reihe von RFCs eingereicht.

Jede Eingabe wird in die Liste für den TCP/IP-Standard aufgenommen. Nicht alle Elemente sind jedoch für eine Implementierung erforderlich. Eigentlich sind es nur einige wenige Eingaben, die verbindlich sind.

Administratoren vertrauen darauf

Wenn das Netzwerkbetriebssystem über TCP/IP kommunizieren kann, kann es mit der Welt kommunizieren. Jedes größere Netzwerkbetriebssystem verwendet dieses Protokoll, auch die hier aufgeführten Betriebssysteme:

- Microsoft Windows 2000, NT und 95/98
- Novell NetWare 4.x und 5.x (jetzt eigene Dienste über TCP/IP möglich)
- UNIX
- Digital VMS und Pathworks
- IBM AS/400 und Mainframe System

Diese Betriebssysteme decken gut 95% aller Netzwerk-Server ab. Das TCP/IP-Protokoll wird seit über 20 Jahren verwendet. Ähnlich wie das Betriebssystem UNIX gibt es TCP/IP schon sehr lange, sodass sich die Benutzer darauf verlassen und anderen Protokollen nicht trauen.

Alle Funktionen

TCP/IP bezeichnet eigentlich viele unterschiedliche Protokolle und Funktionen, aus denen die Protokollsuite besteht. Diese Protokollsuite umfasst eine Reihe von Protokollen, die sämtliche Facetten der Netzwerknutzung steuern:

- *TCP (Transport Protocol)*. Wird für zuverlässige verbindungsorientierte Verbindungen verwendet.
- *UDP (User Datagram Protocol)*. Wird von TCP/IP für einfache Verbindungen verwendet. UDP ist das Protokoll, das für verbindungslose Verbindungen verwendet wird.
- *IP (Internet Protocol)*. IP definiert das Format der Adresse, auch als *Datagramm* bezeichnet, sowie das Adressenschema.
- *FTP (File Transport Protocol)*. Wird verwendet, um Dateien zuverlässig über ein Netzwerk zu übertragen.
- *HTTP (Hypertext Transfer Protocol)*. Wird für die Übertragung hypertextbasierter Dokumente verwendet. Es ermöglicht eine reibungslose Übertragung von Dokumenten. Im WWW wird dieses Protokoll verwendet.
- *Telnet*. Ein Protokoll für die Kommunikation zwischen Terminals, mit dessen Hilfe Benutzer eine Verbindung zwischen einem Terminal und einem Host-Computer erstellen können.
- *NFS (Network File System)*. Wird verwendet, damit Benutzer Netzlaufwerke mit ihren lokalen Rechnern verbinden und diese Laufwerke in ihrer eigenen Umgebung verwenden können.



Ein *Datagramm* ist die kleinste Einheit, in der Nachrichten über ein IP-Netzwerk gesendet werden. Datagramme werden bei vielen anderen Protokollen als *Pakete* bezeichnet und enthalten Angaben über Ziel und Host sowie die zu übertragenden Daten.

Die ganze Suite besteht aus der Kombination dieser und vieler anderer Protokolle.

Stärken und Schwächen

Und das sind die Stärken von TCP/IP:

- Umfassende Installations- und Anwenderunterstützung.
- Stabil und zeitgetestet.
- Von Natur aus routbar.
- Kostenfreie WAN-Dienste zwischen Standorten über das Internet.

Und das sind die Schwächen von TCP/IP:

- Jedem Knoten muss eine Netzwerkadresse zugewiesen werden. Die Adresse muss immer manuell zugewiesen werden, gleichgültig ob die Zuweisung über DHCP oder statisch erfolgt.
- IP-Routing und Segmentierung kann sehr komplex werden, wenn Sie nur über wenige registrierte Adressen verfügen.

- IP steht jedem, der dieses Protokoll verwenden möchte, zur Verfügung. Das kann eine Sicherheitslücke in Ihrem System darstellen.

15.1.5 IPX/SPX

Viele Benutzer sehen in IPX/SPX einen Standard, der nahezu ebenso leistungsfähig ist wie TCP/IP. IPX/SPX wurde zwar nicht von der amerikanischen Regierung entwickelt. Dennoch konnte es einen großen Teil des privaten Bereichs erobern. Das kommt daher, weil IPX/SPX bis 1998 das einzige Protokoll war, das für Verbindungen mit Novell NetWare, dem produktivsten Netzwerkbetriebssystem der letzten fünfzehn Jahre, verwendet werden konnte.

IPX/SPX wurde von Novell als Teil des Betriebssystems NetWare entwickelt und war ursprünglich ein proprietäres Protokoll. Dann wurde die Protokollfamilie für die Öffentlichkeit freigegeben und ist heute Teil praktisch aller Netzwerkbetriebssysteme. Das Protokoll wurde so vorherrschend, weil das Netzwerkbetriebssystem, in dem es integriert war, zu einem Zeitpunkt in seiner Geschichte etwa 70% Marktanteile innehatte. Das hat sich inzwischen geändert. Das Protokoll ist jedoch so in unserer Geschäftswelt verankert, dass es so schnell nicht von der Bildfläche verschwinden wird und wohl auch nicht soll.

In der Welt von Microsoft Windows ist IPX/SPX unter der Bezeichnung *NWLink IPX/SPX-kompatibler Transport* bekannt. Das *NW* bezieht sich auf die Tatsache, dass es sich hierbei um ein NetWare-bezogenes Protokoll handelt. Es kann jedoch auch ein Hinweis darauf sein, wann Microsoft möchte, dass dieses Protokoll verwendet wird. IPX/SPX hat einige sehr nette Funktionen und kann in kleinen Netzwerken das Leben einfacher machen.

Schlank und effizient

IPX/SPX bietet eine sehr saubere und effiziente Möglichkeit, eine große Anzahl von Benutzern mit sehr geringem Aufwand miteinander zu verbinden. Ein Großteil der bei TCP/IP erforderlichen Vorbereitungen ist in der Welt von IPX/SPX überflüssig, da dieses Protokoll sich in vielen Bereichen selbst konfiguriert.

IPX entspricht dem IP-Teil des TCP/IP-Protokolls. Es ist das verbindungslose Protokoll, das für die meisten Verbindungen verwendet wird. Es verfügt über eine einheitliche Adressenfunktion, mit deren Hilfe Administratoren die Netzwerkadresse einmal definieren und dann nicht mehr daran zu denken brauchen. Darüber hinaus muss der Administrator keine Hostadressen erstellen.

Für das Adressenschema von IPX müssen Netzwerkadressen verwendet werden, die der Administrator während der Installation des ersten Host (häufig der erste Server) im Netzwerksegment erstellt. Für jedes neue Netzwerksegment wird bei der Einrichtung dieses Segments eine neue Netzwerkadresse definiert, die dann ab diesem Punkt für dieses Segment verwendet wird. Die Netzwerkadresse besteht aus einer achtstelligen Hexadezimalzahl (z.B. 0529FA43). Freie Stellen werden am Anfang der Adresse mit Nullen ergänzt. Somit wird beispielsweise aus der Adresse 39DA3A die Adresse 0039DA3A.



Hexadezimalzahlen werden für viele Computer-Einstellungen verwendet. Beim Hexadezimalsystem handelt es sich um ein Zahlensystem, das aus den Ziffern 0, 1, 2, 3, 4, 5, 6, 7, 8 und 9 und den Buchstaben A, B, C, D, E und F besteht. (Kennen Sie den alten Witz: Wenn Gott gewollt hätte, dass wir mit Hexadezimalzahlen rechnen, hätte er uns 16 Finger gegeben.) Mit Hilfe dieses Zahlensystems ist es möglich, sämtliche binären Darstellungen eines Bytes (acht Bits) mit einer zweistelligen Hexadezimalzahl auszudrücken. Hexadezimalzahlen beginnen mit einem h oder 0x, um zu kennzeichnen, dass es sich bei der Zahl um eine Hexadezimalzahl handelt. Die binäre Zahl 00101110 entspricht beispielsweise der Hexadezimalzahl h2E. Die Zahl h2E ist einfacher zu verstehen und lässt sich einfacher schreiben als 00101110.



Tricks mit Hexadezimalzahlen

Mit ein bisschen Einfallsreichtum kann ein Administrator die Netzwerkadresse als Hinweis darauf, wo sich ein Segment befindet, verwenden. Bei der Fehlersuche kann es recht hilfreich sein, wenn Telefonnummern von Standorten, Zimmernummern oder auch Nummern von Schaltschränken verwendet werden. Auch »Wörter« wie C0FFEE, FEEFEE, ABE, CA5E kann man sich zu Nutze machen.

Wenn die Netzwerkadresse bei der Installation eines Segments definiert worden ist, kommuniziert jedes zu diesem System neu hinzugefügte System mit den Mitgliedern dieses Segments über diese Netzwerknummer.

Eine vollständige Netzwerkadresse für ein Host-System besteht aus der Netzwerkadresse und der Hardware-Adresse des Systems oder aus einer so genannten *MAC-Adresse* (Media Access Control). Jeder Netzwerkkarte in einem Ethernet-Netzwerk wird eine eindeutige MAC-Adresse zugewiesen. Andere Netzwerkkarten verfügen in der Regel über eine eindeutige Hardware-Adresse. Diese Adresse besteht meist aus einer zwölfstelligen Hexadezimalzahl.

WAN-freundlich

Die eindeutige Adresse eines Host im Netzwerk setzt sich aus Hardware-Adresse und Netzwerkadresse zusammen. Ein Beispiel für die IPX-Adresse eines Host wäre 00400530EE76:4CA98221 (Knoten:Netzwerk).

Das Schöne an diesem System ist, dass die Computer nicht neu starten, wenn die Netzwerkadresse definiert worden ist. Schwierig ist es allerdings, anhand der Host-Adresse ein System bzw. dessen Standort ausfindig zu machen. In der Welt von IP kontrollieren die Administratoren die Host- und Netzwerkadresse, sodass sie wissen, wer welche Adresse hat. Bei IPX gibt es eine solche Kontrolle nicht. Da die Adressen aus einer Netzwerk- und einer Host-Adresse bestehen, ist IPX/SPX mit Hilfe der meisten kommerziellen Router, darunter auch Windows NT (ab Service Pack 3), routbar.

Störender Nachbar

Wenn Windows in Netzwerken verwendet wird, müssen die Namen aufgelöst werden, damit Ressourcen wie Drucker und Dateifreigaben veröffentlicht werden können. In der Welt von TCP/IP werden Produkte wie WINS und DNS verwendet, um den Verkehr, der durch das Auflösen dieser Namen entsteht,

möglichst gering zu halten. Auch IPX/SPX verwendet das NetBIOS-Protokoll für die Namensauflösung, tut dies jedoch durch zeitlich definierte Rundsendungen von NetBIOS-Namen über das Netzwerk oder über das SAP-Protokoll (Service Advertising Protocol).

SAP-Informationen werden über das RIP-Protokoll (Router Information Protocol) angefordert. Wenn eine Liste der verfügbaren NetBIOS-Hosts angefordert wird, stellt das IPX/SPX-Netzwerk eine Liste der am SAP-Verkehr beteiligten Hosts zur Verfügung. Der Verkehr, der durch die Anforderung und die Antwort entsteht, wird als *RIP/SAP-Verkehr* bezeichnet. Wenn ein neues Netzwerk in Betrieb genommen wird oder Ressourcen an einen neuen Standort verlegt werden, ist dieser Verkehr ziemlich heftig.

Stärken und Schwächen

Die Stärken von IPX/SPX sind folgende:

- Erfordert wenig Planung in Bezug auf Netzwerkadressen.
- Sehr schnelle und effiziente Standardverbindungen.
- Routbar.

Die Schwächen von IPX/SPX sind folgende:

- Weniger Kontrolle über die Netzwerkadressen.
- Nicht so allgemein anerkannt wie IP.
- Nicht zulässig im Internet.
- RIP/SAP-Verkehr.

15.1.6 AppleTalk

Auch wenn die PC-Welt es nicht so recht wahrhaben will, die Macintosh-Computer von Apple dominieren in der Geschäftswelt. Es gibt einfach viele Aufgaben, die mit diesem Computer besser bewältigt werden können. Daher werden Administratoren von großen Netzwerken in Unternehmen früher oder später wohl einmal Macintosh-Computer in ihr Netzwerkschema integrieren müssen. Windows 2000 und ältere Versionen bis hin zum LAN Manager für OS/2 boten schon immer die Möglichkeit der Kommunikation mit der Macintosh-Welt.

Das von Macintosh verwendete Protokoll wurde von Apple Computer entwickelt und heißt *AppleTalk*. Dieses Protokoll ist ebenso leistungsstark wie die gesamte Produktlinie von Macintosh. Das bedeutet, dass das Protokoll dem Benutzer sämtliche Ressourcen im Netzwerk anzeigt und nicht dem Benutzer die Entdeckung dieser Ressourcen überlässt.

Noch ein störender Nachbar

AppleTalk-Geräte geben ihre Namen kontinuierlich über das Netzwerk bekannt. Macintosh-Clients rufen mit der Schnittstelle *Chooser* (siehe Abbildung 15.3) eine Liste der verfügbaren Ressourcen auf, die im Netzwerk veröffentlicht werden. Der Client kann eine Verbindung zu einer Ressource herstellen, indem er einen Ressourcentyp und eine bestimmte Ressource auswählt. Allein die Menge der veröffentlichten Ressourcen und Hosts kann schnell dazu führen, dass das Netzwerk zusammenbricht.

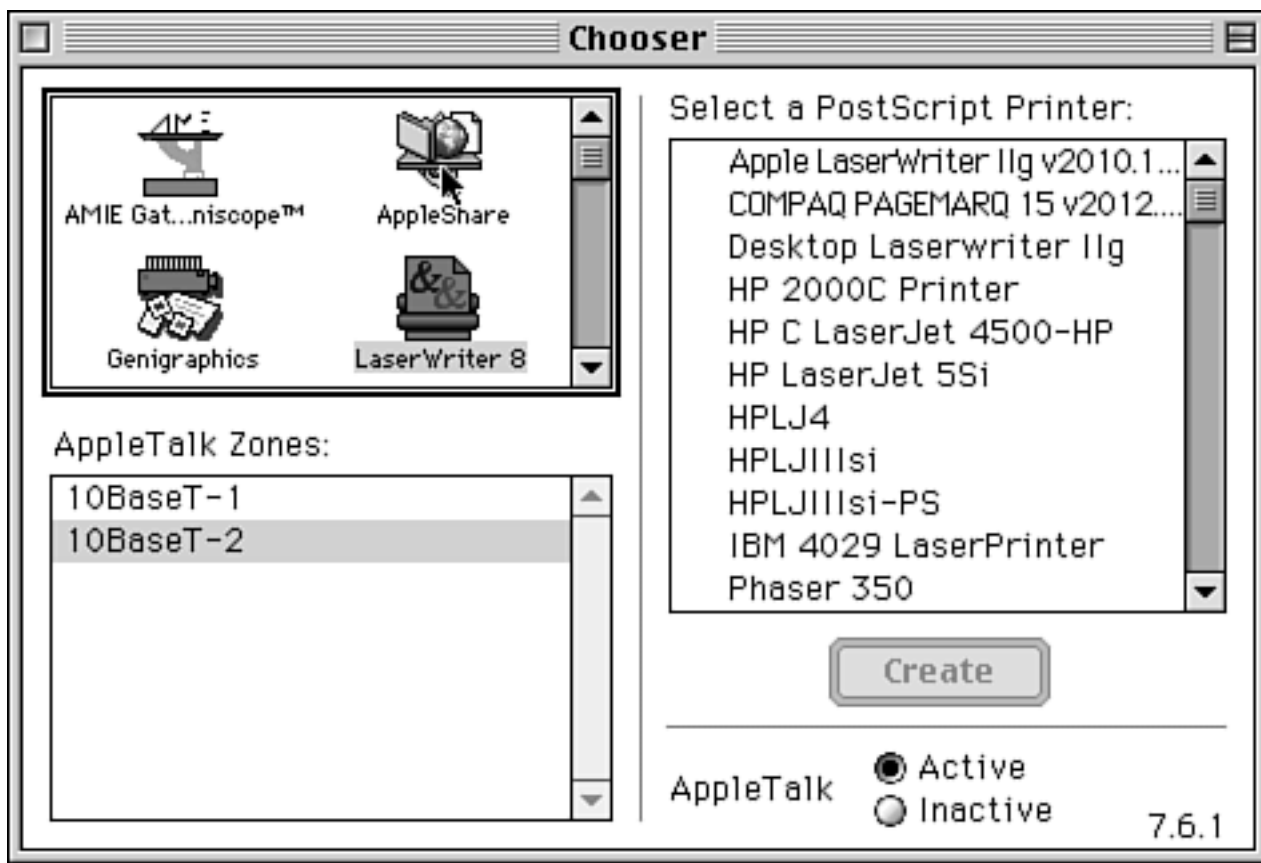


Abbildung 15.3: Der Chooser von Macintosh

Adressenschemata

Wie IP- und IPX-Adressen bestehen auch AppleTalk-Adressen aus Netzwerk- und Host-Adressen. Somit ist das Protokoll routbar. Das Protokoll verwendet im Vergleich zu IP oder IPX ein einfaches Nummerierungsschema, bei dem jedem Netzwerk einfach eine Dezimalzahl zwischen 1 und 253 zugewiesen wird. Jedes Netzwerk kann aus beliebig vielen Hosts bestehen. Wenn es in einem Netzwerk jedoch mehr als 253 Hosts gibt, wird aus der Netzwerknummer ein Netzwerkbereich mit aufeinander folgenden Nummern.

Wenn beispielsweise ein Netzwerk eingerichtet, diesem die Netzwerknummer 100 zugewiesen und dann der 254ste Host hinzugefügt wird, wird aus der ursprünglichen Netzwerknummer die Nummer 100-101. Wenn das Netzwerk 584 Hosts enthält, lautet die Netzwerknummer 100-102. Dieser Bereich umfasst aber immer noch ein Netzwerk.

Adressen der Arbeitsplatzrechner sind ebenso Zusätze zur Netzwerkadresse wie IP-Adressen, wobei diese Adressen nur durch einen Punkt voneinander getrennt werden. Die Host-Adresse wird wie beim IPX-Schema dynamisch erstellt, ist jedoch bei weitem nicht so komplex wie die MAC-Adresse. Jedem Host wird eine Host-Adresse zugewiesen, bei der es sich einfach um eine Nummer handelt, die mit der Verbindung zum Netzwerk zu tun hat. Somit hat beispielsweise ein Host mit einer Verbindung zum Netzwerk 100-102 die Adresse 100.1, dann 100.2, 100.3 usw.

Aufgrund der Natur des Macintosh-Computers wird der Benutzer an der Hand durch diesen Prozess geführt, wobei jedem einzelnen Netzwerk, den so genannten *Zonen*, ein Name zugewiesen wird. Mit den Zonen soll verhindert werden, dass Benutzer in großen Netzwerken nicht ewig in einer Fülle von

Ressourcen nach der Ressource neben sich suchen müssen. Daher muss ein Benutzer in einem Netzwerk mit mehreren Segmenten zuerst die Zone angeben, in der sich die Ressource befindet. Erst dann kann er gezielt nach der gewünschten Ressource suchen.

Zone ist einfach nur eine nette Bezeichnung für Netzwerksegment. Es ist daher für Benutzer einfach zu verstehen, dass eine Ressource, die sich beispielsweise im 4. Stockwerk befindet, in der Zone »Vierte Etage« zu finden ist. Benutzer müssen nicht wissen, dass dies das Netzwerk 100-102 ist. Der Administrator muss jedoch das Nummerierungsschema der Zonen kennen, um für ein konsistentes Modell sorgen zu können.

Stärken und Schwächen

Die Stärken von AppleTalk sind folgende:

- Ermöglicht Verbindungen zwischen Macintosh-Computern und Windows-Servern.
- Bietet den Clients, die dieses Protokoll verwenden, umfassende Hilfestellung.
- Routbar.

Die Schwächen von AppleTalk sind folgende:

- Weniger Kontrolle über die Netzwerkadressen.
- Belegt Bandbreiten durch die Rundsendungen von notwendigen Informationen an die Macintosh-Clients.
- Nur für eine proprietäre Gruppe von Computern wirklich nützlich.
- Nicht zulässig im Internet.

15.1.7 NetBEUI

Das NetBEUI-Protokoll gibt es eigentlich in der Windows-Netzwerkwelt schon von Anfang an. Die Idee, die sich hinter diesem Protokoll verbirgt, ist die, dass man ein Protokoll haben wollte, das einfach NetBIOS als Schnittstelle verwendet. NetBEUI steht für *NetBIOS Extended User Interface*. Das bedeutet einfach, dass NetBIOS das Netzwerk ist.

Das Protokoll besteht aus Netzwerk-Peers, die über Rundsendungen Hosts im Netzwerk ausfindig machen und sich an diese Hosts wenden, wenn eine Ressource benötigt wird. Das Protokoll sollte lediglich dazu dienen, mit PCs über das Netzwerk zu kommunizieren.

Rundsendungen erfolgen von Natur aus nur innerhalb des Segments, in dem sie erzeugt werden. Da das NetBEUI-Protokoll auf Rundsendungen beruht, ist es nicht routbar.

Ein eigenartiger Zufall will es, dass NetBEUI Netzwerkressourcen im lokalen Netzwerk findet, die andere Protokolle nicht finden. Windows NT und andere Produkte von Microsoft scheinen eine kosmische Verbindung zu diesem Protokoll zu haben. Tatsache ist, dass menschliche Hände die einfache Struktur dieses Protokolls kaum beschädigen können. NetBEUI sucht einfach nach NetBIOS-Einheiten und zeichnet diese auf, nicht mehr und nicht weniger.

Aufgrund dieses Verhaltens eignet sich NetBEUI für eine RAS-Verbindung oder für ein kleines, unkompliziertes Netzwerk sehr gut. Dank seiner einfachen Struktur sorgt dieses Protokoll für eine

äußerst schnelle Verbindung.

Stärken und Schwächen

Die Stärken von NetBEUI sind folgende:

- Schnell und effizient in kleinen, aus einem Segment bestehenden Netzwerken.
- Eignet sich für grundlegende Netzwerkfunktionen bei der Fehlersuche, da es NetBIOS-Komponenten finden kann und auf »Hilfe« durch den Benutzer nicht angewiesen ist.

Die Schwächen von NetBEUI sind folgende:

- Nicht routbar. Daher sind keine Netzwerke mit mehreren Segmenten möglich.
- Wird von vielen anderen Anbietern nicht unterstützt.

15.2 Routing- und RAS-Dienst

Als Teil des Windows 2000-Updates wurde ein Produkt aktualisiert, das jetzt Teil des Betriebssystems ist. Für die Kommunikation über Telefonleitungen und über serielle Leitungen stellte Windows NT ein Produkt mit der Bezeichnung *RAS-Dienste (Remote Access Services)* zur Verfügung. Die logische Weiterentwicklung dieses Produkts wird als *Routing- und RAS-Dienst* bezeichnet. Das RAS-Paket wurde um die Funktion des Routing erweitert, damit Verbindungen zu kleinen entfernten Systemen erleichtert werden. Dadurch, dass der Windows-Server sowohl die Funktion des Routers als auch die des Servers wahrnimmt, ist das Routing günstiger und einfacher möglich.

Der Routing- und RAS-Dienst ist für folgende Bereiche zuständig:

- Routing von LAN zu LAN
- Routing von LAN zu WAN
- VPN (Virtual Private Networks)
- NAT (Network Address Translation)
- Verwendung von normalen Telefonleitungen für DFÜ-Verbindungen.
- Sorgt für DFÜ-Client-Verbindungen im Netzwerk.

Da der Routing- und RAS-Dienst bereits beschrieben worden ist, sollen in diesem Kapitel lediglich die damit verbundenen Protokolle erläutert werden.

15.2.1 PPP

In der Welt der Netzwerke wurden Verbindungen schon immer über Telefonleitungen hergestellt. Damit das überhaupt geht, ist ein spezielles Protokoll erforderlich, das es dem PC ermöglicht, das LAN-Protokoll über ein Modem in ein analoges Signal umzuwandeln. Dadurch ist es möglich, dass der Computer das Modem verwendet, als wäre es eine Netzwerkkarte im PC, und nur damit ist es möglich, dass der PC herkömmliche Telefonleitungen als LAN-Kabel verwendet.

Ursprünglich wurde dieses Protokoll als *SLIP (Serial Line IP)* bezeichnet, da es dem Computer in einem IP-Netzwerk eine Verbindung über eine serielle Leitung (in der Regel über ein Modem) zur Verfügung

stellt. Heute wird das gängigere PPP-Protokoll (Point-to-Point Protocol) verwendet. Dieses Protokoll kann verwendet werden, um mittels IP, IPX, AppleTalk und sogar NetBEUI über eine Telefonleitung mit dem Netzwerk zu kommunizieren. Der Routing- und RAS-Dienst verwendet das PPP-Protokoll, um Verbindungen herzustellen.

15.2.2 RIP

Es gibt zwei Arten, wie Router von verfügbaren Netzwerkleitungen erfahren: Die eine besteht darin, dass Benutzer diese direkt angeben. Die andere besteht darin, dass der Router selbst herausfindet, welche Leitungen verfügbar sind. Damit Router sich gegenseitig finden können, müssen sie an einem Protokoll beteiligt sein, das zum Auffinden von Informationen dient. Das RIP-Protokoll (Router Information Protocol) ist genau solch ein Protokoll, das zeitgetestet ist. Das RIP-Verfahren ist grundlegender Bestandteil sowohl der TCP/IP- als auch der IPX/SPX-Protokollfamilie und ist erforderlich, damit Netzwerke gegenseitig von ihrer Existenz erfahren.

RIP-Router machen sich einfach gegenseitig bekannt und fragen ihre Nachbarn, ob diese in letzter Zeit von neuen Routern gehört haben. Damit ist das Verfahren stark vereinfachend erklärt. Es ist aber im Prinzip das, was geschieht. Um in ein Segment des Netzwerks zu gelangen, mit dem ein Router nicht direkt verbunden ist, benötigt dieser einen anderen Router.

Jedes Mal, wenn ein Router eine Verbindung zu einem neuen Netzwerk herstellt, zeichnet er den Pfad zu diesem Netzwerksegment auf. Im Laufe der Zeit stellt sich jeder Router eine immer umfassendere Liste von Leitungen zusammen und wird dadurch immer effizienter. An dieser Sammlung und Nutzung von Routing-Informationen sind viele unterschiedliche Protokolle beteiligt, die alle denselben Zweck erfüllen. Das Internet ist ein Beispiel für ein sehr großes derartiges System.

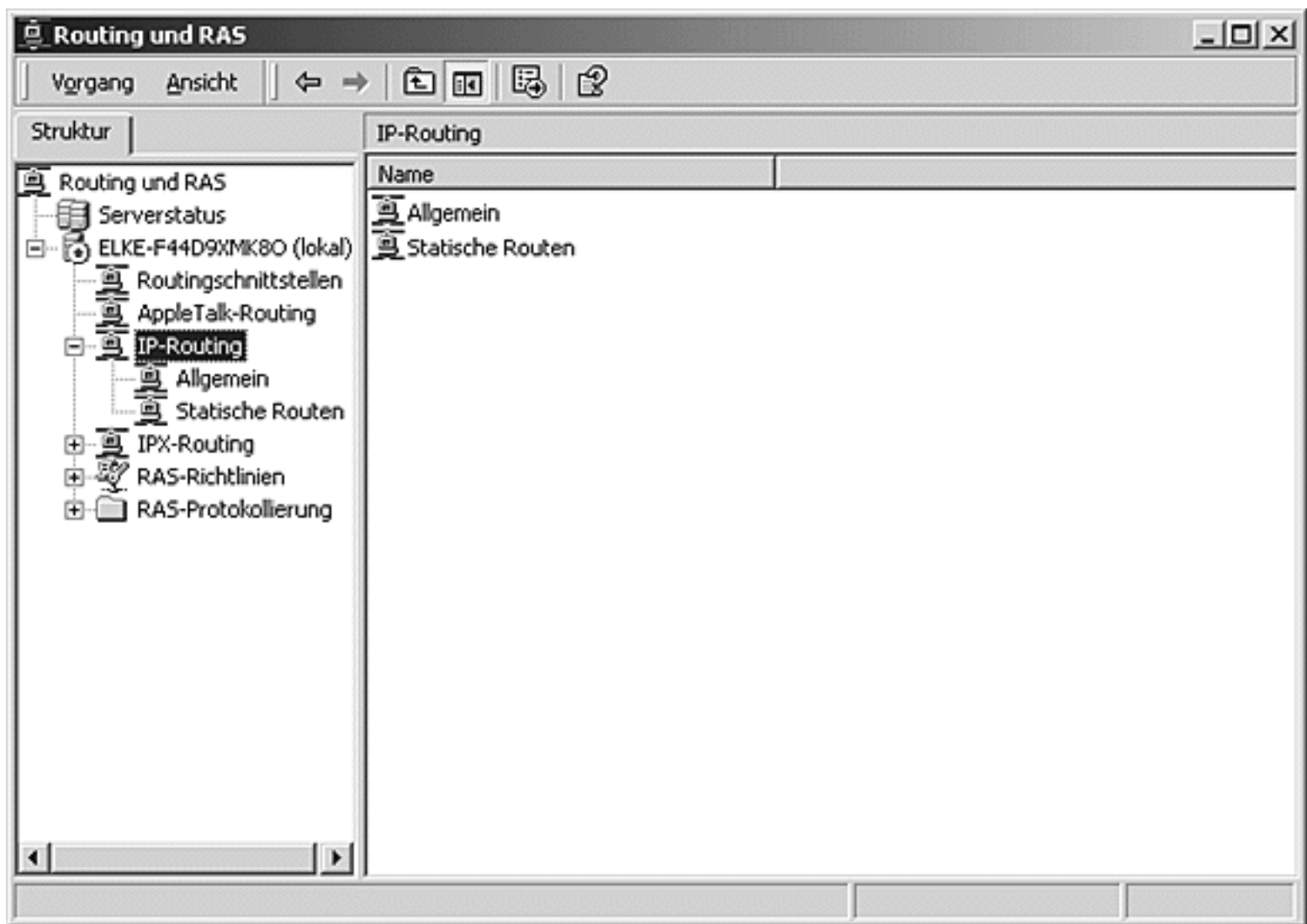


Abbildung 15.4: Die Konsole Routing und RAS

Der Vorteil bei der Verwendung des RIP-Protokolls ist der, dass dieses Protokoll äußerst einfach zu konfigurieren und zu nutzen ist. Der Nachteil an diesem Protokoll besteht darin, dass es große bzw. sehr große Netzwerke nicht skalieren kann. RIP-Router können maximal 15 Hop-Counts verarbeiten. Netzwerke, zwischen denen 16 Hops und mehr liegen, sind unerreichbar. Da Netzwerke im Laufe der Zeit größer werden, können die periodisch wiederkehrenden Bekanntmachungen der RIP-Router zu einem hohen Verkehrsaufkommen führen. Ein weiterer Nachteil des RIP-Protokolls ist dessen lange Wiederherstellungszeit. Wenn sich die Netzwerktopologie ändert, kann es mehrere Minuten dauern, bis sich die RIP-Router dieser neuen Topologie entsprechend neu konfiguriert haben. Während sich das Netzwerk selbst neu konfiguriert, kann es zu Routing-Schleifen kommen, die dazu führen, dass Daten verloren gehen oder nicht übertragen werden können. Angesichts all der Informationen, die ausgetauscht werden, ist das Protokoll doch etwas störend.

Das RIP-Protokoll für IP und IPX kann im Dialogfeld **Routing und RAS** (siehe Abbildung 15.4) aktiviert werden. Öffnen Sie dazu die Konsole **Routing und RAS**, klicken Sie mit der rechten Maustaste auf die Schnittstelle, die Sie für das RIP-Routing konfigurieren möchten, und klicken Sie anschließend auf **Eigenschaften**. Wählen Sie auf der Registerkarte **Allgemein** ein ausgehendes Protokoll und wiederholen Sie den Vorgang für das eingehende Protokoll.

15.2.3 Fehlersuche

Wenn Sie mehr über IP erfahren möchten, dann lesen Sie in Kapitel 21 weiter. Hier sollen lediglich einige Verfahren für die Fehlersuche vorgestellt werden, mit deren Hilfe Sie feststellen können, ob Sie den Routing- und RAS-Dienst richtig konfiguriert haben, und ob Routing-Informationen tatsächlich passieren können:

- RAS-RIP-Rundsendungen werden *nicht* über serielle oder über ISDN-Schnittstellen versendet. RIP-Rundsendungen werden nur über LAN-Schnittstellen oder LAN-Karten wie T1 und Frame Relay gesendet, die Windows als LAN-Schnittstellen betrachtet.
- Stimmt das Standard-Gateway für den NT-Router? Verwenden Sie nur ein auf der entsprechenden Netzwerkkarte konfiguriertes Standard-Gateway.
- Denken Sie daran, dass die Leitung über das Standard-Gateway nur verwendet wird, wenn es keinen anderen gültigen Weg zum Ziel gibt. Daher wird die Standardleitung nur für Adressen außerhalb Ihres Unternehmens oder eines autonomen Systems verwendet. Alle Leitungen innerhalb des Unternehmens werden über RIP in Erfahrung gebracht.



Um die für Ihren Arbeitsplatzrechner konfigurierten IP-Informationen aufzurufen, können Sie je nachdem, mit welchem Betriebssystem Ihr Arbeitsplatzrechner arbeitet, eine der folgenden Anwendungen verwenden: WINIPCFG für Windows 95 und IPCONFIG für Windows 2000 bzw. NT. Diese Programme werden über die DOS-Eingabeaufforderung ausgeführt.

- Prüfen Sie die Konfiguration, d.h. IP-Adresse, Subnet Mask und Standard-Gateway des Client.

Ping

Ping ist ein Programm, das verwendet wird um festzustellen, ob Ihr Rechner einen anderen Rechner im Netzwerk finden kann. Dieses Programm wird *Ping* genannt, weil es das Verhalten eines Schiffes nachahmt, das einen Sonarimpuls (engl. ping) aussendet und das Echo abhört um festzustellen, ob sich ein anderes Schiff oder U-Boot in der Nähe befindet. Mit Hilfe von Ping sendet Ihr Rechner ein Signal an eine Adresse im IP-Netzwerk um festzustellen, ob es überhaupt mit dem Netzwerk verbunden ist, und ob das System im Moment verfügbar ist. Im Folgenden wird beschrieben, wie Sie mit Hilfe von Ping einem Routing-Problem auf den Grund gehen können:

- *Überprüfen Sie sich selbst mit Ping.* Damit können Sie feststellen, ob TCP funktioniert. Sie können damit *nicht* feststellen, ob Ihre Netzwerkkarte funktioniert.
 - *Überprüfen Sie Ihr Standard-Gateway oder den Router des nächsten Hop mit Ping.* Damit können Sie feststellen, ob der Router funktioniert.
 - *Prüfen Sie die Router über den nächsten Router hinaus mit Ping.* Welche Antwort bekommen Sie, wenn die Überprüfung mit Ping fehlschlägt? »Zeitlimit erreicht« kann bedeuten, dass der Ziel-Host nicht erreichbar ist oder dass es keine Route zurück zu Ihnen gibt. Bei »Zielnetz nicht erreichbar« wird die IP-Adresse des Routers angezeigt, der versucht hat, das Paket weiterzuleiten, jedoch keine gültige Route hatte.
-

Kapitel 16 Überlegungen zum Arbeitsplatzrechner

Beim Lesen dieses Kapitels sollten Sie darüber nachdenken, wie Sie die Anzahl der vielen unterschiedlichen Betriebssysteme und Client-Versionen in Ihrer Organisation reduzieren können. Die Arbeit, die dazu getan werden muss, ist die eigentliche technische Arbeit, die in diesem Kapitel beschrieben wird. Dieses Kapitel soll dem Leser nicht nur die Verbindung zwischen Client und Windows 2000 Server näher bringen, sondern es bietet darüber hinaus auch Anweisungen, wie Sie für die Organisation Schritt für Schritt eine Netzwerkumgebung einrichten können.

16.1 Client-Dienste - ein kurzer Überblick

Dieses Kapitel ist insbesondere dann von Bedeutung, wenn Ihre Organisation keine reine 32-Bit-Windows-Welt ist. Oder anders ausgedrückt: Wenn sämtliche Client-Computer in Ihrer Organisation mit Windows 95, Windows 98, Windows 98 Second Edition, Windows NT Workstation oder Windows 2000 Professional arbeiten, dann ist Ihre Arbeit ein Kinderspiel. Um Verbindungen von diesen Client-Computern zu einem Windows 2000-Server einzurichten, müssen Sie lediglich ein oder mehrere Netzwerkprotokolle - TCP/IP, IPX/SPX oder NetBEUI - sowie die Software Client für Microsoft-Netzwerke (oder ein ähnliches Programm) installieren und für die entsprechende Hardware (Netzwerkkarte, Kabel, Hub usw.) sorgen. Und schon steht Ihr Netzwerk! Alle anderen müssen natürlich mit der Realität, d.h. mit Windows 3.x-, Macintosh-, UNIX-, Novell- und vielleicht sogar mit OS/2 Warp-Client-Computern zurecht kommen. All diese Rechner benötigen Datei- und Druckdienste von unserem Windows 2000 Server-Computer.

Wenn Sie erst einmal festgestellt haben, welche Client-Betriebssysteme auf den Windows 2000 Server-Computer zugreifen werden, sollten Sie als Nächstes bestimmen, wie viele Clientzugriffslizenzen Sie benötigen. Eine Clientzugriffslizenz ist das Recht, das Ihre Organisation für jeden einzelnen Client-Computer erwerben muss, der auf einen der folgenden, von Ihrem Windows 2000-Server zur Verfügung gestellten Dienste zugreifen wird:

- *Dateidienste.* Wenn DOS-, Windows 3.x-, Windows 9x-, Windows NT-, Windows 2000- oder ähnliche Client-Betriebssysteme, die sich zu diesem Zeitpunkt auf Ihrem Windows 2000 Server-Rechner befinden, Dateien auflisten, aufrufen, anzeigen und/oder auf eine andere Art und Weise verarbeiten.
- *Datei- und Druckdienste für Macintosh.* Immer, wenn ein Macintosh-Computer für eine Art von Datei- und/oder Druckdienst zusammen mit Windows 2000 Server verwendet wird, muss für jeden Macintosh-Computer eine Clientzugriffslizenz erworben werden.
- *Druckdienste.* Dieser Dienst kommt zum Einsatz, wenn ein Windows 2000 Server-Rechner die Druckdienste von Windows 2000 Server für DOS-, OS/2-, Windows 3.x-, Windows NT-, Windows 2000- und ähnliche Client-Betriebssysteme freigibt, auflistet, verwaltet und/oder nutzt.
- *Datei- und Druckdienste für Novell NetWare.* Immer, wenn ein NetWare-Client-Computer für eine Art von Datei- und/oder Druckdienst zusammen mit Windows 2000 Server verwendet wird, muss für jeden NetWare-Client-Computer eine Clientzugriffslizenz erworben werden.

- *RAS-Dienste.* Immer, wenn ein anderer Rechner auf einen Windows 2000 Server-Rechner über eine Remote-Verbindung (d.h. eine indirekte Netzwerkverbindung wie z.B. eine DFÜ-Verbindung) zugreift, muss dieser Rechner über eine gültige Clientzugriffslizenz für diesen einen Windows 2000 Server-Rechner verfügen.

Das Lizenzieren ist für die meisten Microsoft-Produkte mit Ausnahme der Home-Lizenzierung ziemlich kompliziert. Das Ganze kann schnell sehr komplex werden, wenn Sie festlegen müssen, wie viele Clientzugriffslizenzen Sie für die Windows 2000-Server Ihrer Organisation benötigen. Nur weil Sie eine legale Kopie von Windows 95, Windows 98, Windows 2000 Professional oder von welchem Betriebssystem auch immer erworben haben, bedeutet das beispielsweise noch lange nicht, dass Sie damit die Anforderungen von Microsoft für Clientzugriffslizenzen erfüllen. Die Anzahl der benötigten Lizenzen hängt von der Anzahl der Client-Verbindungen zum Windows 2000 Server-Rechner ab.

Eine Clientzugriffslizenz gibt einem Client-Computer in Ihrem Netzwerk das Recht, eine Verbindung (lokal oder über RAS) zum Windows 2000-Server herzustellen. Denken Sie jedoch daran, dass Sie die Clientzugriffslizenzen nicht berechtigen, mit diesem Client-Computer auf das Betriebssystem des Client oder des Servers zuzugreifen. Darüber hinaus ist es nicht unbedingt erforderlich, dass Sie für jeden Benutzer innerhalb der Organisation eine eigene Clientzugriffslizenz benötigen. In einem Call-Center benutzen beispielsweise häufig mehrere Benutzer denselben Client-Computer jedoch zu unterschiedlichen Zeiten (Schichtdienst, Wochenende, Ferienarbeit usw.). Obwohl ein Unternehmen vielleicht zehn Angestellte hat, die im Laufe einer Woche alle mit demselben Computer arbeiten, muss nur eine Clientzugriffslizenz für Windows 2000 Server erworben werden, da immer jeweils nur eine Verbindung von diesem Computer zu Windows 2000 Server hergestellt werden kann. Im Falle eines Beraters, der beispielsweise mit zwei Laptops auf denselben Windows 2000 Server-Rechner zugreift, müssen dagegen zwei Clientzugriffslizenzen erworben werden, obwohl es ein und derselbe Angestellte ist, der die beiden Verbindungen zum Server-Rechner herstellt. Wichtig ist, dass Sie sich merken, dass die Lizenzen pro Betriebssystem vergeben werden, das auf Windows 2000 Server zugreift.

Bei Windows 2000 Server gibt es zwei Möglichkeiten, die Clientzugriffslizenzen zu verwalten:

- *Innerhalb einer Windows 2000-Domäne.* Dabei klicken Sie auf **Start/Verwaltung** und dann auf das Symbol **Lizenzierung**.
- *Eigenständiger Server.* Damit lizenzieren Sie Windows 2000-Server, die nicht Teil einer Domäne sind. Dabei klicken Sie in der Systemsteuerung von Windows 2000 auf das Symbol **Lizenzierung**.

Die beiden Verwaltungsprogramme für die unterschiedlichen Lizenzierungen funktionieren im Wesentlichen gleich. Der einzige Unterschied besteht darin, ob die Lizenzierung auf der Unternehmens- bzw. Domänenebene oder auf der Ebene eines einzelnen, eigenständigen Servers erfolgt. Wenn Sie beispielsweise die Clientzugriffslizenzen für einen eigenständigen Windows 2000 Server-Rechner verwalten, müssen Sie auf **Start/Einstellungen** und **Systemsteuerung** klicken. Damit öffnen Sie die Systemsteuerung, in der Sie mit einem Doppelklick auf das Symbol **Lizenzierung** das Dialogfeld **Lizenzierungsmodus wählen** aufrufen (siehe Abbildung 16.1).

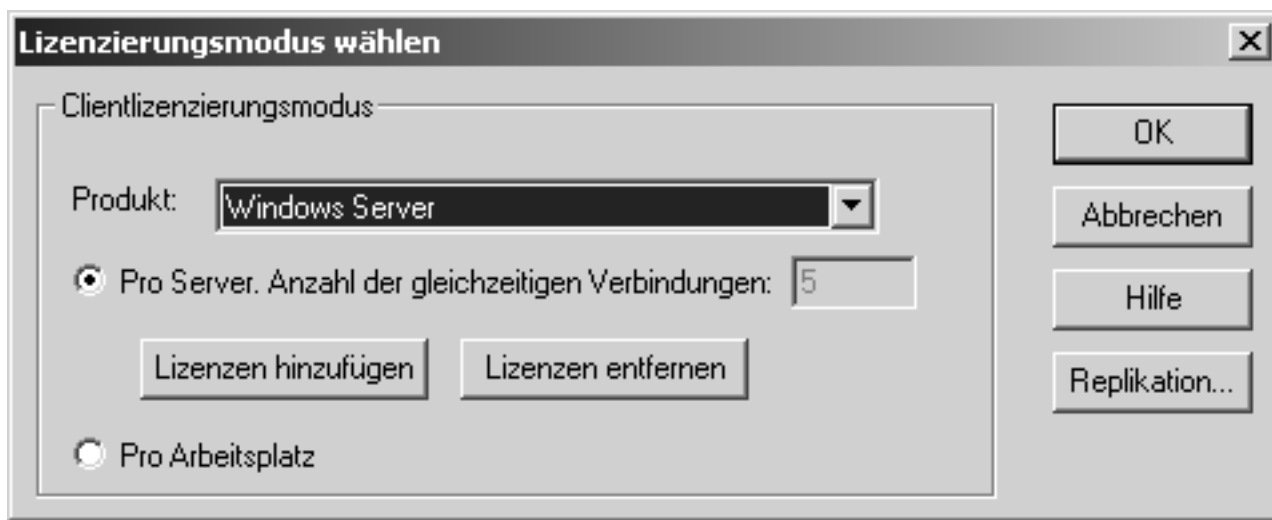


Abbildung 16.1: Das Dialogfeld Lizenzierungsmodus wählen

Das daraufhin erscheinende Dialogfeld **Lizenzierungsmodus wählen** besteht im Wesentlichen aus einem Dropdown-Listenfeld, mit dessen Hilfe Sie das Produkt auswählen können, für das Sie Lizenzen hinzufügen möchten. Wie Sie in der Abbildung sehen können, wird Windows Server mit fünf gültigen Lizenzen im Pro-Server-Modus angezeigt.

Bei Windows 2000 gibt es zwei unterschiedliche Lizenzierungsmodi: pro Server und pro Arbeitsplatz. *Pro Server* bedeutet, dass die Organisation ebenso viele Clientzugriffslizenzen erwirbt, wie Client-Computer und Benutzer auf diesen Server zugreifen. Das geschieht beispielsweise bei einem eigenständigen Server oder bei einem Server in einem Internet oder in einem DFÜ-Netzwerk. Wenn sich derselbe Benutzer allerdings von zwei unterschiedlichen Computern aus anmeldet, benötigt dieser eine Benutzer bereits zwei Clientzugriffslizenzen.

Pro Arbeitsplatz bedeutet, dass für jeden Client-Computer eine Clientzugriffslizenz erworben wird (auch wenn der Lizenzprotokolldienst diese Lizenzen auf der Basis der Benutzernamen zuweist und überwacht). Die Lizenzierung pro Arbeitsplatz eignet sich am besten, wenn Ihre Organisation in einer Active Directory/Domänencontroller- oder Multiserver-Umgebung operiert.

Legen Sie mit Hilfe des Dropdown-Listenfeldes neben **Produkt** fest, für welches Produkt Sie die Lizenzierung verwalten möchten. Anschließend können Sie mit den Schaltflächen **Lizenzen hinzufügen** und **Lizenzen entfernen** Lizenzen auf Ihrem Windows 2000 Server hinzufügen bzw. entfernen. Um weitere Lizenzen hinzuzufügen (nehmen wir einmal an, Sie hätten diese erworben), klicken Sie auf die Schaltfläche **Lizenzen hinzufügen**. Daraufhin erscheint das in Abbildung 16.2 dargestellte Dialogfeld **Neue Clientzugriffslizenz**.



Abbildung 16.2: Hinzufügen einer Clientzugriffslizenz

In diesem Dialogfeld können Sie mit Hilfe der Bildlaufleiste eine beliebige Zahl von 0 bis 999.999 eingeben. Diese Zahl gibt die gesamte Anzahl der Lizenzen an, die Sie für ein bestimmtes Produkt hinzufügen möchten. Wenn Sie beispielsweise 25 Clientzugriffslizenzen für Windows Server hinzufügen möchten, wählen Sie einfach im oberen Dropdown-Listenfeld das Produkt aus und geben dann die Anzahl der Lizenzen ein, die Sie hinzufügen möchten.



Sie können den Pro-Server-Lizenzierungsmodus nicht mehr in einen Pro-Arbeitsplatz-Modus ändern. Das kommt daher, weil der Masterlizenzierungsmodus für einen bestimmten Windows 2000-Server nur einmal geändert werden kann. Das bedeutet Folgendes: Wenn Sie Ihren Windows 2000-Server mit einer Pro-Server-Lizenz installieren, können Sie diese Lizenz nur einmal - nicht beliebig oft - in eine Pro-Arbeitsplatz-Lizenz ändern.

Wenn die gewünschte Anzahl von Lizenzen erscheint, die Sie hinzufügen möchten, klicken Sie auf **OK**. Daraufhin erscheint ein kleines Dialogfeld. Hier müssen Sie bestätigen, dass Sie die Anzahl der Clientzugriffslizenzen, die Sie eben angegeben haben und nun hinzufügen möchten, auch tatsächlich erworben haben (siehe Abbildung 16.3).

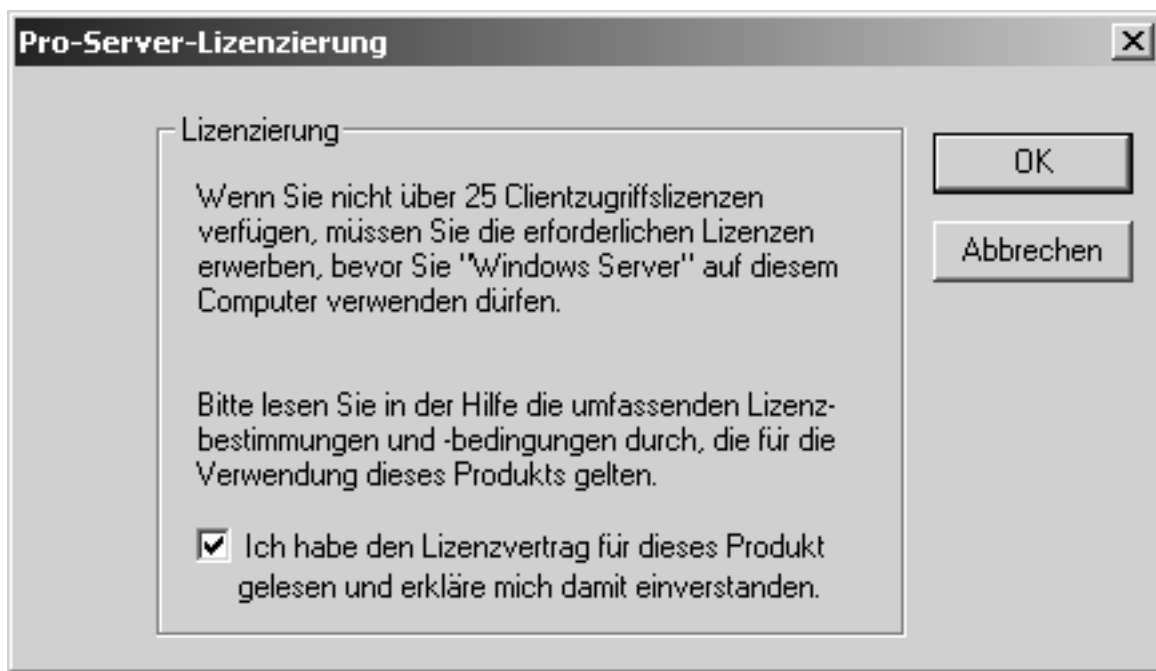


Abbildung 16.3: Einverständniserklärung zum Lizenzvertrag

Um dem Lizenzvertrag zuzustimmen, klicken Sie in das Kontrollkästchen, das daraufhin mit einer entsprechenden Markierung versehen wird. Damit wird die Schaltfläche **OK** aktiviert. (Sie können den Vorgang erst fortsetzen, wenn Sie das Kontrollkästchen aktiviert haben. Bis dahin können Sie den Vorgang nur abbrechen.)

Nachdem Sie das Kontrollkästchen aktiviert haben (vorausgesetzt, Sie haben die Lizenzen tatsächlich erworben), klicken Sie auf **OK**, um den Vorgang fortzusetzen. Daraufhin erscheint automatisch wieder das Dialogfeld **Lizenzierungsmodus wählen** (siehe Abbildung 16.4).

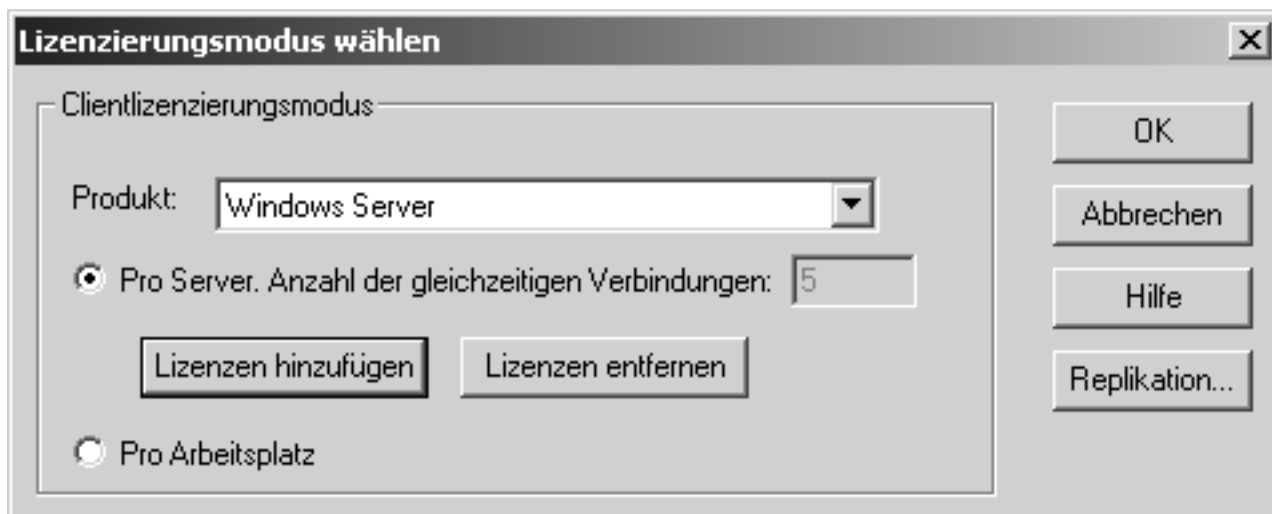


Abbildung 16.4: Dialogfeld Lizenzierungsmodus wählen

Hier können Sie nun die Gesamtzahl der Clientzugriffslizenzen für das gewählte Produkt sehen, zu der die neu hinzugefügten Clientzugriffslizenzen bereits addiert wurden. Nehmen wir einmal an, Sie haben sich vertan und versehentlich mehr Lizenzen hinzugefügt, als Sie wirklich benötigen (oder vielleicht wollten Sie nur eine oder mehrere Clientzugriffslizenzen von Ihrem Server entfernen), dann können Sie diese Lizenzen über die Schaltfläche **Lizenzen entfernen** von Ihrem Server entfernen. Wenn Sie auf

diese Schaltfläche klicken, erscheint das Dialogfeld **Zertifikat zum Entfernen von Lizenzen wählen** (siehe Abbildung 16.5).

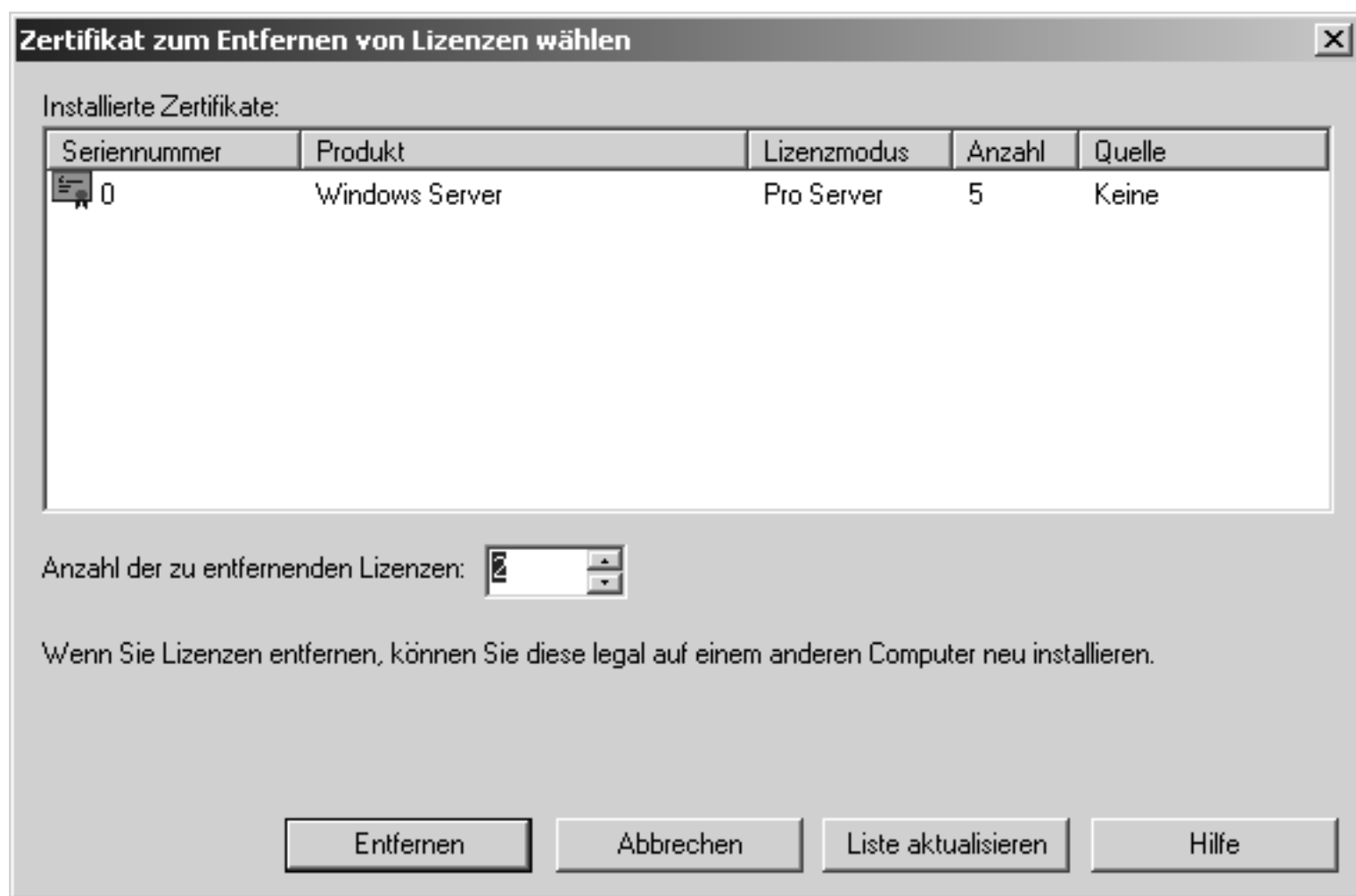


Abbildung 16.5: Auswahl eines Zertifikats zum Entfernen von Lizenzen

Mit Hilfe dieses Dialogfelds kann der Systemadministrator Lizenzen einzeln aus der Windows 2000 Server-Umgebung entfernen. Dabei kann es sich um Clientzugriffslizenzen für Windows 2000 Server handeln, aber auch um Lizenzen für andere Produkte aus der Microsoft BackOffice-Familie (Windows NT, Windows 2000 Server-Familie, Site Server, Site Server Commerce Edition, SQL Server, SNA Server, Systems Management Server, Exchange Server, Proxy Server, Internet Information Server sowie die gesamte BackOffice 4.x-Produktlizenz). Die Lizenzen, die Sie selbst über die mit Windows 2000 Server zur Verfügung gestellten Tools zur Verwaltung der Lizenzierung hinzufügen, sind mit kleinen, fortlaufenden Nummern versehen. Die Lizenzen, die als Teil der formalen Produktinstallation installiert werden (wenn Sie also beispielsweise BackOffice Server 4.5 installieren), verfügen über ernstere Nummern.

Um eine Lizenz zu entfernen, klicken Sie auf das Produkt, das Sie ändern möchten, und geben Sie dann im Dialogfeld **Anzahl der zu entfernenden Lizenzen** mit Hilfe der Bildlaufleiste die Anzahl der Lizenzen ein, die Sie entfernen möchten. Seien Sie aber vorsichtig! Man ist geneigt, hier die Anzahl der noch verbleibenden Lizenzen (die Gesamtzahl der Lizenzen abzüglich der entfernten Lizenzen) einzugeben. Statt dessen muss jedoch die Anzahl der zu entfernenden Lizenzen eingegeben werden. Wenn Sie diese Zahl eingegeben haben, klicken Sie auf die Schaltfläche **Entfernen**, um diese Lizenzen zu entfernen. Daraufhin erscheint ein kleines Dialogfeld, das Sie auffordert, Ihre Entscheidung zu

bestätigen (siehe Abbildung 16.6).

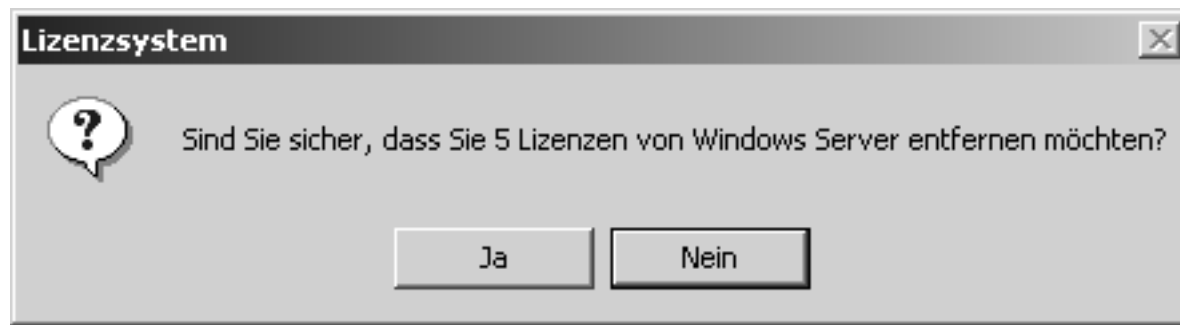


Abbildung 16.6: Das Löschen einer Lizenz bestätigen

Wenn Sie hier auf die Schaltfläche **Ja** klicken, werden die Lizenzen entfernt und es erscheint wieder das Dialogfeld **Zertifikat zum Entfernen von Lizenzen wählen**. Hier können Sie sofort erkennen, wie viele Lizenzen Sie entfernt haben (siehe Abbildung 16.7).

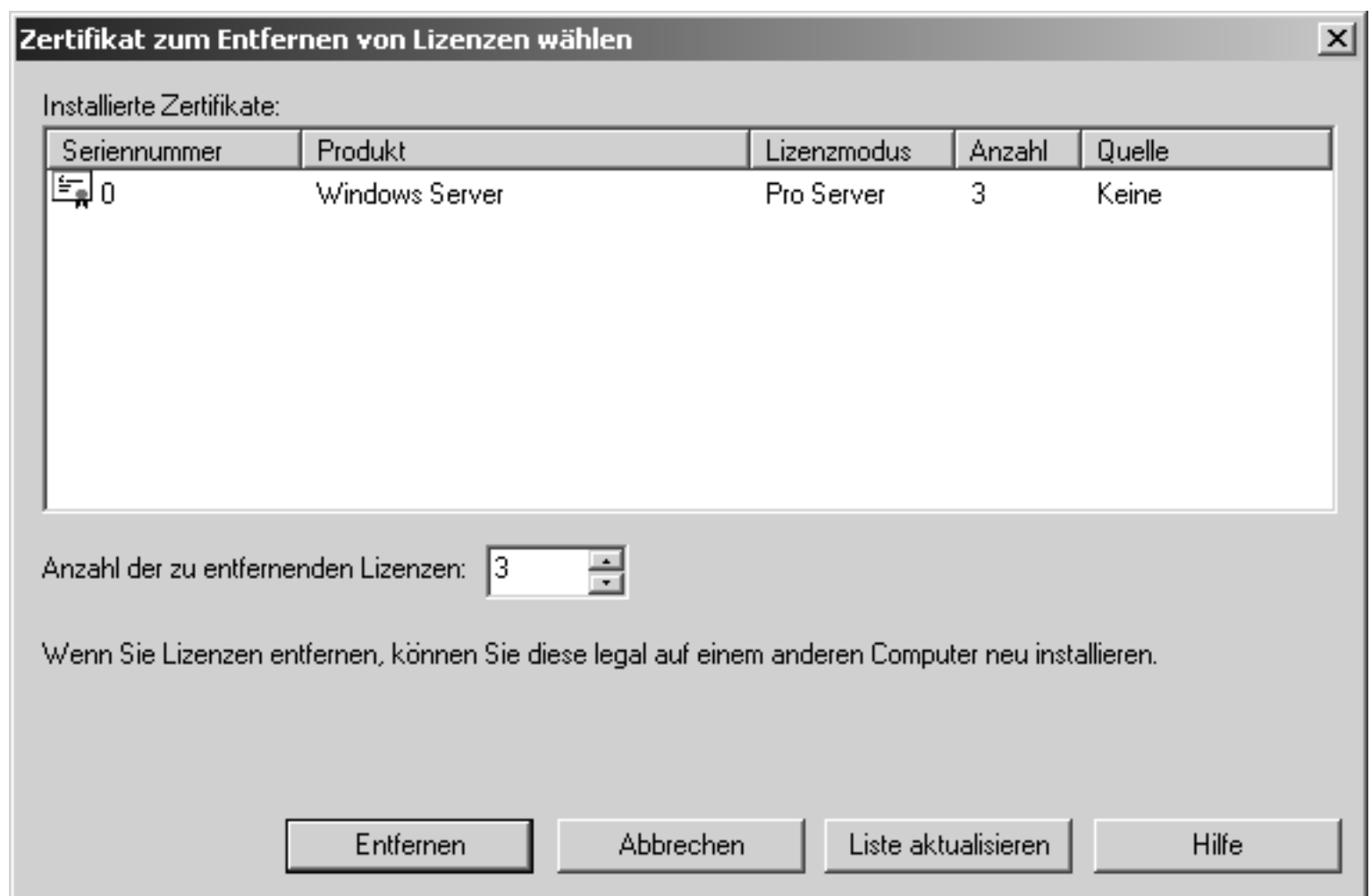


Abbildung 16.7: Prüfen der Anzahl der Lizenzen

Wenn Sie alle gewünschten Lizenzen entfernt haben, möchten Sie dieses Dialogfeld sicherlich wieder verlassen. Microsoft hat jedoch vergessen, dieses Dialogfeld mit der Schaltfläche **Schliessen** zu versehen. Daher müssen Sie auf die Schaltfläche **Abbrechen** klicken, um dieses Dialogfeld zu schließen. Aber es gibt keinen Grund zur Sorge. Sämtliche Änderungen, die Sie vorgenommen haben, wurden bereits gespeichert und Sie kehren wohlbehalten zum Dialogfeld **Lizenzierungsmodus wählen** zurück.

In diesem Dialogfeld sehen Sie wieder die beiden Optionen **Pro Server** und **Pro Arbeitsplatz**. Wenn Sie sich schon einmal gefragt haben, was wohl geschieht, wenn Sie den Lizenzierungsmodus ändern, haben Sie nun vielleicht die Möglichkeit, dies auszuprobieren. Wenn Sie Ihren Server bei der Installation von Windows 2000 Server im Pro-Arbeitsplatz-Modus konfiguriert haben, haben Sie leider kein Glück. Dann können Sie Ihren Server nicht mehr im Pro-Server-Modus konfigurieren. Wenn Sie Windows 2000 Server jedoch im Pro-Server-Modus installiert haben, können Sie nun den Lizenzierungsmodus ändern. Dazu klicken Sie auf das Optionsfeld **Pro Arbeitsplatz**. Daraufhin kann unter Umständen eine Warnmeldung erscheinen (siehe Abbildung 16.8).

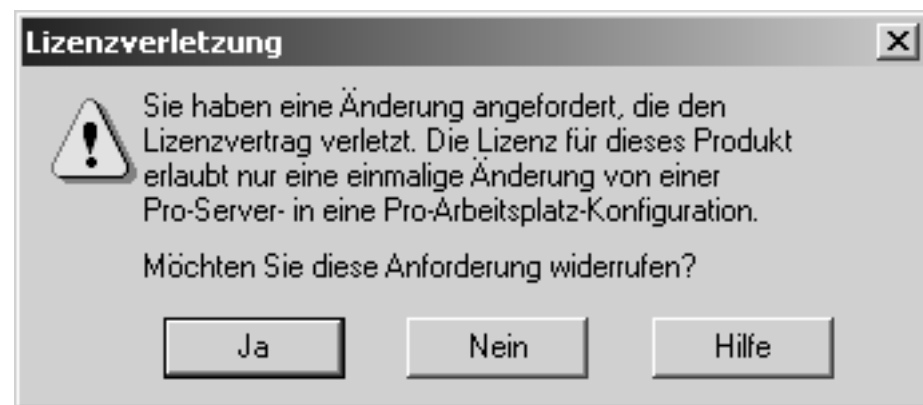


Abbildung 16.8: Lizenzverletzung

Wenn Sie den Lizenzierungsmodus für Ihren Server noch nie geändert haben, erscheint diese Warnmeldung nicht und Sie können den Modus für Ihre Clientzugriffslizenzen einfach ändern. Wenn Sie den Lizenzierungsmodus jedoch schon einmal geändert haben (oder mit diesen Einstellungen schon einmal herumgespielt haben), erscheint diese Warnmeldung. Um den Lizenzierungsmodus zu ändern, klicken Sie auf die Schaltfläche **Nein**. Wenn Sie den Vorgang hier jedoch abbrechen möchten, klicken Sie auf die Schaltfläche **Ja**. Dann erscheint wieder das Dialogfeld **Lizenzierungsmodus wählen**.

Schließlich steht Ihnen in diesem Dialogfeld noch die Option **Replikation** zur Verfügung. Mit dieser Option kann der Systemadministrator die Replikation der Lizenzierungsinformationen vom Lizenz-Server der Organisation nach anderen Windows 2000- und Windows NT 4.0 Server-Domänencontrollern im Netzwerk der Organisation sowie von den Domänencontrollern nach dem Lizenz-Server konfigurieren. Dies geschieht automatisch, wenn sämtliche beteiligten Server mit einer Version des Betriebssystems Windows 2000 Server (Server, Advanced Server oder DataCenter) arbeiten.

Um den Rechner für die Replikation zu konfigurieren, müssen Sie zunächst die Häufigkeit, mit der die Replikation erfolgen soll, festlegen. Diese hängt davon ab, ob die Replikation jeden Tag zu einer bestimmten Zeit beginnen, oder ob die Replikation immer nach einer bestimmten Anzahl von Stunden erfolgen soll. Dabei kann für die Anzahl der Stunden eine Zahl zwischen 1 und 72 angegeben werden. Wählen Sie die von Ihnen gewünschte Option, indem Sie das entsprechende Optionsfeld aktivieren. Beachten Sie, dass Sie nur eine der beiden Optionen wählen können (siehe Abbildung 16.9).



Abbildung 16.9: Konfigurieren der Replikation von Lizenzierungsinformationen

Nachdem Sie die von Ihnen gewünschte Option gewählt haben, geben Sie mit Hilfe der Bildlaufleisten einen Wert für das Feld ein. Denken Sie daran, dass Sie bei den Feldern neben **Startzeit** zuerst auf das entsprechende Feld klicken müssen, bevor Sie mit den Bildlaufleisten arbeiten können. Wenn Sie die Häufigkeit und die Uhrzeit bzw. die Anzahl der Stunden festgelegt haben, klicken Sie auf **OK**. Daraufhin erscheint das Dialogfeld **Lizenzierungsmodus wählen**. Klicken Sie auch hier auf **OK**, um die Konfiguration der Lizenzierung abzuschließen.

16.2 Betriebssysteme für Clients

Es gibt einiges zu beachten, wenn Client-Computer, die mit einem Nicht-32-Bit-Windows-Betriebssystem arbeiten, auf Windows 2000-Server zugreifen sollen. Zu diesen Betriebssystemen zählen:

- *Microsoft Windows 3.x*. Diese Version von Windows kam 1990 auf den Markt und war die erste »populäre« Version von Windows, die als Netzwerk-Client verwendet wurde (sie wird üblicherweise für die Verbindung mit Novell NetWare- oder IBM LAN Manager-Server verwendet).
- *Microsoft Windows für Workgroups 3.1x*. Kam Ende 1992 als Version 3.10 auf den Markt und wurde bis zur Version 3.11 im Oktober 1993 aktualisiert. Windows für Workgroups war der erste Versuch eines Peer-zu-Peer-Betriebssystems von Microsoft. Es war diese Version, die angeblich die Basis für die erste Version von Windows NT (Version 3.1) darstellte, die ebenfalls im Oktober 1993 auf den Markt kam.
- *IBM/Microsoft OS/2*. Microsoft entwickelte Ende der 80er-Jahre ursprünglich auf Geheiß von IBM das Betriebssystem OS/2 (die Versionen 1.0 bis 2.1). Dem folgten Jahre des ideologischen Kampfes, der damit endete, dass IBM die Entwicklung von OS/2 übernahm (die Versionen 2.1 bis heute, einschließlich sämtlicher »Warp«-Versionen seit 1992). OS/2 basiert auf der Netzwerktechnologie LAN-Manager und sollte ein Peer-zu-Peer-Betriebssystem mit einer soliden grafischen Benutzeroberfläche mit einem überdurchschnittlich guten Kommunikationsdesign sein. Und entsprach es diesen Vorstellungen? Vielleicht, vielleicht auch nicht. Es gibt immer noch ein paar auf OS/2 basierende Clients und sogar noch einige wenige auf OS/2 basierende Server. Obwohl es nur noch wenige sind, ist deren Existenz wichtig genug, dass Microsoft für Verbindungsmöglichkeiten mit Windows 2000-Servern sorgt.
- *Macintosh*. Dieses Technologieteam wurde 1979 von dem damaligen Technikguru von Apple

Computer, Jeff Rushkin, gegründet. Dieses Team entwickelte 1983 Lisa (nach der Tochter von Steve Jobs benannt), die erste Version des Betriebssystems, und 1984 das unter der Bezeichnung Macintosh bekannte Rushkin-Projekt. Der Macintosh-Computer ist im Wesentlichen ein ausschließlicher Client-Computer (es gibt kaum Macintosh-Server), der mit den meisten anderen x86-Client-Computern, die es heute praktisch überall gibt, nicht kompatibel ist. Der Macintosh ist auch mit anderen Apple-Computern nicht kompatibel.

- **UNIX.** Als zum letzten Mal gezählt wurde, gab es über 140 bekannte Versionen von UNIX (System V von AT&T, XENIX von Microsoft, AIX von IBM, UX von HP, OS und Solaris von Sun, die unzähligen Versionen von Linux von Caldera bis zu RedHat usw.) und zahllose Varianten und Versionen dieser bekannten Versionen. Es gibt zwar viele verschiedene Arten, mit diesen Betriebssystemen auf Windows 2000 Server zuzugreifen. Dabei gibt es jedoch einige Dinge, die Sie beachten sollten, bevor Sie ein UNIX-System in Ihrem Windows 2000-Netzwerk integrieren.

Wenn Sie festgelegt haben, welche Arten von Client-Betriebssystem mit Ihrer Windows 2000 Server-Umgebung verbunden werden müssen, sollte sich die Organisation überlegen, ob es angesichts des erhöhten Aufwands und den damit verbundenen erhöhten Kosten für die Verwaltung und Unterstützung dieser älteren Client-Betriebssysteme (die aktuelleren UNIX- und Macintosh-Client-Computer sind damit nicht gemeint) wirklich sinnvoll ist, diese älteren Betriebssysteme weiter zu verwenden. Diese Frage sollte geklärt sein, lange bevor Sie damit beginnen, diese älteren Client-Betriebssysteme mit Ihren neuen Windows 2000-Servern zu konfigurieren und zu verwalten.

Vorausgesetzt, diese Betriebssysteme sollen weiter verwendet werden, sollten Sie sich für die nun folgende Arbeit rüsten. Was Sie dafür neben den Clientzugriffslizenzen benötigen, hängt vom Betriebssystem der Client-Computer ab. Die folgenden vier Abschnitte sollten Ihnen bei der Vorbereitung auf diese manchmal widerspenstigen, aber notwendigen Konfigurationen behilflich sein.

16.2.1 Novell NetWare-Clients

Damit Novell NetWare-Client-Computer Windows 2000 Server für Datei- und Druckdienste nutzen können, muss zuerst der Gateway Service für NetWare auf dem Windows 2000-Server installiert werden. Denken Sie daran, dass es sich dabei um »reine« NetWare-Clients handelt, und nicht um Windows 9x-, Windows NT- oder Windows 2000-Clients, die zufällig sowohl auf Ihre Novell NetWare-Server als auch auf Ihre Windows 2000-Server zugreifen. Um den Gateway Service für NetWare zu installieren, klicken Sie auf dem Desktop von Windows 2000 Server mit der rechten Maustaste auf **Netzwerkumgebung**. Daraufhin erscheint das in Abbildung 16.10 dargestellte Menü.

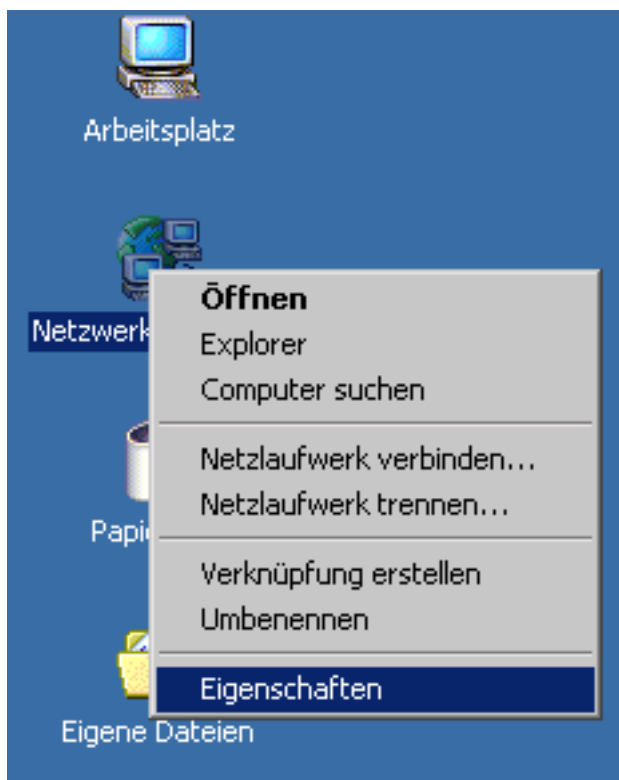


Abbildung 16.10: Auswahl der Option Eigenschaften für die Netzwerkumgebung

Wählen Sie unten in diesem Menü die Option **Eigenschaften**. Daraufhin öffnet sich das Dialogfeld **Netzwerk- und DFÜ-Verbindungen** (siehe Abbildung 16.11).



Abbildung 16.11: Ihre Netzwerk- und DFÜ-Verbindungen

Klicken Sie in diesem Dialogfeld mit der rechten Maustaste auf das Symbol **LAN-Verbindung**. Dabei öffnet sich wieder ein Menü, in dem Sie erneut die Option **Eigenschaften** wählen. Daraufhin erscheint das Dialogfeld **Eigenschaften von LAN-Verbindung** (siehe Abbildung 16.12).



Abbildung 16.12: Eigenschaften für LAN-Verbindung

In diesem Dialogfeld können Sie auf die Schaltfläche **Installieren** klicken, die sich unterhalb des Bereichs befindet, in dem die installierten Komponenten aufgelistet sind. Das Entscheidende daran ist, dass Sie den Gateway Service für NetWare erst nutzen können, wenn Sie ihn installiert haben. Werfen Sie dennoch einen kurzen Blick auf die Liste der installierten Komponenten, um sich zu vergewissern, dass der Gateway Service für NetWare nicht bereits installiert ist. Wenn Sie sich vergewissert haben, dass Sie den Gateway Service für NetWare installieren müssen, klicken Sie auf die Schaltfläche **Installieren**. Daraufhin erscheint das Dialogfeld **Typ der Netzwerkkomponente auswählen** (siehe Abbildung 16.13).

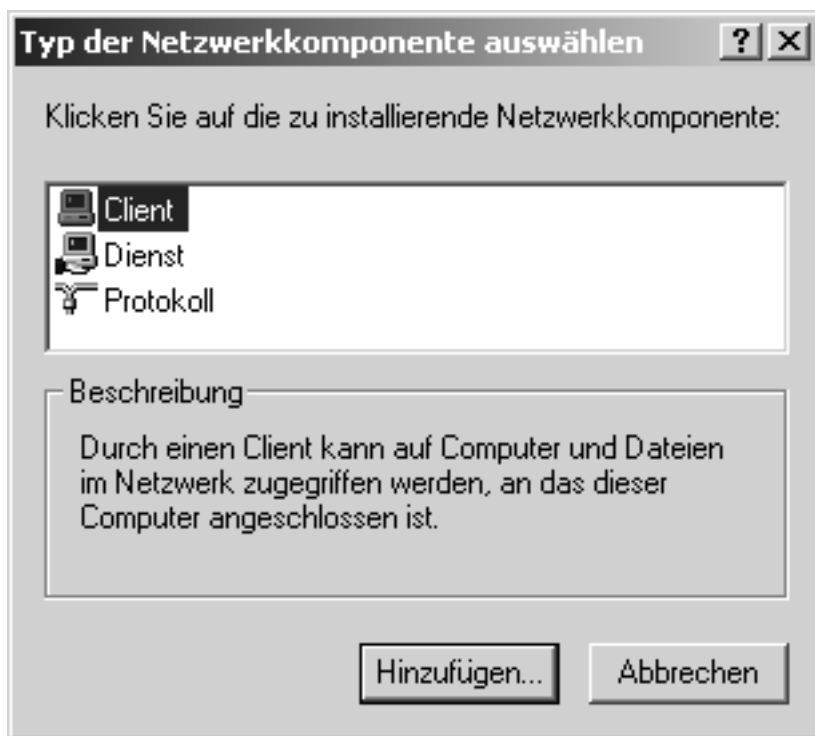


Abbildung 16.13: Auswahl einer neuen Netzwerkkomponente

Klicken Sie in diesem Dialogfeld auf den Client-Typ, um ihn zu markieren. Klicken Sie dann auf die Schaltfläche **Hinzufügen**. Daraufhin erscheint das Dialogfeld **Netzwerkclient wählen** (siehe Abbildung 16.14).

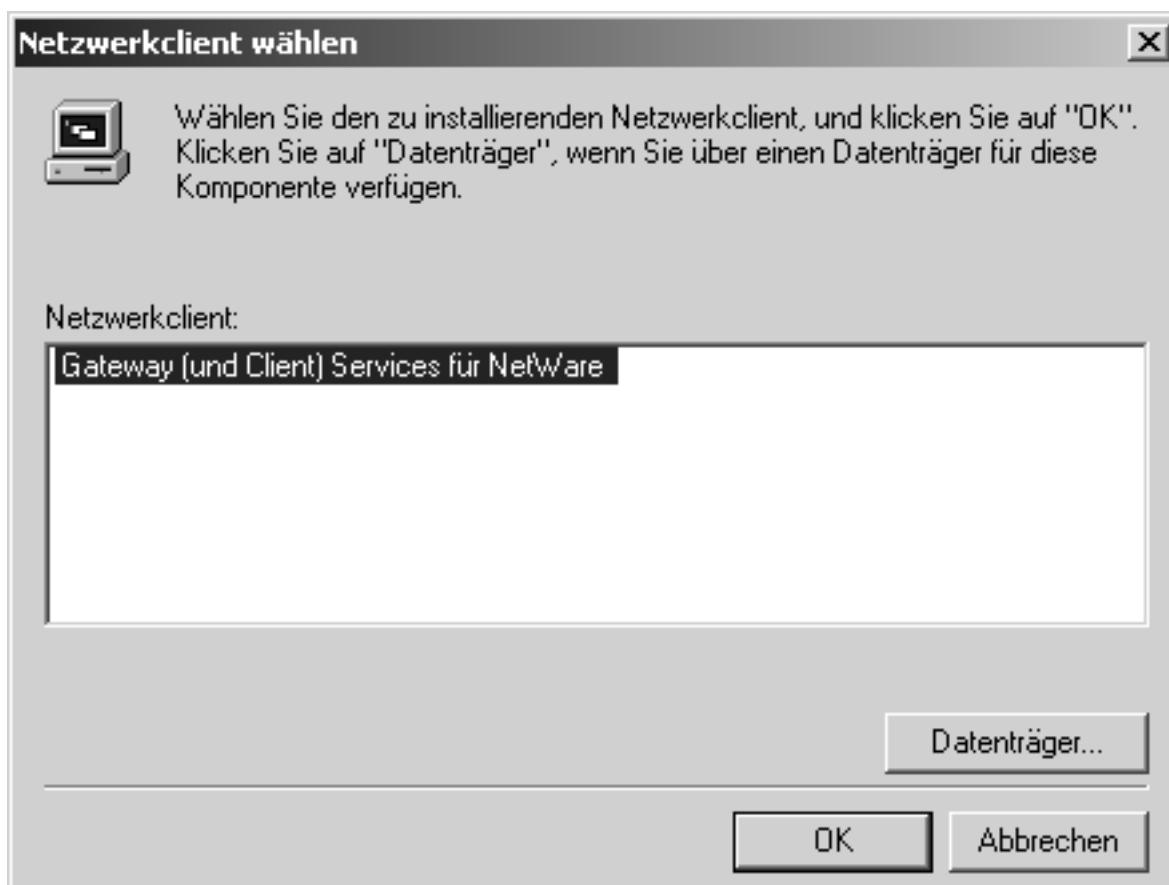


Abbildung 16.14: Auswahl des Gateway (und Client) Services für NetWare

Wenn Sie dieses Dialogfeld zum ersten Mal aufrufen, wird hier nur eine Komponente für eine mögliche Installation angezeigt: Gateway (und Client) Services für NetWare. Die Entscheidung fällt dabei leicht. Klicken Sie einfach auf **Gateway (und Client) Services für NetWare**, um diese Option auszuwählen, und bestätigen Sie dann mit **OK**, um den Installationsvorgang zu beginnen. Nun benötigen Sie die CD-ROM von Windows 2000 Server, um einige Dateien zu kopieren, die für die Installation von Gateway (und Client) Services für NetWare erforderlich sind. Wenn diese Dateien kopiert sind, erscheint das Dialogfeld **Bevorzugte NetWare-Anmeldung wählen** (siehe Abbildung 16.15).



Abbildung 16.15: Auswahl der bevorzugten NetWare-Anmeldung

Dieses Dialogfeld erscheint jedoch nicht immer. Wenn dieses Dialogfeld erscheint, müssen Sie als Erstes entscheiden, mit welchem bevorzugten Server das Verwaltungskonto Ihres Windows 2000-Servers verbunden werden soll. Das ist wichtig, weil dies auch der Novell NetWare-Server ist, den sämtliche NetWare-Clients passieren, um auf den Windows 2000-Server zuzugreifen. Wenn Sie jedoch einen Windows 2000-Server als Gateway-Verbindung für die NetWare-Client-Computer verwenden, sollten Sie beachten, dass die Novell-Anmeldeskripten für diese NetWare-Clients nicht ausgeführt werden. Benutzer müssen direkt auf einen Novell-Server zugreifen, damit ihre Anmeldeskripten richtig ausgeführt werden. Das ist nichts Dramatisches, aber der Systemadministrator sollte es beachten.

Ähnliches wie für den bevorzugten NetWare-Server gilt auch für eine *Standardstruktur und -kontext*. Die Entscheidung, einen bevorzugten NetWare-Server oder eine Standardstruktur und einen Standardkontext zu verwenden, ist einfach: Wenn Ihre Organisation NDS (NetWare Directory Service) von Novell verwendet, dann sollten Sie die Option **Standardstruktur und -kontext** wählen. Ansonsten sollten Sie die Option **Bevorzugter Server** wählen. Klicken Sie dazu auf das entsprechende Optionsfeld und geben Sie dann den entsprechenden Server oder den Namen der Struktur und den Benutzerkontext an. Wenn Sie das getan haben, müssen Sie sich entscheiden, ob Sie bei der Anmeldung Ihr Anmeldeskript ausführen möchten. Dabei handelt es sich um das Skript, das auf dem Novell-Server, nicht auf dem Windows 2000-Server ausgeführt wird. Wenn Sie alle Entscheidungen getroffen haben, klicken sie auf

OK, um Ihre Einträge zu speichern und zum Dialogfeld **Eigenschaften von LAN-Verbindung** zurückzukehren (siehe Abbildung 16.16).



Abbildung 16.16: Eigenschaften von LAN-Verbindung

Wenn dieses Dialogfeld wieder erscheint, werden Sie feststellen, dass nun die Option **Gateway (und Client) Services für NetWare** installiert ist. Und noch etwas Erstaunliches geschieht: Sie werden nicht aufgefordert, Ihren Windows 2000 Server-Rechner neu zu starten, damit Sie den Dienst nutzen können! Das ist eine sehr willkommene Änderung im Vergleich zu der älteren Windows NT 4.0 Server-Version desselben GSNW-Dienstes (Gateway Services für NetWare). Nur um sicherzugehen, dass alles richtig konfiguriert worden ist, sollten Sie im Bereich der installierten Komponenten (das ist das große weiße Feld im mittleren Bereich des Dialogfelds, in dem Komponenten, Protokolle und Dienste aufgelistet sind) nachsehen, ob die Option **NWLink IPX/SPX/NetBIOS-kompatibles Transportprotokoll** aufgeführt ist. Markieren Sie dieses Protokoll. Klicken Sie dann auf die Schaltfläche **Eigenschaften**, um das in Abbildung 16.17 dargestellte Dialogfeld aufzurufen.

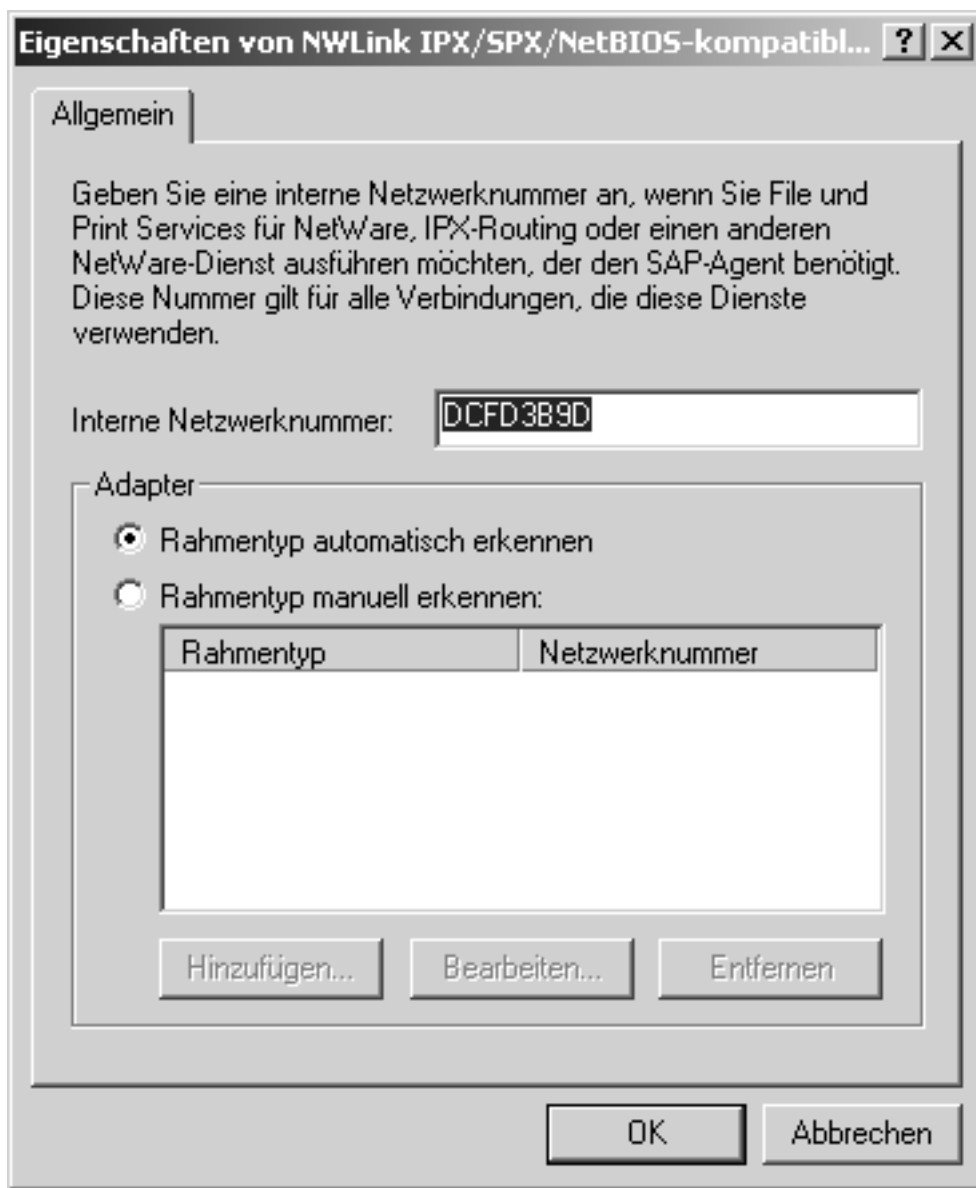


Abbildung 16.17: Zuweisen einer internen Netzwerknummer für die NetWare-Konnektivität

Die wohl wichtigste Option in diesem Dialogfeld ist die Einstellung der internen Netzwerknummer. Windows 2000 verwendet standardmäßig acht Nullen (00000000), was Sie bei Bedarf ändern können. Im Wesentlichen müssen Sie darauf achten, dass NetWare für jeden seiner Server und Gateways einheitliche Netzwerknummern verlangt. Daher kann es sein, dass Sie diese Nummer ändern müssen, damit Ihr neu installierter GSNW-Dienst richtig funktioniert. Ebenso kann es zu Konflikten bezüglich der in Ihrem lokalen und/oder WAN-Netzwerk verwendeten Ethernet-Rahmentypen kommen. Wenn dies der Fall ist, dann ändern Sie die Einstellung des Rahmentyps und wählen statt der (oberen) Standardeinstellung **Rahmentyp automatisch erkennen** die Option **Rahmentyp manuell erkennen**. Dies geschieht, indem Sie in das entsprechende Optionsfeld und dann auf **OK** klicken, um die Einstellungen zu speichern. Damit kehren Sie zum Optionsfeld **Eigenschaften von LAN-Verbindung** zurück. Dort müssen Sie nochmals auf **OK** klicken, um Ihre sämtlichen Einstellungen abschließend zu speichern und dieses Dialogfeld zu schließen.

Es gibt noch einige weitere Dinge, die Sie beachten sollten, wenn Sie eine Verbindung zwischen einem Windows 2000 Server-Rechner und einem Novell-Client herstellen möchten:

- *Umgebungsvariable*. Dies sind die Einstellungen, die üblicherweise in der config.sys-,

autoexec.bat- oder verschiedenen anderen Stapel- oder *.ini-Dateien sowie innerhalb der Registrierungsdateien von Windows 3.x- und Windows 9x-Client-Computern vorgenommen werden. Änderungen innerhalb dieser Dateien können die Art und Weise, wie ein NetWare-Client auf einen Windows 2000-Server zugreift, dramatisch ändern. Es kann auch dazu kommen, dass überhaupt keine Verbindung zustande kommt. Seien Sie also mit diesen Arten von Dateien vorsichtig.

- *IPX/SPX-kompatibler Transport zum Drucken.* Novell NetWare-Clients können mit Hilfe des IPX/SPX-kompatiblen Transports (ein Netzwerkprotokoll, das kostenlos bei Microsoft erhältlich ist) Druckaufträge direkt an einen Windows 2000-Server senden, der sich im Druckserver-Modus befindet. Dazu müssen Sie lediglich auf dem Windows 2000-Server die Datei- und Druckdienste für Microsoft sowie sämtliche verwendbaren Drucker installiert haben.
- *File und Print Services für NetWare.* Dieses Produkt kann zusätzlich zu der Software des Betriebssystems Windows 2000 Server erworben werden. Es unterscheidet sich von dem gewöhnlicheren IPX/SPX-kompatiblen Transport zum Drucken insofern, als dass sich damit ein Windows 2000-Server für NetWare-Clients als NetWare-Server präsentieren kann. Das bedeutet, dass die verschiedenen NetWare-Clients in Ihrem Netzwerk zwischen dem Windows 2000-Server und den Novell NetWare-Servern nicht unterscheiden können. Das wiederum bedeutet, dass Sie Ihre Datei- und Druckdienste aus Ihrem Novell-Netzwerk entfernen und in Ihrem Windows 2000 Server-Netzwerk installieren können, ohne dazu einen Ihrer NetWare-Client-Computer auch nur berühren zu müssen. Das ist ein recht erstaunliches Stück Technologie für die Organisationen, die aus ihrer gemischten Windows 2000/Novell NetWare LAN-Umgebung eine reine Windows 2000-Netzwerkumgebung machen möchten.

16.2.2 DOS, OS/2, Windows 3.x und Windows für Workgroups

Sowohl Windows 3.x als auch Windows für Workgroups ist nichts anderes als eine auf das alte DOS (Disk Operating System) aufgepfropfte grafische Benutzeroberfläche. Weil das so ist, unterscheiden sich diese beiden Betriebssysteme in ihrer Konnektivität zu Windows 2000 Server nicht wesentlich von den auf DOS basierenden Systemen (sei es nun MS-DOS von Microsoft oder DR-DOS von Digital Research). Die Konnektivität zu einem Windows 2000-Server auf Seiten des Client herzustellen, ist mit Ausnahme der Installation der geeigneten Client-Hardware und -Software nicht allzu schwierig. Die Hardware wird wohl die schwierigere Aufgabe für Dateidienste sein, da Sie Netzwerkkarten mit den entsprechenden Software-Treibern finden müssen, die noch unter DOS, Windows 3.x und/oder Windows für Workgroups arbeiten. OS/2 wurde dagegen von Microsoft und IBM gemeinsam als die Zukunft sowohl von Windows als auch von Peer-zu-Peer-Betriebssystemen entwickelt. Es kam dann aber bekanntlich angesichts der Entwicklung von Windows NT und dann von Windows 2000 anders.

Da Microsoft mit der Herausgabe von Windows 95 vor über fünf Jahren der 16-Bit-Windows-Welt den Rücken gekehrt hat und angesichts der Tatsache, dass Microsoft seither eine zweite Version von Windows 95 (OSR2) und zwei Versionen von Windows 98 auf den Markt gebracht hat, dürfte es ziemlich schwierig sein, die Hardware- und Software-Treiber zu finden, die die physikalische Verbindung zu Ihrem Windows 2000-Netzwerk möglich machen. Viele Organisationen arbeiten noch mit einer beträchtlichen Menge an älteren 16-Bit-Versionen des Windows-Betriebssystems. Daher nehmen wir an, dass Sie die Hardware vorfinden werden, die für eine physikalische Verbindung erforderlich ist.

Wenn Sie die Hardware installiert haben, müssen Sie ein geeignetes Netzwerkprotokoll für die Verbindung Ihrer DOS-, Windows 3.x- und/oder Windows für Workgroups-Clients mit dem Windows 2000 Server-Rechner suchen. Für die DOS-Clients eignet sich wohl das Netzwerkprotokoll IPX/SPX am besten, da dies das Protokoll war, das DOS-Clients für den Zugriff auf die alten Novell NetWare-Server in der Regel verwendeten. Für die Windows 3.x-Client-Computer sollten Sie am besten auch das Netzwerkprotokoll IPX/SPX verwenden. Wenn es sich jedoch um eine kleine lokale Arbeitsgruppe handelt (d.h. weniger als 25 Benutzer und Netzwerk ohne Router), dann ist das Netzwerkprotokoll NetBEUI von Microsoft besser geeignet. Auch wenn sich TCP/IP für Sie vielleicht besser anhört, ist dieses für Windows 3.x-Systeme nicht verfügbar. Ihre Windows für Workgroups-Clients profitieren am meisten, wenn Sie die TCP/IP-Netzwerk-Software installieren, die Microsoft speziell für diese Peer-zu-Peer-Version von Windows 3.1 und 3.11 auf den Markt brachte.

Wenn Sie sich für ein Netzwerkprotokoll entschieden haben, müssen Sie dafür sorgen, dass diese Protokolle auf Ihrem Windows 2000-Server installiert sind. Um zu prüfen, welche Protokolle installiert sind, müssen Sie wieder das Dialogfeld **Eigenschaften von LAN-Verbindung** aufrufen, das Sie bereits bei der Konfiguration Ihrer Novell NetWare-Client-Computer kennen gelernt haben. Wenn Sie diesen Abschnitt übersprungen haben oder nicht mehr so genau wissen, wie Sie zu diesem Dialogfeld gelangen, dann befolgen Sie einfach die folgenden Anweisungen. Ansonsten können Sie diesen Abschnitt nun überspringen und bei dem Abschnitt über die Installation des Netzwerkprotokolls NetBEUI weiterlesen.

Um das Dialogfeld **Eigenschaften von LAN-Verbindung** aufzurufen, klicken Sie auf dem Desktop von Windows 2000 Server mit der rechten Maustaste auf **Netzwerkumgebung**. Daraufhin erscheint ein kleines Menü. Wählen Sie unten in diesem Menü die Option **Eigenschaften**. Daraufhin öffnet sich das Dialogfeld **Netzwerk- und DFÜ-Verbindungen**. Klicken Sie in diesem Dialogfeld mit der rechten Maustaste auf das Symbol **LAN-Verbindung**. Dabei öffnet sich wieder ein Menü, in dem Sie erneut die Option **Eigenschaften** wählen. Daraufhin erscheint das Dialogfeld **Eigenschaften von LAN-Verbindung**. Suchen Sie nun mit Hilfe der Bildlaufleiste die folgenden Netzwerkprotokolle:

- NetBEUI-Protokoll
- NWLink IPX/SPX/NetBIOS-kompatibles Transportprotokoll
- NWLink NetBIOS (erscheint, wenn Sie das erste NWLink-Netzwerkprotokoll installieren)
- Internetprotokoll (TCP/IP)

Das Internetprotokoll (TCP/IP) ist immer installiert, da dies das Standardprotokoll für Windows 2000 Server ist. Wenn Sie Gateway (und Client) Services für NetWare bereits installiert haben, werden auch beide NWLink-Protokolle in der Liste aufgeführt. Es ist allerdings sehr wahrscheinlich, dass Sie das NetBEUI-Protokoll nicht vorfinden werden. Daher sollten Sie dieses Protokoll jetzt installieren.

Um das NetBEUI-Protokoll zu installieren, klicken Sie im Dialogfeld **Eigenschaften von LAN-Verbindung** auf die Schaltfläche **Installieren**. Daraufhin öffnet sich das Dialogfeld **Typ der Netzwerkkomponente auswählen** (siehe Abbildung 16.18).

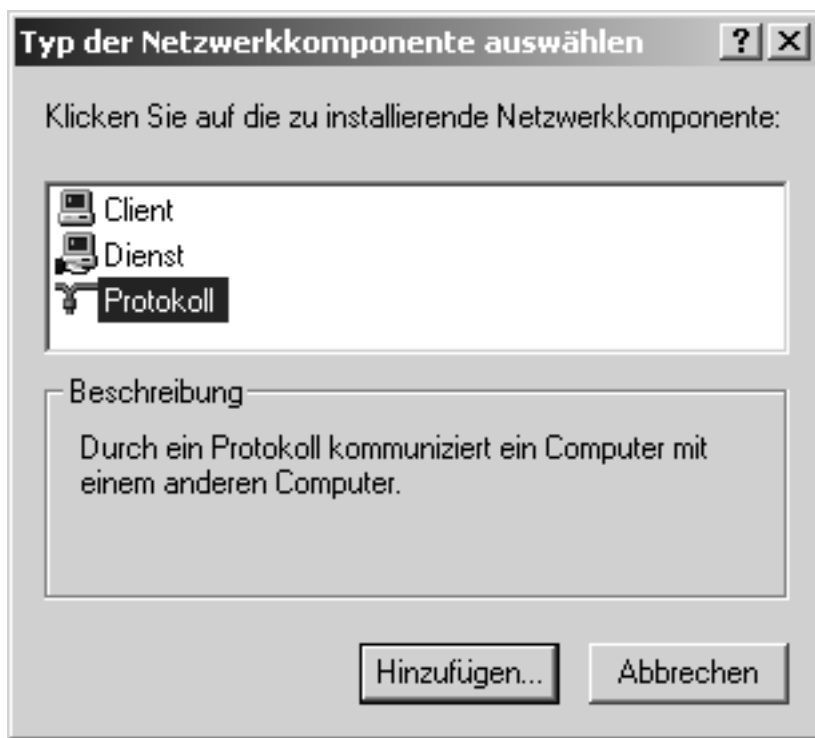


Abbildung 16.18: Auswählen eines neuen Netzwerkprotokolls

Klicken Sie in diesem Dialogfeld auf das Protokoll und dann auf die Schaltfläche **Hinzufügen**. Daraufhin erscheint das Dialogfeld **Netzwerkprotokoll wählen** (siehe Abbildung 16.19).



Abbildung 16.19: Installieren des Netzwerkprotokolls NetBEUI

Klicken Sie in diesem Dialogfeld auf die Option **NetBEUI-Protokoll** und dann auf **OK**, um mit der Installation zu beginnen. Dazu benötigen Sie die CD-ROM von Windows 2000 Server oder eine Netzwerkfreigabe, die die entsprechenden Dateien für diesen Vorgang enthält. Wenn die Installation abgeschlossen ist, erscheint wieder das Dialogfeld **Eigenschaften von LAN-Verbindung**. Sie werden sehen, dass hier nun das NetBEUI-Protokoll mit den anderen Protokollen aufgeführt wird (Abbildung 16.20).



Abbildung 16.20: Bestätigen der Installation des Netzwerkprotokolls NetBEUI

Die Installation ist auf Seiten des Windows 2000-Servers abgeschlossen, wenn dieses Dialogfeld wieder erscheint. Auch hier müssen Sie den Windows 2000-Server nicht neu starten, um das neue Netzwerkprotokoll zu aktivieren. Klicken Sie einfach auf die Schaltfläche **Schliessen**, um dieses Dialogfeld zu schließen. Nun können die DOS-, Windows 3.x- und Windows für Workgroups-Clients auf Ihren Server zugreifen.

Wenn ein Windows 2000-Server als Druck-Server verwendet werden soll, müssen Sie einige weitere Dinge berücksichtigen:

- **16-Bit-Druckertreiber.** Sie müssen auf den DOS-Clients die entsprechenden 16-Bit-Druckertreiber installieren, da die Clients nicht in der Lage sind, die Funktionen des Windows 2000

Server-Betriebssysteme für den Druckvorgang zu nutzen. Sehen Sie auf der Web-Seite Ihres Software-Pakets nach, ob es noch DOS-Druckertreiber für den von Ihnen gewünschten Drucker gibt. Falls nicht, müssen Sie selbst ein Treiberprogramm schreiben, was keine einfache Aufgabe ist.

- *Umleitung von Druckaufträgen.* Bei Druckeranforderungen von älteren DOS-, Windows 3.x- und Windows für Workgroups-Clients müssen die Druckaufträge üblicherweise von den seriellen COM- bzw. von den parallelen LPT-Anschlüssen an einen Netzwerkanschluss umgeleitet werden. Bei DOS wird dafür in der Regel der Redirector des LAN Manager verwendet. Bei Windows 3.x-Clients wird der Redirector von Microsoft Network Client 3.0 für Windows verwendet, während Windows für Workgroups-Clients den im Betriebssystem Windows für Workgroups integrierten Redirector verwenden. Die Umleitung kann über eines der unterstützten Netzwerkprotokolle (NetBEUI, NWLink oder TCP/IP) erfolgen und der Befehl lässt sich im Wesentlichen leicht anwenden. Um beispielsweise einen Drucker am parallelen Anschluss LPT1 (1 steht für die Anschlussnummer) umzuleiten, wird der Befehl `net use` verwendet:

```
Net use lpt1 \\DruckServerName\DruckerFreigabeName
```

Damit wird dem Client-Computer mitgeteilt, dass der Druckerverkehr vom lokalen LPT1-Anschluss an den freigegebenen Netzwerkdrucker, der sich auf einem bestimmten Windows 2000-Druck-Server befindet, umgeleitet werden soll. Dieser Befehl sieht je nach dem Betriebssystem, auf dem er ausgeführt wird, etwas anders aus. Aber das ist im Wesentlichen die Befehlsstruktur. Darüber hinaus kann ein Befehl wie dieser als Teil einer Stapeldatei wie z.B. der Datei `Autoexec.bat` oder der Anmeldeskript-Datei des Client-Computers ausgeführt werden.

- *OS/2-Druckkonnektivität.* Damit ein Computer, der mit einem OS/2-Client- oder Server-Betriebssystem arbeitet, auf die Datei- und Druckdienste eines Windows 2000-Servers zugreifen kann, muss auf diesem Computer der LAN Manager 2.x (oder eine neuere Version) installiert sein. Dazu zählen auch Computer, die mit den Warp-Versionen von OS/2 arbeiten. Da die meisten Installationen von OS/2 auf TCP/IP basieren, ist die Netzwerkkonnektivität selbst nicht so schwer zu erreichen wie bei einigen anderen Client-Computern. Die Umleitung der Druckeranschlüsse erfolgt auf dieselbe Art und Weise wie bei einem Windows für Workgroups-Client.
- *Windows 2000 Server-Fonts und -Formulare.* Die Fonts und Formulare, die die Windows 2000-Druck-Server anderen Windows 2000- und Windows NT 4.0-Computern zur Verfügung stellen, sind für Client-Computer wie UNIX-, Macintosh-, DOS-, OS/2-, Windows 3.x- und Windows für Workgroups-Computer nicht verfügbar.

Wenn Sie mit diesen älteren Client-Computern auf Datei- und Druckdienste auf Ihren Windows 2000-Servern zugreifen möchten, sollten Sie sich immer fragen: »Warum?« Warum versuchen Sie diese Versionen mit ihren erhöhten Kosten für Verwaltung und Benutzerunterstützung zu verwenden, wenn es viele andere Client-Betriebssysteme mit deutlich geringeren Gesamtkosten (Total Cost of Ownership) gibt? Es ist natürlich technisch möglich, die älteren Client-Computer Ihrer Organisation in der Windows 2000 Server-Welt weiterhin zu verwenden. Aber die Gesamtkosten der Organisation sind um einiges höher, als sie eigentlich sein müssten. Das ist das Wichtigste, was Sie sich im Zusammenhang mit Windows 2000 Server merken sollten: Dieses Betriebssystem wird Ihre Gesamtkosten für die

Client-Computer senken, aber nur, wenn Sie das zulassen.

16.2.3 Macintosh

Die Entwicklungsgeschichte von Macintosh nimmt einen recht einförmigen Verlauf, wenn man sich einmal den Weg von der Entstehung über die Blüte in den späten 80er-Jahren bis hin zu den ruhigeren Zeiten in den 90er-Jahren betrachtet. Es sind genau dieselben Aspekte der grafischen Benutzeroberfläche von Macintosh, die dieses Betriebssystem einerseits so beliebt gemacht und andererseits zu dessen Problemen bei der technischen Unterstützung geführt haben. Das Unternehmen Apple Computer kopierte die grafische Benutzeroberfläche für die Macintosh-Computer von Xerox und machte daraus eine »benutzerfreundliche« Benutzeroberfläche für die breite Masse. Dabei wurde leider die Integration der Welt des PC und der effizienten Netzwerkwelt außer Acht gelassen.

Damit Ihre Macintosh-Clients auf einen Windows 2000-Server zugreifen können, müssen Sie auf beiden Rechnern einige Änderungen vornehmen: Auf dem Windows 2000-Server müssen spezielle Dienste installiert und ausgeführt werden und beim Macintosh-Rechner müssen Sie die Netzwerkkonnektivität über Ethernet sowie die Unterstützung des Netzwerkprotokolls AppleTalk sicherstellen. Das bedeutet, dass Ihr Windows 2000-Server wie jedes andere AppleTalk-Druckgerät erscheinen muss.

Um nun diese Dienste zu installieren, klicken Sie auf dem Desktop von Windows 2000 Server mit der rechten Maustaste auf **Netzwerkumgebung**. Daraufhin erscheint ein kleines Menü. Wählen Sie unten in diesem Menü die Option **Eigenschaften**. Daraufhin öffnet sich das Dialogfeld **Netzwerk- und DFÜ-Verbindungen**. Öffnen Sie in diesem Dialogfeld das Menü **Erweitert** und wählen Sie die Option **Optionale Netzwerkkomponenten** (siehe Abbildung 16.21).

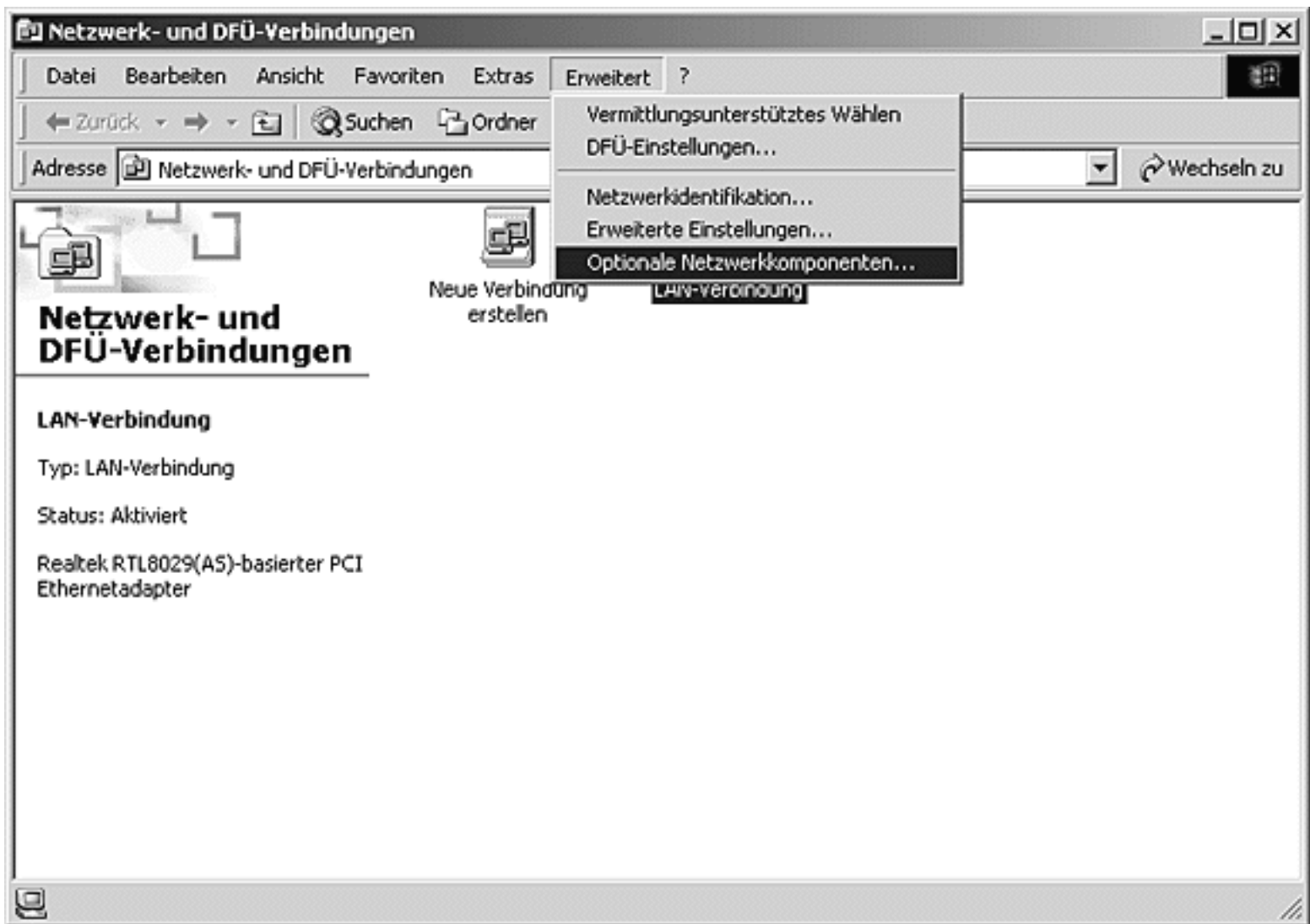


Abbildung 16.21: Installieren von optionalen Netzwerkkomponenten

Damit rufen Sie den in Abbildung 16.22 dargestellten **Assistenten für die optionalen Windows-Netzwerkkomponenten** auf.

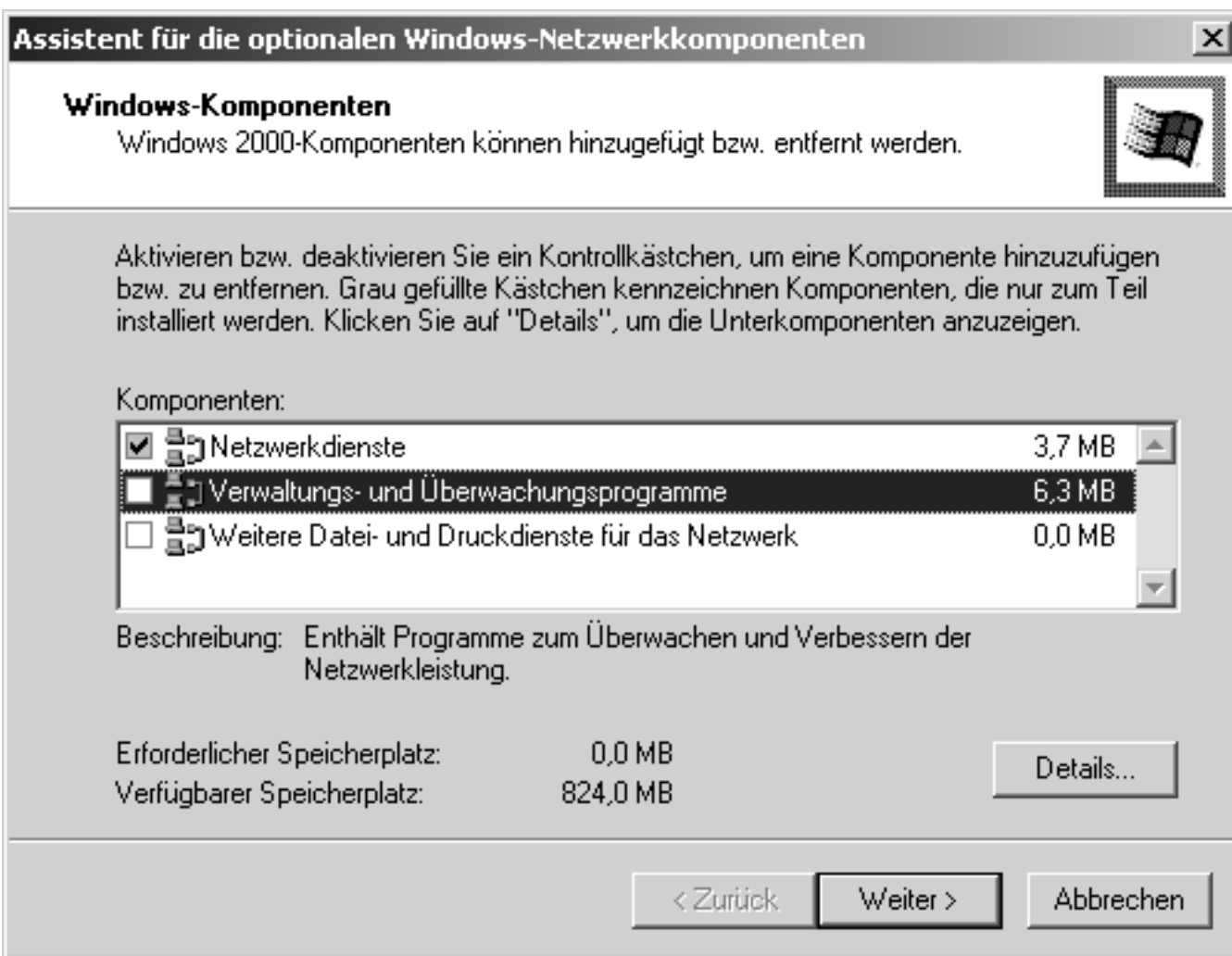


Abbildung 16.22: Aufrufen des Assistenten für die optionalen Windows-Netzwerkcomponenten

Einige der hier dargestellten Elemente sind bereits mit einem Häkchen gekennzeichnet, was bedeutet, dass diese optionalen Netzwerkcomponenten bereits installiert sind. Andere Elemente sind mit einem Häkchen gekennzeichnet und grau hinterlegt. Das bedeutet, dass mindestens eine optionale Netzwerkcomponente installiert ist, dass es in diesem Bereich jedoch mindestens eine weitere optionale Netzwerkcomponente gibt, die noch nicht installiert ist. Um nun zu erreichen, dass Ihr Macintosh-Client auf den Windows 2000-Server zugreifen kann, müssen Sie das Kontrollkästchen neben **Weitere Datei- und Druckdienste für das Netzwerk** aktivieren und dann auf die Schaltfläche **Details** klicken. Daraufhin werden die einzelnen Komponenten dieser Option angezeigt (siehe Abbildung 16.23).

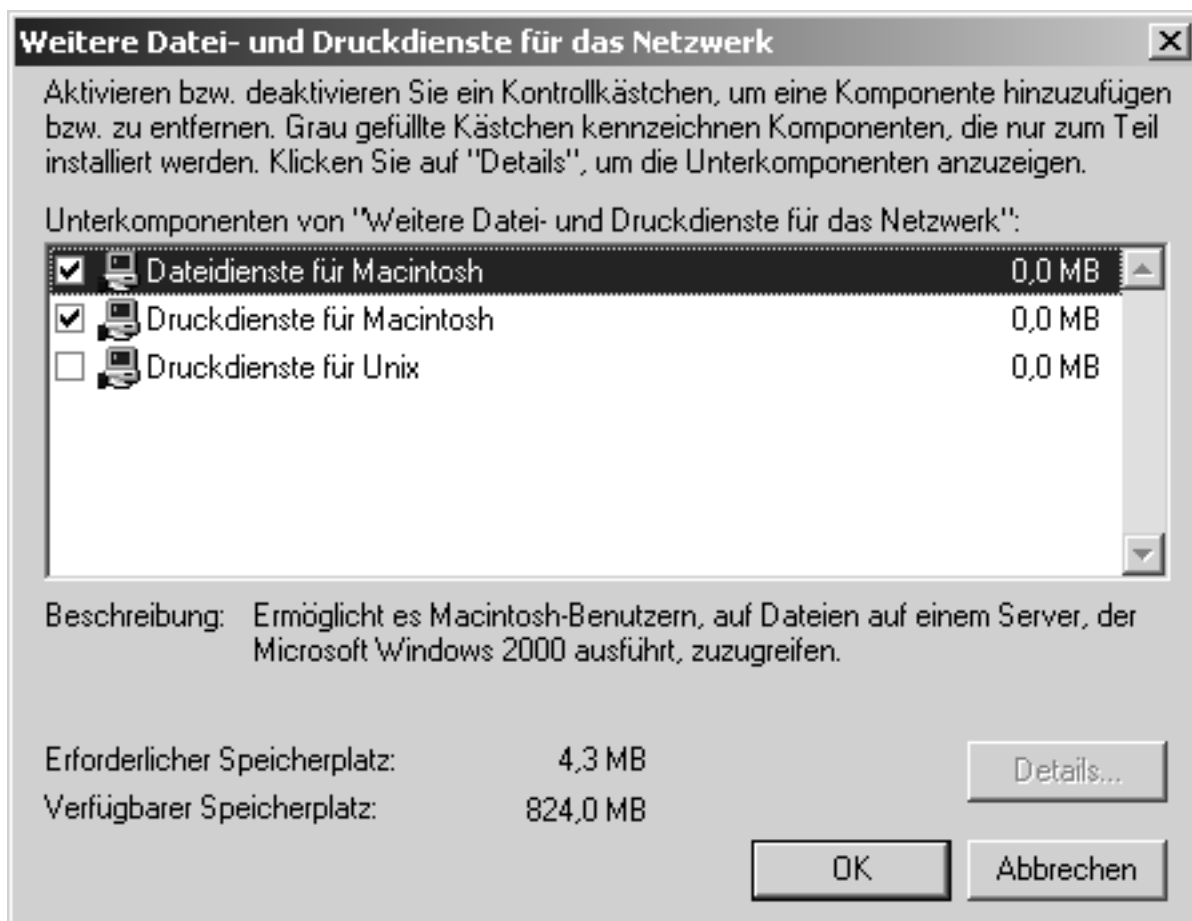


Abbildung 16.23: Auswahl weiterer Datei- und Druckdienste für das Netzwerk

Wählen Sie nun die beiden oberen Optionen: **Dateidienste für Macintosh** und **Druckdienste für Macintosh**. Klicken Sie dazu auf die Kontrollkästchen links neben den entsprechenden Optionen. Daraufhin erscheint jeweils ein Häkchen in den Kontrollkästchen. Klicken Sie anschließend auf **OK**, um die Installation der Software zu starten (siehe Abbildung 16.24). Sie benötigen dazu Ihre CD-ROM von Windows 2000 Server.

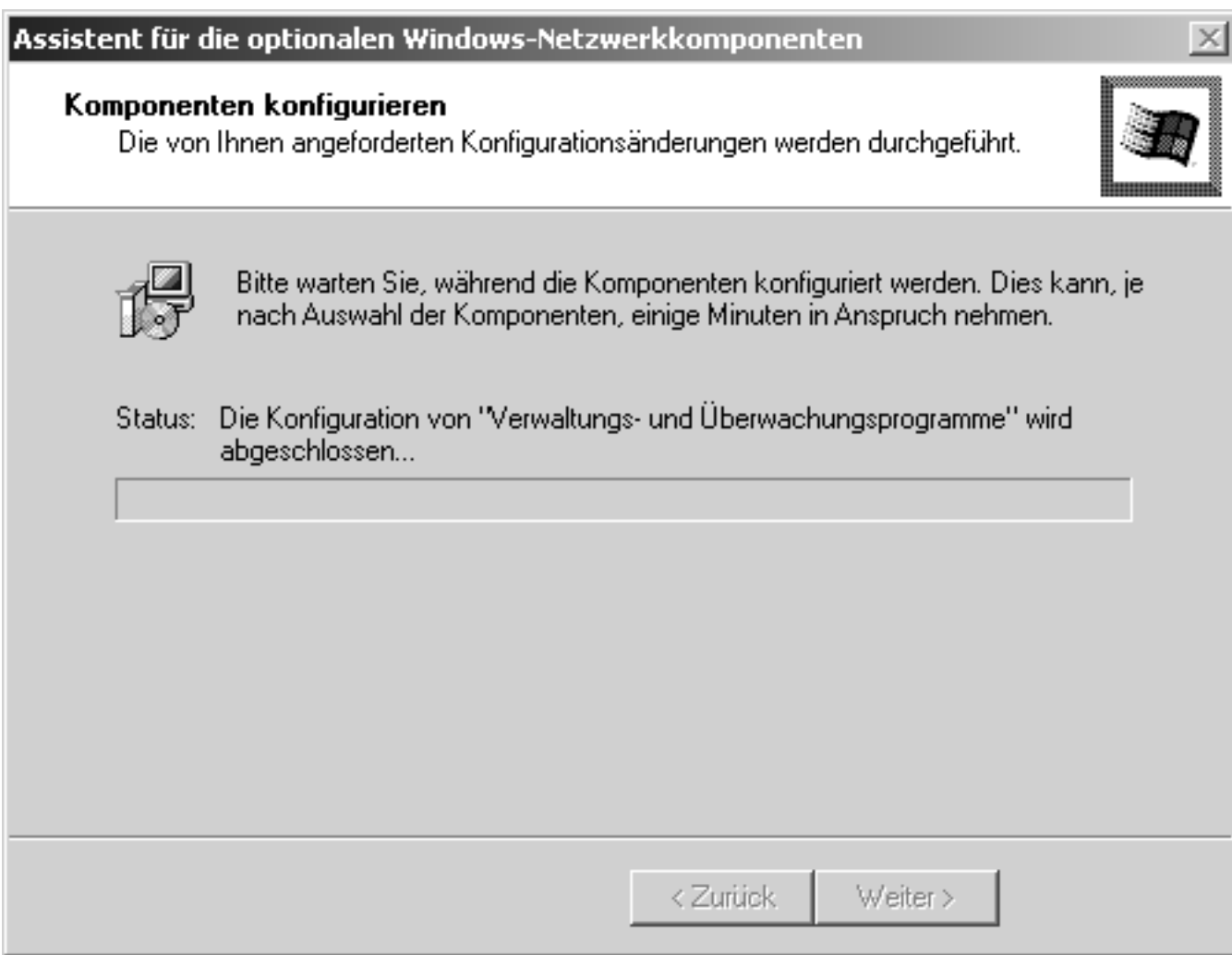


Abbildung 16.24: Die Netzwerkkomponenten werden konfiguriert

Der Assistent meldet, dass der Vorgang einige Minuten in Anspruch nehmen kann. Um diesen Vorgang abzuschließen, sind jedoch weniger als zwei bis drei Minuten erforderlich. Abschließend erscheint ein weiteres Dialogfeld, das Sie über die erfolgreiche Installation informiert. Danach wird kein weiteres Dialogfeld mehr angezeigt.

Jetzt, da die Windows 2000 Server-Dateien installiert sind, sollten Sie sich darüber Gedanken machen, welche Sicherheitsstufe Sie für Ihre Macintosh-Clients verwenden möchten. Bei Windows 2000 Server stehen Ihnen drei Stufen zur Auswahl:

- *Gast.* Bei dieser Stufe wird das herkömmliche Gastkonto von Windows 2000 Server verwendet.
- *Benutzer verwendet ein Kennwortschema in Klartext.* Der Benutzer meldet sich am Windows 2000-Server mit einer lesbaren Benutzer-ID an, die als Klartext über die Netzworkkabel versendet wird.
- *Benutzer verwendet ein verschlüsseltes Kennwortschema.* Der Benutzer meldet sich am Windows 2000-Server mit einer verschlüsselten Benutzer-ID an, sodass diese sicher im Netzwerk der Organisation versendet wird.

Wenn Sie eine Entscheidung getroffen haben, müssen Sie diese in Ihrer Organisation implementieren. Wenn Sie sich die Festplatte Ihres Servers ansehen, werden Sie feststellen, dass es einen neuen Ordner gibt: Der Datenträger **Microsoft UAM** wurde direkt unterhalb des Stammlaufwerks Ihres Windows 2000

Servers erstellt. Ihre Macintosh-Clients greifen über diesen Ordner auf Dateien zu, die sich auf dem Server befinden. Auch andere Windows 2000 Server-Clients speichern Dateien in diesem Ordner, sodass Ihre Macintosh- und PC-Benutzer Dateien nach Bedarf austauschen können.

Nun müssen Sie noch die Authentifizierungsdateien auf Ihren Macintosh-Clients installieren. Rufen Sie auf dem Macintosh-Computer das Programm Chooser auf. Klicken Sie auf **AppleShare**, wählen Sie die AppleTalk-Zone, in der sich Ihr Windows 2000-Server befindet, und klicken Sie dann auf diesen Server. Doppelklicken Sie anschließend auf das daraufhin auf Ihrem Macintosh-Desktop erscheinende Symbol **Microsoft UAM**. Nun erscheint ein Bereich, in dem Sie auf **MS UAM Installer** doppelklicken. Der Installationsvorgang dauert - je nach Geschwindigkeit und verfügbarem Speicherplatz Ihres Macintosh-Computers - nicht lange.

Wenn sowohl der Windows 2000-Server als auch die Macintosh-Clients für den Einsatz von Windows 2000 konfiguriert sind, müssen Sie für Ihre Macintosh-Benutzer Benutzerkonten erstellen. Dies geschieht genau so, wie für jeden anderen Benutzer jedes anderen Client-Betriebssystems. Viele Systemadministratoren sind versucht, das übliche Gastkonto von Windows 2000 Server für ihre Macintosh-Gemeinde zu verwenden. Sie sollten dieser Versuchung jedoch widerstehen und für jeden Macintosh-Benutzer ein eigenes Benutzerkonto erstellen. Aus Sicherheitsgründen sollten Ihre Benutzer immer für ihre Aktionen verantwortlich sein. Bei einem allgemeinen Gastkonto ist das nie möglich.

Wenn die Benutzer der Macintosh-Clients auf Ihren Windows 2000-Server zugreifen, müssen sie sich je nach Version des Betriebssystems, das auf den lokalen Macintosh-Computern verwendet wird, authentifizieren. Wenn auf dem Macintosh-Computer System 7.1 oder eine neuere Version verwendet wird, gibt es nur eine Möglichkeit: Der Client verwendet die Microsoft-verschlüsselte Authentifizierung. Wenn der Client eine ältere Version des Betriebssystems System 7 verwendet, kann der Macintosh-Client wählen: Er kann entweder die Microsoft-verschlüsselte Authentifizierung oder den Klartext-Kennwortschutz in Form der Standard-UAMs von Apple verwenden. Denken Sie daran, dass dies auch dann möglich ist, wenn Sie sowohl die Klartext- als auch die Gastanmeldeoption für Ihre Macintosh-Benutzer auf dem Windows 2000-Server deaktiviert haben.

Wenn es um die Unterstützung Ihrer Macintosh-Benutzer beim Drucken über Ihren Windows 2000 Server-Druckserver geht, gibt es nur eines, an das Sie denken müssen: Sicherheit. Die Sicherheit kann ein Problem sein, da AppleTalk keine Client-Benutzernamen oder -Kennwörter unterstützt. Das bedeutet, dass sich Ihre Macintosh-Clients im Windows 2000-Netzwerk Ihres Unternehmens nicht ausweisen können, was wiederum bedeutet, dass Ihr Windows 2000-Server den Macintosh-Clients keinen Sicherheitsmechanismus auf Benutzerebene auferlegen kann. Das hat bedeutende Auswirkungen: Wenn Ihre Macintosh-Clients einen Druckauftrag an den Drucker senden können, haben sie für diesen Drucker implizite Berechtigungen. Sie als Windows 2000 Server-Administrator können für all Ihre Macintosh-Benutzer Berechtigungen auf Benutzerebene definieren, indem Sie diese zu einer Gruppe hinzufügen und dann dieser Druckgruppe die entsprechenden Berechtigungen zuweisen.

16.2.4 Verbindung zu UNIX

Wie bei Macintosh-Clients so ist auch bei UNIX-Clients die Installation zusätzlicher Software auf Ihren Windows 2000-Servern sowie auf den UNIX-Clients erforderlich. Grundlegende Dateidienste können über eine Technologie ermöglicht werden, die unter der Bezeichnung *FTP-Protokoll (File Transfer Protocol)* bekannt ist. Etwas benutzerfreundlicher ist die *NFS-Technologie (Network File Services)*.

Druckerkonnektivität für UNIX-Clients bietet Windows 2000 über die Funktion Druckdienste für UNIX. Diese Funktion umfasst die Unterstützung des LPD-Dienstes (Line Printer Daemon), den UNIX-Clients benötigen, um drucken zu können. Um diesen Windows 2000 Server-Dienst zu installieren, klicken Sie auf dem Desktop von Windows 2000 Server mit der rechten Maustaste auf **Netzwerkumgebung**. Daraufhin erscheint ein kleines Menü. Wählen Sie unten in diesem Menü die Option **Eigenschaften**. Daraufhin öffnet sich das Dialogfeld **Netzwerk- und DFÜ-Verbindungen**. Wählen Sie im Menü **Erweitert** dieses Dialogfeldes die Option **Optionale Netzwerkkomponenten**, um den **Assistenten für die optionalen Windows-Netzwerkkomponenten** zu starten (siehe Abbildung 16.25).

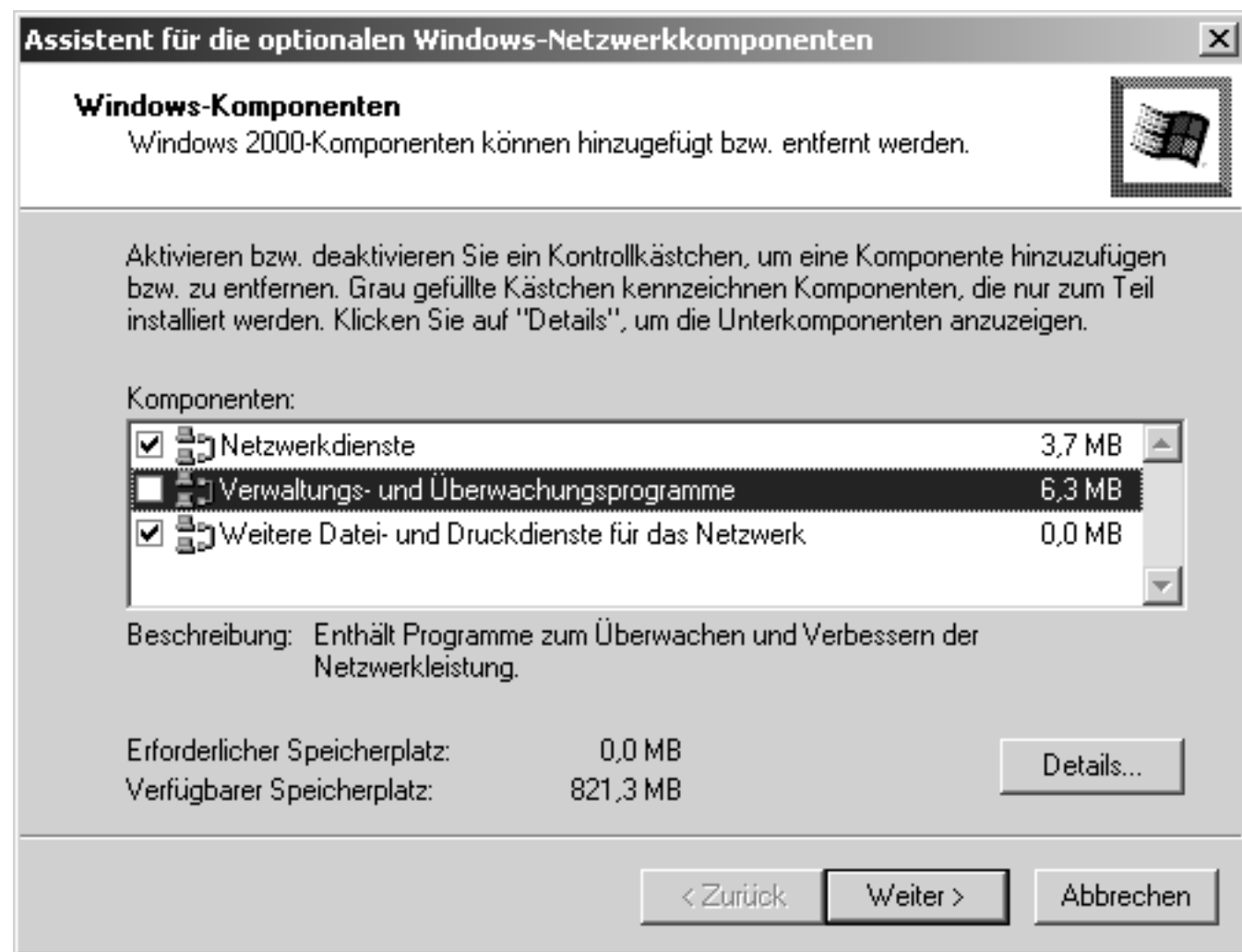


Abbildung 16.25: Auswahl weiterer Datei- und Druckdienste

Um die Druckfunktionen für den UNIX-Client zu aktivieren, klicken Sie auf das Kontrollkästchen links neben der Option **Weitere Datei- und Druckdienste für das Netzwerk** und dann auf die Schaltfläche **Details**. Daraufhin werden die einzelnen Komponenten dieser Option angezeigt (siehe Abbildung 16.26).

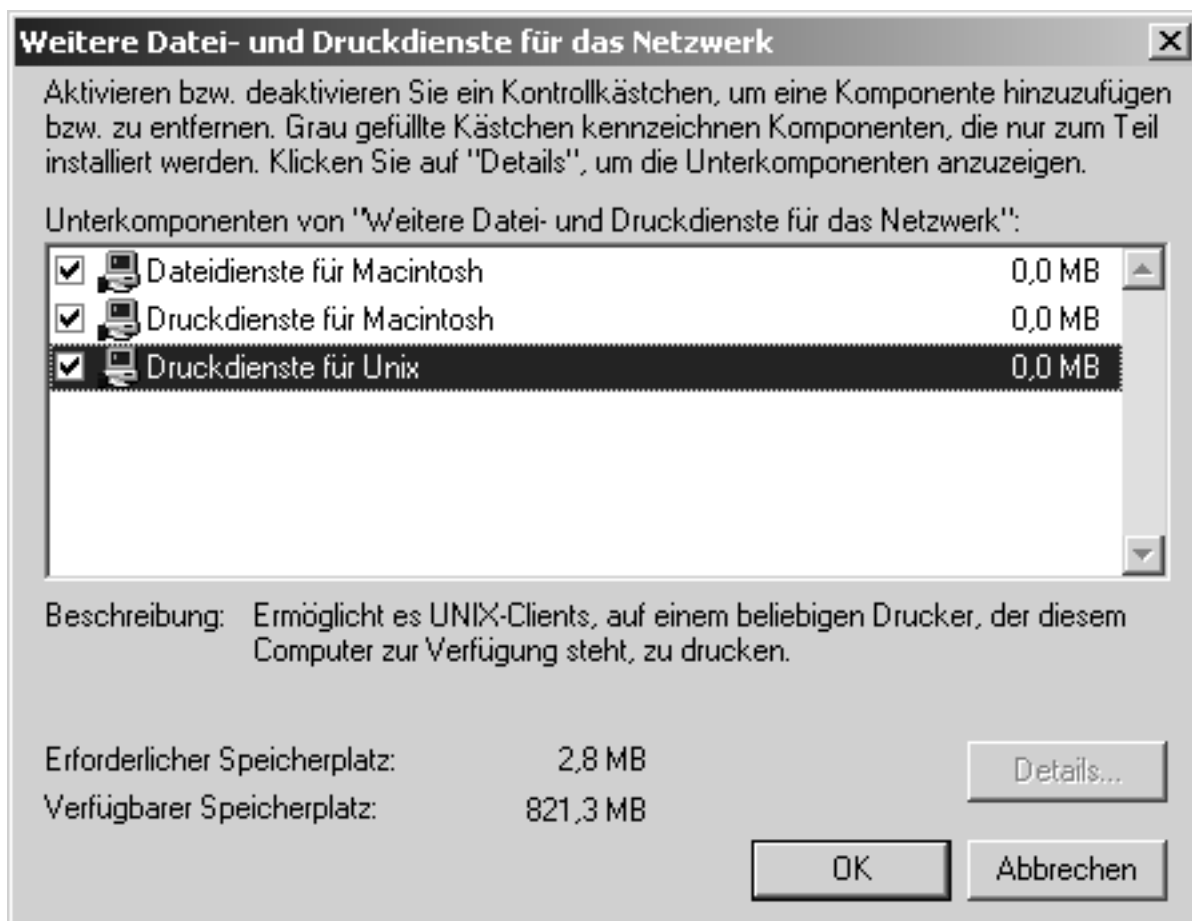


Abbildung 16.26: Installieren der Druckdienste für UNIX

Wählen Sie nun die untere Option: **Druckdienste für UNIX**. Klicken Sie dazu auf die Kontrollkästchen links neben den entsprechenden Optionen. Daraufhin erscheint ein Häkchen in dem Kontrollkästchen. Klicken Sie anschließend auf **OK**, um die Installation der Software zu starten (siehe Abbildung 16.27). Sie benötigen dazu Ihre CD-ROM von Windows 2000 Server.

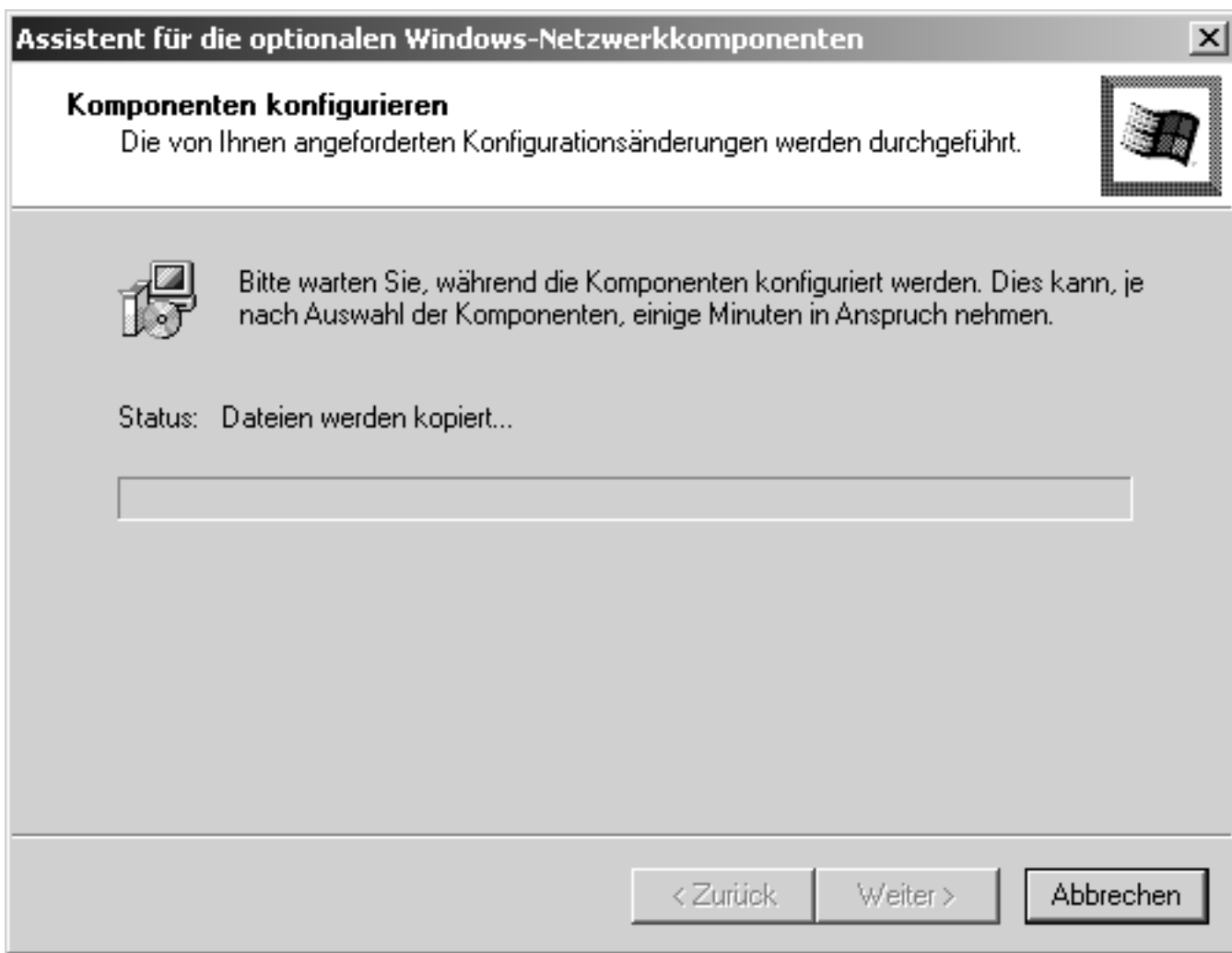


Abbildung 16.27: Die neue Netzwerkkomponente wird konfiguriert

Der Assistent meldet, dass der Vorgang einige Minuten in Anspruch nehmen kann. Um diesen Vorgang abzuschließen, ist jedoch weniger als eine Minute erforderlich. Nach Abschluss erscheint ein weiteres Dialogfeld, das Sie über die erfolgreiche Installation informiert. Danach erscheint kein weiteres Dialogfeld mehr.

Sie können nun Ihren Windows 2000-Server als Druckserver für Ihre UNIX-Clients verwenden. Vergessen Sie nicht, dass Sie auf dem UNIX-Client die geeigneten Druckertreiber installieren und sicherstellen müssen, dass die Betriebssysteme Ihrer UNIX-Clients eine RFC-gemäße Version der LPR-Dienste (Line Printer Remote) unterstützen. Das ist wichtig, weil nicht alle UNIX-Betriebssysteme diese Dienste unterstützen. Darüber hinaus werden die UNIX-Clients ihre Druckanforderungen mittels LPR-Befehl in folgendem Format an Ihren Windows 2000 Server senden:

```
lpr -S Server-Name -P Drucker-Name -d Dateiname
```

Da UNIX in der Regel zwischen Groß- und Kleinschreibung unterscheidet, sollten Sie die Parameter so wie hier verwenden.

© Copyright [Markt+Technik Verlag](#), ein Imprint der Pearson Education Deutschland GmbH
Elektronische Fassung des Titels: Windows 2000 Server Kompendium, ISBN: 3-8272-5611-9 Kapitel:
Überlegungen zum Arbeitsplatzrechner

Verbindung zu anderen Betriebssystemen

Teil IV

17. [Verbindung zu Novell NetWare](#)

18. [Verbindung zwischen UNIX und Windows 2000 Server](#)

© Copyright [Markt+Technik Verlag](#), ein Imprint der Pearson Education Deutschland GmbH
Elektronische Fassung des Titels: Windows 2000 Server Kompendium, ISBN: 3-8272-5611-9 Kapitel:
IV

Kapitel 17 Verbindung zu Novell NetWare

Die einzige wirkliche Herausforderung für Windows auf dem Markt der Netzknetriebssysteme ist das Betriebssystem NetWare von Novell. NetWare konnte noch bis vor kurzem einen Marktanteil von 70 % verzeichnen. Und es kann gesagt werden, dass es in praktisch allen der tausend erfolgreichsten Unternehmen zu finden ist. Wenn es in der Geschäftswelt nur ein einziges anderes Netzknetriebssystem gäbe, mit dem Microsoft zusammen arbeiten könnte, dann wäre das NetWare.

NetWare bietet auch einen Verzeichnisdienst (*NDS* bzw. Novell Directory Service), den es bereits seit sechs Jahren gibt. Das ist aufgrund der tiefen und komplexen Struktur eines Unternehmensverzeichnisses ganz schön viel in der Welt der Verzeichnisdienste. Ausgereiftheit bedeutet behobene Fehler.

17.1 Konzeptuelle Unterschiede

Windows und NetWare haben nicht denselben Weg verfolgt, haben jedoch in vielerlei Hinsicht dieselben Wurzeln. Windows 2000 und NetWare haben beide als Programme begonnen, die PCs die Möglichkeit boten, Ressourcen gemeinsam zu nutzen. Darüber hinaus hatten beide Betriebssysteme UNIX und VMS als Vorbild und konnten von diesen Programme übernehmen. Das war es dann aber auch schon mit den Gemeinsamkeiten.

Windows 2000 entstand aus einer kompletten Betriebssystemfamilie, nämlich Windows NT. Wie UNIX wurde auch Windows NT so entwickelt, dass es sowohl als Client- als auch als Server-Betriebssystem verwendet werden kann. Aus diesem Grund waren Administratoren auch sofort zu diesem Betriebssystem als Anwendungsserver hingezogen.

NetWare wurde als Server-Betriebssystem entwickelt und wird nach wie vor als solches verwendet. Benutzer werden nie an einem NetWare-Server sitzen und ihre Dissertation schreiben oder ihre Steuerformulare ausfüllen. Aus diesem Grund wird NetWare als Netzknetriebssystem ernster genommen.

17.1.1 Sicherheit

Zu den Unterschieden, die für einen NetWare-Administrator sofort offensichtlich werden, der mit Windows 2000 arbeitet, gehört die Tatsache, dass Windows 2000 ein Offen-Geschlossen-System ist. Wenn in Windows 2000 eine freigegebene Ressource erstellt wird, steht sie automatisch der Gruppe Jeder zur Verfügung.

NetWare-Administratoren sind an ein Geschlossen-Offen-System gewöhnt. Wenn in einem NetWare-System eine Ressource freigegeben wird, hat außer dem Administrator keiner Zugriffsberechtigungen für diese Freigabe.

Das ist ein entscheidender Unterschied, den der Administrator kennen sollte. Stellen Sie sich vor, Sie verbringen einen Nachmittag damit, Ressourcen zu erstellen, die am darauf folgenden Tag verwaltet werden sollen. Wenn in diesen Ressourcen Informationen gespeichert werden, kann auf diese

Informationen bis zum nächsten Tag, wenn die Berechtigungen geändert werden, zugegriffen werden. Keine der beiden Möglichkeiten ist richtig oder falsch. Aber der Unterschied ist entscheidend.

17.1.2 Active Directory und NetWare Directory Services

Wenn dieses Buch vor zwei Jahren geschrieben worden wäre, wäre es sehr einfach gewesen, die Verzeichnisdienste von Windows und NetWare miteinander zu vergleichen. Der Unterschied bestand darin, dass das, was Microsoft als Verzeichnisdienst bezeichnete, sonst von niemandem in der Industrie als solcher bezeichnet wurde. Das, was Microsoft als Verzeichnisdienst bezeichnete, wies nicht einmal eine hierarchische Struktur auf. Der Verzeichnisdienst von NetWare, der 1993 auf den Markt kam, ist ein mehrschichtiger, hierarchischer, objektorientierter Verzeichnisdienst.

Vor zwei Jahren kam Microsoft mit einem eigenen Verzeichnisdienst, dem *Active Directory*, auf den Markt. Seine Verwendbarkeit war zu diesem Zeitpunkt noch fraglich, aber immerhin war es schon ein hierarchischer Verzeichnisdienst. Active Directory war ein Zusatzprodukt zum Betriebssystem Windows NT.

 Wenn Betriebsangehörige von Microsoft gefragt wurden, wie die hierarchische Verzeichnisstruktur von Windows aussehen werde, sagten viele von ihnen, man solle sich schon mal mit Exchange Server vertraut machen. Der Exchange Server hatte von Anfang an ein hierarchisches Verzeichnis.

 Da der Begriff »hierarchische Verzeichnisstruktur« jetzt schon so häufig erwähnt wurde - was ist denn nun überhaupt eine hierarchische Verzeichnisstruktur? Bei einer hierarchischen Verzeichnisstruktur werden Verzeichnisobjekte (Benutzer, Gruppen usw.) in einer Basisstruktur wie der des Dateisystems angeordnet. Das Verzeichnissystem hat ebenso wie das Dateisystem einen Stamm. Das Verzeichnissystem verfügt ebenfalls über Unterverzeichnisse, die jedoch als *Containerobjekte* bezeichnet werden.

Der Vorteil dabei ist der, dass Objekte und Beziehungen zwischen Objekten so einfach zu verwalten sind wie das Dateisystem. Da sämtliche Objekte im Verzeichnis Teil derselben Struktur sind, muss keine Beziehung bzw. kein Pfad erstellt werden, um von einem Objekt zu einem anderen zu gelangen, genau so wenig wie es erforderlich ist, eine Beziehung zwischen Unterverzeichnissen im Dateisystem herzustellen.

Mit der Einführung von Windows 2000 wurde Active Directory zum integralen Bestandteil des Betriebssystems. Jedes Objekt im Betriebssystem steht in irgendeiner Verbindung mit dem Verzeichnis.

Es gibt drei wesentliche Unterschiede in der Struktur der Verzeichnisse:

- *Delegieren der Autorität.* Bei NetWare kann jedes Objekt im Verzeichnis die Autorität an andere Objekte delegieren. Bei Active Directory kann jedes Benutzerobjekt die Autorität an Containerobjekte delegieren.
- *Partitionierung und Replikation.* NetWare-Partitionen werden anhand der Container eingeteilt, Active Directory-Partitionen anhand von Standorten.
- *Namenskonvention.* Die NetWare-Namenskonvention ist frei und entspricht keinen Suchmustern. Das Verzeichnis basiert ausschließlich auf dem X.500-Schema der Verzeichnisstruktur. Active

Directory basiert zwar immer noch auf dem X.500-Schema, orientiert sich jedoch stark an der DNS-Namenskonvention. Während bei beiden Systemen die X.500-Namenskonvention angewendet wird, gibt es nur bei Active Directory die DNS-Schicht. Beide Systeme können mit dem Internetstandard LDAP für die Suche nach Verzeichnisobjekten in Verbindung gebracht werden.

Da es nicht Aufgabe dieses Buches ist, einen Verzeichnisdienst-Champion zu küren, wollen wir einfach festhalten, dass beide Systeme ihre Vor- und Nachteile haben.

Die Funktion, in der Verzeichnisstruktur von Active Directory Objekte finden zu können, wird durch die Bindung an DNS deutlich verbessert. Es ist wirklich einfach, Verzeichnisobjekte in das Internet einzubinden, wenn für die internen Netzwerkfreigaben dieselbe Namenskonvention verwendet wird. Auf der anderen Seite kann es vorkommen, dass Sie versehentlich Ressourcen freigeben, wenn die DNS-Struktur nicht entsprechend überwacht wird. Das geht jedoch wieder auf die grundlegenden philosophischen Unterschiede zurück.

Bezüglich der Partitionen ist es sinnvoller, diese anhand des Netzwerks statt anhand der Container vorzunehmen. Partitionen (Standorte) werden in erster Linie erstellt, um Replikationsverkehr mit großen Bandbreiten über Bereiche des Netzwerks hinweg zu verhindern. Novell empfiehlt Administratoren, Partitions Grenzen anhand der Container zu definieren. Das ist in der Regel nicht weiter schwierig. Wenn Sie jedoch nach größerer Freiheit streben, ist die Microsoft-Lösung die bessere.

Bei NetWare wird das Delegieren von Verantwortung an einen Einzelnen oder an eine Gruppe weitaus flexibler gehandhabt. Die Funktion, jede Objektberechtigung zuweisen zu können, ermöglicht ein weitaus feingliedrigeres Verwaltungsschema, als wenn vor Containergrenzen Halt gemacht werden muss, wie das bei Active Directory der Fall ist. Es stellt sich natürlich die Frage, wie viele sich überhaupt mit diesem Problem konfrontiert sehen werden. Aber Tatsache bleibt, dass NetWare hier eine größere Flexibilität bietet.

Aus der Sicht des Administrators ist klar, dass beide Lösungen ihre Vorteile haben. Der eindeutige Gewinner ist der Microsoft-Administrator, der nicht mehr länger an das nicht hierarchische Verzeichnis gebunden ist, das im Unternehmen recht mühselig zu verwalten ist.

17.1.3 Dateifreigaben

Die gemeinsame Nutzung von Dateien ist die grundlegendste Form des Networking, die es überhaupt gibt. Dabei gibt es große Unterschiede zwischen Windows und NetWare. Die beiden Systeme unterscheiden sich darin, wie Benutzer auf die Dateistruktur zugreifen, und darin, wie die Freigaben verfügbar gemacht und das Verzeichnis strukturiert wird.

In der Welt von Windows können - wie Sie bereits gelernt haben - Freigaben an jeder Stelle in der Verzeichnisstruktur erstellt werden. Ein Administrator kann ein beliebiges Verzeichnis auf dem Server auswählen und freigeben.

In der Welt von NetWare werden Freigaben nicht als *Freigaben*, sondern als *Datenträger* bezeichnet. Das kommt daher, weil die Freigaben, die von einem NetWare-Server dargestellt werden, eigentlich die Datenträger sind, die auf den Servern erstellt werden. Jeder Datenträger, der auf einem NetWare-Server erstellt wird, kann für die Benutzerbasis verfügbar gemacht werden. Verzeichnisse können jedoch nicht

als separate Einheiten veröffentlicht werden.

Um diesen Unterschied auszugleichen, müssen Sie, wenn Sie mit einem NetWare-Server verbunden sind, verstehen, dass der Benutzer Laufwerkzuordnungen erstellen kann, die auf ein beliebiges Verzeichnis auf dem Server verweisen. Diese Zuordnungen werden als *Zuordnungsstämme* bezeichnet. Um sich den Unterschied klarzumachen, vergleichen Sie einfach, wie ein Benutzer auf dasselbe Verzeichnis auf jedem der beiden Server zugreift.

Überlegen Sie sich beispielsweise einmal, wie Sie Benutzern den Zugriff auf den Ordner **Personalwesen** gewähren, ohne die Dateien und Verzeichnisse anzuzeigen, die in diesem Ordner ebenfalls enthalten sind. Jede Abteilung soll Zugriff auf seine eigenen Dateien und die Abteilung Personalwesen soll Zugriff auf sämtliche Abteilungsverzeichnisse haben.

- Bei Microsoft werden alle Unterverzeichnisse freigegeben und die Benutzer in den Gruppen den Verzeichnissen zugewiesen, auf die sie zugreifen können müssen.
- Bei NetWare werden alle Benutzer direkt zu dem Verzeichnis zugewiesen, auf das sie zugreifen können müssen.

Das könnte zu einem Problem werden, wenn Windows-Server keine Grenze für die Anzahl der Freigaben hätten, die sie verarbeiten können. Jede Freigabe, die veröffentlicht wird, nimmt ein gewisses Maß an CPU- und Speicherressourcen für sich in Anspruch. Wenn ein Administrator für 1.800 Benutzer Basisverzeichnisse erstellen und jeden Benutzer dem Stammverzeichnis dieser Verzeichnisse zuordnen wollte, würden die meisten Server in die Knie gehen.

Eine Funktion, die für den Administrator recht hilfreich ist, ist die Möglichkeit, über Kontingente zu definieren, wie viel Speicherplatz die Benutzer auf dem Server zur Verfügung haben. Bis vor kurzem gab es für Windows-Server diese Steuerungsmöglichkeit noch nicht. Für verstimzte Angestellte gab es eine besonders unangenehme Art, einen Server in die Knie zu zwingen, indem sie nämlich mehr Dateien auf den Server kopierten, als dieser Speicherplatz zur Verfügung hatte. Ein gewiefter Administrator speichert die Systemdateien nicht auf einem freigegebenen Datenträger, aber ein Datei-Server ohne Dateikapazität ist ziemlich nutzlos. Sowohl Windows 2000 als auch NetWare verfügen heute über Datenträgerkontingente. Es gibt jedoch große Unterschiede bezüglich der Definition dieser Kontingente.

Bei Windows 2000 wird ein Datenträgerkontingent durch eine Grenze oder eine Warnstufe definiert. Damit wird die Datenmenge festgelegt, die ein Benutzer auf dem Datenträger speichern darf. Wenn ein Kontingent definiert wird, kommt es zu zwei Reaktionen. Die erste ist die, dass der Benutzer keine weiteren Daten auf dem Datenträger speichern kann. Die zweite ist die, dass ein Ereignis im Ereignisprotokoll gespeichert wird. Diese beiden Reaktionen erfolgen unabhängig voneinander, sodass der Administrator zwar erkennen kann, dass ein Benutzer das Limit überschritten hat, dass aber eine wichtige Auftragsfunktion nicht unterbrochen wird.

Wenn Benutzern Grenzen gesetzt werden, kann auch eine Warnstufe definiert werden. Dann wird den Benutzern mitgeteilt, wenn sie einen bestimmten Prozentsatz des Kontingents belegt haben.

Bei NetWare können Grenzen an jeder Stelle in der Verzeichnisstruktur definiert werden. Somit können Administratoren die Menge an Speicherplatz für Benutzer in deren eigenen Basisverzeichnissen festlegen. Der Unterschied ist dann der, dass die Benutzer das Verzeichnis wechseln können und dann über andere Kontingente verfügen. Wenn der Administrator möchte, dass die Benutzer beispielsweise nur eine bestimmte Menge von Daten in ihren Stammverzeichnissen auf dem Server, dafür aber mehr

Daten in den Ordnern der Abteilungen speichern können, so kann er das tun.

Der Vorteil des Windows-Systems ist der, dass verhindert wird, dass ein Hacker einen Datenträger von einem unkontrollierten Standort aus füllt. Der Vorteil des NetWare-Systems ist der, dass es eine höhere Flexibilität und mehr Steuerungsmöglichkeiten bietet. Letztlich lässt sich jedoch alles auf den grundlegenden Unterschied in der Art und Weise, wie Freigaben behandelt werden, zurückführen.

17.1.4 Drucken

Aus der Sicht des Benutzers ist der Zugriff auf freigegebene Drucker bei diesen beiden Betriebssystemen derselbe. Benutzer von Windows 95/98 werden keinen Unterschied merken, ob sie nun auf einen NetWare-Druck-Server oder auf einen Windows 2000-Druck-Server zugreifen. Der Benutzer hat Zugriff auf den Drucker, indem der Drucker einfach hinzugefügt und auf die Netzwerkfreigabe gezeigt wird. Der technische Unterschied zwischen den beiden Modellen stellt bei der täglichen Arbeit keinen wirklichen Unterschied dar.

Die Unterschiede werden bedeutender, wenn ein Windows 2000- oder ein Windows NT-Client auf den Drucker zugreifen möchte. Bei Windows 2000 bzw. NT werden die Treiber automatisch an einen Windows 2000- bzw. Windows NT-Client vermittelt, wenn der Client den Drucker aus der Netzwerkumgebung wählt. NetWare-Server können Treiber an diese oder andere Clients vermitteln, bei Windows ist das jedoch nicht ganz so einfach. Windows 95/98-Clients können ebenfalls Treiber vom Windows 2000/NT-Server zur Verfügung gestellt bekommen, aber dies muss wie bei einem NetWare-Server entsprechend konfiguriert werden.

Wenn der NetWare-Client auf einem Windows-Client installiert wird, reagieren NetWare-Druck-Server auf den Windows-Befehl `NET USE LPT1\\Server-Name\Drucker-Freigabename`. Der Befehl der NetWare-Umgebung lautet jedoch `CAPTURE`.

Der `CAPTURE`-Befehl ist dem `NET USE`-Befehl sehr ähnlich. Der Benutzer muss den Namen des Druck-Servers und den Namen der Freigabe (Warteschlange oder Druckobjekt) kennen. Führen Sie den Befehl mit den hier aufgeführten Variablen aus:

CAPTURE Variablen Common Variablenliste

- **L=**. An diese Variable wird die Nummer des LPT-Anschlusses angehängt, der verwendet und an die Netzwerkressource gesendet werden soll. `L=1` ist z.B. `LPT1`.
- **Q=**. An diese Variable wird der Name der Druckerwarteschlange bzw. des zu druckenden Druckobjekts angehängt. Mit dem Befehl `Q=rec_Drucker1` werden Druckaufträge an die Druckerwarteschlange `rec_Drucker1` gesendet.
- **S=**. Die hier aufgeführte Variable steht für den Server, der die gewünschte Druckerwarteschlange enthält. Diese Variable ist nicht erforderlich, wenn die gewählte Warteschlange ein Druckobjekt in NDS ist. Mit dem Befehl `S=Server1` werden Druckaufträge an `Server1` gesendet.
- **Ti=**. Diese Variable bezieht sich auf die Zeit zwischen dem Beginn des Datenflusses eines Druckauftrags an den Server und dem Zeitpunkt, zu dem der Drucker zu drucken beginnt. Diese Variable war weitaus wichtiger, als noch DOS-Anwendungen vorherrschten, da die Druckaufträge

erst an den Drucker freigegeben wurden, wenn die Anwendung beendet war. Mit dem Befehl `Ti=15` startet der Druckauftrag 15 Sekunden nachdem die ersten Druckdaten am Druck-Server ankommen.

- NB. Mit der Variablen NB wird dem Druck-Server mitgeteilt, er solle nicht nach jedem Druckauftrag eine Trennseite drucken. Bei NetWare wird standardmäßig eine Trennseite gedruckt. Eine Trennseite gibt an, wer das jeweils nachfolgende Dokument druckt.
- NEF. Diese Variable wird verwendet, um einen Seitenvorschub nach dem Drucken auf einem Matrix- bzw. Zeilendrucker zu unterdrücken.
- SH. Wenn Sie den Befehl `CAPTURE SH` eingeben und auf die Eingabetaste drücken, werden sämtliche LPT-Anschlüsse sowie deren aktuelle CAPTURE-Einstellungen angezeigt.

17.2 Die Verbindung zu NetWare

NetWare-Server sind Windows-Servern in Bezug darauf, dass sie viele unterschiedliche Arten der Verbindung zulassen, sehr ähnlich. Die Art der Verbindung, die erforderlich ist, um all die verfügbaren Dienste auf dem Server nutzen zu können, wird als *systemeigene Verbindung* bezeichnet.

Um den Unterschied zwischen einer systemeigenen Verbindung und anderen Verbindungen zu verstehen, hilft es, wenn man das Internet-Konzept einer Web-Verbindung mit einer Verbindung von einem Windows-Client vergleicht, der auf eine Datenträgerfreigabe zugreifen möchte. Ein Web-Client kann nur auf einen einzigen Vorgang zugreifen und kann keine Datenträger- der Druckfreigaben zuordnen. Benutzer eines NetWare-Systems können die systemeigenen NetWare-Utilities wie Anzeigen verfügbarer NetWare-Server, Senden von Nachrichten an andere NetWare-Benutzer und Zugriff auf NetWare-Freigaben über lokale Laufwerksbuchstaben (Zuordnung) und Druckerpfade (Zuweisung) voll nutzen.

Beim Zugriff auf NetWare-Server gibt es zwei verschiedene Arten der systemeigenen Verbindung:

- Bindery
- NDS

Die Bindery-Verbindung ist vergleichbar mit der Windows NT Workgroup-Verbindung. Benutzer greifen einzeln auf jeden Server zu und jeder Server verfügt über eine eigene Benutzer- und Gruppenliste. NDS verwendet dieselbe Art der Verbindung wie die, die in Active Directory verwendet wird. Ein Benutzer greift auf das Verzeichnis zu und bekommt dann die Zugriffsberechtigung für die Ressourcen, die das Verzeichnis zu bieten hat.

Es hat wenig Sinn, diese Konzepte über diese Beispiele hinaus ausführlicher zu besprechen. Der Unterschied wird jedoch besonders deutlich, wenn es darum geht, dass Sie mit einem NetWare-Server ab Version 4.0 Informationen migrieren bzw. austauschen. Bei NetWare 4.x (auch unter der Bezeichnung intraNetWare bekannt) und bei NetWare 5 ist es erforderlich, dass ein Benutzer eine Verbindung zu einem NDS-Objekt herstellt, bevor auf administrative Informationen zugegriffen werden kann.

17.2.1 Gateway Service für NetWare

Das erste Programm, das in der Welt von Windows verwendet wurde, um einen Windows-Server in eine NetWare-Umgebung zu integrieren, war Gateway Service für NetWare. Dieser Dienst ermöglicht Benutzern in einer Windows-Domäne die nahtlose Kommunikation mit einem NetWare-Server ohne direkte Verbindung zu diesem Server. Damit ist Novell jedoch nicht so ganz glücklich.

Der Gateway Service für NetWare ist lediglich ein Netzwerkdienst, der auf einem Windows-Server ausgeführt wird und ein Gateway zu NetWare-Servern erstellt. Dazu ist ein Administrator erforderlich, der eine Verbindung mit einer auf einem NetWare-Server zur Verfügung gestellten Freigabe (Drucker oder Laufwerk) herstellt und dann die Ressourcen freigibt, als ob es sich dabei um eine freigegebene Ressource auf dem Windows-Server handelte. Der Vorteil dabei ist der, dass Benutzer in der Windows-Domäne keine NetWare-Client-Software installieren, und die Benutzer nicht von der NetWare-Seite verwaltet werden müssen.

Sie sollten wissen, dass dies nicht als Ausweg für den Erwerb einer Benutzerlizenz von Novell gedacht ist. Tatsache ist, dass sogar Microsoft möchte, dass Administratoren für jeden Benutzer eine Lizenz erwerben, der auf diese Art und Weise auf eine NetWare-Ressource zugreift. Der Windows-Server verwendet nur eine Lizenz für diese Verbindung zum NetWare-Server. Der Administrator ist Novell gegenüber gesetzlich verpflichtet, für jede Benutzerverbindung, die zum Gateway aus diesem Grund erstellt wird, eine Lizenz zu erwerben.

Der andere wichtige Vorteil bei dieser Art der Integration besteht darin, dass auf den Clients nicht mehr so viele Protokolle erforderlich sind. Clients in der Windows-Domäne benötigen lediglich die Protokolle, die für die Verbindung zu dieser Domäne (aller Wahrscheinlichkeit nach TCP/IP) erforderlich sind. Der Gateway-Server stellt nur die IPX/SPX-Verbindung zum NetWare-Server her.

Der Dienst unterstützt nur die Verbindung zum NetWare-Server über NWLink IPX/SPX. Auch wenn der Server mit NetWare Server 5 arbeitet und in einer reinen IP-Umgebung ausgeführt wird, muss das IPX/SPX-Protokoll auf beiden Servern installiert werden. Wenn das NWLink-Protokoll auf dem Windows-Server nicht installiert wird, wird es automatisch hinzugefügt, wenn Sie diesen Dienst installieren. Das sorgt für eine interessante Unterhaltung mit dem NetWare-Administrator, der letztlich von seinen Windows-Brüdern überzeugt wurde, zu IP zu wechseln.

Der Gateway Service in Windows 2000 kann Verbindungen sowohl zu NDS- als auch zu Bindery-Ressourcen herstellen. Ältere Versionen des Produkts konnten nur auf Bindery-Ressourcen zugreifen. Jede Ressource, auf die ein Windows 2000-Client für NetWare zugreifen kann, kann über das Gateway zugewiesen und bedient werden.

NetWare vorbereiten

Als Erstes müssen Sie überlegen, ob der NetWare-Server vorbereitet ist, den Benutzer zu empfangen, der über den Gateway Service eine Verbindung herstellt. Auf dem NetWare-Server muss es eine Gruppe mit der Bezeichnung *NTGATEWAY* sowie ein Benutzerkonto geben, das Mitglied der Gruppe ist, die vom Gateway Service verwendet wird.

Sie sollten wissen, dass jede Berechtigung, die der Gruppe *NT-GATEWAY* erteilt wird, automatisch dem

Dienstbenutzerkonto zugewiesen wird. Jeder Benutzer des Gateway verwendet diese Berechtigungen. Wenn der Gruppe *NTGATEWAY* also für den Datenträger *SYS* auf dem NetWare-Server die Berechtigung Supervisor erteilt wird, verfügt jeder Benutzer, der das Gateway verwendet, über diese Berechtigung. Wenn sich das besonders unangenehm anhört, dann deshalb, weil es besonders unangenehm ist. Administratoren müssen beim Definieren dieser Beziehung sehr vorsichtig sein. Diese Beziehung sollte nur vorübergehend für die Zeitdauer der Migration und nicht dauerhaft eingerichtet werden.

Installieren des Gateway Service

Wenn auf dem NetWare-Server ein Konto eingerichtet und das Konto Mitglied der Gruppe *NTGATEWAY* ist, müssen Sie als Nächstes den Gateway Service installieren. Um diesen Dienst zu installieren, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf **Netzwerkumgebung** und wählen Sie die Option **Eigenschaften**.
2. Klicken Sie mit der rechten Maustaste auf eine bestehende Netzwerkverbindung und wählen Sie die Option **Eigenschaften**.



Wenn dieser Dienst für eine Verbindung installiert wird, wird er für alle Verbindungen installiert. Wenn Sie ihn für eine bestimmte Verbindung deinstallieren möchten, müssen Sie das für jede einzelne Verbindung nach der Installation tun.

3. Klicken Sie auf die Schaltfläche **Installieren**. Klicken Sie auf den Client und dann auf die Schaltfläche **Hinzufügen**.
4. Nun wird der Dienst **Gateway (und Client) Services für NetWare** angezeigt. Klicken Sie auf diesen Dienst und dann auf **OK** (siehe Abbildung 17.1).
5. Klicken Sie im Dialogfeld **Eigenschaften** auf **Schliessen**.

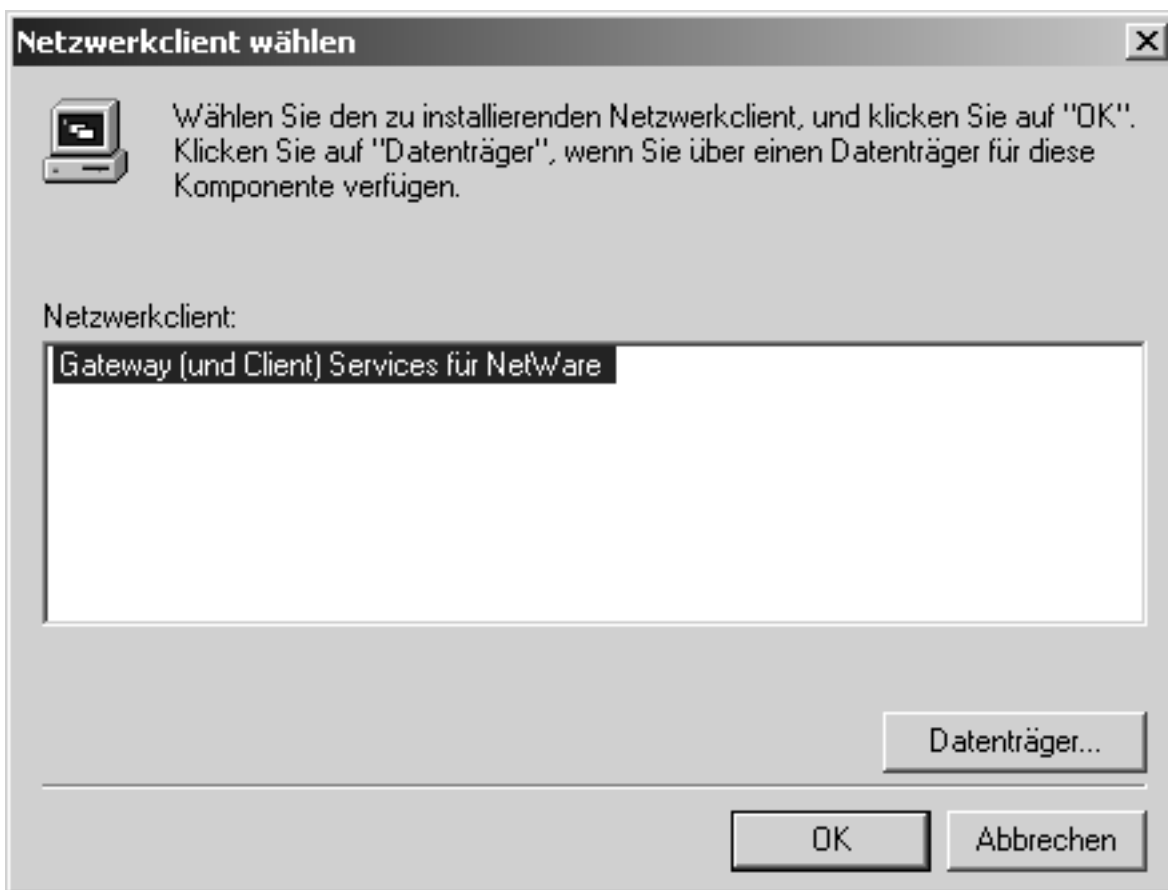


Abbildung 17.1: Das Dialogfeld für die Installation des Gateway Service

Wenn der Dienst installiert ist, muss er konfiguriert werden, damit auf die Ressourcen auf dem NetWare-Server bzw. auf den NetWare-Servern zugegriffen werden kann. Bei der Installation des Dienstes werden Sie nach den Einstellungen für diese Verbindung gefragt (siehe Abbildung 17.2).

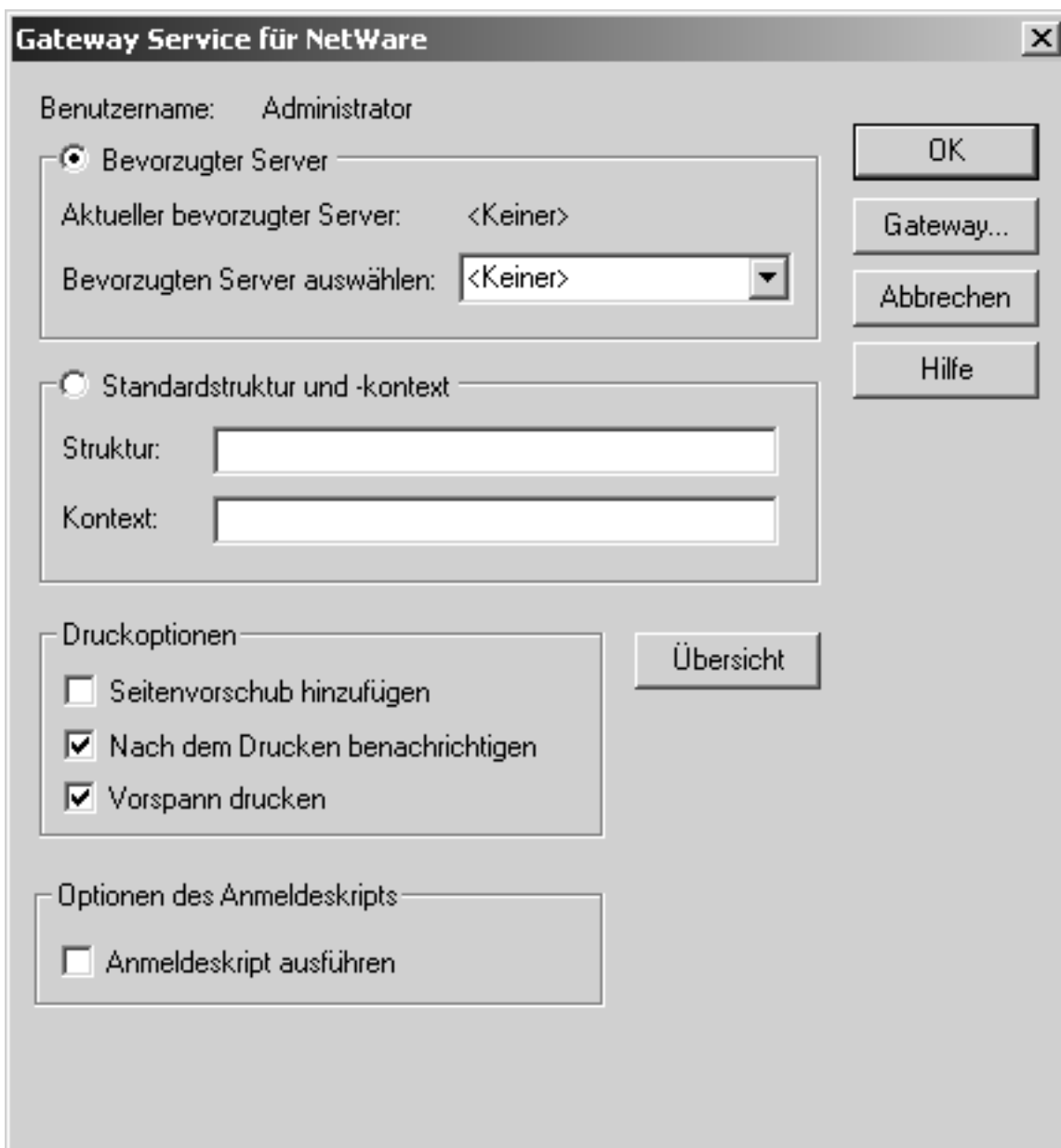


Abbildung 17.2: Auswahl einer NetWare-Verbindung

Wenn Sie eine bevorzugte Ressource auswählen, sollten Sie sich zuerst überlegen, ob eine Verbindung zu einem bestimmten Server mit Bindungssicherheit oder zu einer NDS-Struktur eingerichtet werden soll. Diese Option ist einfach, aber wichtig. Wenn auf einen einzigen NetWare 3.x- oder älteren Server zugegriffen werden soll, dann wählen Sie im Dropdown-Menü dieses Dialogfelds diesen Server. Wenn Sie auf einen 4.x- oder neueren Server zugreifen möchten, sollten Sie eine NDS-Struktur wählen.

Die andere Option in diesem Dialogfeld ist die, ob das Anmeldeskript für das Benutzerobjekt, das Sie anmelden, vom Server oder von der NDS-Struktur ausgeführt werden soll. Aus der Sicht eines Windows-Servers hat diese Option keine Bedeutung. Denken Sie daran, dass dieses Tool sowohl ein Client als auch ein Dienst ist und daher einige Tools für einen einfachen NetWare-Client umfasst. Das Anmeldeskript auszuführen, ist bei einem Server selten ein guter Gedanke, da dies zu Konflikten bei der Zuordnung lokaler Datenträger und zu Chaos im Verhalten des Servers führen kann. Wenn der Server nicht als Client verwendet wird, was Sie nach Möglichkeit vermeiden sollten, dann aktivieren Sie Anmeldeskripten nicht.

Konfigurieren des Gateway

Der Gateway Service kann noch nicht auf freigegebene Ressourcen zugreifen. Nur weil der Dienst installiert ist, bedeutet das noch lange nicht, dass irgendetwas vom NetWare-Server veröffentlicht wird. Der Administrator muss jeweils jede zu veröffentlichende Ressource einzeln veröffentlichen.

Die Konfiguration dieses Dienstes erfolgt in der Systemsteuerung über das Symbol **GSNW** (wofür diese Abkürzung steht, muss wohl nicht erläutert werden). Nach einem Doppelklick auf das Symbol können Sie die Verbindung auswählen (siehe Abbildung 17.3). Die wichtigste Aufgabe der Systemsteuerung bei Windows 2000 Server ist jedoch die Konfiguration von Ressourcen. Über die Schaltfläche **Gateway** können Sie die Zuordnung von Ressourcen konfigurieren.

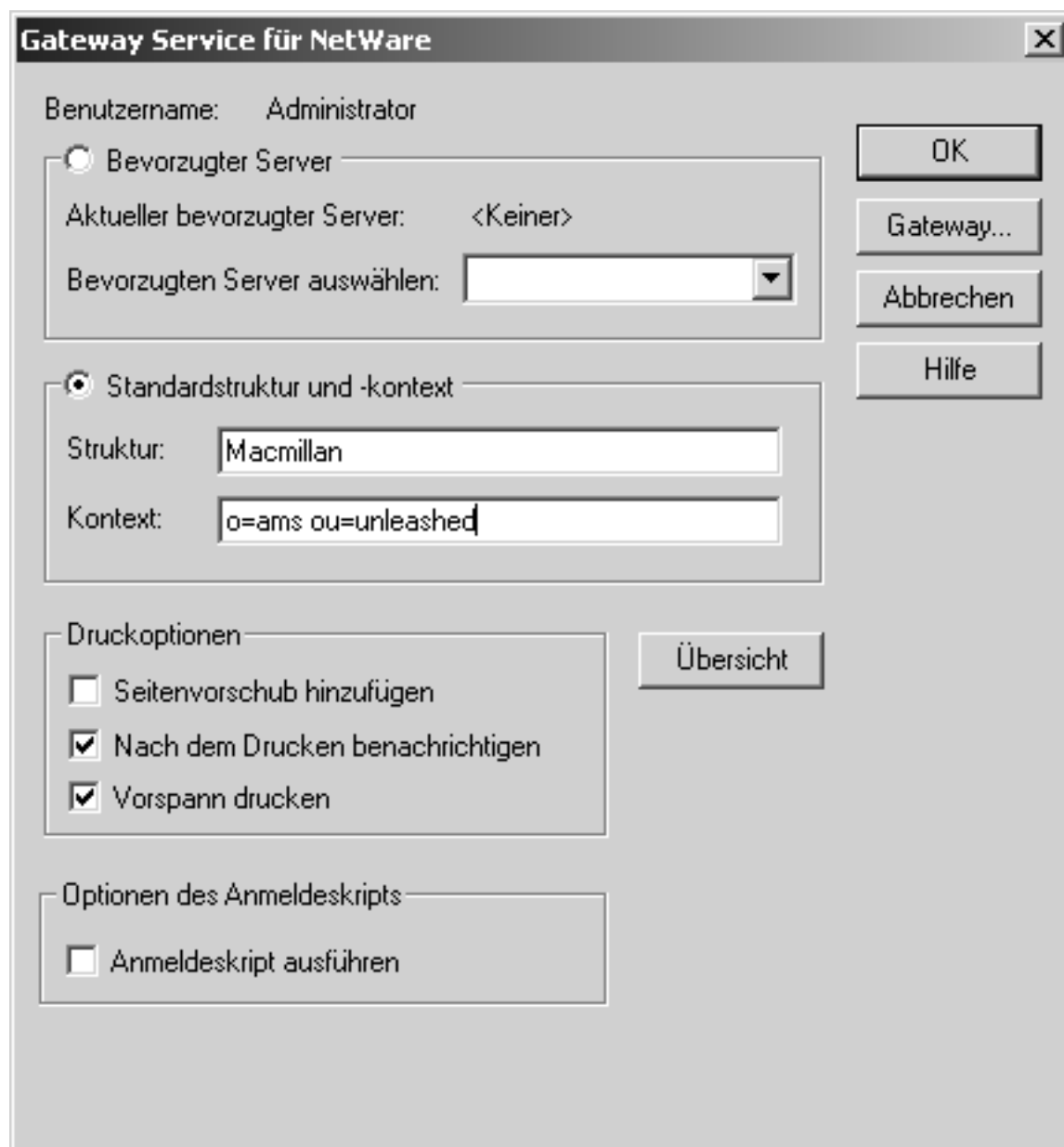


Abbildung 17.3: GSNW in der Systemsteuerung

Bevor Sie eine Ressource erstellen, müssen Sie das Gateway aktivieren. Um das Gateway zu aktivieren, klicken Sie einfach im Dialogfeld **Gateway konfigurieren** auf das Kontrollkästchen neben **Gateway aktivieren**. Geben Sie dann den Benutzernamen und Kennwort sowie die Kennwortbestätigung ein, die

für dieses Gateway in der NetWare-Umgebung erstellt worden sind. Denken Sie daran, dass dieses Konto ohne menschliches Zutun immer angemeldet wird, wenn der Server startet. Nun können Sie auf diesem System Ressourcen erstellen.

Um eine Ressource zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie auf die Schaltfläche **Hinzufügen**. Daraufhin erscheint das Dialogfeld **Neue Freigabe** (siehe Abbildung 17.4).



Abbildung 17.4: Das Dialogfeld Neue Freigabe für das Gateway

2. Geben Sie in dem Feld **Freigabename** den Namen der Freigabe ein, so wie er vom Windows-Server dargestellt wird. Drücken Sie dann die Tabulatortaste.
3. Geben Sie in dem Feld **Netzwerkpfad** den UNC-Pfad für die Ressource auf dem NetWare-Server ein, zu der eine Verbindung eingerichtet werden soll (z.B. \\server1\vol1). Drücken Sie dann die (Tab)-Taste.
4. Wenn Sie möchten, dass für den Windows-Client ein Kommentar angezeigt wird, geben Sie diesen in das Feld **Kommentar** ein und drücken Sie dann die (Tab)-Taste.
5. Klicken Sie auf den Abwärtspfeil neben dem Dropdown-Menü **Laufwerk** und wählen Sie einen Laufwerksbuchstaben für die Verbindung auf dem Gateway aus. Drücken Sie dann die (Tab)-Taste.
6. Wenn Sie die Anzahl der Benutzer begrenzen möchten, die diese Verbindung nutzen können (aus Gründen der Lizenzierung und Bandbreite), dann aktivieren Sie das Kontrollkästchen **Max.** und geben in das Eingabefeld die Anzahl der Benutzer ein.
7. Klicken Sie auf **OK**, um die Konfiguration des Gateway fertig zu stellen.

Wenn das Gateway konfiguriert ist, können für das Gateway Berechtigungen definiert werden:

1. Klicken Sie auf die Freigabe, für die Sie Berechtigungen definieren möchten, und klicken Sie dann auf **Berechtigungen**.
2. Klicken Sie auf **Hinzufügen**.
3. Wählen Sie unter **Name** die Gruppe bzw. den Benutzer und klicken Sie dann auf **Hinzufügen**.

4. Klicken Sie unter **Berechtigung** auf die Berechtigung, die Sie für diesen Benutzer bzw. diese Gruppe definieren möchten.

17.2.2 File und Print Services für NetWare

File und Print Services für NetWare ist zwar nicht Teil des Windows 2000 Server-Produkts, kann jedoch von der Microsoft-Website heruntergeladen werden und wir möchten es deshalb nicht unerwähnt lassen. Es ist das genaue Gegenteil des oben beschriebenen Gateway Service. Mit diesem Dienst können NetWare-Benutzer auf einen Windows 2000- oder NT-Server zugreifen, als wäre es ein NetWare 3.x-Server.

Dieser Dienst funktioniert im Prinzip so wie der Gateway Service, jedoch aus entgegengesetzter Richtung. Er ist während einer Übergangsphase recht hilfreich, wenn die Clients in einem bestehenden NetWare-Netzwerk den neuen Server als einen NetWare-Server wahrnehmen können. Damit kann ein Client nach dem anderen bearbeitet werden, wobei die Clients auch schon ohne Aktualisierung Zugriff auf den neuen Server haben.

NetWare-Clients können eine Verbindung zum Windows-Server herstellen und NetWare-Utilities verwenden, als wären sie mit einem NetWare-Server verbunden.

17.2.3 Migrationsprogramm für den Verzeichnisdienst

Die Übertragung eines NetWare-Verzeichnisses in ein Microsoft Active Directory wäre praktisch nicht möglich, wenn dies vom Administrator manuell zu bewerkstelligen wäre. Wenn das Verzeichnis groß genug ist, ist der Administrator besser beraten, von vorne zu beginnen, als eine Übertragung zu versuchen. Microsoft hält dafür auf seiner Website glücklicherweise ein Programm bereit, das *Migrationsprogramm für den Verzeichnisdienst*, leider allerdings in englischer Sprache.

Wie das alte Migrationsprogramm für NetWare von Windows NT soll auch dieses Programm dazu dienen, die Benutzer, Gruppen und Daten von NetWare-Servern zu übertragen. Dieses Programm kann verwendet werden, um NetWare-Server auszutauschen, oder es kann verwendet werden, um einfach die Benutzer- und Gruppeninformationen von der bestehenden NetWare-Umgebung zu replizieren. In beiden Fällen erspart es eine ganze Menge Arbeit.

Eine der besten Funktionen dieses Programms besteht darin, dass eine Simulation der Migration durchgeführt werden kann, bevor ein Benutzerkonto oder auch nur ein Stückchen Information tatsächlich kopiert wird. Damit kann sich der Administrator auf Komplikationen vorbereiten, bevor diese auftreten. Wenn eine Simulation richtig funktioniert hat, kann die Migration in Echtzeit ausgeführt werden.

Das Migrationsprogramm kann während der Installation von Windows 2000 oder zu einem späteren Zeitpunkt installiert werden. Dabei muss das Programm lediglich in der Systemsteuerung unter Software hinzugefügt werden.

Migrieren von Verzeichnisobjekten

Wenn das Programm installiert ist, erscheint es im Startmenü unter **Programme/Verwaltung**. Über das Startfenster können Sie ein neues Projekt erstellen (siehe Abbildung 17.5). Projekte werden erstellt, um die für die Migration erforderliche Simulation zu definieren.

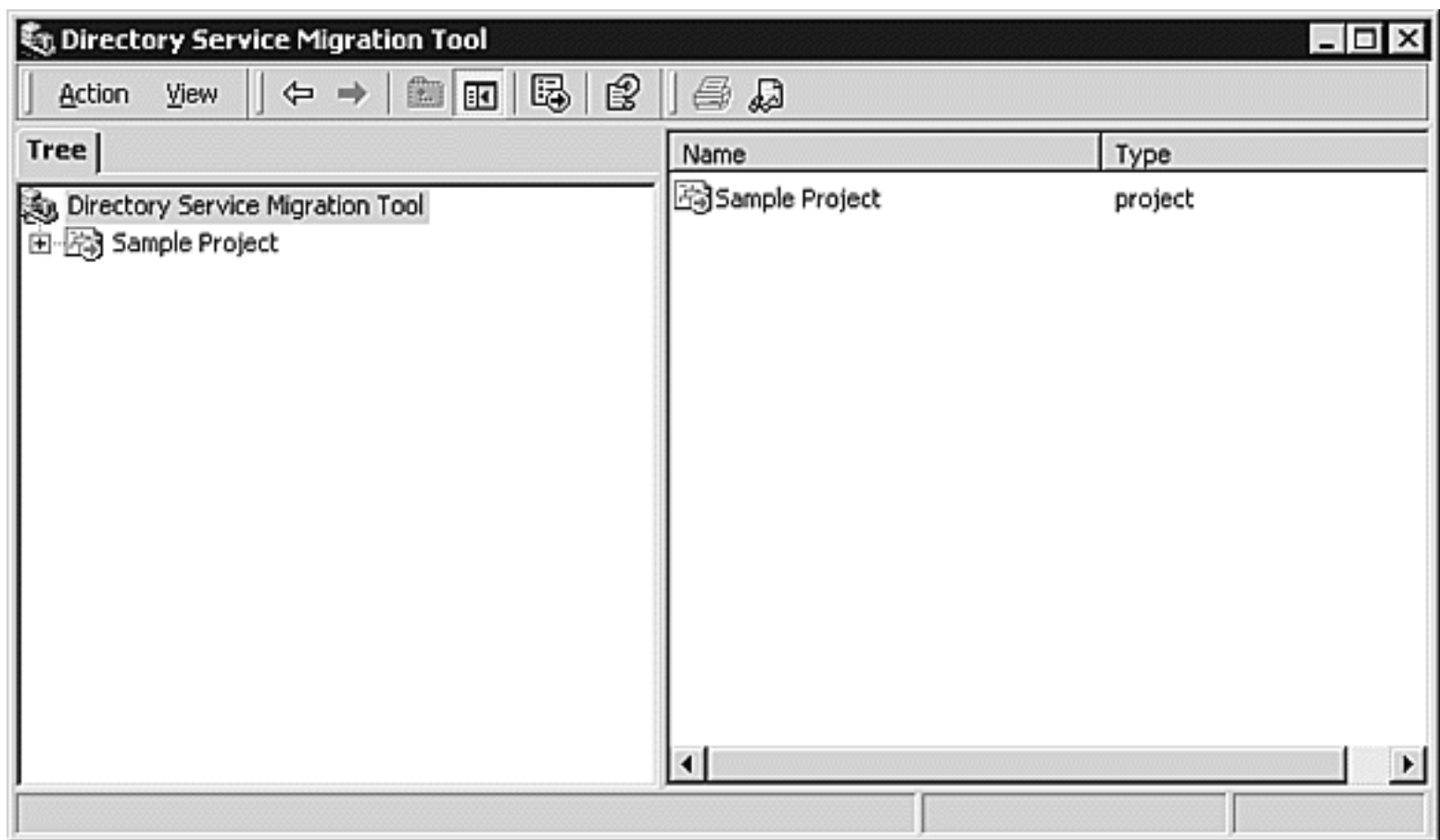


Abbildung 17.5: Das Startfenster des Migrationsprogramms

Bevor Sie ein Projekt erstellen, sollten Sie die Optionen definieren, die das Projekt durch unterschiedliche Daten führen werden. Mit Hilfe der Optionen kann der Administrator festlegen, wie das Programm auf die Unterschiede und mögliche Konflikte zwischen den beiden Systemen reagieren soll. Damit Sie die verfügbaren Optionen verstehen, werden deren Bedeutungen im Folgenden erläutert.

Folgende Optionen stehen zur Verfügung:

- *General.* Auf dieser Registerkarte wird sowohl der Speicherort der Projektdatei festgelegt als auch Filter für die Objekte definiert, die während des Projekts angezeigt werden. Wenn Sie das Kontrollkästchen **Display Supported Objects only in Discover and Configure Wizards** deaktivieren, werden Objekte angezeigt, die nicht zum Active Directory hinzugefügt werden können. Das kann bei einem Testlauf für Elemente, die nicht migrieren, recht hilfreich sein (siehe Abbildung 17.6).

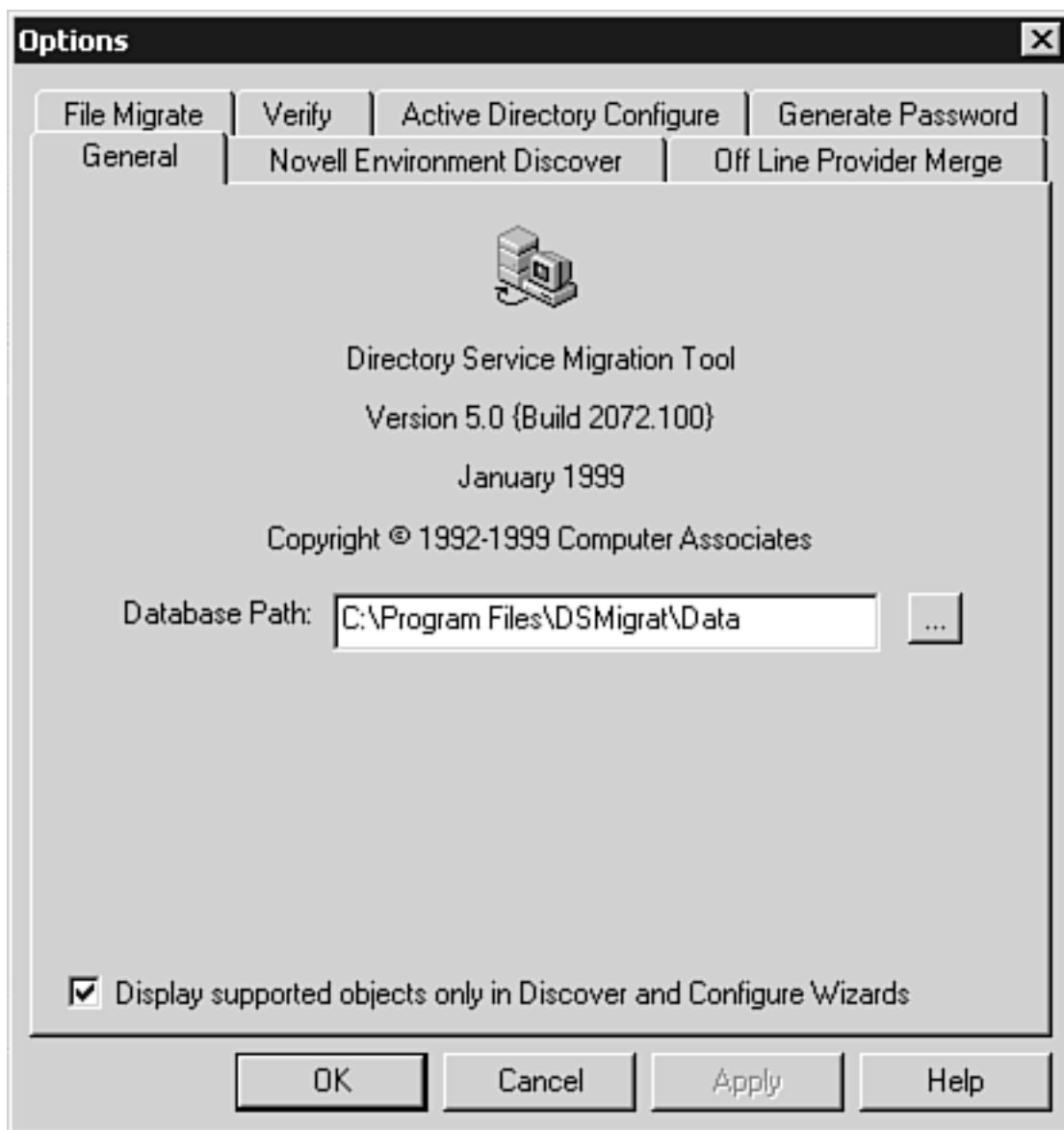


Abbildung 17.6: Das Register General

- *Novell Environment Discover*. Um das in diesem Projekt erstellte Standardorganisationsobjekt zu definieren, müssen Sie dieses in das Textfeld **Default Bindery Organization Name** eingeben (siehe Abbildung 17.7).

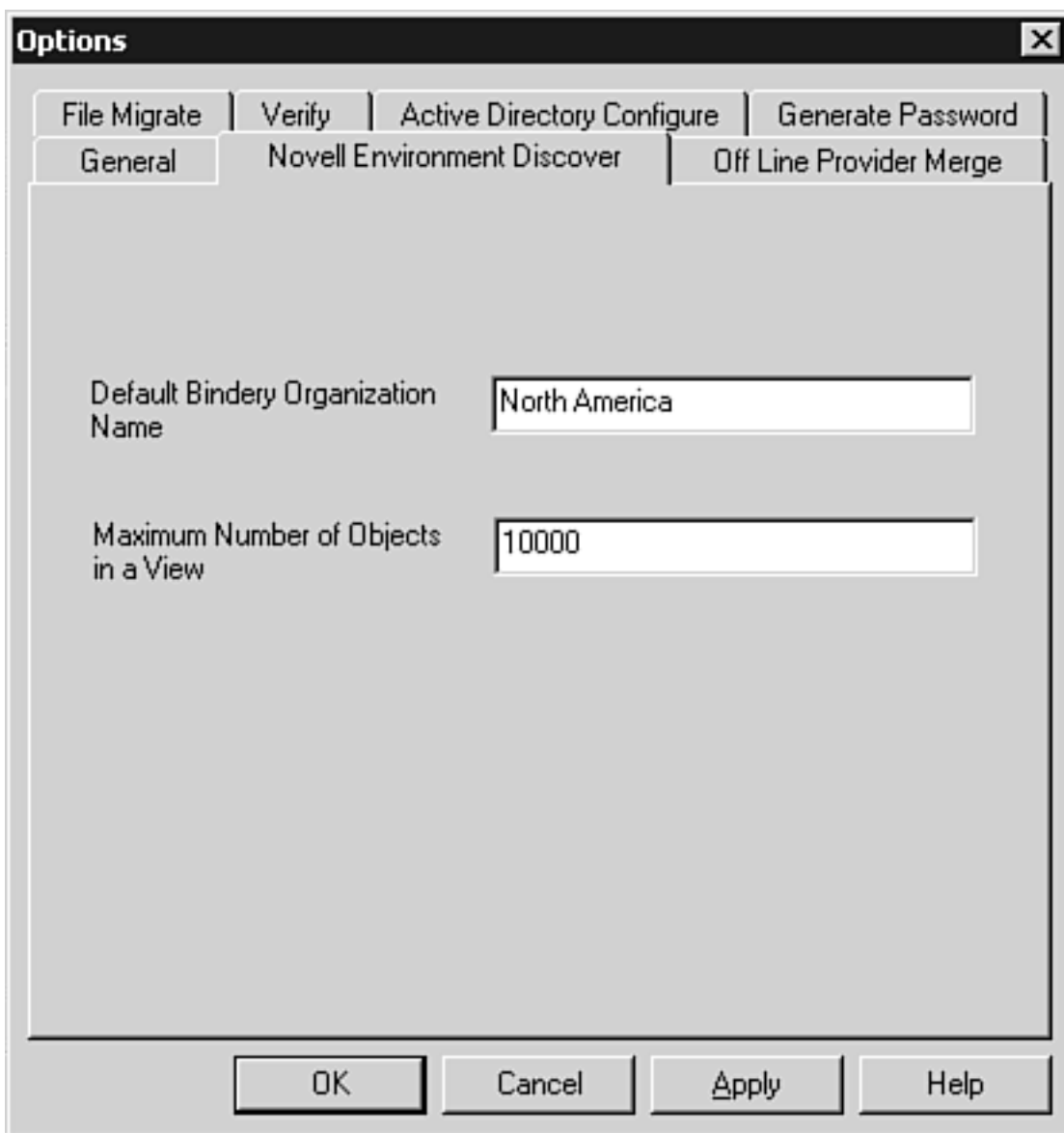


Abbildung 17.7: Das Register Novell Environment Discover

Wenn Sie im Textfeld **Maximum Number of Objects in a View** eine Zahl eingeben, wird das Projekt angehalten, sobald eine nicht mehr verwaltbare Anzahl von Objekten erreicht wird. Wenn Sie hier eine Zahl eingeben, kann das jedoch auch dazu führen, dass das Projekt nicht abgeschlossen wird. Am besten verwenden Sie diese Option als eine Möglichkeit, mit der Sie auf die Größe eines Projekts hingewiesen werden können, und nicht als einen Regler im Prozess.

- *File Migrate*. Wenn Sie Dateien und Verzeichnisse migrieren, kann es vorkommen, dass einige Verzeichnisse und Dateien auf beiden Servern in einem Projekt existieren. Wenn dies geschieht, können Sie Regeln definieren, die dem System sagen, wie es sich in einem solchen Fall verhalten soll. Wenn diese Optionen nicht manuell definiert werden, werden Verzeichnisse und Dateien möglicherweise überschrieben (siehe Abbildung 17.8).

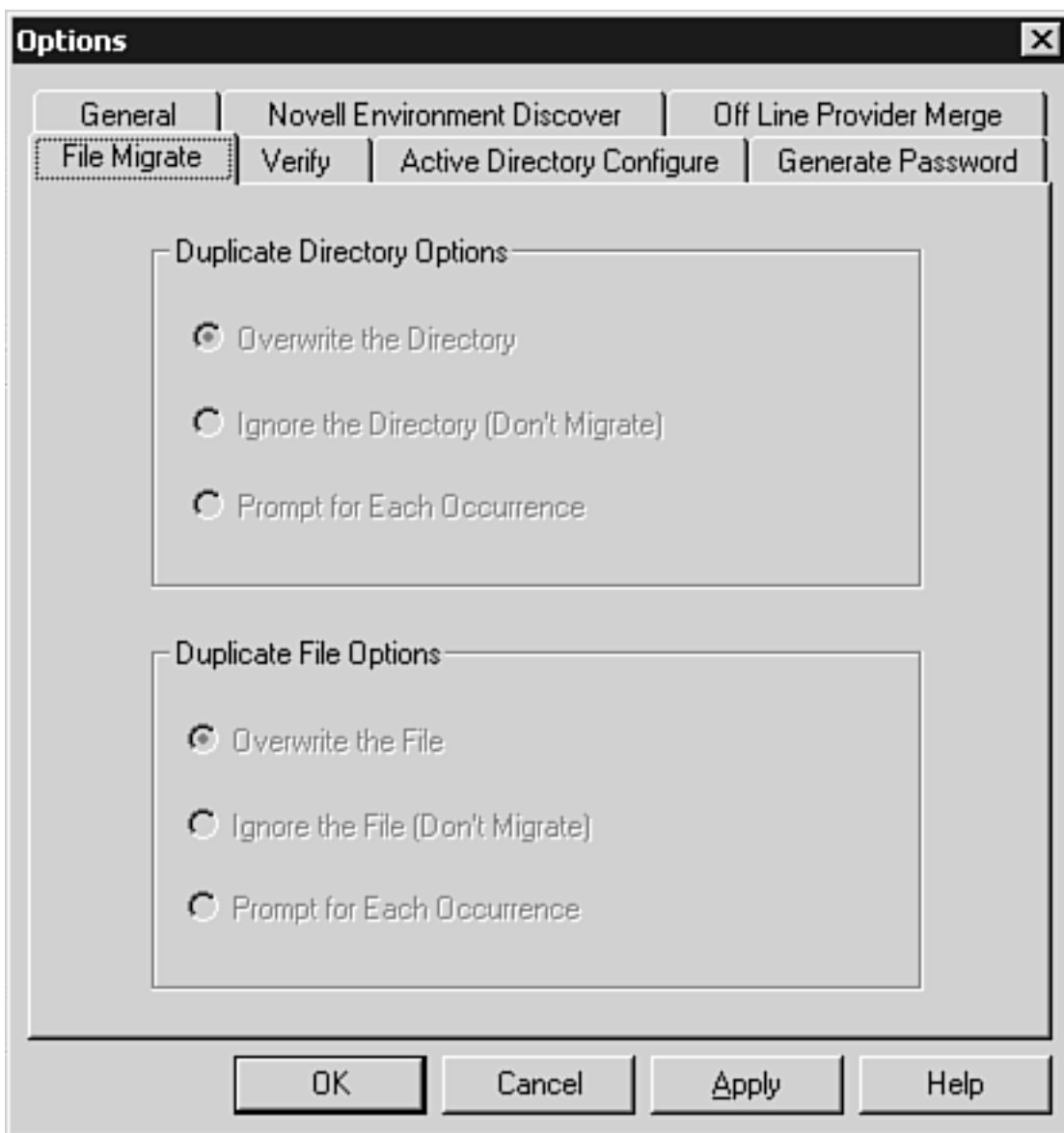


Abbildung 17.8: Die Registerkarte File Migrate

- *Verify Tree Matrix*. Bei der Migration der NDS-Struktur zum Active Directory werden Benutzer- und Gruppenabhängigkeiten geprüft. Im Zusammenhang mit dieser Prüfung hat der Administrator die Möglichkeit, die Anzahl und den Wert der Objekte zu definieren, die in das Verzeichnis gebracht werden (siehe Abbildung 17.9).

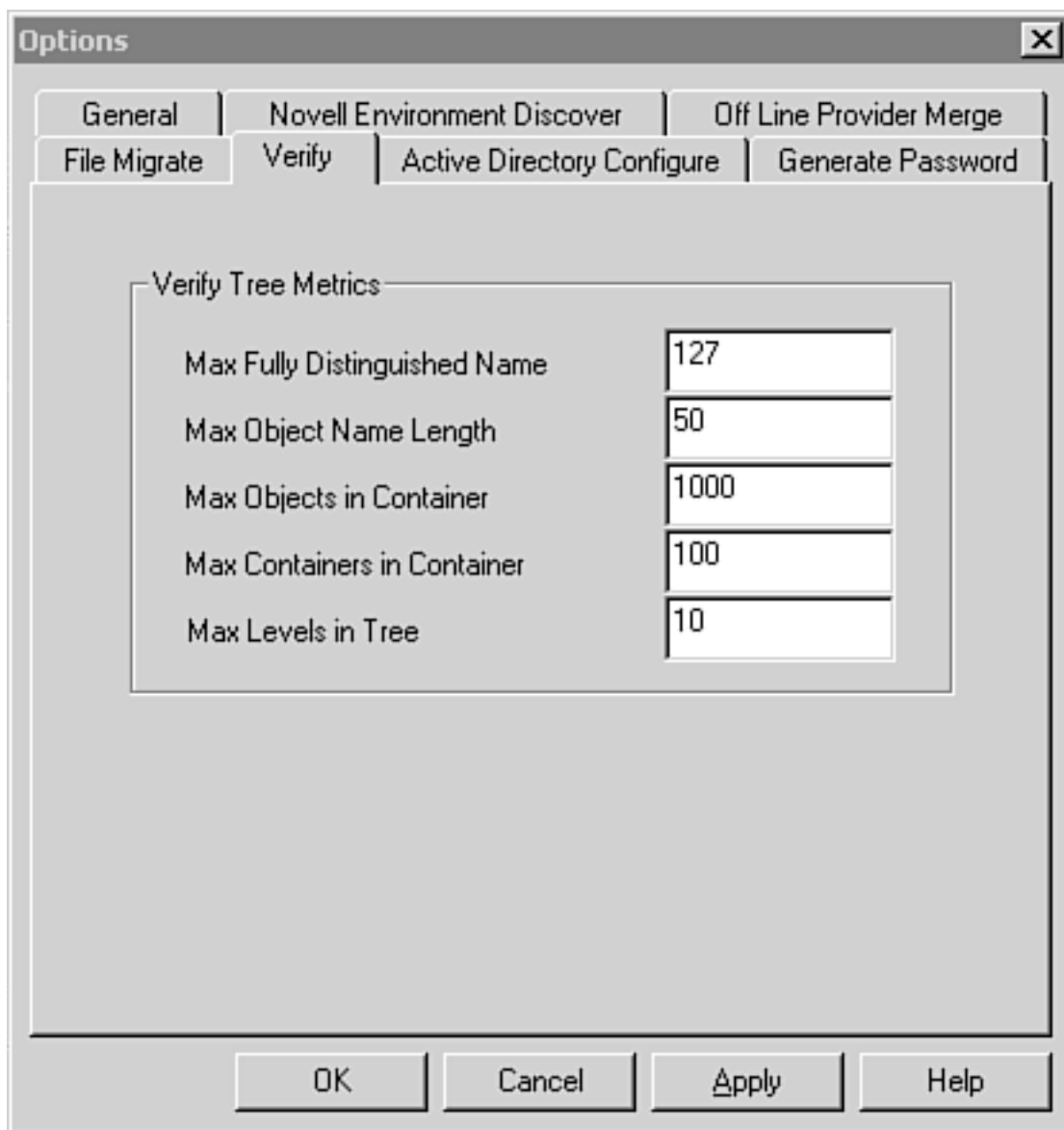


Abbildung 17.9: Die Registerkarte Verify

- *Active Directory Configure*. Einige Verzeichnisobjekte werden während der Migration möglicherweise dupliziert. Daher ist es notwendig, für das Migrationsprogramm Regeln zu definieren, damit es weiß, wie es in einem solchen Fall verfahren soll. Dies geschieht auf der Registerkarte **Offline Provider Merge**. Der Unterschied zwischen einem einwertigen (Single Valued) und einem mehrwertigen (Multi Valued) Objekt besteht darin, dass ein mehrwertiges Objekt mehrere Objekte enthalten kann. Objekte wie Gruppen sind mehrwertig (siehe Abbildung 17.10).

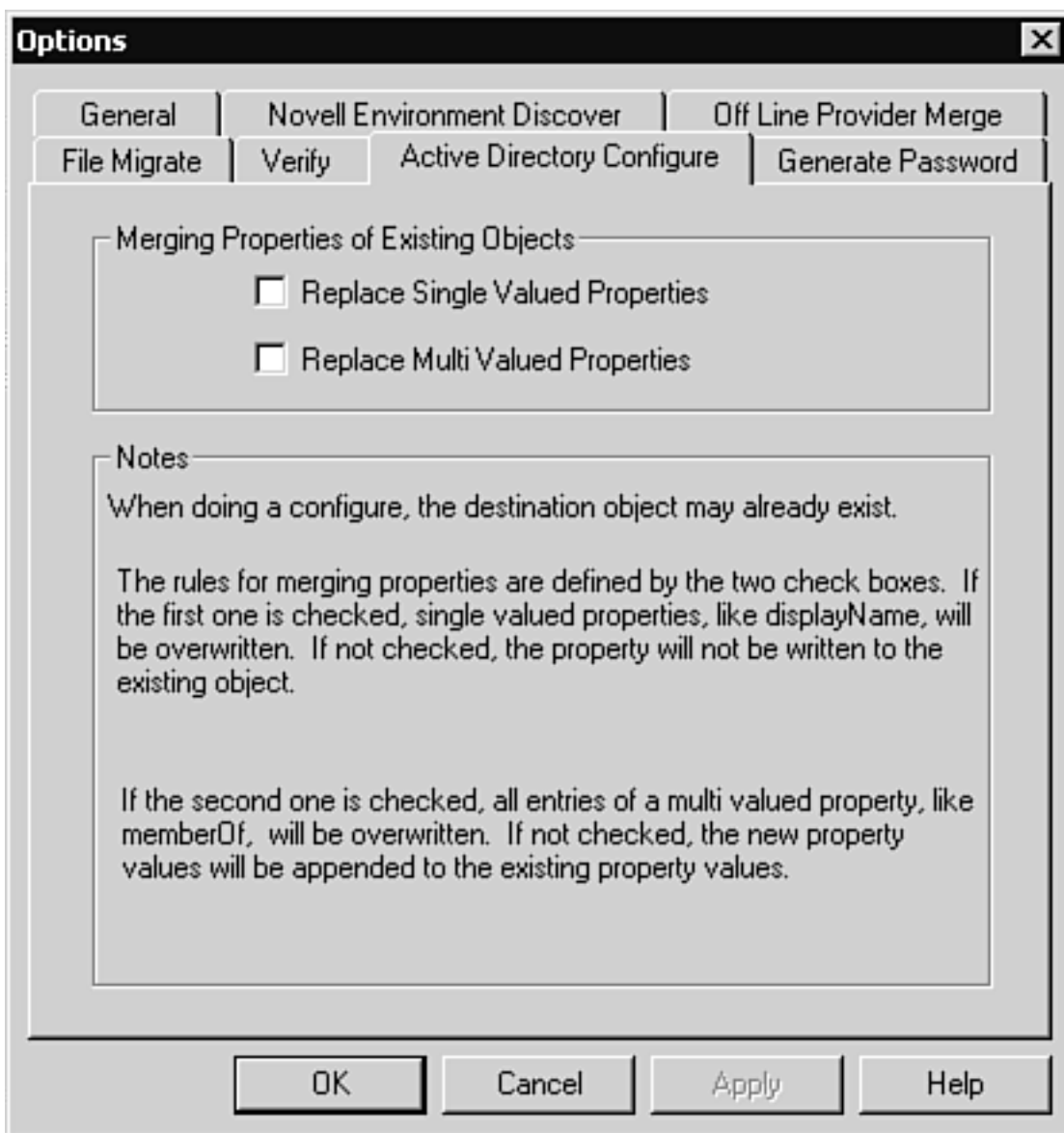


Abbildung 17.10: Die Registerkarte Active Directory Configure

- *Generate Password.* Bei der Migration kann Windows die Kennwörter in der NDS-Struktur nicht lesen, auch nicht mit den entsprechenden Administratorrechten. Daher muss ein Administrator eine Regel für die Handhabung der Kennwörter definieren, die den migrierten Benutzern für deren erste Anmeldung zugewiesen werden (siehe Abbildung 17.11).

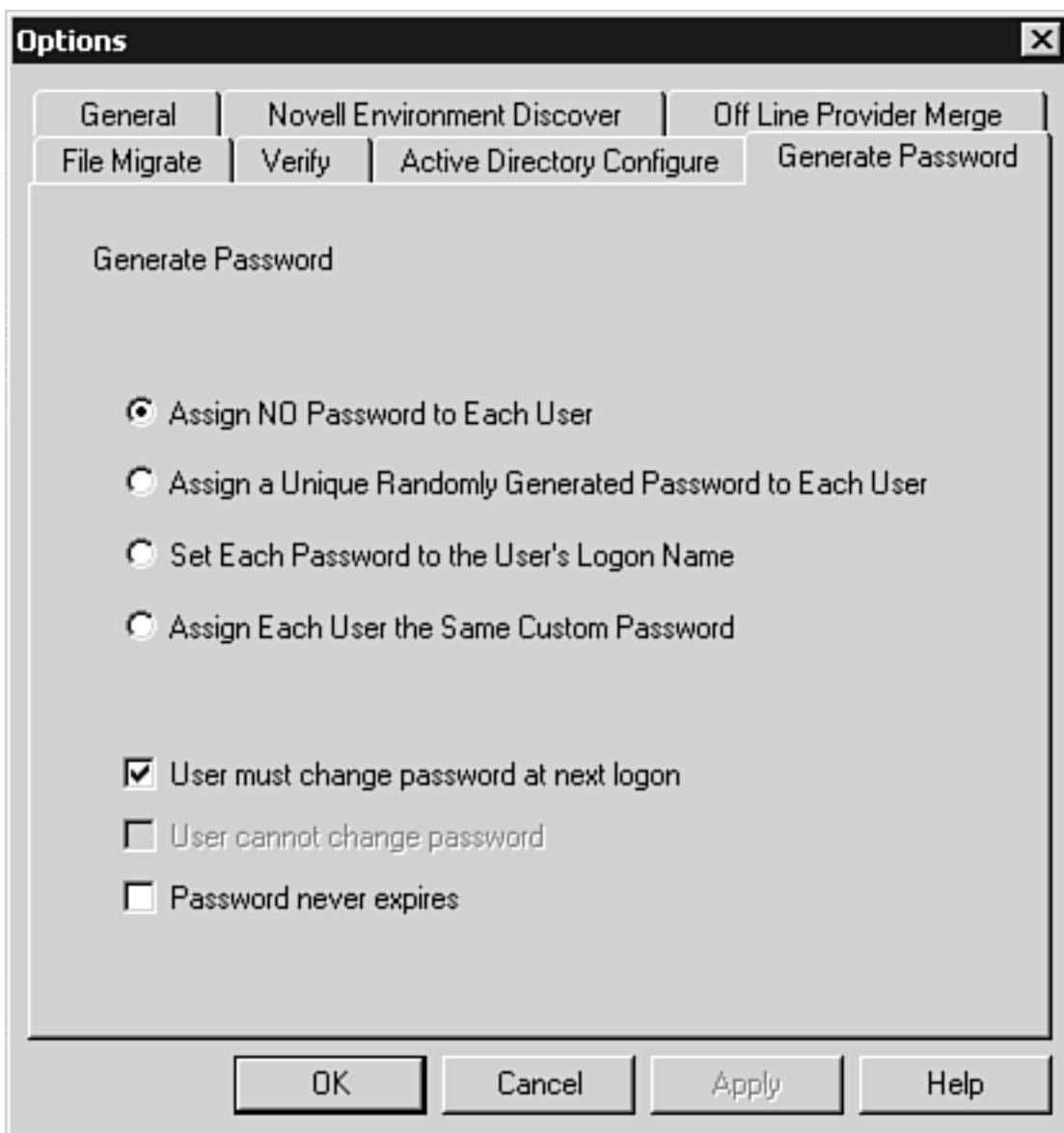


Abbildung 17.11: Die Registerkarte Generate Password

Sie haben die Möglichkeit, kein Kennwort (No Password), ein nach Zufallsprinzip erstelltes Kennwort (Randomly Generated Password), ein vom Benutzernamen abgeleitetes Kennwort oder für alle Benutzer dasselbe Kennwort zu erstellen. Wenn das Kennwort erstellt (bzw. nicht erstellt) ist, kann der Administrator dafür sorgen, dass die Benutzer ihre Kennwörter bei deren erster Anmeldung ändern müssen, oder dass die Benutzer ihre Kennwörter überhaupt ändern können. Wenn die Option gewählt wurde, mit deren Hilfe ein Kennwort nach Zufallsprinzip erstellt wird, können Benutzer Kennwörter, die sie sich dann besser merken können, selbst erstellen, wenn die Option gewählt wird, mit deren Hilfe die Benutzer ihre Kennwörter bei der nächsten Anmeldung ändern müssen. Wenn allen Benutzern dasselbe Kennwort zugewiesen wird, sollten Sie auf jeden Fall die Option **User must change password at next logon** aktivieren.

Wenn die Optionen erst einmal definiert sind, ist das Erstellen des Projekts relativ einfach. Um ein neues Projekt zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie auf die Menüoption **Action** und dann auf **New Project**.
2. Geben Sie in dem dafür vorgesehenen Feld den Namen des Projekts ein und drücken Sie dann die Eingabetaste.

Das ist schon alles. Ein Projekt ist erstellt. Nun muss das Projekt mit den Ressourcen, die migriert werden sollen, gefüllt werden. Sie müssen darüber hinaus auch angeben, wohin diese migriert werden sollen. Das Füllen des Projekts wird als »Erstellen von Ansichten« bezeichnet. Eine *Ansicht (View)* ist ein grafisches Tool, das verwendet werden kann, um die zu migrierenden Objekte zu sammeln. Die zusätzlichen Objekte oder nicht kompatiblen Objekte werden nicht aufgeführt, was in großen Umgebungen zu Problemen führen kann.

Die erste zu erstellende Ansicht ist die »Ansicht von NetWare«. Diese Ansicht ist die anfängliche Ansicht der zu migrierenden Bindery- bzw. NDS-Objekte. Damit kann sich der Administrator des Projekts durch die Bindery- bzw. NDS-Struktur der Objekte bewegen.

Um die »Ansicht von NetWare« zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf das Projekt, zeigen Sie auf **New** und klicken Sie dann auf **View from NetWare**.
2. Geben Sie den Namen der Ansicht, den Namen des Autors und optional eine Beschreibung ein und klicken Sie dann auf **Next**. Daraufhin erscheint eine Liste mit den für das Durchsuchen verfügbaren Servern.
3. Wählen Sie das Bindery- bzw. NDS-Server-Objekt und doppelklicken Sie auf dessen Strukturen.
4. Klicken Sie auf eine Struktur und doppelklicken Sie dann auf die Struktur, um deren Containerobjekte anzuzeigen.
5. Klicken Sie auf ein Containerobjekt und doppelklicken Sie dann auf den Container, um dessen untergeordnete Objekte anzuzeigen.
6. Nachdem Sie ein Objekt gewählt haben, klicken Sie auf **Add Context**, um den Suchkontext auf das gewählte Objekt abzustimmen. Daraufhin erscheint der vollständige Name des gewählten Objekts in diesem Dialogfeld im Feld **Details**.
7. Klicken Sie auf **Next**. Nun zeigt das Dialogfeld eine Übersicht über den Namen der Ansicht und den festgelegten Kontext für die Suchoperation an.
8. Klicken Sie auf **Finish**. Daraufhin zeigt ein Statusdialogfeld die Fortschrittsmeldungen an.

Wenn eine Ansicht der NetWare-Ressource erstellt worden ist, wird das Migrationsprogramm mit den Objekten gefüllt, die migriert werden können. Das Migrieren dieser Objekte ist so einfach wie das Kopieren, Verschieben oder Einfügen von Objekten im Windows Explorer. Wenn Sie sich damit auskennen, kennen Sie sich mit dem Verschieben von Objekten aus. Die Optionen, die für das Migrationsprogramm oder das Projekt selbst festgelegt wurden, führen das System mehr oder weniger durch den gesamten Prozess.

Das Wichtigste, an das Sie beim Verschieben von Objekten denken sollten, ist die Beziehung zwischen dem Objekttyp und dem Objekt, in das bzw. von dem diese verschoben werden. Ein einfaches Beispiel dafür ist, dass eine Organisationseinheit nicht in ein Gruppenobjekt kopiert werden kann. Denken Sie an die in Kapitel 9 beschriebenen Verzeichnisregeln bezüglich der Container- und Gruppenobjekte und den Elementen, die diese enthalten können.

Migrieren von Datei- und Verzeichnisstrukturen

Das Migrieren von Dateien von Server zu Server oder von mehreren Servern zu einem Server sollte

innerhalb des Migrationsprogramms erfolgen. Wenn Sie Dateien und Verzeichnisse mit diesem Programm migrieren, werden die Attribute und Berechtigungen zusammen mit den Daten verschoben. Dies kann ohne dieses Programm schwierig oder auch schlichtweg nicht möglich sein.

Um eine Migration durchzuführen, sollten Sie den Assistenten für die Migration von Dateien (File Migration Wizard) verwenden (siehe Abbildung 17.12). Dieser Assistent führt Sie durch den Vorgang des Auswählens und Kopierens.

Um den Assistenten aufzurufen und zu verwenden, gehen Sie wie folgt vor:

1. Klicken Sie in der Directory Service Migration-Konsole mit der rechten Maustaste auf das Directory Service Migration Tool-Objekt oder auf ein Datenträgerobjekt und klicken Sie anschließend auf **All Tasks** und dann auf **File Copy**.
2. Wenn der Assistent erscheint, klicken Sie auf **Next**.
3. Klicken Sie auf **Yes**, um die Dateien zu migrieren. Klicken Sie anschließend auf **Next**.
4. Um alle Datenträger und Verzeichnisse in Ihrer NetWare-Konfiguration anzuzeigen, doppelklicken Sie auf die Quellansicht.



Abbildung 17.12: Der Assistent für die Migration von Dateien (File Migration Wizard)

5. Klicken Sie auf einen Quelldatenträger oder ein Quellverzeichnis und ziehen Sie diesen bzw. dieses in eine Zielfreigabe.
6. Klicken Sie auf **Next**.
7. Wählen Sie ein Quellansichtselement und klicken Sie dann auf **Delete**, um das Objekt zu löschen. Sie können auch auf **Edit** klicken, um ein Dialogfeld für die Bearbeitung aufzurufen.
8. Klicken Sie auf **Browse** neben dem Zielverzeichnis. Daraufhin wird eine Liste der verfügbaren Verzeichnisspeicherorte angezeigt. Wählen Sie ein Zielverzeichnis.
9. Aktivieren Sie die Option **Create Share**, um einen neuen Freigabespeicherort zu erstellen. Klicken Sie dann auf **Next**.
10. Klicken Sie auf **Next**, um sämtliche Dateien zu migrieren. Daraufhin erscheint wieder das Bearbeitungsdialogfeld zum Migrieren von Freigaben und Dateien. Klicken Sie wieder auf **Next**. Sie werden nun aufgefordert, Datenträgerobjekte zu aktualisieren. Wählen Sie einzelne Datenträgerobjekte aus oder klicken Sie auf **Select All**.
11. Klicken Sie auf **Check Disk Space** um zu überprüfen, ob für die geplante Migration genügend Platz vorhanden ist. Klicken Sie anschließend auf **Next**.
12. Klicken Sie auf **Update** oder auf **Don't Update**. Klicken Sie dann auf **Next**. Sie werden aufgefordert, die Migration abzuschließen. Klicken Sie auf **Finish**, um die Migration zu starten.

17.2.4 NDS for NT (von Novell)

Novell hat ganz offensichtlich seine eigene Meinung über diese ganze Koexistenz. Die Produktlinie von NetWare bietet ein Produkt für die beiden nebeneinander existierenden Systeme, wendet jedoch eine andere Taktik an. Das Produkt ermöglicht dem Administrator einer NDS-Struktur auch Windows-Server von derselben Schnittstelle aus zu verwalten. Das Produkt, das von Novell (unabhängig von deren NetWare-Produktlinie) erhältlich ist, heißt *NDS for NT*.

Wenn das Produkt installiert wird, erscheinen sämtliche NetWare NDS-Objekte im NetWare NDS Administrator-Tool (NWADMIN) und auch die Windows-Server erscheinen. Die Idee, die sich dahinter verbirgt, ist die, dass alle Benutzer, Gruppen und Objekte Teil desselben Verzeichnisdienstes (NDS) werden. Damit wird es möglich, dass IT-Teams keine zwei Verzeichnisse verwalten müssen, sondern sich auf einen Verzeichnisdienst konzentrieren können. Das Produkt von Novell bietet Native-IP-Support.

Windows-Domänen werden NDS-Objekte und werden damit über NetWare synchronisiert. In beiden Umgebungen werden dieselben Benutzerkennwörter verwendet. Berechtigungen werden nun von einem Programm aus verwaltet.

Der einzige Nachteil ist der, dass auf Arbeitsplatzrechnern der Novell-Client für NetWare (Client 32 oder der Z.E.N. Works-Client) installiert sein muss. Dies ist erforderlich, damit der Arbeitsplatzrechner Zugriff auf die NDS-Dienste hat. Wenn der Client jedoch weiterhin als ein normaler Windows NT-Client fungieren soll, kann weiterhin der Microsoft-Client verwendet werden.

© Copyright [Markt+Technik Verlag](#), ein Imprint der Pearson Education Deutschland GmbH
Elektronische Fassung des Titels: Windows 2000 Server Kompendium, ISBN: 3-8272-5611-9 Kapitel:
Verbindung zu Novell NetWare

Kapitel 18 Verbindung zwischen UNIX und Windows 2000 Server

Eine der größten Stärken von Windows 2000 ist seine Fähigkeit, eine Verbindung zu unterschiedlichen Betriebssystemen und Umgebungen herzustellen. UNIX ist das Betriebssystem, das das Internet in absehbarer Zeit beherrschen wird. In diesem Kapitel geht es darum, wie Windows 2000- und UNIX-Systeme Informationen miteinander austauschen. Dies umfasst Konzepte wie Sicherheit, Dateifreigabe, Druckerfreigabe und Konnektivität auf Anwendungsebene.

Die Themen in diesem Kapitel werden aus der Sicht eines Windows 2000-Servers, der SMB-Clients (Server Message Block) Dienste zur Verfügung stellt, sowie aus der Sicht eines Windows 2000-Rechners, der auf Datei- und Druckerfreigaben auf einen UNIX-Host zugreift, beschrieben. Diese Aktivitäten sind für Stapelverarbeitungsprozesse wie Aktivitäten zur Unterstützung von Datenbanken, wobei Windows 2000 Daten an UNIX senden und von UNIX empfangen muss, sehr nützlich. Darüber hinaus können Windows 2000 Professional-Rechner für unterschiedliche Aufgaben direkt auf UNIX zugreifen.

Hier ein kurzer Überblick über das Kapitel:

- Konzeptuelle Unterschiede zwischen Windows 2000 Server und UNIX-Betriebssystemen
- Unterschiedliche Varianten von UNIX
- Einfache TCP/IP-Tools
- Zugriff auf NFS
- Samba
- Drucken in einer UNIX-Umgebung
- Die Zukunft: Microsoft und UNIX

18.1 Konzeptuelle Unterschiede zwischen Windows 2000 Server und UNIX-Betriebssystemen

Windows 2000 Server wurde als ein Unternehmens-Server entwickelt, der Client-Rechnern, die Windows ausführen, Datei-, Druck- und Anwendungsdienste zur Verfügung stellt. UNIX wurde sowohl als Client als auch als Server sowie für die Kommunikation mit anderen UNIX-Clients entwickelt. So kommt es zu unterschiedlichen Ansätzen bezüglich der Probleme mit Benutzerkonten, Sicherheit und Verzeichnisdiensten.

18.1.1 Benutzerkonten

Benutzerkonten definieren, wie ein Betriebssystem entscheidet, welche Benutzer welche Operationen durchführen können. Bei Windows 2000 gibt es eine Administratorengruppe, der mehrere Benutzer zugewiesen werden können. Die Mitglieder dieser Gruppe haben im Prinzip die volle Kontrolle über sämtliche Aspekte des Rechners. Bei UNIX gibt es ein Konto, *root* genannt, das über ähnliche

Berechtigungen verfügt. Bei Windows 2000 werden die Benutzerkonten in der Registrierung gespeichert, während die Konten bei UNIX wie jede andere Konfigurationsinformation in einer Textdatei gespeichert werden. Benutzer werden in einer Textdatei, in der Regel `passwd` genannt, definiert, die ein systemabhängiges Format aufweist und üblicherweise den Namen des Benutzers, Gruppenzugehörigkeiten, eine verschlüsselte Version des Benutzerkennworts, das Basisverzeichnis des Benutzers sowie die Shell enthält, die ausgeführt werden soll, wenn sich der Benutzer anmeldet. Bei den meisten Systemen gibt es auf jedem UNIX-System, auf das der Benutzer Zugriff hat, Benutzerkonten sowie unterschiedliche Schemata für das Kopieren der Kontoinformationen über ein Netzwerk hinweg.

Bei UNIX gibt es etwas Ähnliches wie die Gruppen bei Windows 2000. *Gruppen* ermöglichen einer Reihe von Benutzern den Zugriff auf eine Reihe von Ressourcen, ohne dass für jede einzelne Ressource jeder Benutzerzugriff einzeln gewährt werden muss. Wie bei Windows 2000 können Benutzerkonten von UNIX-Betriebssystemen ebenfalls mehreren Gruppen zugewiesen werden.

18.1.2 Sicherheit

Die UNIX-Sicherheit basiert vollständig auf dem Konzept einer *Datei*. Für eine Datei auf einem Datenträger können drei Sicherheitsebenen definiert werden: Besitzer, Gruppe und Jeder. Jede Datei gehört einem bestimmten Benutzer und einer bestimmten Gruppe. Es gibt drei Attribute, die auf jeder Ebene definiert werden können: lesen, schreiben und ausführen. Diese werden in der Regel wie folgt angezeigt:

```
-rwxr--r--    1 milles    root          15483 Jun 26 11:57 ch6.rtf
-rw-r--r--    1 milles    root          56320 Jun 26 13:02 final.doc
```

Für die erste Datei, `ch6.rtf`, gilt Folgendes: Der Benutzer ist `milles`. Er ist Mitglied der Gruppe `root`. Die Dateigröße beträgt 15.483 Byte. Die Datei wurde am 26. Juni erstellt. Die Zeile beginnt mit `-rwxr--r--`. Das bedeutet, dass der Besitzer der Datei (`milles`) über die Rechte Lesen (`r` von `read` = lesen), Schreiben (`w` von `write` = schreiben) und Ausführen (`x` von `eXecute` = ausführen) für die Datei verfügt. Die Besitzergruppe (`root`) hat nur Lesezugriff. Die Gruppe Jeder hat ebenfalls Lesezugriff. Vollzugriff für die Gruppe Jeder wird als `-rwxrwxrwx` dargestellt. Dabei ist der erste Bindestrich für das Sticky-Bit reserviert. Das *Sticky-Bit* gibt an - wenn es definiert ist, wird aus dem Bindestrich ein `S` - welches Benutzerkonto das Programm tatsächlich ausführt. Wenn es ein Programm gäbe, bei dem das Sticky-Bit definiert wäre und jeder das Recht hätte, dieses Programm auszuführen (das wäre dann `srwxr-xr-x`), dann hätte dieses Programm denselben Benutzerzugriff wie der Besitzer der Datei.

Das ist sehr hilfreich, wenn dem Benutzer für eine Datei das Recht zu lesen und zu schreiben, allerdings nur von einem bestimmten Programm aus (wenn beispielsweise das Programm Ergebnisse in eine Datei mit einem leicht zu verfälschenden Format schreibt), zugewiesen werden soll. Das Programm würde so konfiguriert, dass ein Benutzer, der Zugriff auf die Datei hat, Besitzer ist, und die einzelnen Benutzer keinen Zugriff auf die Datei hätten. Ein weiteres Beispiel ist ein Programm, das nur zu bestimmten Zeiten ausgeführt werden soll. Wenn es beispielsweise nur nach Feierabend möglich sein soll, Spiele zu spielen, werden die Spielprogramme einem Konto zugewiesen, das sich nur nach Feierabend anmelden kann, und das Sticky-Bit wird definiert, sodass jeder die Programme ausführen kann. Da sich das Konto

nur nach Feierabend anmelden kann, wird das Programm nur außerhalb der Arbeitszeit ausgeführt.

Ein weiterer wichtiger Hinweis bezüglich der Sicherheit bei UNIX: Alles bei UNIX ist eine Datei. Wenn also jemand eine Audiodatei ausführen möchte, wird diese Datei an ein Audiogerät gesendet, das bei einigen Varianten von UNIX mit der Datei `/dev/audio` verbunden ist. Das setzt voraus, dass der Benutzer, der die Datei ausführt, Schreibzugriff auf die Datei `/dev/audio` hat.

Windows 2000 arbeitet mit der Idee einer *Benutzerimitation*, die allerdings nicht so leicht verfügbar ist wie das Sticky-Bit-System von UNIX. Sie ist vielmehr tief in der Win32-API und in der Architektur verborgen und kann nur genutzt werden, wenn sie gleich zu Beginn entsprechend programmiert wird. Ansonsten ähneln sich die Sicherheitsmodelle stark, d.h. es können jeweils Lese-, Schreib- und Ausführungsrechte für Benutzer, Gruppen und jeden definiert werden. Bei Windows 2000 gibt es das spezielle Benutzerkonto Jeder. Dieser Gruppe gehört jeder außerhalb der definierten Benutzer und Gruppen an. Bei Windows 2000 gibt es darüber hinaus die Möglichkeit, mehrere Gruppen bzw. Benutzer direkt mit einer Datei zu verbinden. Diese Möglichkeit bietet UNIX nicht. Bei UNIX müssen stattdessen sämtliche Benutzer einer bestimmten Gruppe zugewiesen werden, und dann muss diese Gruppe Besitzer der Datei werden.

18.1.3 Verzeichnisdienste

Verzeichnisdienste wie Active Directory und NDS sind das Rückgrat der unternehmensweiten Sicherheit. Diese Systeme ermöglichen Administratoren die zentrale Verwaltung sämtlicher Sicherheitsaspekte, was natürlich sehr vorteilhaft ist. Sicherheits-einstellungen werden bei diesen Systemen einmal an einer Stelle vorgenommen und verbreiten sich dann selbst im gesamten Netzwerk.

UNIX-Betriebssysteme haben in Bezug auf Verzeichnisdienste Pionierarbeit geleistet. Sun Microsystems brachte mit den damals so genannten *Yellow Pages (YP)* das Ganze ins Rollen. An dem Namen hat sich irgendwo irgendeine Telefongesellschaft gestoßen und so wurde der Dienst in *NIS (Network Information System)* umbenannt. Mit Hilfe von NIS können Benutzernamen und Kennwörter innerhalb eines Domänenkontexts so verwendet werden, dass Benutzer innerhalb einer Domäne auf Ressourcen zugreifen können, ohne dass ein einzelnes Benutzerkonto auf jedem Rechner in der Domäne erstellt werden muss. NIS ist größtenteils ein Transportsystem. Es übernimmt die Authentifizierung von Benutzern nicht selbst. Stattdessen leitet es die Benutzername/Kennwort-Paare (und gegebenenfalls andere Informationen) durch das Netzwerk, damit die üblichen Authentifizierungsmechanismen greifen können.

UNIX-Systeme verfügen darüber hinaus auch über ein anderes Programm zur Verzeichnisverwaltung. Dies stellt die LDAP-Dienste (Lightweight Directory Access Protocol) zur Verfügung, die bisher jedoch nur als eine Anwendung zum Suchen von Personen implementiert sind und E-Mail-Adressen, Telefonnummern und Büroadressen angeben. Zur Zeit bietet dieses Programm nicht das Maß an Integration in das Sicherheitsmodell wie dies Windows 2000 und Active Directory tun.

Die Programmfamilie Samba, die später in diesem Kapitel noch ausführlicher beschrieben wird, ermöglicht es einigen UNIX-Systemen (Silicon Graphics IRIX, Linux, FreeBSD und SunOS, um nur einige zu nennen), Windows NT 4.0-Server, sowohl Domänencontroller als auch eigenständige Server, zu imitieren. Es ist zu erwarten, dass das Samba-Projekt weitere Kreise zieht und in der Lage sein wird, Windows 2000 Active Directory zu emulieren. Dann werden Systeme, die Samba ausführen, die gleichen

Verzeichnisdienstfunktionen wie Windows 2000-Server haben.

Windows 2000-Verzeichnisdienste in der Form von Active Directory sind wesentlich fortschrittlicher. Das Active Directory ist deutlich einfacher zu konfigurieren, verwalten und dokumentieren als das NIS-System und es scheint weitaus mehr Funktionen als jedes gegenwärtig erhältliche UNIX-basierte Verzeichnissystem zu haben.

18.2 Unterschiedliche Varianten von UNIX

Windows 2000 und UNIX sind zwei sehr verschiedene Betriebssysteme. Windows 2000 wird von einem Unternehmen, nämlich Microsoft, hergestellt und unterstützt. Als solches ist jede Installation von Windows 2000 jeder anderen Installation sehr ähnlich. Und Programme, die auf einem Rechner funktionieren, funktionieren immer auch auf einem anderen Rechner, vorausgesetzt, die Rechner verfügen jeweils über dieselbe Prozessorarchitektur. Bei Windows gibt es Standardverzeichnisse für DLL-Dateien (%SYSTEMROOT%\Winnt\System32), Standardverzeichnisse für Client-Programme (\Programme) und ein Standardformat für das Speichern von Konfigurationsinformationen (die Registrierung). Diese Standards zusammen mit einer umfangreichen Benutzerbasis machen das Programmieren für Windows-Plattformen einfacher und vorteilhafter als es ohne diese Standards wäre. Es trägt darüber hinaus auch bis zu einem gewissen Maß dazu bei, Kosten zu reduzieren, da bei einem Satz Windows-Rechner alle Rechner im Prinzip mehr oder weniger gleich sind. Und wenn bei einem Rechner eine Änderung in der Registrierung vorgenommen werden muss, muss exakt dieselbe Änderung auch bei den anderen Rechnern vorgenommen werden. Windows-Systeme sind außerdem alle binärkompatibel innerhalb derselben Architektur. Das bedeutet, dass ein Programm, das unter Windows 98 läuft, aller Wahrscheinlichkeit nach auch unter Windows 2000 auf Intel-Hardware problemlos laufen wird.

In der Welt von UNIX ist das alles nicht so einfach. UNIX wurde von AT&T entwickelt und war ein Open-Source-System. Somit konnte jeder, der UNIX hatte, Änderungen an diesem Betriebssystem vornehmen. Nach dem Auseinanderbrechen von AT&T durfte das Unternehmen UNIX verkaufen, was es auch tat, und zwar zu ordentlichen Preisen. So kam es, dass einige Leute an der Berkeley-Universität in Kalifornien ein komplett neues UNIX-Betriebssystem entwickelten. Sie nannten ihre Version des Betriebssystems Free-BSD. Das *Free* im Namen bezieht sich darauf, dass es keinen AT&T-Code gab, und das Produkt damit frei von AT&T-Urheberrechten war. Zu den BSD-Versionen (Berkeley System Development) gehören gegenwärtig Free-BSD und Net-BSD.

Etwa zur gleichen Zeit versuchte ein Student in Finnland, Linus Torvalds, ein gutes, kostengünstiges System für seinen neuen Arbeitsplatzrechner zu finden. Sein Problem war, dass AT&T immer noch UNIX besaß, das sehr teuer war, und die Betriebssysteme anderer Anbieter entsprachen nicht seinen Bedürfnissen. So kam es, dass er etwas tat, von dem sich andere wünschen, es auch zu können: Er entwickelte sein eigenes Betriebssystem und nannte es Linux. Nach Jahren der Entwicklung durch Tausende von Menschen rund um die Welt ist Linux nun eines der dominierenden Betriebssysteme im Internet. Linux liegt zwischenzeitlich in unterschiedlichen Varianten von verschiedenen kommerziellen und nicht kommerziellen Unternehmen wie RedHat, Caldera und SuSE vor.

Neben Free-BSD und Linux stellen Anbieter von UNIX-Arbeitsplatzrechnern eigene Varianten von UNIX zur Verfügung wie z.B. Sun (SunOS), Data General (DG/UX) und Hewlett Packard (HP/UX), um

nur einige wenige zu nennen. Jedes dieser Betriebssysteme ist aus Teilen des ursprünglichen Systems V von AT&T und den BSD-Varianten zusammengesetzt.

Den UNIX-Betriebssystemen liegen einige gemeinsame architektonische Voraussetzungen zugrunde. Die Implementierung der Betriebssysteme kann jedoch sehr unterschiedlich ausfallen. Mitte bis Ende der 80er-Jahre machten die UNIX-Anbieter eine Menge Lärm darum, dass ihre Systeme dem einen oder anderen Standard entsprächen. Dennoch gibt es gerade auch bei wichtigen Elementen wie dem Betriebssystemstart (System V Init oder BSD Init), bei Speicherort und Format der Protokolldateien sowie Format, Speicherort und Dateinamen von Konfigurationsinformationen große Unterschiede. Die meisten dieser Unterschiede gibt es leider bis heute und sie sind Gegenstand von regelrechten Glaubenskriegen darüber, welches nun das bessere System sei. Das Ganze führte jedenfalls dazu, dass UNIX-Programme auch bei gleicher Architektur in der Regel nicht binärkompatibel sind. Darüber hinaus werden auch die Protokolldateien und Konfigurationsdateien bei den unterschiedlichen Systemen an unterschiedlichen Stellen gespeichert.

18.3 Einfache TCP/IP-Tools

TCP/IP-Tools wie Telnet und FTP, mit denen heute gearbeitet wird, gibt es schon seit langer Zeit auf unterschiedlichen Betriebssystemen und unterschiedlicher Hardware. Wenn Sie diese Tools verwenden möchten, ist es wichtig, dass Sie die richtige Version des gewünschten Tools entweder für den Client oder für den Server finden. Bei Windows 2000 Server gibt es glücklicherweise die Client-Software FTP und Telnet. Server-Software gibt es leider nur für FTP. Bei UNIX gibt es Telnet und FTP sowohl für Clients als auch für Server: Die Clients werden einfach `ftp` und `telnet`, deren Gegenstücke für den Server `ftpd` und `telnetd` genannt (wobei das `d` für `daemon` steht, der Name von UNIX für Prozesse, die im Hintergrund ablaufen, um bestimmte Dienste anzubieten). Darüber hinaus gibt es noch eine ganze Reihe von weniger bekannten Programmen wie TFTP und Finger, die einige interessante Nutzungsmöglichkeiten bieten.

18.3.1 Telnet

Telnet bietet Terminaldienste über ein Netzwerk. In der UNIX-Welt wird dieses Programm allgemein für die Fernausführung und Fernverwaltung verwendet. Da die meisten UNIX-Arbeitsplatzrechner über eine sehr bequeme und leistungsfähige Shell verfügen, stellt Telnet ein sehr leistungsstarkes Programm dar. Denn damit ist es Administratoren möglich, Änderungen an der Konfiguration eines Rechners vorzunehmen, angefangen beim Starten und Beenden von Diensten bis hin zum Ändern der Konfigurationen und der IP-Adressen. Telnet vermittelt das Gefühl, man würde vor einer Konsole sitzen.



Das Arbeiten mit Telnet ist wirklich so, als würde man vor der Konsole sitzen. Wenn Sie also über Telnet auf einen Host zugreifen, wird alles, was Sie während der Telnet-Sitzung eingeben, Zeichen für Zeichen an den Host übertragen. Das bedeutet, dass auch Ihr Kennwort übertragen wird. Wenn Sie Cracker fürchten, die mit Netzwerkpaket-Sniffer arbeiten, dann sollten Sie Telnet nicht verwenden.

Windows 2000 bietet zwei Versionen von Telnet. Eine Version ist eine Version von Telnet im Konsolenmodus. Sie ist in der Regel unter `%SYSTEMROOT%\System32\telnet.exe` zu finden (siehe Abbildung 18.1). Dabei handelt es sich um einen Standard-Telnet-Client und der wird somit komplett

über die Befehlszeile ausgeführt. Um das Programm aufzurufen, klicken Sie auf **Start** und **Ausführen** und geben dann `telnet` ein. Sie können auch `telnet` und den Namen des Rechners eingeben, zu dem eine Verbindung hergestellt werden soll, also z.B. `telnet kermit` für einen Rechner, der Kermit heißt.

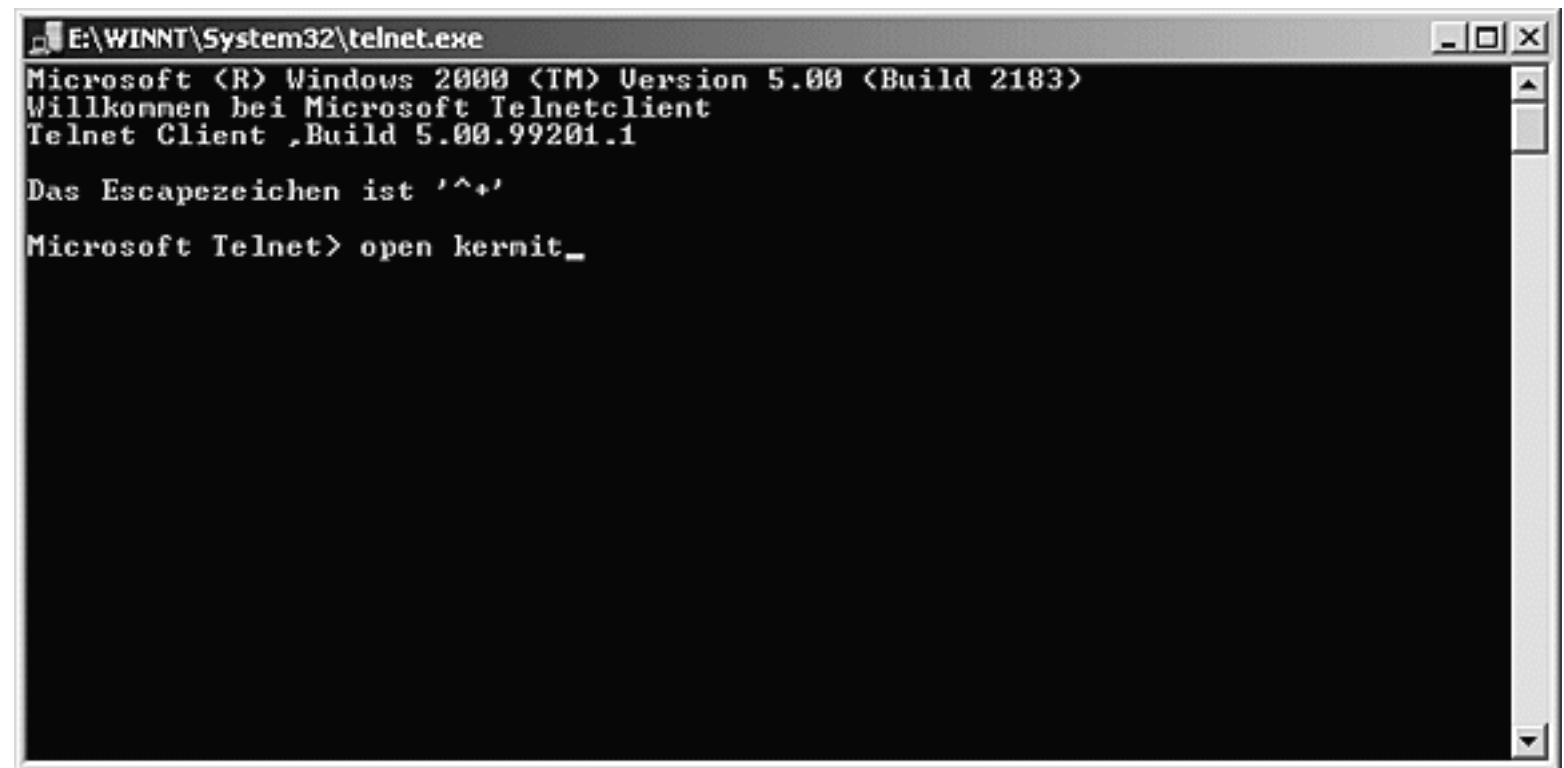


Abbildung 18.1: Der Zeichenmodus von Telnet. Diese Konsole stellt mit Hilfe des Befehls `open` eine Verbindung zum Rechner »Kermit« her.

Das konsolenbasierende Telnet wird in zwei Modi ausgeführt. Der Konsolenmodus verfügt über eine Eingabeaufforderung, die wie folgt aussieht:

```
Microsoft Telnet>
```

Diese Eingabeaufforderung bedeutet, dass sich das System im Konsolenmodus befindet. Um eine Liste von in der Konsole zu verwendenden Befehlen aufzurufen, geben Sie den Befehl `help` ein. Daraufhin erscheint folgende Liste:

```
Microsoft Telnet> help
Befehle können abgekürzt werden. Folgende Befehle werden unterstützt:
close      Trennt die aktuelle Verbindung
display    Zeigt Befehlsparameter an
open       Stellt Verbindung her
quit       Beendet Telnet
set        Legt Optionen fest (geben Sie 'set ?'
           für eine Liste ein)
```


status	Zeigt Statusinformationen an
unset	Hebt Optionsfestlegungen auf (Geben Sie 'unset ?' für eine Liste ein)
?/help	Hilfe anzeigen

Microsoft Telnet>

Für die Verwendung von Telnet sind einige grundlegende Konsolenbefehle erforderlich. Wenn in der Befehlszeile kein Computernamen angegeben wird, stellt der Befehl **open** eine Verbindung her. Wenn Sie also im Dialogfeld **Ausführen** nur **telnet** eingeben, wird lediglich Telnet gestartet. Wenn Sie dagegen **telnet open kermit** eingeben, wird eine Verbindung zum Rechner mit dem Namen Kermit hergestellt. Die Bedeutung der anderen Befehle erschließt sich von selbst.

Wenn der Telnet-Client eine Verbindung hergestellt hat, geht er automatisch in den Verbindungsmodus über. Um wieder in den Konsolenmodus zu gelangen und die Verbindung dennoch aufrecht zu erhalten, drücken Sie die Tasten (Strg) und (J). Um wieder in den Verbindungsmodus zu gelangen, drücken Sie in einer Leerzeile die Eingabetaste. Um eine Telnet-Konsole zu beenden, trennen Sie die Verbindung und geben in der Konsole den Befehl **quit** ein.

Der andere Telnet-Client ist eine nette grafische Schnittstelle zu Telnet, die sich üblicherweise in *%SYSTEMROOT%\System32\ TelnetC.exe* befindet. Er bietet zwei unterschiedliche Terminalemulationen: VT-100/ANSI und VT-52. In der Regel wird VT-100/ANSI verwendet. Dies ist die Standardeinstellung. Um auf die Konfigurationsoptionen zugreifen zu können, klicken Sie im Menü **Terminal** auf **Einstellungen** (siehe Abbildung 18.2). In diesem Dialogfeld können Sie auch die Hintergrundfarbe sowie die Schriftart ändern.

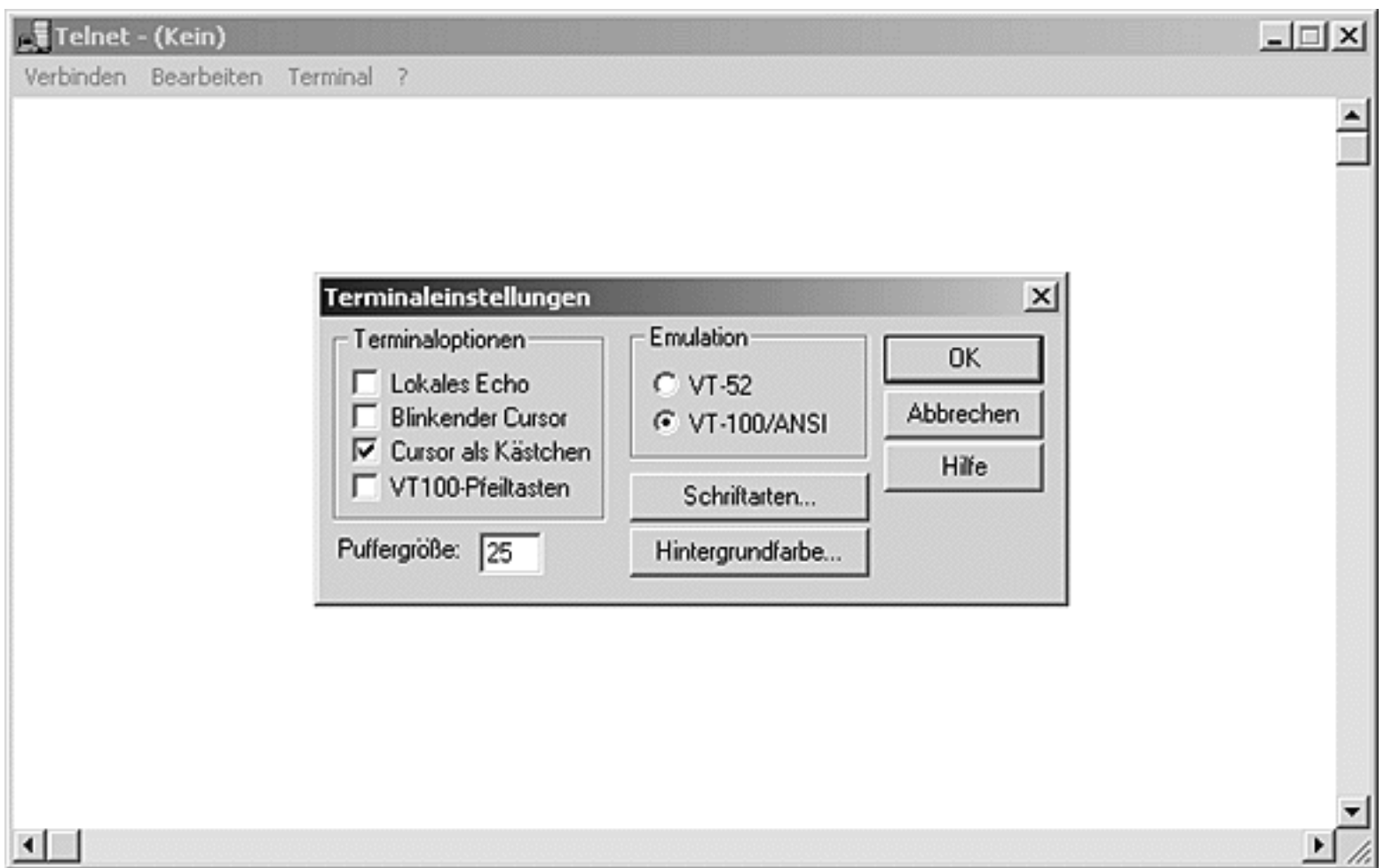


Abbildung 18.2: Die grafische Benutzeroberfläche von Telnet mit dem Dialogfeld Terminaleinstellungen

Ein besseres Programm, das denselben Dienst zur Verfügung stellt, ist das Shareware-Programm NetTerm, das über die meisten Shareware-Seiten im Internet erhältlich ist. Es stellt ein Telnet-Programm mit Anmeldung, konfigurierbaren Schlüsselzuordnungen und DFÜ-Unterstützung zur Verfügung. Wenn Sie den Telnet-Client häufig nutzen, sollten Sie nach einem Programm wie NetTerm suchen, das besser ist als das in Windows 2000 enthaltene Programm.

Darüber hinaus gibt es auch Telnet-Server für Windows 2000-Systeme. Das Unternehmen Seattle Labs stellt einen Telnet-Server her, der von jedem beliebigen Telnet-Client aus verwendet werden kann. Er eignet sich hervorragend für Systemadministratoren, da sie mit diesem Programm Operationen durchführen können, die große Bandbreiten beanspruchen, wie z.B. das Kopieren von umfangreichen Dateien, ohne dabei Verbindungen mit großen Bandbreiten nutzen zu müssen.

18.3.2 FTP

Das Protokoll FTP (File Transfer Protocol) ermöglicht Dateiübertragungen von Servern zu Clients. FTP beruht auf einer Reihe von Befehlen zum Wechseln in das richtige Verzeichnis und zum Starten der Dateiübertragungen. Die Datei nimmt eine Benutzer-ID und ein Benutzerkennwort und arbeitet innerhalb der Dateisicherheit des Betriebssystems um festzulegen, welche Dateien gelesen werden können, und ob eingehende Dateien angenommen werden oder nicht.

Es gibt mehrere unterschiedliche FTP-Clients. Windows NT ist mit zweien ausgestattet. Um auf den ersten zuzugreifen, geben Sie in einem Web-Browser eine FTP-URL wie z.B. `ftp://ftp.microsoft.com` ein. Daraufhin erscheint die bekannte grafische Benutzeroberfläche von FTP, die wie ein gewöhnliches Explorer-Fenster aussieht (siehe Abbildung 18.3). Der andere FTP-Client ist ein Befehlszeilen-Client. Er kann über die Eingabeaufforderung oder über das Startmenü durch Eingeben des Befehls `ftp <Adresse>` aufgerufen werden, wobei die Adresse einfach nur der Name des Rechners ist, an den die FTP-Anforderung gesendet wird.

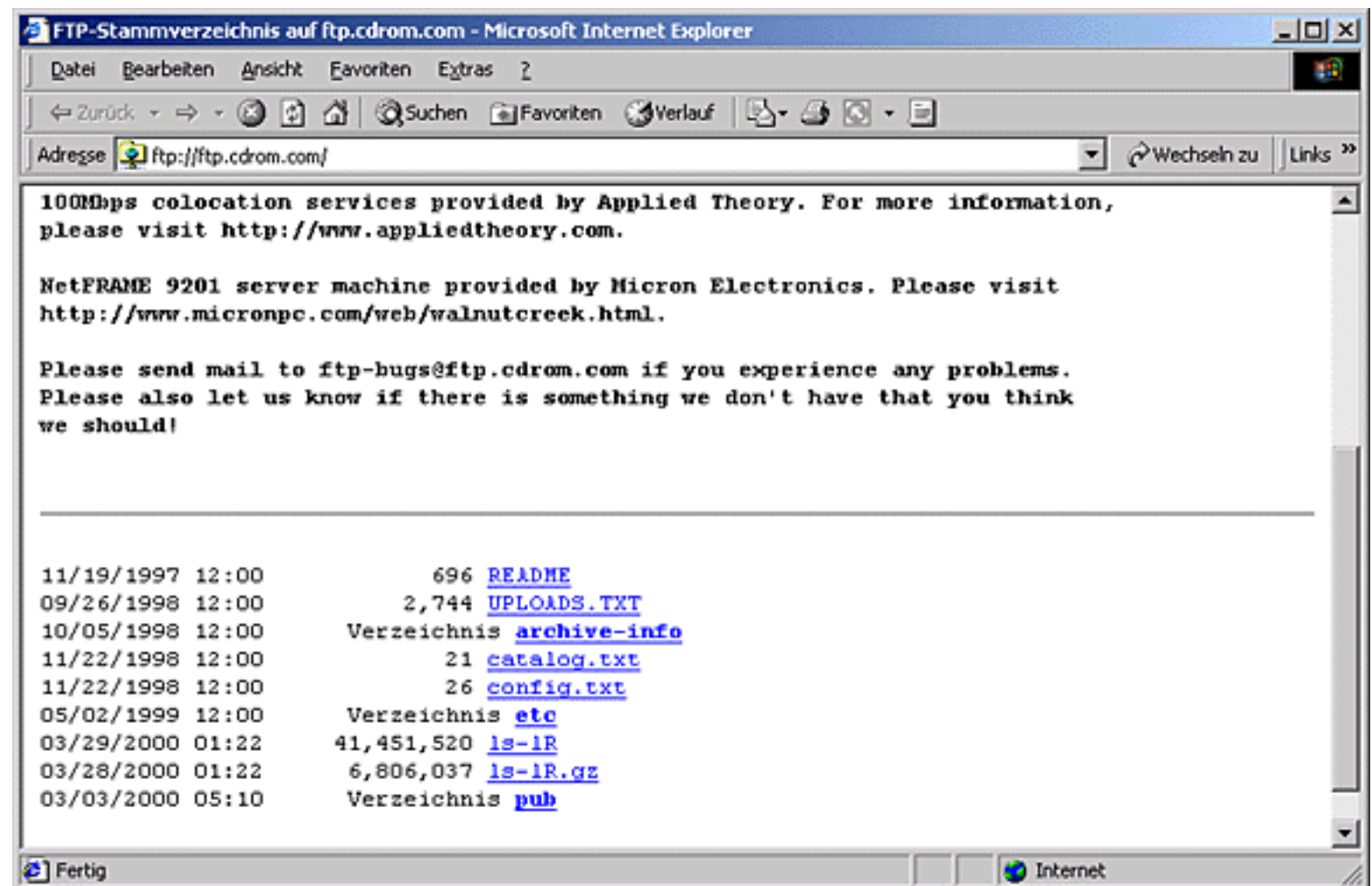


Abbildung 18.3: Dies ist eine FTP-Verbindung zu der bekannten Seite `ftp.cdrom.com`. Sie können sie aufrufen, indem Sie auf Start und Ausführen klicken und dann `ftp: //ftp.cdrom.com` eingeben.

Folgende FTP-Befehle stehen zur Verfügung:

- **OPEN.** Wird verwendet, um eine Verbindung herzustellen (mit `OPEN . FTP . MICROSOFT . COM` wird beispielsweise eine Verbindung zum FTP-Server bei Microsoft hergestellt).
- **USER.** Der Benutzername, der verwendet wird, um die Verbindung zu authentifizieren. Dabei handelt es sich entweder um den Benutzer Anonym mit dem Kennwort Gast oder um einen tatsächlichen Benutzernamen.
- **PASSWORD.** In der Regel mit `PASS` abgekürzt, wird der Befehl `PASSWORD` für die Übertragung des Kennworts verwendet. Beachten Sie, dass wie beim Telnet-Protokoll auch beim FTP-Protokoll Kennwörter in Klartext über das Netzwerk übertragen werden. Das bedeutet, dass Cracker ein leichtes Spiel haben. Ein FTP-Server fragt beim Aufbau einer Verbindung automatisch nach dem

Benutzernamen und nach dem Kennwort. Die Befehle **USER** und **PASS** werden in der Regel nur in Skripten verwendet.

- **BINARY**. Häufig mit **BIN** abgekürzt, stellt dieser Befehl den Dateiübertragungsmodus Binär ein. Die meisten Server verwenden ASCII als den Standardmodus für Dateiübertragungen. Da es sich beim ASCII-Modus um einen Sieben-Bit-Standard handelt, werden sämtliche im ASCII-Übertragungsmodus übertragenen Binärdateien beschädigt. Bei diesem Befehl handelt es sich um einen Befehl zum Einstellen des Dateiübertragungsmodus. Sämtliche Übertragungen erfolgen im Binärmodus, bis der Befehl **ASCII** eingegeben wird.
- **ASCII**. Häufig mit **ASC** abgekürzt, stellt dieser Befehl den Dateiübertragungsmodus ASCII ein. Wenn dieser Modus bei der Übertragung einer Binärdatei verwendet wird, wird die Datei beschädigt. Hierbei handelt es sich um einen Befehl zum Einstellen des Dateiübertragungsmodus. Sämtliche Übertragungen erfolgen im ASCII-Modus, bis der Befehl **BINARY** eingegeben wird.
- **HASH**. Dieser Befehl teilt FTP mit, für jeweils 2.048 übertragene Byte ein Nummernzeichen (#) auszugeben. Dies ist eine gute Möglichkeit, bei interaktiven Sitzungen sicherzustellen, dass die Übertragung nicht unterbrochen worden ist.
- **CD**. Change Directory. Dieser Befehl wechselt vom aktuellen Verzeichnis zu einem Zielverzeichnis auf dem Server. Er funktioniert so wie der Befehl **CD** in der Befehlszeile. So wird beispielsweise mit **CD pub** in das Verzeichnis **pub** gewechselt, während **CD . .** in der Verzeichnishierarchie um eine Ebene nach oben wechselt.
- **LCD**. Local Change Directory. Dieser Befehl wechselt vom lokalen Verzeichnis auf dem Client zum angegebenen Pfad.
- **LS** oder **DIR**. Zeigt den Inhalt des angegebenen Verzeichnisses oder, wenn kein Verzeichnis angegeben wird, den Inhalt des aktuellen Verzeichnisses an. UNIX-Optionen wie **ls -l** für lange Verzeichnis-Listings und **ls -C** für Verzeichnisse in Spalten (beachten Sie, dass bei den Optionen nach Groß- und Kleinschreibung unterschieden wird) werden unterstützt. Mit dem Befehl **ls -l foo.txt** wird eine Verzeichnisliste erstellt und in der Datei **foo.txt** im aktuellen Verzeichnis gespeichert. Das ist praktisch, weil so die Ausgabe umgeleitet werden kann. Befehle wie **ls -l /more** können verwendet werden, um die Ausgabe seitenweise anzuzeigen.
- **GET**. Der Befehl **GET** wird zusammen mit dem Namen der Datei eingegeben, die zum Client übertragen werden soll. Mit dem Befehl **GET** wird eine Datei übertragen. Es wird kein Verzeichnis übertragen, und es können keine Platzhalter verwendet werden. Der Befehl **GET *.*** würde beispielsweise nach der Datei ***.*** suchen und sie nicht finden. Es würde keine Übertragung stattfinden. Das Nette an diesem Befehl ist, dass eine Zielfile angegeben werden kann. Somit wird mit dem Befehl **GET DATEI1 MEINEDATEI** die Datei **DATEI1** kopiert und in die Datei **MEINEDATEI** übertragen.
- **PUT**. Der Befehl **PUT** wird zusammen mit dem Namen der Datei eingegeben, die zum Server übertragen werden soll. Ebenso wie beim Befehl **GET** können auch mit diesem Befehl keine Platzhalter verwendet werden.
- **MGET** und **MPUT**. Das **M** steht für *mehrere*. Der Befehl **MGET** überträgt mehrere Dateien zum Client und akzeptiert Platzhalter. Der Befehl **MPUT** überträgt mehrere Dateien zum Server und akzeptiert Platzhalter. Platzhalter sind natürlich UNIX-Standard.
- **DELETE** und **MDELETE**. In der Regel mit **DEL** und **MDEL** abgekürzt, dienen diese Befehle dazu, Dateien zu löschen. **DEL** löscht jeweils eine Datei, während **MDEL** Platzhalter akzeptiert.

- !. Dieser Befehl startet innerhalb der FTP-Sitzung eine Shell.
- QUIT. Dieser Befehl beendet die FTP-Sitzung.

Es stellt sich nun die Frage, warum man sich mit all diesen Befehlen herumärgern soll, wenn es eine schöne grafische Benutzeroberfläche gibt. Die Antwort ist ganz einfach die, weil es viele Fälle gibt, in denen das FTP-Programm im Befehlszeilenmodus ausgeführt werden muss, z.B. um eine Kopie der Transaktionen des Vortags für das Importieren in eine lokale SQL Server-Datenbank zu bekommen. In diesem Fall ist es angenehm, eine Reihe von Befehlen in ein FTP-Skript einzugeben und dieses dann entweder mit dem Befehl AT oder einem anderen Zeitplandienst auszuführen. Erstellen Sie dazu mit Hilfe von Notepad eine gewöhnliche Textdatei mit den Befehlen, die FTP zum Ausführen braucht. Hier ein Beispiel:

```
OPEN ftp.microsoft.com
USER anonym
gast
CD /bussys
GET README.TXT
QUIT
```

Beachten Sie, dass der Befehl PASS fehlt. Manche Server benötigen diesen Befehl, andere nicht. Es hat sich herausgestellt, dass die Server von Microsoft diesen Befehl nicht benötigen. Um dieses Skript auszuführen, rufen Sie einfach den FTP-Befehl über die Befehlszeile mit den entsprechenden Argumenten auf:

```
ftp -s:ftp.scr -n
```

Dabei ist `ftp.scr` der Name des auszuführenden Skripts. Mit der Option `-n` wird dem FTP-Client mitgeteilt, er solle sich nicht automatisch anmelden. Wenn diese Option nicht gesetzt ist, sollten Sie den Befehl `USER` löschen, aber den Benutzernamen `Anonym` stehen lassen. Wie gesagt, bei einigen Servern ist das erforderlich, bei anderen nicht. Sie müssen ein bisschen herumprobieren, um den richtigen Befehl herauszufinden. Ein weiterer nützlicher Hinweis: Leiten Sie die Ausgabe immer um, um sie leichter auf Fehler prüfen zu können. Wenn Sie beispielsweise folgenden Befehl ausführen:

```
ftp -s:ftp.scr -n > ftp.out
```

Dann enthält die Datei `ftp.out` das gesamte Protokoll der FTP-Sitzung:

```
ftp> Connected to ftp.microsoft.com.
OPEN ftp.microsoft.com
220 ftp Microsoft FTP Service (Version 4.0).
```

```
ftp> USER anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.

230-This is FTP.MICROSOFT.COM
230-Please see the dirmap.txt file for
230-more information.
230 Anonymous user logged in.
ftp> ftp>
CD /bussys
250 CWD command successful.
ftp> GET README.TXT
200 PORT command successful.
150 Opening ASCII mode data connection for README.TXT(1715 bytes).
226 Transfer complete.
ftp: 1715 bytes received in 0.29Seconds 5.89Kbytes/sec.
ftp> QUIT
221 Thank you for using Microsoft Products!
```

Sie können jede Kombination der oben genannten Befehle in einem FTP-Skript angeben, sodass Dateien gesendet oder empfangen werden können. Das ist für nächtliche Stapelverarbeitungen sehr nützlich, wenn eine Datei von einem UNIX-Rechner geholt werden muss. Aber das funktioniert auch mit jedem anderen Rechner, der FTP ausführen kann.

Es gibt eine ganze Reihe von FTP-Programmen von Drittanbietern, die vom Mehr-oder-weniger-Standard CuteFTP (unter www.cuteftp.com erhältlich) bis hin zum frei erhältlichen LeechFTP reichen.

18.3.3 Die weniger bekannten Programme

Das TCP/IP-Protokoll hat im Laufe der Jahre viele interessante Utilities hervorgebracht, von denen viele kaum noch verwendet werden. Dazu zählen Programme wie Finger, TFTP und RSH.

TFTP

Das Programm TFTP arbeitet mit dem TFTP-Protokoll (Trivial File Transfer Protocol). Im Gegensatz zum FTP-Protokoll, das Daten über TCP-Verbindungen überträgt, verwendet TFTP UDP-Verbindungen (User Datagram Protocol), die über keinerlei Mechanismus zur Fehlerprüfung verfügen. Es gibt zwei Gründe, warum dieses Programm nicht so häufig verwendet wird: Einer davon ist das Fehlen eines Fehlerprüfmechanismus. Der andere Grund ist der, dass eine Reihe von Sicherheitsproblemen aufgetreten sind. Das Programm selbst ist relativ einfach. Es besteht nur aus einer Befehlszeile:

```
tftp [-i] Hostname [GET | PUT] Quelle [Ziel]
```

Der Parameter `-i` gibt an, dass mit TFTP eine Binärdatei und keine ASCII-Datei übertragen wird. Hostname gibt den Host an, zu dem TFTP eine Verbindung herstellen soll. GET oder PUT müssen für die Richtung, in der die Übertragung erfolgen soll, angegeben werden. Quelle ist der Name der zu übertragenden Datei und Ziel gibt die Stelle an, an die die Datei übertragen werden soll.

Finger

Der Befehl `finger` wird nicht verwendet, um Menschen über das Netzwerk zu beleidigen. Er wird vielmehr dazu verwendet, Informationen über einen bestimmten Benutzer an einem bestimmten Host abzufragen. Auch hierbei handelt es sich um ein einzeliliges Programm:

```
finger [-l] [Benutzer] @Host
```

Der Parameter `-l` sagt dem Finger-Programm, es solle die Informationen im langen Listenformat anzeigen. Mit den Parametern Benutzer und @Host wird der Benutzer definiert, über den Informationen angezeigt werden sollen. Wenn nur der Parameter Benutzer eingegeben wird, sucht das Programm auf dem lokalen Rechner nach den Informationen. Ansonsten sucht das Programm den angegebenen Benutzer am angegebenen Host. Hier ist beispielsweise das lokale Netzwerk des Autors:

```
finger millcs@kermit
```

```
[kermit]
Login: millcs                      Name: Chris Miller
Directory: /home/millcs           Shell: /bin/bash
On since Sun Jun 27 14:03 (CDT) on ttyp0 from 10.254.254.5
    8 seconds idle
No mail.
No Plan.
```

Auf einem UNIX-Rechner können Benutzer in ihrem Basisverzeichnis die Datei `.plan` sowie die Datei `.project` erstellen, die von Finger statt `No Plan.` angezeigt wird. Auch Finger hat Sicherheitsprobleme, da Benutzer außerhalb des Netzwerks gültige Benutzerkonten finden und feststellen können, wann das Konto zum letzten Mal verwendet worden ist (in dem Beispiel oben war der Benutzer `millcs` angemeldet, als Finger ausgeführt worden ist, sodass angezeigt wird `On since ...`).

RSH

RSH oder Remote Shell führt einen Befehl über das Netzwerk an einem entfernten Rechner aus. Folgende Befehlszeile wird verwendet:

```
rsh Hostname [-l Benutzername] [-n] Befehl
```

Wenn kein Benutzername angegeben wird, verwendet RSH den Anmeldenamen des Benutzers, der RSH ausführt. Das `-n` sagt RSH, keine Ausgabe zu erzeugen. `Befehl` ist der auszuführende Befehl. Das RSH-Programm sendet Kennwörter in Klartext über das Netzwerk. Die häufig wiederholten Warnungen vom FTP- und Telnet-Lager gelten hier also auch.

Das sind dann auch schon die weniger bekannten UNIX-Tools. Im Folgenden geht es nun darum, wie zwischen Windows-Anwendungen und UNIX-Hosts Verbindungen hergestellt werden können.

18.4 Verbindung zwischen UNIX und Windows-Anwendungen

TCP/IP unterstützt eine Vielzahl unterschiedlicher Verbindungsmechanismen zwischen Clients und Servern. UNIX verfügt über eine Vielzahl von unterschiedlichen Standardmechanismen für die Verbindung zwischen Clients und Servern, darunter XWindows, RPC und andere proprietäre Protokolle. In der Datei `SERVICES` in `%SYSTEMROOT%\Winnt\System32\drivers\etc` befindet sich eine Liste der Standardanschlüsse, die von UNIX-Systemen für die Übertragung unterschiedlicher Arten von Daten verwendet werden. Die Datei zeigt eine Liste der von IANA (Internet Assigned Numbers Authority) zugewiesenen bekannten Anschlüsse an. Sämtlichen weitverbreiteten Anwendungen werden Anschlussnummern zugewiesen, sodass sie nicht miteinander in Konflikt geraten. Die Anschlussnummer wird dann jeweils an das IP-Paket angefügt, sodass die Netzwerkdienste jedes Paket an das richtige Programm routen können. Sie können Telnet verwenden, um ein Gefühl dafür zu bekommen, was diese Anschlüsse tun. Mit dem Befehl `telnet localhost qotd` wird ein Zitat des Tages vom lokalen Rechner erstellt. Vorausgesetzt allerdings, der lokale Rechner führt den Simple TCP/IP Services-Dienst aus. Der Anschluss `qotd` ist in der Datei `SERVICES` definiert.



Um die Zitate des Tages zu ändern, bearbeiten Sie die Datei `%SYSTEMROOT%\Winnt\System32\drivers\etc\quotes`. Übernehmen Sie das in der Datei verwendete Format. Musterzitate, auch als *Fortunes* bezeichnet, stehen im richtigen Format im Internet zur Verfügung. Verwenden Sie einfach Ihre bevorzugte Suchmaschine, um welche zu finden.

18.4.1 XWindows und Windows 2000

Lange vor Windows NT 3.1 verwendeten UNIX-Benutzer eine Umgebung mit grafischer Benutzeroberfläche, die unter der Bezeichnung XWindows (oder auch nur X) bekannt ist. X wird auch als DFÜ-Ausführungsprogramm verwendet und es gibt sogar Hardware, die als *X-Terminals* bezeichnet wird, mit deren Hilfe Benutzer auf X zugreifen und Programme an einem entfernten Rechner ausführen können. Terminal Server ist weder eine Erfindung von Citrix noch eine Innovation von Microsoft. Mit UNIX kann dieses Programm seit Ende der achtziger Jahre verwendet werden. Für Windows 2000 muss spezielle Software erworben werden, um eine Verbindung zu X herstellen zu können. Ein Anbieter solcher Software, Hummingbird Communications (www.hummingbird.com) hat eine Reihe von Windows-zu-X-Lösungen im Angebot.



In der Welt von X ist ein Client ein Server und ein Server ist ein Client. X sieht die Definitionen aus einem anderen Blickwinkel: Ein X-Server bietet X-Clients grafische Funktionen u.ä. Somit führt ein X-Terminal einen X-Server aus.

18.5 Zugriff auf NFS

NFS (Network File System) ist ein Satz Protokolle, die von Sun Microsystems entwickelt wurden, und die Arbeitsplatzrechnern die gemeinsame Nutzung von Dateien ermöglicht. Diesen liegt dasselbe Konzept zugrunde, als würde man ein Netzlaufwerk in Windows laden. Aber es funktioniert völlig anders. Für einen Rechner, der als Server verwendet wird, gibt es einen Satz Netzwerkfreigaben. Der Server konfiguriert nach Bedarf Sicherheitseinstellungen und Privilegien für die Freigaben. Wenn der Client auf eine Freigabe zugreift, werden die Sicherheitsparameter überprüft und die Freigabe wird in einem bestimmten Verzeichnis in UNIX geladen.

Zwei wichtige Hinweise zu UNIX-Dateien und -Verzeichnissen: UNIX unterstützt ausschließlich den Schrägstrich als Verzeichnistrennzeichen. Somit stellt der Pfad */home/millics* keine Reihe von Befehlszeilenparameter dar, sondern ist tatsächlich ein Verzeichnis.

UNIX-Betriebssysteme verwenden eine einzige Hierarchie für ihr gesamtes Dateisystem. Die Funktionsweise ist der von Microsoft-Systemen sehr ähnlich, mit der einen Ausnahme, dass es bei UNIX den Begriff eines Laufwerksbuchstabens nicht gibt. Bei UNIX werden vielmehr unterschiedliche Laufwerke in Teile des Verzeichnisses »geladen«. Das erste Boot-Laufwerk wird in der Regel mit dem Hauptverzeichnis (root) verbunden und als »/*« bezeichnet. Wenn sich in diesem Laufwerk eine weitere Partition befindet, kann diese in /data geladen werden. Ein Benutzer, der einen Befehl wie z.B. cd /data eingibt, sieht automatisch die Daten auf einem anderen Laufwerk oder in einer anderen Partition. Einige Benutzer halten dies für sinnvoller, als ständig zwischen den einzelnen Laufwerken hin und her springen zu müssen. Darüber hinaus gibt es auch in Windows 2000 Funktionen, mit denen das Konzept des Ladens von UNIX emuliert werden kann.*

Um mit einem Windows 2000-Arbeitsplatzrechner über NFS auf einen UNIX-Rechner zugreifen zu können, ist Software von Drittanbietern erforderlich. Ein Beispiel für ein solches Produkt ist AccessNFS Gateway von Intergraph. Mit Hilfe dieses Produkts kann ein Windows 2000-Server auf einen UNIX-Host und über NFS auf Dateien zugreifen. Das Produkt von Intergraph ist sehr interessant, weil es nicht nur den Zugriff auf NFS-Freigaben ermöglicht, sondern es darüber hinaus auch möglich ist, dass Windows diese Freigaben wiederum für Windows-Arbeitsplatzrechner im Netzwerk freigibt.

Nachdem die Software installiert ist, was übrigens eine leichte Übung ist, rufen Sie in AccessNFS Gateway das Programm Disk Administrator auf, indem Sie nacheinander auf **Start/Programme/AccessNFS Gateway/Disk Administrator** klicken. Wenn Sie einen NFS-Datenträger auslagern möchten, geben Sie im Dialogfeld **Share Name** den Freigabenamen ein und legen dann den Buchstaben des Laufwerks fest, dem der NFS-Datenträger zugeordnet werden soll. Geben Sie entweder durch Suchen im Dialogfeld **Network Resources** oder durch die Eingabe des Namens in das Feld **Network Resource** an, auf welchen NFS-Datenträger zugegriffen werden soll. Wenn Sie alles ausgefüllt haben, klicken Sie auf die Schaltfläche **Connect**. Daraufhin müssen Sie einen Benutzernamen und ein Kennwort eingeben. Wenn Sie keinen Benutzernamen und kein Kennwort eingeben, wird die Verbindung trotzdem aufgebaut und Sie sind als anonymer Benutzer angemeldet, vorausgesetzt, der NFS-Datenträger lässt anonyme Verbindungen zu.

Wenn die Option **Share Name** ausgefüllt wurde, wird nun der NFS-Datenträger ausgelagert und steht Windows-Benutzern zur Verfügung.

18.6 Über Samba

NFS eignet sich hervorragend, wenn Sie einen Windows 2000-Computer haben, der auf UNIX zugreifen muss. Was ist aber, wenn Sie einen UNIX-Computer haben, der auf Windows 2000 zugreifen muss? Wie wäre es, wenn Sie einen UNIX-Rechner Daten mit bereits im Netzwerk befindlichen Windows-Computern transparent gemeinsam nutzen lassen?

Um dieses Problem zu lösen, wurde das Open-Source-Projekt Samba (www.samba.org) gestartet. Samba ermöglicht vielen UNIX-Hosts die Imitation von Windows, sodass Clients praktisch keinen Unterschied mehr erkennen können. Dateiberechtigungen und Sicherheitsmechanismen sind integriert und die neuesten Versionen können an der Domänenauthentifizierung teilnehmen.



Samba wurde nach dem SMB-Protokoll (Server Message Block) benannt, das von Windows-Systemen für die Freigabe von Dateien verwendet wird. SMB heißt jetzt aber *CIFS* (Common Internet File System), sodass der Name Samba keinen Sinn mehr ergibt. Aber viele halten ihn trotzdem für einen coolen Namen.

Und wie leistungsfähig ist Samba? Die, die sich nicht auskennen, werden wohl denken, weil Samba ein Open-Source-Projekt und kostenlos ist, funktioniert es nicht richtig. Es ist jedoch so, dass es so schnell ist wie Windows NT 4.0 auf vergleichbarer Hardware. Und es kommt noch besser: Da UNIX auf größerer Hardware als NT läuft, können Sie sich vorstellen, dass Samba Dateien schneller als jeder Windows-Rechner zur Verfügung stellen kann. Dieser Benchmark wurde natürlich auf einem SGI Oxygen-Server mit RAM-Speicher, Netzwerkverbindungen und Prozessoren durchgeführt, wie sie bei kaum einem Windows 2000-Server vorzufinden sind. Dieses Produkt ist schnell, effizient und funktioniert hervorragend.

Samba wird als zwei Dämons bzw. Dienstprogramme auf UNIX-Rechnern ausgeführt. Der erste Dämon, *nmbd*, ist für das Browsen und die Arten von Aktivitäten zuständig, die früher von WINS unterstützt wurden. Der zweite Dämon, *smbd*, ist der eigentliche Prozess, der für die Dateifreigabe und die Sicherheitsdienste verantwortlich ist.

Das Samba-Projekt ist raschen Änderungen unterworfen, um mit den Änderungen von Windows 2000 und CIFS mithalten zu können. Microsoft hat kein Interesse am Erfolg des Samba-Projekts, sodass mit dem Samba-Projektteam praktisch keine Informationen ausgetauscht werden. Das führt dazu, dass sich die Software ebenso wie die unterschiedlichen Konfigurationsdateien häufig ändern. Um Samba verwenden und installieren zu können, müssen Sie sich eine Kopie von Samba unter <http://www.samba.org> herunterladen. Lesen Sie dann die mitgelieferte Dokumentation, insbesondere die Datei *Samba-HOWTO*. Hier finden Sie die neuesten Installations- und Konfigurationsanweisungen sowie die Adressen von Newsgroups und Mailing-Listen enthalten.

18.7 Drucken in einer UNIX-Umgebung

Es gibt mehrere Möglichkeiten, UNIX und Windows 2000 in eine völlige Netzwerk-Drucker-Lösung zu integrieren. Das im vorhergehenden Abschnitt beschriebene Produkt Samba enthält alle notwendigen Schnittstellen, um an UNIX-Arbeitsplatzrechnern angeschlossene Drucker freizugeben, sodass sämtliche

Windows-Clients auf diese Drucker zugreifen können. Samba kann auch verwendet werden, um von UNIX Druckaufträge an Windows zu senden.

Das herkömmliche UNIX-Drucksystem heißt »lp« für Line Printer (Zeilendrucker). Das ist ein archaischer Name, denn heute verwendet kein Mensch mehr Zeilendrucker. Die Software ist jedoch flexibel genug, um mit jedem vorstellbaren Drucker, angefangen beim alten Matrixdrucker über schreibischgroße elektrostatische Plotter bis hin zu spezialisierter Rendering-Software, klarzukommen. Das Drucksystem lp funktioniert so, dass Anforderungen je nach UNIX-Version auf den Datenträger im Verzeichnis `/var/spool/lpd` gespooled werden. Die gespooled Datei kann dann an eine Rendering-Software geleitet werden. Anschließend wird eine Verbindung zum Drucker hergestellt, der die Datei ausdruckt. Die Rendering-Software kann sehr einfach sein und z.B. PostScript-Kopf- und -Fußzeilen an Textdateien anhängen, sodass diese von einem PostScript-Drucker ausgedruckt werden können. Die Rendering-Software kann jedoch auch recht komplex sein, wie die, die in elektrostatischen Plottern verwendet wird.

Um einen Windows 2000-Server an einen UNIX-Rechner anzuschließen, müssen Sie zunächst dafür sorgen, dass der am betreffenden UNIX-Rechner angemeldete Benutzer richtig drucken kann. Wenn ein lokaler Benutzer nicht drucken kann, kann ein Netzwerkbenutzer ebenfalls nicht drucken. Beheben Sie zuerst die lokalen Probleme und konfigurieren Sie dann den Windows 2000-Server. Wenn der Drucker richtig funktioniert, klicken Sie in der Systemsteuerung auf **Drucker** und dann auf **Neuer Drucker**. Lesen Sie die Anweisungen und klicken Sie dann auf die Schaltfläche **Weiter**. Ob Sie es nun glauben oder nicht, Sie müssen hier den lokalen Drucker wählen, obwohl sich der Drucker in einem Netzwerk befindet. Deaktivieren Sie die Option **Automatische Druckererkennung und Installation von Plug & Play-Druckern** und klicken Sie dann auf die Schaltfläche **Weiter**.

Als Nächstes erscheint das Fenster für die Auswahl des Druckeranschlusses, womit der Netzwerkteil des Drucksystems konfiguriert wird. Wählen Sie die Option **Einen neuen Anschluss erstellen**. Klicken Sie dann im Dropdown-Listenfeld **Typ** auf **LPR-Anschluss**. Geben Sie den Namen des Servers und den Namen des Druckers ein und klicken Sie auf **OK**. Der Rest der Konfiguration ist wie bei der Konfiguration eines normalen Druckers. Wie Sie dabei vorgehen, können Sie in Kapitel 6 nachlesen.

18.8 Die Zukunft: Microsoft und UNIX

Die Geschichte von Microsoft und der Unterstützung von UNIX besteht aus zwei verschiedenen Perioden. Microsoft versuchte von seiner Geburtsstunde an bis dahin, wo das Unternehmen erkennen musste, dass Netscape im World Wide Web absahnte, einfach so zu tun, als gebe es UNIX nicht. Wenn Sie das nicht glauben, dann sehen Sie sich doch einfach einmal die zu dieser Zeit erhältlichen Integrationsprodukte wie das Microsoft-Programm Mail SMTP Gateway an, das mit DNS nichts anzufangen wusste. Oder nehmen Sie das Windows NT Advanced Server 3.1-System, das eine der Umgebungen mit der schlechtesten Leistung und den miesesten Funktionen überhaupt enthielt. Als Microsoft erkannte, dass man mit dem Internet richtig Geld verdienen konnte, und dass praktisch das gesamte Internet von UNIX dominiert wurde, verbesserte sich der Umgang von Microsoft mit UNIX deutlich. Exchange Server, der Ersatz für Microsoft Mail, verfügt über die ausgezeichnete SMTP-Komponente Internet Mail Connector. Microsoft verfügt über einen TCP/IP-Stapel, der gut funktioniert, obwohl er ständig von Dienstverweigerungsattacken heimgesucht wird. Microsoft kann inzwischen Fortschritte bei dynamischem DNS, Verzeichnisdiensten und anderen Diensten vorzeigen,

die hilfreiche Zusätze für das Internet darstellen. Nahezu jede Internet-Integrationsfunktion ist eine UNIX-Integrationsfunktion, da UNIX stark mit dem Internet verbunden ist. In dieser Beziehung hat sich Microsoft eng an UNIX angeschlossen und es gibt hier kein Zurück mehr.

© Copyright [Markt+Technik Verlag](#), ein Imprint der Pearson Education Deutschland GmbH
Elektronische Fassung des Titels: Windows 2000 Server Kompendium, ISBN: 3-8272-5611-9 Kapitel:
Verbindung zwischen UNIX und Windows 2000 Server

Kommunikation übers Internet

Teil V

19. Internet Information Server (IIS)

20. Virtuelle private Netzwerke

© Copyright [Markt+Technik Verlag](#), ein Imprint der Pearson Education Deutschland GmbH
Elektronische Fassung des Titels: Windows 2000 Server Kompendium, ISBN: 3-8272-5611-9 Kapitel:
V

Kapitel 19 Internet Information Server (IIS)

Der Auftritt von Microsoft in der Welt der Internet-Server erfolgte in Form der IIS-Technologie. Microsoft vereinte mit diesen Diensten mehrere Technologien, darunter einen Webserver, einen FTP-Server sowie einen Newsgroup-Server. IIS ist nun voll in das Betriebssystem Windows 2000 Server integriert, was eine Veränderung gegenüber den früheren Internet-Informationsdiensten darstellt. Im ersten Abschnitt erfahren Sie einiges über die Geschichte der Internet-Informationsdienste und erhalten eine Einführung in die unterschiedlichen Technologien, aus denen die IIS-Dienste zusammengesetzt sind.

19.1 Internet-Informationsdienste

Die unter der Bezeichnung Internet Information Server (IIS) bekannte Technologie ist eine relativ neue in der Welt von Windows NT bzw. Windows 2000. IIS gibt es seit dem Erscheinen von Windows NT 3.51 als einen HTTP-Webserver- (Hypertext Transfer Protocol) und FTP-Serverdienst (File Transfer Protocol) mit einem sehr eingeschränkten Bereich. Vor der Version 3.51 von Windows NT bot Microsoft mit seinen Betriebssystemen kaum Unterstützung für das Internet.

Die Version 2.0 von IIS kam im Juli 1996 mit Windows NT Server 4.0 auf den Markt. ASP (Active Server Pages), das heute die meisten als den Kern von IIS ansehen, gab es bei den ersten beiden Versionen von IIS noch gar nicht. Microsoft führte das Konzept von ASP erst mit der Version 3.0 von IIS ein. Dies war zusammen mit einem Update des Internet Explorer und mehreren Multimediaprogrammen Teil des dritten Service Pack von Windows NT Server 4.0. Nur kurze Zeit später machte Microsoft laut Bill Gates Ernst damit, das Internetunternehmen der Zukunft zu werden und brachte die Version 4.0 von IIS auf den Markt. IIS 4.0 wurde der Öffentlichkeit in Form des Windows NT Option Pack angeboten. Das war, auf eine nette Art und Weise gesagt, ein kostenfreies Add-On für das Betriebssystem Windows NT 4.0. IIS 4.0 blieb bei den nächsten drei Versionen des Windows NT 4.0 Service Packs (4, 5 und 6) im Wesentlichen unverändert.

Mit Windows 2000 kommt nun eine neue Version von IIS, nämlich IIS 5.0, auf den Markt. Dabei handelt es sich um eine aus Gründen der Sicherheit und Skalierbarkeit vollständig in das Betriebssystem integrierte Version von IIS. Diese Version enthält eine ganze Reihe von neuen Funktionen, darunter folgende:

- Verbesserung von ASP (Active Server Pages).
- Verwaltungstechnische Änderungen wie z.B. die vollständige Unterstützung der MMC-Technologie (Microsoft Management Console), verbesserte Remoteverwaltung sowie eine bessere Fehlerverfolgung und -protokollierung.
- Zahlreiche Änderungen in der Registrierung.
- Sicherheit; vollständige Integration der Kerberos-basierten Verschlüsselung.
- Leistung; ein überarbeiteter Ansatz des Socket-Pooling.
- Deutlich verbesserte Dokumentation, darunter ein HTML-basiertes Hilfeprogramm, mit dessen

Hilfe nach sämtlichen Dokumenten gesucht werden kann, sowie ein verbessertes Stichwortverzeichnis.

Die Windows 2000-Version von IIS lediglich als ein Update der älteren Versionen zu bezeichnen, wäre nicht gerecht. IIS 5.0 bietet so viele neue Funktionen sowie zahlreiche Verbesserungen bekannter Funktionen, dass es zu einem ausgezeichneten Internet-Diensteserver geworden ist.

19.2 Bevor Sie mit IIS beginnen

Bevor Sie Ihre neue Karriere als Internet-Dienstanbieter oder virtueller Webmaster beginnen, sollten Sie in Bezug auf IIS einige Dinge bedenken:

- Zunächst einmal müssen Sie entsprechend der Hardwarekompatibilitätsliste von Microsoft für Windows 2000 Server die geeignete Hardware erwerben und konfigurieren.
- Danach sollten Sie dafür sorgen, dass eine geeignete Netzwerkverbindung vorhanden ist, wenn Sie einen LAN- bzw. WAN-basierten Intranet-Server einrichten möchten. Wenn Sie beabsichtigen, diesen IIS-Server als einen Haltepunkt im Internet zu verwenden, benötigen Sie die entsprechende Anbindung an das Internet.
- Darüber hinaus sollten Sie über eine geeignete Hardware, Software und Benutzerprozeduren für Datensicherungen sowie einen Sicherheitsplan verfügen, um Ihren IIS-Server zu schützen, nachdem Sie ihn im Intranet Ihrer Organisation in Betrieb genommen haben oder im Zusammenhang mit dem Internet verwenden.

19.2.1 Systemanforderungen

IIS 5.0 funktioniert nur bei den Betriebssystemen der Reihe Windows 2000:

- Professional
- Server
- Advanced Server
- DataCenter Server

Die Windows 2000 Professional-Version von IIS ist im Vergleich zu den drei Server-Versionen eine insbesondere im Bereich der Unterstützung einiger Transaktions- und Sicherheitsereignisse etwas abgespeckte Version. Da es sich bei diesem Buch um ein Windows 2000 Server-Buch handelt, geht es hier jedoch um die Installation, Konfiguration und um die Verwendung von IIS bei Windows 2000 Server.

In Bezug auf die Hardware wäre es ratsam, wenn Sie eine etwas bessere Ausrüstung als eine, die den von Microsoft empfohlenen Anforderungen entspricht, hätten. Microsoft empfiehlt folgende Systemanforderungen:

- CPU: Pentium ab 166 MHz
- Speicher: 64 Mbyte RAM
- Verfügbarer Festplattenspeicher: 2 Gbyte
- Laufwerk: CD-ROM-Laufwerk, 12fach

- Bildschirm: 16 Farben, SVGA mit einer Auflösung von mindestens 800 x 600
- Zeigegerät: vorzugsweise Maus (von Microsoft natürlich)

Ein IIS-Server beansprucht die CPU und die Speicherressourcen des Systems etwas mehr als das eigentliche Betriebssystem. Das ist nicht ungewöhnlich oder schlecht, denn alle Anwendungsprogramme, die Sie auf Windows 2000 Server installieren, beanspruchen zumindest etwas mehr als die von Microsoft für eine Windows 2000 Server-Umgebung empfohlenen physikalischen Ressourcen.

Wenn Ihr Server als Webserver eingesetzt werden soll, sollten Sie dafür sorgen, dass Ihre Netzwerkfunktionen DNS (Domain Name Service) bzw. DDNS (Dynamic Domain Name Service) einsatzbereit sind. Die Verwendung von DNS bzw. DDNS ist für einen Webserver nicht unbedingt erforderlich. Für Ihre Benutzergemeinde ist es jedoch in der Regel wesentlich einfacher, sich für die Suche des Webservers im Intranet oder im Internet statt einer TCP/IP-Adresse einen Computernamen zu merken.



DNS ist ein Internet- und TCP/IP-Standarddienst für die Auflösung von Namen, mit dessen Hilfe Client-Computer Namen von Computern registrieren und auflösen können. Die Windows 2000-Implementierung von DNS unterscheidet sich von der Implementierung der Vergangenheit dadurch, dass DNS nun Computernamen und IP-Adressen dynamisch aktualisiert, speichert und aufruft. Diese neue Version wird als *DDNS (Dynamic Domain Name System)* bezeichnet.

Ebenso wäre es sehr hilfreich, wenn Sie bereits ein Programm zum Erstellen von Websites hätten. Wie gesagt, dabei handelt es sich nicht um eine obligatorische Anforderung, denn jeder kann im Notepad von Windows 2000 Server HTML-Code schreiben. Mit einem richtigen Programm zum Erstellen von Websites wird das Ganze allerdings sowohl für den Webmaster (der IIS-Administrator, der für den Web-Teil des Servers verantwortlich ist) als auch für die Endbenutzer (denen Grafiken und auffallende Elemente auf Websites so gut gefallen, die jedoch mit einfachem HTML sehr schwierig zu erstellen sind) deutlich einfacher.

Windows 2000 Server ist die einzig erforderliche Software, denn IIS ist in Windows 2000 integriert. Wenn Sie Windows 2000 Server installieren, wird IIS automatisch installiert, außer Sie verhindern die Installation dieses Dienstes absichtlich. Auch bei der Aktualisierung des Systems wird IIS automatisch installiert, vorausgesetzt, dass mit der vorhergehenden Version des Betriebssystems bereits eine Version von IIS installiert war.

19.2.2 Anbindung an das Internet

IIS kommt problemlos ohne eine Anbindung an das Internet aus, besonders dann, wenn der IIS-Server als ein Web- oder FTP-Server für ein Intranet eines Unternehmens verwendet wird. Ein IIS-Server kann ein sehr netter Intranet-Server für Ihre Organisation sein, den Sie zu relativ günstigen Kosten für Ihre Organisation installieren, konfigurieren und betreiben können. Wenn Ihre Organisation jedoch wie die meisten Organisationen ist, dann haben Sie sich auf das IIS-Abenteuer eingelassen, weil Sie einen Internet-basierten Webserver haben möchten.

Eines der wichtigsten Dinge für eine Anbindung an das Internet ist entweder eine Netzwerkkarte oder ein Modem. Wenn Sie davon ausgehen, dass mehr als ein bis zwei Personen Ihre Website gleichzeitig benutzen, sollten Sie sich überlegen, ob Sie statt einer wesentlich langsameren Wählverbindung über ein

Modem nicht eine Netzwerkkarte verwenden möchten, die über eine Hochgeschwindigkeitsleitung mit dem Internet verbunden werden kann. Ihre Anbindung an das Internet kann beispielsweise so ähnlich aussehen wie die in Abbildung 19.1 dargestellten Verbindungen.

Verbindung an IIS-Server:

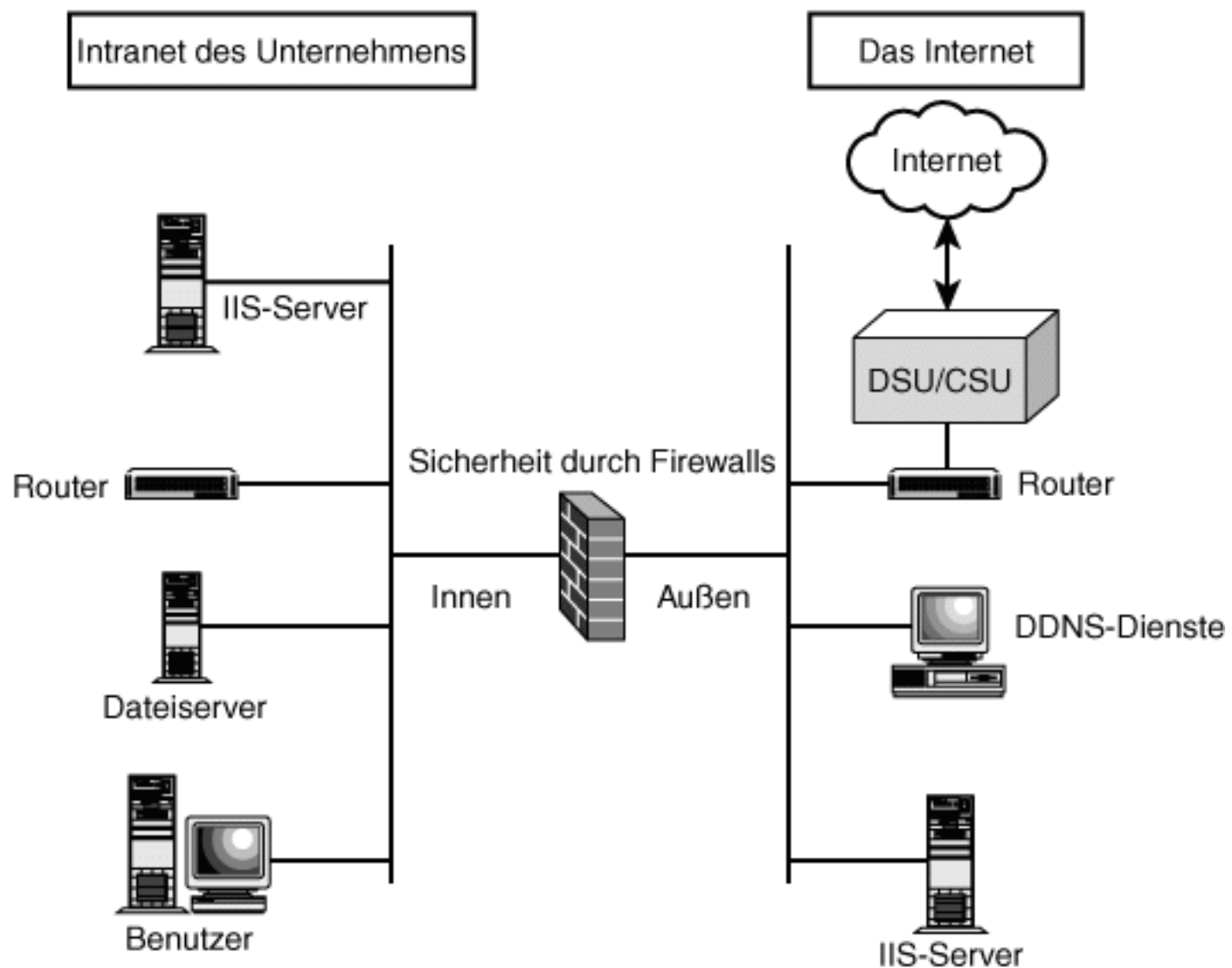


Abbildung 19.1: Einfache IIS-Verbindung

Kurz einige Dinge, die Sie wissen sollten. Die Verwendung einer Firewall ist zwar allgemein üblich, für die Anbindung an das Internet jedoch nicht erforderlich. Wenn Sie sich Abbildung 19.1 ansehen, werden Sie feststellen, dass es keine Firewall zwischen dem IIS-Server und der Internet-Verbindung rechts im Bild gibt.

DSU/CSU ist ein digitales Modem für den Anschluss LAN-basierter Server an ein WAN oder direkt an das Internet, weshalb es in dieser Abbildung dargestellt wird. Ein Router kann niemals ohne jegliche Hardware für die Telekommunikation direkt an das Internet angebunden werden.

In Abbildung 19.1 ist der IIS-Server, der den Intranetsites der Organisation dient, links und die Anbindung an das Internet rechts dargestellt. Wie Sie erkennen können, befinden sich sämtliche

Benutzer links (also »innerhalb«) der Firewall. Der IIS-Server, der für die Web- und FTP-Sites der Organisation verantwortlich ist, befindet sich dagegen rechts (also »außerhalb«) der Firewall. Gehen Sie nicht davon aus, dass der IIS-Server ungeschützt wie ein Opferlamm ist, nur weil er in der Abbildung außerhalb der Firewall dargestellt ist. Das ist er definitiv nicht. Es sind Sicherheitsmechanismen im Router zwischen dem IIS-Rechner und dem Internet sowie im IIS-Server selbst integriert. Darüber hinaus wurden hier, um das Buch nicht noch umfangreicher zu machen, einige ausführlichere Sicherheitstechniken nicht erwähnt, die von jedem Unternehmen normalerweise angewendet werden, um die IIS-Server und Informationen vor unbefugtem Zugriff zu schützen. Dazu gehört beispielsweise auch eine Hardware- bzw. Software-basierte Firewall zwischen dem IIS-Server und dem Internet. Wenn Sie mehr über den geeigneten Schutz Ihrer IIS-Server wissen möchten, sollten Sie eine der folgenden Websites von Microsoft aufsuchen:

<http://www.microsoft.com/security>

<http://www.microsoft.com/technet/win2000>

Alternativ können Sie auch zur Website von Network Computing surfen, die Sie unter folgender Adresse finden:

<http://www.networkcomputing.com/core/core8.html>

Wenn Sie in der Lage sind, eine physikalische Verbindung zum Internet herzustellen, benötigen Sie immer noch entweder einen Internet-Dienstanbieter oder Sie müssen Ihre eigene Direktverbindung zum Internet einrichten (d.h. die Dienste von Ihrer lokalen Telefongesellschaft in Anspruch nehmen). Danach können Sie Ihren IIS-Server an das Internet anbinden.

Der letzte Schritt beim Einrichten eines Webservers (d.h. nicht des IIS-Teils) besteht darin, sich einen Domännennamen zu sichern, der im Zusammenhang mit Ihrer Website verwendet werden kann. Dazu müssen Sie sich an Network Solutions (<http://www.networksolutions.com/>) wenden, wo Ihnen nicht nur bei der Suche nach einem noch nicht verwendeten Namen geholfen wird, sondern wo Sie auch die Rechte für den von Ihnen gewählten Namen erwerben können. (Beachten Sie, dass dieser Domänenname der Identifizierung Ihres Web- bzw. FTP-Servers im Internet dient. Verwechseln Sie das nicht mit den Windows 2000 Server-Domännennamen, die Sie wahrscheinlich irgendwo in Ihren Computerumgebungen haben.) Solch ein Domänenname kostet für die ersten beiden Jahre \$70. Alle weiteren Jahre gibt es dann zu einem günstigeren Preis. Damit Sie einen Namen finden, der nicht schon von jemand anderem verwendet wird, sollten Sie die Website »Whois« von Network Solutions aufrufen. Diese Seite finden Sie unter folgender Adresse:

<http://www.networksolutions.com/cgi-bin/whois/whois>

Wenn Sie die Hardware- und Software-Anforderungen für IIS erfüllen, Ihre Anbindung an das Internet

entwickelt und zumindest einen Domännennamen für das Internet für sich reserviert haben, dann können Sie damit beginnen, IIS auf Ihrem Windows 2000-Server zu installieren (falls erforderlich) und zu konfigurieren.

19.3 Installieren von IIS

Wie bereits erwähnt, wird IIS bei der Installation von Windows 2000 Server auf Ihrem Computer automatisch installiert, wenn es sich um eine Neuinstallation des Betriebssystems handelt. Wenn Sie eine bereits vorhandene Version von Windows NT oder Windows 9x aktualisieren und eine Version von IIS bereits vorhanden oder der PWS (Personal Web Server) von Windows 9x bzw. Windows NT Workstation bereits installiert ist, aktualisiert Windows die ältere Version von IIS automatisch auf IIS 5.0.

Wenn Sie eine bereits installierte Version von Windows NT oder Windows 9x aktualisieren, und IIS noch nie installiert gewesen ist, dann rufen Sie den Assistenten für Windows-Komponenten wie folgt auf:

1. Klicken Sie auf die Schaltfläche **Start**. Wählen Sie die Option **Einstellungen** und klicken Sie dann auf **Systemsteuerung**. Daraufhin erscheint die Systemsteuerung von Windows 2000.
2. Doppelklicken Sie auf das Symbol **Software**. Daraufhin erscheint das Fenster **Software**.
3. Klicken Sie links unten in diesem Fenster auf die Schaltfläche **Windows-Komponenten hinzufügen/entfernen**. Daraufhin erscheint der in Abbildung 19.2 dargestellte **Assistent für Windows-Komponenten**.
4. Wählen Sie im Fenster des Assistenten für Windows-Komponenten die Option **Internet-Informationdienste (IIS)**. Von den vielen Elementen, die in diesem Fenster angezeigt werden, erfordern nur einige Ihre sofortige Aufmerksamkeit:
 - **Zertifikatsdienste** - Mit Hilfe des über diese Option zur Verfügung gestellten Zertifikationsservers können Sie einfache digitale Signatur- und Verschlüsselungszertifikate erstellen, um diese mit Ihrer Website zu verwenden. So müssen Sie diese Dienste nicht von einem Drittanbieter wie z.B. Thawte oder VeriSign erwerben.
 - **Indexdienst** - Der Indexdienst bietet nicht nur Indexfunktionen für Ihren gesamten Computer, sondern auch für all Ihre Web- und FTP-Sites. Aber keine Sorge. Diese Option lässt sich gut konfigurieren und stellt kein Sicherheitsrisiko für Ihre Arbeitsumgebung dar, wenn sie richtig konfiguriert ist.
 - **Internet-Informationdienste (IIS)** - Diese Option ist im Moment offensichtlich die wichtigste in diesem Dialogfeld. Sie besteht aus den Web-, FTP- und Newsgroup-Serverdiensten, die erforderlich sind, damit die anderen Internet-Dienste richtig funktionieren.

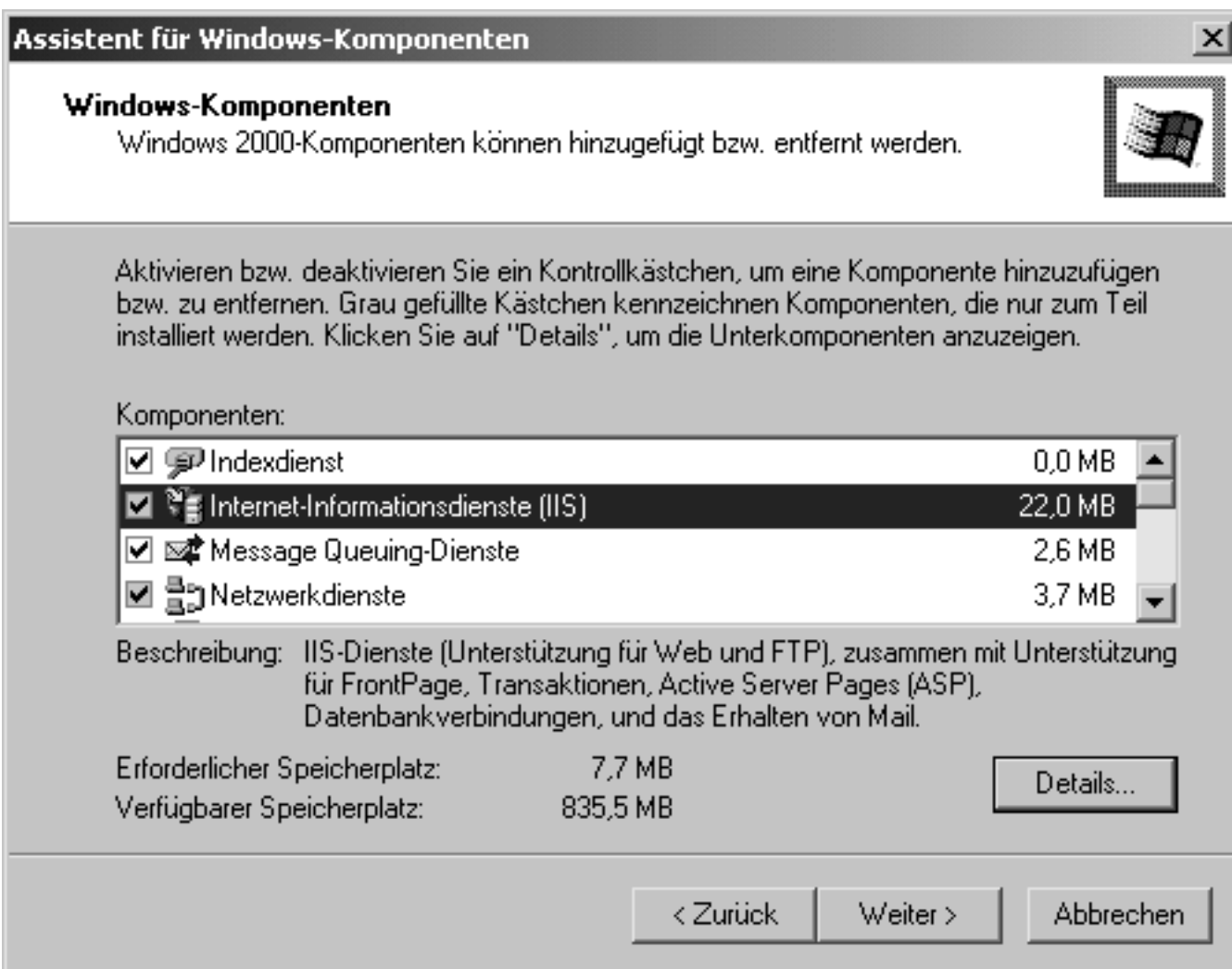


Abbildung 19.2: Hinzufügen neuer Windows-Komponenten

Um diese Dienste zu installieren, klicken Sie auf das Kästchen links neben der entsprechenden Option, sodass ein Häkchen in dem jeweiligen Kästchen erscheint. Wenn ein Kästchen mit einem Häkchen versehen, aber statt weiß grau hinterlegt ist, wurde diese Option nicht vollständig aktiviert, d.h. es wurden nicht alle Unteroptionen dieser Option aktiviert. Wenn Sie sich die einzelnen Unteroptionen der unterschiedlichen Dienste ansehen möchten, klicken Sie einfach auf die Schaltfläche **Details**. Daraufhin erscheint das in Abbildung 19.3 dargestellte Dialogfeld.

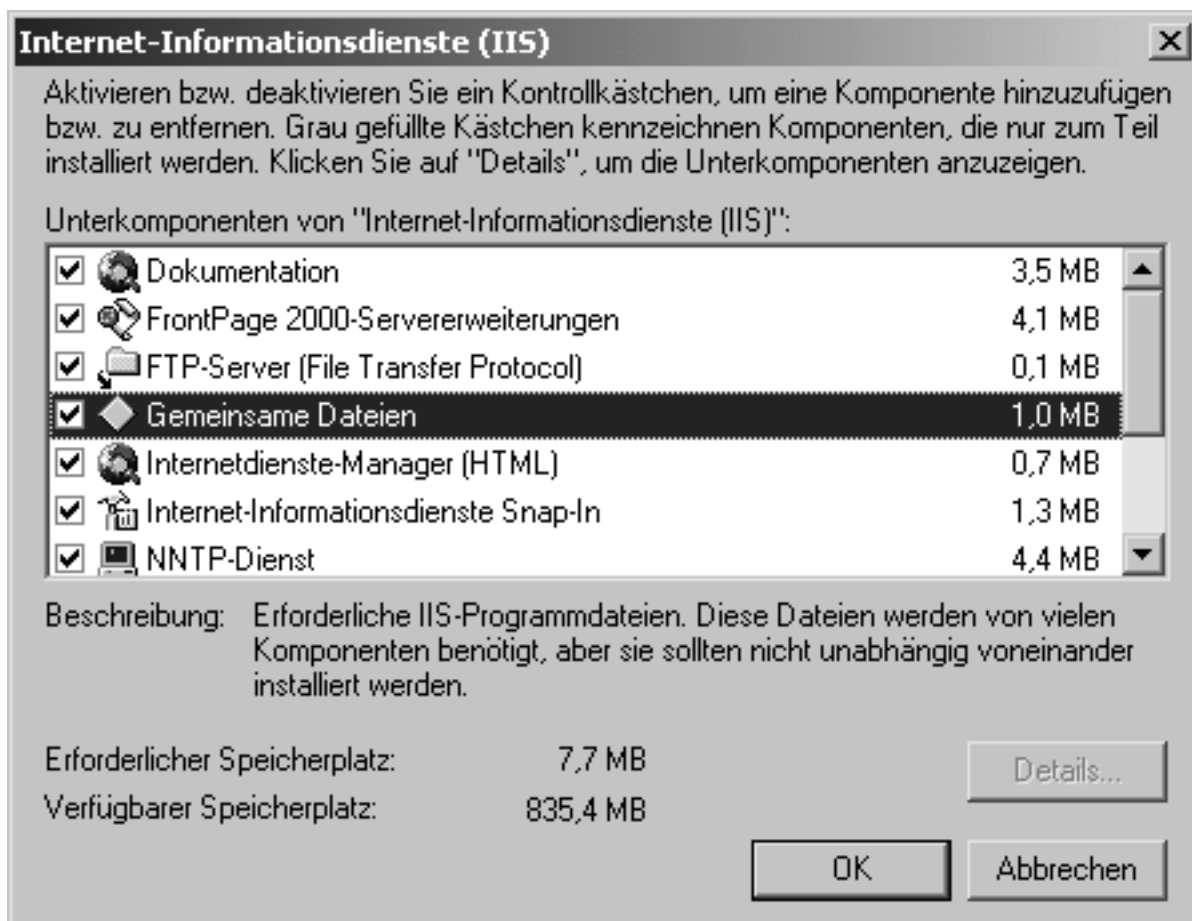


Abbildung 19.3: Hinzufügen einer IIS-Komponente

Das Dialogfeld **Internet-Informationsdienste (IIS)** enthält die folgenden Elemente:

- **Gemeinsame Dateien** - Dabei handelt es sich um die Dateien, aus denen das elementare IIS-System besteht.
- **Dokumentation** - Dabei handelt es sich um die allgemeinen IIS-, ASP-, Web- und FTP-Informationen.
- **FTP-Server (File Transfer Protocol)** - Dieser enthält die binären Dateien, die erforderlich sind, um die FTP-Serverdienste zu installieren.
- **FrontPage 2000-Servererweiterungen** - Dieses Element sorgt dafür, dass Microsoft FrontPage 2000 und Microsoft Visual InterDev 6.0 als Dokumentenerstellungs-, Entwicklungs- und Verwaltungsprogramme für Ihre Internet-Sites verwendet werden können.
- **Internet-Informationsdienste Snap-In** - Dabei handelt es sich um die Schnittstelle der Verwaltungskonsole für die umfassende Verwaltung von IIS.
- **Internetdienste-Manager (HTML)** - Dabei handelt es sich um die Web-basierte Version des Verwaltungsprogramms Internet-Informationsdienste Snap-In.
- **NNTP-Dienst** - Dieser Dienst unterstützt das NNTP-Protokoll (Network News Transfer Protocol), das für Newsgroups verwendet wird.
- **SMTP-Dienst** - Dieser Dienst unterstützt das SMTP-Protokoll (Simple Mail Transfer Protocol), das für E-Mails verwendet wird.
- **Unterstützung von InterDev RAD für Remote-Bereitstellung** - Mit dieser Option können Sie

auf Ihrem Internet-Server unterschiedliche Anwendungen remote bereit stellen. Sie sollten diese Option sparsam und nur auf Entwicklungsservern verwenden. Installieren oder aktivieren Sie dieses Element aufgrund der vielen damit verbundenen Sicherheitsrisiken niemals auf in Betrieb befindlichen IIS-Servern.

- **WWW-Server** - Das Herzstück des IIS-Servers. Wenn dieser Dienst installiert ist, kann er nicht mehr deaktiviert werden, da sonst das gesamte IIS-System abstürzt.

Nachdem Sie sämtliche von Ihnen gewünschten Optionen aktiviert haben, klicken Sie auf die Schaltfläche **OK**, um Ihre Einstellungen zu speichern und zum Dialogfeld **Assistent für Windows-Komponenten** zurückzukehren.

Den nächsten Bereich, den Sie sich etwas genauer ansehen sollten, ist die Option **Zertifikatsdienste**. Wenn Sie sich die kurze Liste der Unteroptionen ansehen möchten, klicken Sie auf die Schaltfläche **Details**. Daraufhin erscheint das in Abbildung 19.4 dargestellte Dialogfeld **Zertifikatsdienste**.

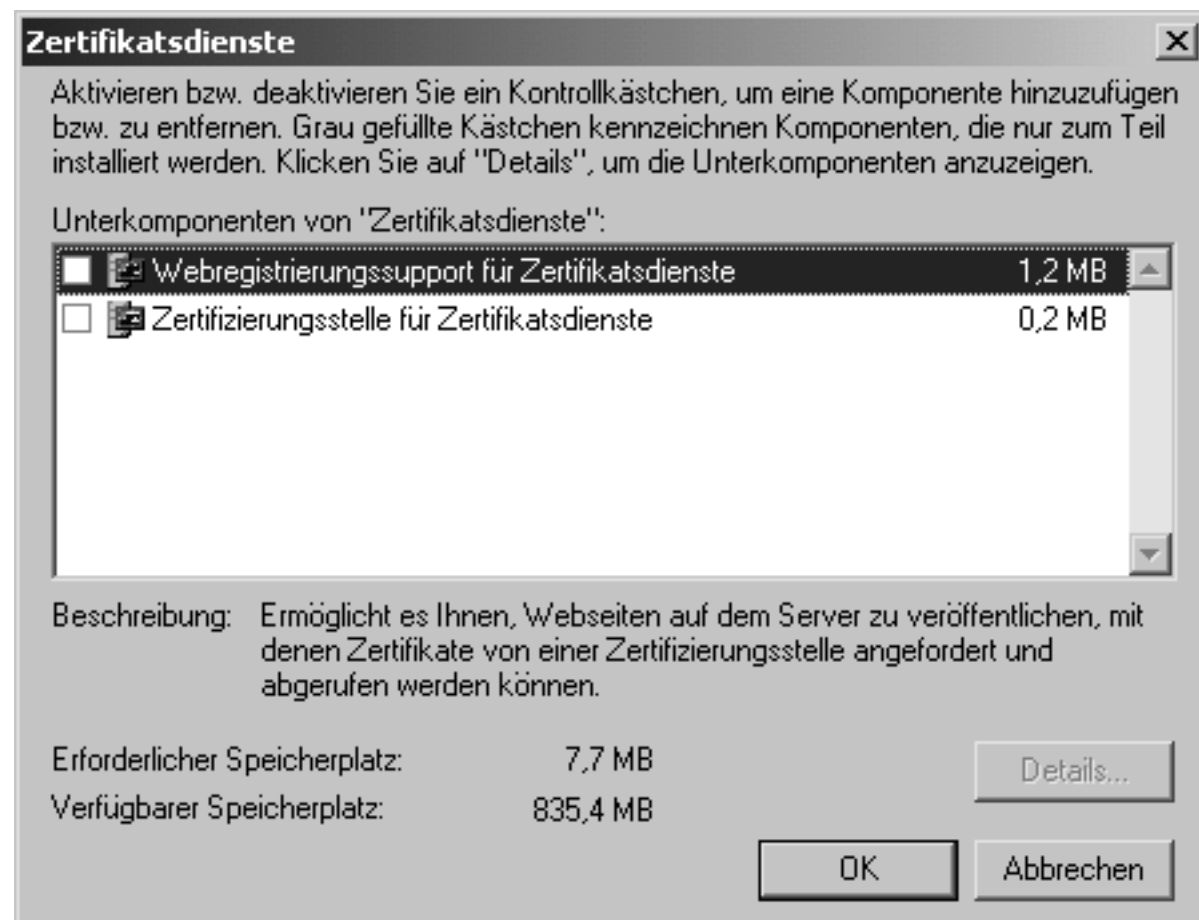


Abbildung 19.4: Hinzufügen von Unterkomponenten der Zertifikatsdienste

In diesem Dialogfeld gibt es zwei Optionen:

- **Zertifizierungsstelle für Zertifikatsdienste** - Dabei handelt es sich um die zentralen Dateien der Zertifizierungsstelle für die Zertifikatsdienste. Wenn Sie Ihre Website für den Einsatz mit SSL (Secure Socket Layer) konfigurieren oder auf Ihrer Site digitale Signaturen verwenden möchten, müssen Sie diese Technologien entweder kaufen oder die in Windows 2000 Server integrierte Zertifizierungsstelle verwenden. Diese wird über die Option **Zertifizierungsstelle für Zertifikatsdienste** installiert. Die meisten Organisationen verwenden diese Optionen für ihre

Intranet-Funktionen und fordern öffentliche Versionen für ihre Internet-Funktionen an.

- **Webregistrierungssupport für Zertifikatsdienste** - Mit diesem praktischen Tool können Sie Webseiten auf Ihrer Site veröffentlichen, von der jeder (mit den entsprechenden Berechtigungen) problemlos Kopien Ihrer Zertifikate für die Verwendung mit Anwendungen (um ausschließlich mit Ihrer Installation des Webservers zu arbeiten) herunterziehen kann.

Nachdem Sie die gewünschten Optionen aktiviert haben, indem Sie auf das Kästchen links neben den entsprechenden Optionen geklickt haben, klicken Sie auf die Schaltfläche **OK**, um Ihre Einstellungen zu speichern und zum Dialogfeld **Internet-Informationdienste (IIS)** zurückzukehren. Da Sie nun alle erforderlichen Einstellungen definiert haben, können Sie auf die Schaltfläche **OK** klicken, um den eigentlichen Installationsprozess zu starten (siehe Abbildung 19.5).

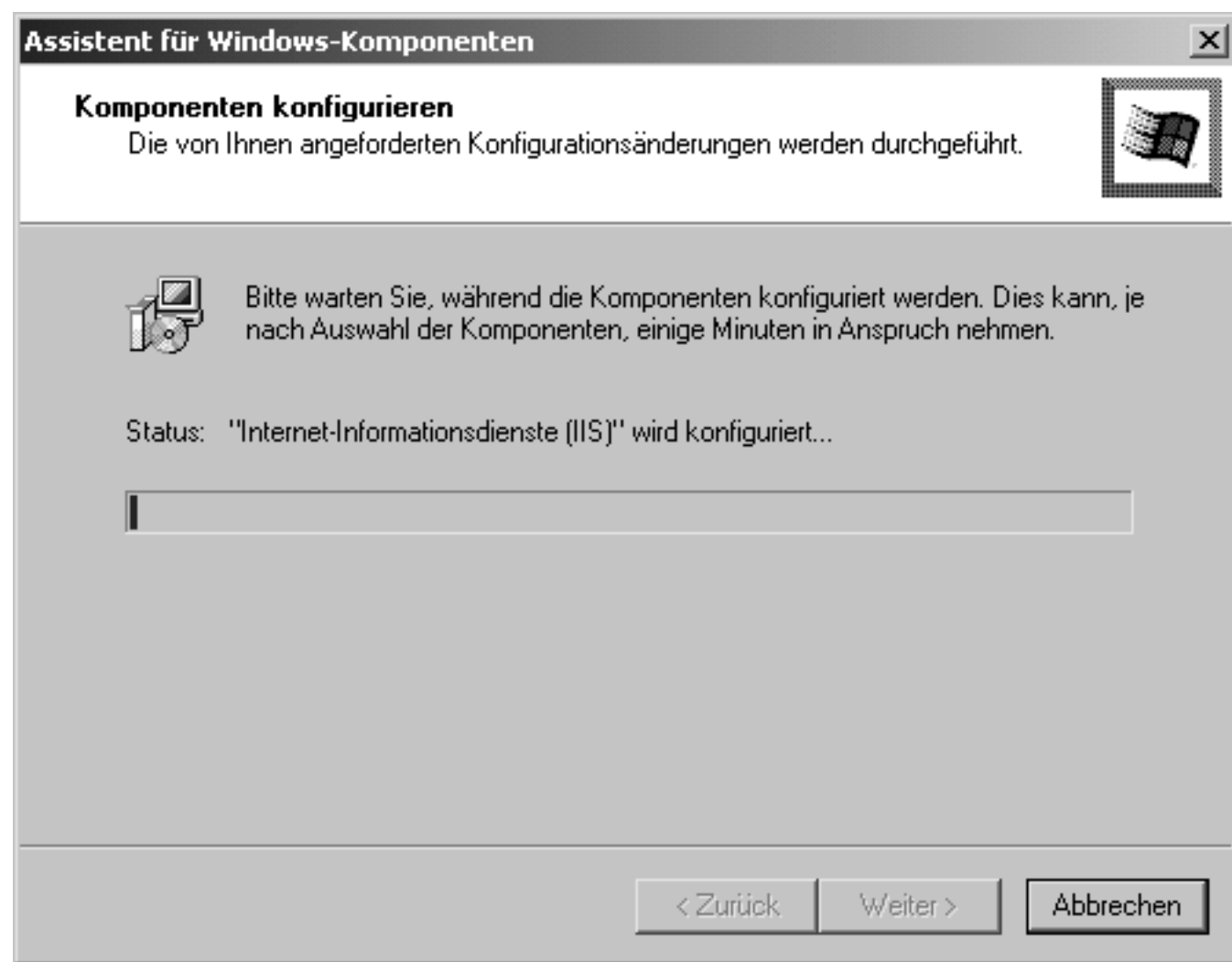


Abbildung 19.5: Statusleiste bei der Installation der Internet-Informationdienste

Dieser Vorgang kann von einer Minute bis hin zu 10 oder 15 Minuten dauern. Das hängt von vielen Faktoren wie z.B. von der Anzahl der gewählten Optionen, vom zur Verfügung stehenden Speicher, von der Geschwindigkeit und vom Standort Ihrer Festplatten ab. Haben Sie etwas Geduld, bis der Vorgang erfolgreich abgeschlossen ist (siehe Abbildung 19.6).



Abbildung 19.6: Fenster zum Fertigstellen des Assistenten nach einer erfolgreichen Installation

Klicken Sie auf die Schaltfläche **Fertig stellen**, um den Assistenten für Windows-Komponenten zu beenden und zum Fenster **Software** zurückzukehren. Je nachdem, welche Optionen Sie gewählt haben, kann es sein, dass Sie Ihren Computer neu starten müssen.

19.4 Verwalten und Konfigurieren von IIS

IIS ist einfach zu verwalten, kann jedoch schwierig zu verstehen sein. D.h., es gibt zwar grafische Benutzeroberflächen für die Verwaltung sämtlicher Aspekte der Web-, FTP-, SMTP- und NNTP-Sites. Aber die zahlreichen Möglichkeiten der Konfiguration und Variation machen es schwierig, die gesamte Verwaltung dieser Technologien vollständig zu überblicken. Bei einigen der komplexeren Funktionen werden Sie sogar durch Ausprobieren herausfinden müssen, welche die für die Internet- bzw. Intranet-Umgebungen Ihrer Organisation geeignete Konfiguration ist.

In diesem Abschnitt werden die Funktionen von IIS beschrieben, damit Sie einfacher herausfinden können, an welcher Stelle sich eine bestimmte Funktion am besten in das Gesamtschema der IIS-Architektur einfügt. Damit sollten Sie die von Ihrer Organisation benötigten IIS-Funktionen besser konfigurieren und verwalten können.

19.4.1 Allgemeine IIS-Einstellungen

Es gibt mehrere Möglichkeiten, eine IIS-Umgebung zu verwalten:

- Grundlegende Diensteseinstellungen - Eine Abhandlung über Elemente wie anonyme Benutzer und die unterschiedlichen Protokollierungsoptionen.
- Verzeichnisverwaltung - Hier werden die Verzeichnisstrukturen von IIS, darunter die von virtuellen Servern, erläutert.
- Erweiterte Verwaltung - Die hier besprochenen Themen sind für Fortgeschrittene gedacht. Hier geht es um Optionen und Funktionen für die Einstellung von Leistung und Bandbreite des IIS-Servers sowie um die Einschränkung des gleichzeitigen Zugriffs mehrerer Benutzer auf den IIS-Server.

Grundlegende Diensteseinstellungen

Innerhalb der Internet-Informationen Dienste gibt es viele grundlegende Einstellungen, von denen die meisten bereits im Hauptverwaltungsfenster zur Verfügung stehen. Um dieses Fenster zu öffnen, klicken Sie auf die Schaltfläche **Start**, dann auf **Programme, Verwaltung** und schließlich auf **Internetdienste-Manager**. Daraufhin erscheint das in Abbildung 19.7 dargestellte Fenster **Internet-Informationen Dienste**.

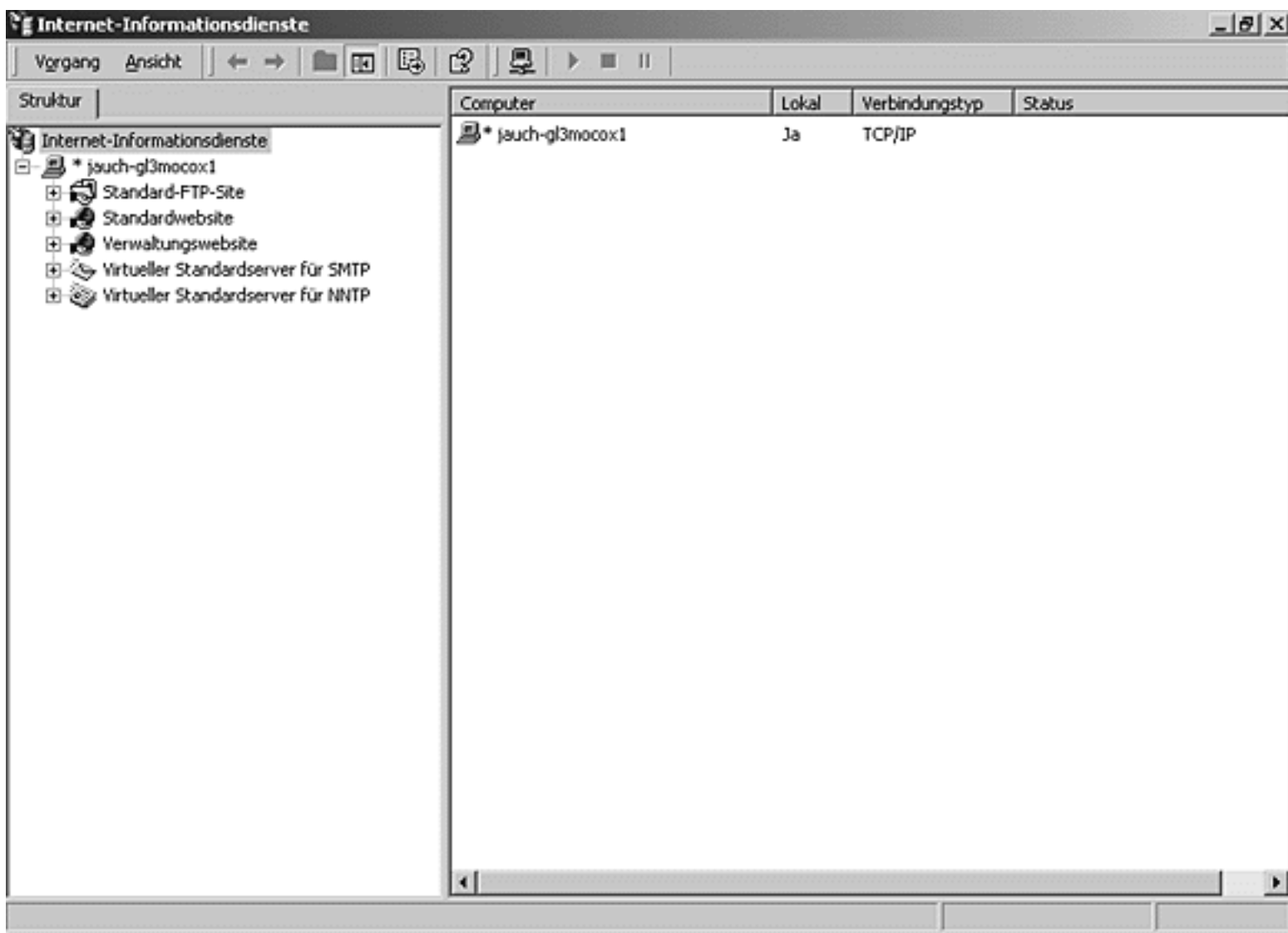


Abbildung 19.7: Das Fenster Internet-Informationsdienste

Dieses Fenster besteht aus drei Hauptbereichen: der Menüleiste, dem linken Fensterbereich und dem rechten Fensterbereich.

In der Menüleiste finden Sie die Dropdown-Menüs **Vorgang** und **Ansicht** sowie die Schaltflächen **Zurück**, **Vorwärts**, **Übergeordnetes Verzeichnis**, **Konsolenstruktur/Favoriten ein-/ausblenden**, **Liste exportieren**, **Zeigt die Hilfedatei an**, **Fügt einen Computer zur Liste hinzu**, **Startet das Element**, **Beendet das Element** und **Hält das Element an**. Über diese Menüleiste können Sie die elementaren Aktivitäten Ihrer FTP-, Web- und Ihrer virtuellen Server für SMTP bzw. NNTP verwalten. Wenn Sie auf **Ansicht** und **Anpassen** klicken, können Sie festlegen, welche Schaltflächen und Menüleisten in der Menüleiste aufgeführt werden.

Im linken Fensterbereich befindet sich mindestens eine Registerkarte, nämlich die Registerkarte **Struktur**, auf der die meisten der hier für uns interessanten Informationen enthalten sind. Über die entsprechenden Symbole können Sie folgende Elemente verwalten:

- **Internet-Informationsdienste** - Mit diesem Element können Sie eine Verbindung zu einem oder mehreren IIS-Servern in Ihrer Domäne oder in Ihrem globalen Katalog (ein Active Directory-Listenserver) herstellen.

- **Computername* - Dabei handelt es sich um den Computernamen des IIS-Servers, der die unterschiedlichen FTP-, SMTP-, NNTP- und Websites enthält. Es gibt immer einen oder mehrere Computernamen unterhalb des Symbols **Internet-Informationsdienste**.
- **FTP-Site(s)** - Dieser Bereich wird verwendet, um die Attribute der FTP-Site(s) zu definieren, die der Kontrolle des IIS-Servers unterliegen. Dazu gehören beispielsweise Sites, die sich auf demselben Computer wie das Betriebssystem Windows 2000 Server befinden, oder auch Sites, die sich auf anderen Computern innerhalb der Windows 2000-Domäne befinden.
- **Website(s)** - Dieser Bereich wird verwendet, um die Attribute der Website(s) zu definieren, die der Kontrolle des IIS-Servers unterliegen. Dazu gehören Sites, die sich auf demselben Computer wie das Betriebssystem Windows 2000 Server befinden sowie sämtliche, an anderer Stelle gespeicherten virtuellen Verzeichnisse.
- **Verwaltungswebsite** - Die Verwaltungswebsite können Sie sich als die Stelle für die Verwaltung der globalen Attribute für sämtliche von diesem IIS-Server kontrollierten Websites vorstellen. Hier können Sie u.a. auch mehrere IDs für diesen Webserver definieren.
- **Virtueller Standardserver für SMTP** - Dabei handelt es sich um das POP3-kompatible E-Mail-System, das von IIS unterstützt und über die hier verfügbaren Einstellungen konfiguriert wird.
- **Virtueller Standardserver für NNTP** - Dabei handelt es sich um das Informationssystem für Newsgroups, das von IIS unterstützt und über die hier verfügbaren Einstellungen konfiguriert wird.

Im rechten Fensterbereich des Dialogfelds werden all die im linken Fensterbereich definierten Einstellungen betreffenden Informationen angezeigt. Wenn Sie beispielsweise im linken Fensterbereich auf das Symbol Internet-Informationsdienste klicken, sehen Sie die diese Einstellung betreffenden Informationen im rechten Fensterbereich (siehe Abbildung 19.7). All die unterschiedlichen Symbole im linken Fensterbereich funktionieren so. Dadurch wird die Verwaltung eines IIS-Servers relativ einfach, wenn Sie erst einmal herausgefunden haben, was Sie möchten (das ist der schwierigere Teil).

Anpassen der Ansicht

Nehmen wir einmal an, hier werden Ihrer Meinung nach zu viele Informationen angezeigt. Dann können Sie die Ansicht dieses Fensters ändern, indem Sie auf das Menü **Ansicht** und dann auf die Option **Anpassen** klicken. Daraufhin erscheint das in Abbildung 19.8 dargestellte Fenster **Anpassen**.

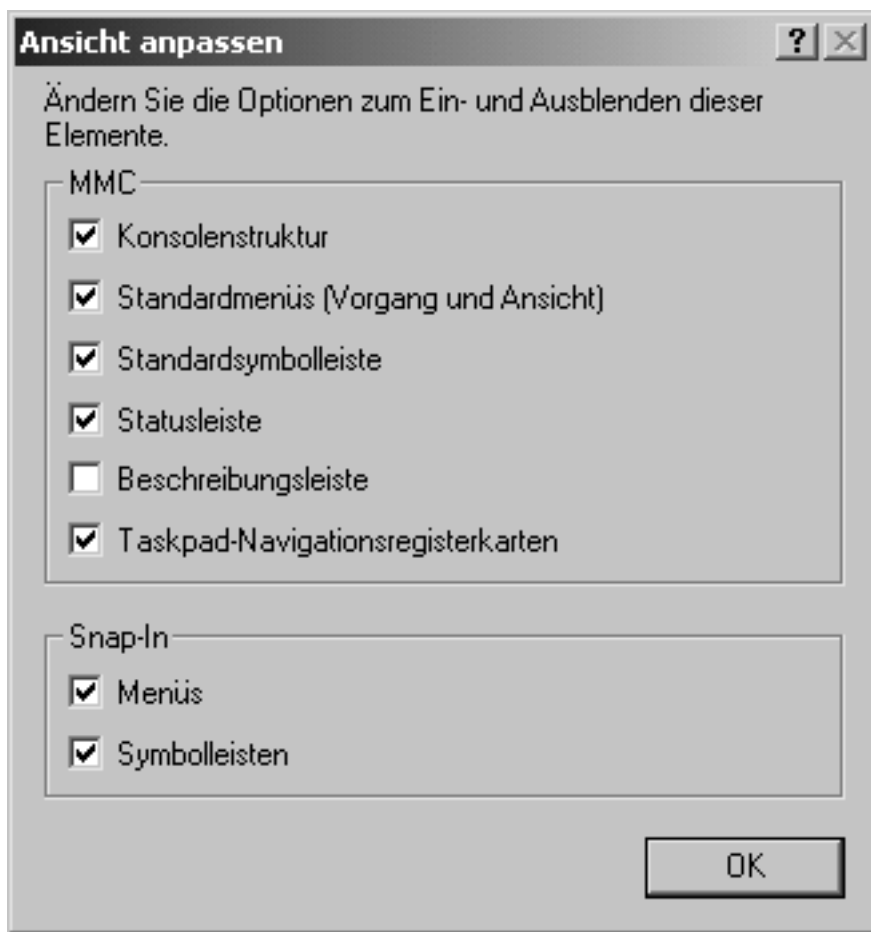


Abbildung 19.8: Anpassen der Ansicht

Indem Sie auf die Kontrollkästchen klicken, können Sie jede der hier beschriebenen Optionen ein- bzw. ausblenden.

⇒
INFO Es ist möglich, alle Menüleisten und Fensterbereiche auszublenden, die sämtliche Verwaltungsaufgaben beinhalten. Das bedeutet, dass Sie sich selbst aus Ihrer eigenen Verwaltungskonsolle ausschließen können. Das ist natürlich nicht besonders angenehm. Wenn das passiert ist, müssen Sie den Internetdienste-Manager verlassen und die Verwaltungskonsolle dieses Dienstes neu starten.

Klicken Sie im linken Fensterbereich auf das Symbol **Computername*, um das in Abbildung 19.9 dargestellte Fenster aufzurufen. (Es kann sein, dass auf Ihrem Windows 2000-Server einige andere Sites angezeigt werden. Aber das ist kein Grund zur Sorge.)

Der rechte Fensterbereich enthält eine Beschreibung jeder der in Ihrem IIS-Manager installierten Sites sowie den momentanen Zustand jeder dieser Sites. Dabei kann sich eine Site in einem der folgenden Zustände befinden:

- **Wird ausgeführt** - Dabei handelt es sich um den üblichen Status. Er bedeutet, dass Ihr Dienst auf diesem IIS-Rechner aktiv ist.
- **Beendet** - Dabei handelt es sich um einen weiteren üblichen Status, der besagt, dass dieser spezielle Dienst auf diesem speziellen IIS-Server nicht mehr ausgeführt wird.
- **Angehalten** - Dies ist der am wenigsten übliche Status, der besagt, dass der Dienst aus irgendeinem Grund vorübergehend angehalten worden ist (beispielsweise, weil Sie auf Ihrer

Verwaltungswebsite gerade Verwaltungsaufgaben durchführen).

Die restlichen Spalten im rechten Fensterbereich - **Hostheadername**, **IP-Adresse**, **Anschluss** und **Status** - dienen dazu, Konfigurationsinformationen eines bestimmten installierten IIS-Dienstes anzuzeigen. So ist es beispielsweise aus sicherheitstechnischen Gründen hilfreich zu wissen, dass jeder Computer mit einer TCP/IP-Adresse auf Ihre Website zugreifen kann. Entsprechend kann es aus verwaltungstechnischen Gründen hilfreich sein, rasch sehen zu können, welchen Sites Hostheadernamen zugewiesen sind.

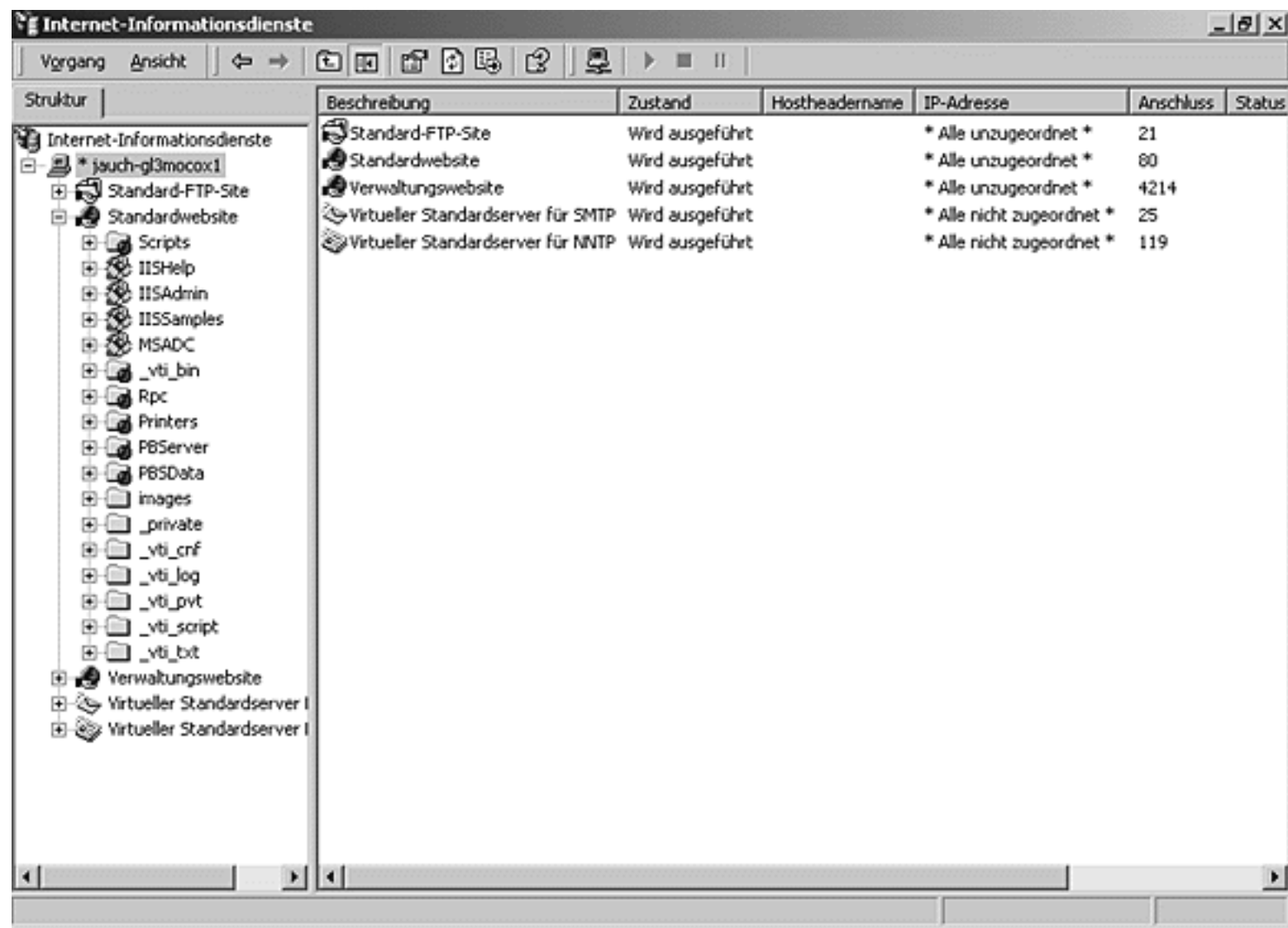


Abbildung 19.9: Anzeige der installierten IIS-Sites

Klicken Sie mit der rechten Maustaste auf **Computername*. Daraufhin erscheint ein Kontextmenü mit mehreren Bereichen (siehe Abbildung 19.10).

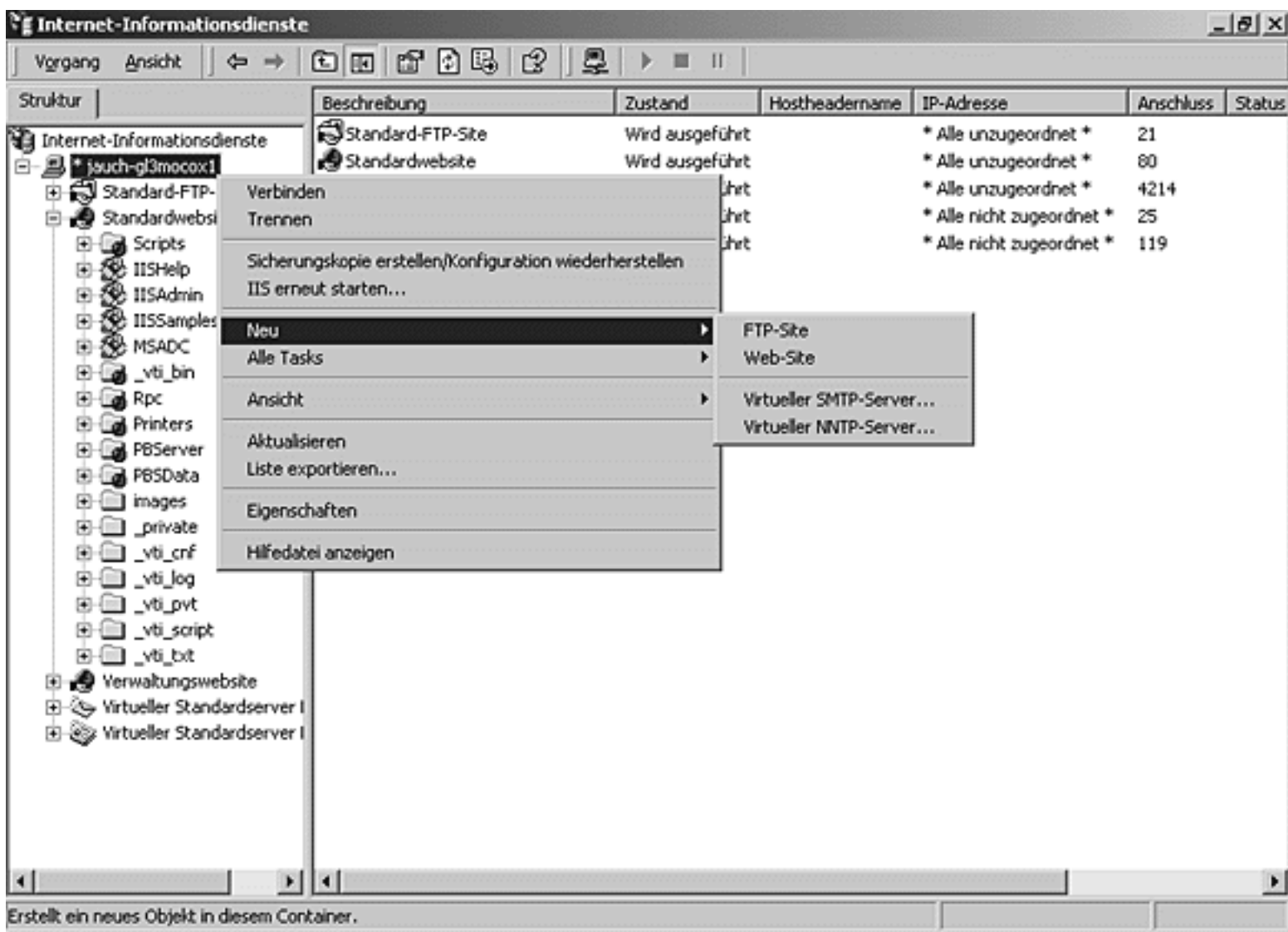


Abbildung 19.10: Hauptmenü für die Verwaltung von IIS

Sie werden die meisten der verwaltungstechnischen Aufgaben für Ihren IIS-Rechner von diesem Menü aus beginnen. Verbindungen zu einem IIS-Server werden über die Optionen im oberen Bereich hergestellt bzw. getrennt.

Der nächste Bereich wird verwendet, um die Konfigurationsinformationen eines bestimmten Computers zu sichern und/oder wiederherzustellen. Dies ist eine Option, die für die Verwaltung des Geschäftsplans Ihres Unternehmens, insbesondere im Bereich des E-Commerce und anderer digitaler Optionen (wie z.B. das Intranet oder das Extranet des Unternehmens usw.) wichtig ist. Darüber hinaus können Sie über diesen Bereich die IIS-Dienste von Windows 2000 Server neu starten. Dies ist ebenfalls eine sehr nützliche Option. Erinnern Sie sich nur daran, dass dies bei den älteren Versionen von IIS wie IIS 3.0 oder 4.0 nicht möglich war.

Mit Hilfe des nächsten Bereichs, der mit der Option **Neu** beginnt, können Sie neue FTP- und Websites sowie virtuelle Server für SMTP und NNTP erstellen. Auf diese Art und Weise können Sie auf jedem IIS-Server eine neue Web- oder FTP-Site am schnellsten einrichten und zum Laufen bringen. Die Option **Alle Tasks** wird verwendet, um die **FrontPage 2000-Servererweiterungen** für Ihren IIS-Dienst zu aktivieren. Wenn Sie IIS nicht für die Verwendung der Entwicklungspakete Microsoft FrontPage 2000 und Microsoft Visual InterDev konfiguriert haben, lässt sich diese Option auf die Konfiguration Ihrer

Organisation natürlich nicht anwenden.

Der nächste Bereich, der die Option **Ansicht** enthält, funktioniert genau so wie die Option **Ansicht** in der Menüleiste.

Der nächste Bereich (mit den Optionen **Aktualisieren** und **Liste exportieren**) wird verwendet, um die Ansicht sowohl des rechten als auch des linken Fensterbereichs zu aktualisieren. (Es ist möglich, dass sich die Ansicht dieser Bereiche ändert, insbesondere dann, wenn jemand anderes die Konfiguration Ihres Internetdienste-Managers über einen anderen Windows 2000-Server irgendwo in der Domäne verwaltet.) Wenn Sie auf die Option **Aktualisieren** klicken, werden im Fenster sämtliche Änderungen erkennbar, die seit der letzten Aktualisierung oder seit dem letzten Öffnen des Fensters vorgenommen worden sind. Mit Hilfe der Option **Liste exportieren** können Sie die im rechten Fensterbereich dargestellte Liste in eine ASCII-Textdatei kopieren. Dies kann für die Dokumentation recht nützlich sein. Darüber hinaus bewahren Sie sich damit einen besseren Überblick über zig, Hunderte oder auch Tausende von auf einem bestimmten IIS-Server gespeicherten Websites.

Der nächste Bereich enthält lediglich eine Option: **Eigenschaften**. Wenn Sie auf diese Option klicken, erscheint das in Abbildung 19.11 dargestellte Dialogfeld **Eigenschaften**. Hier können Sie das allgemeine Erscheinungsbild Ihres IIS-Servers überwachen und verwalten.

Im Dialogfeld **Eigenschaften** definieren Sie die globalen Attribute für sämtliche Websites, die unter der Kontrolle dieses IIS-Servers stehen. Dieses Dialogfeld weist drei Bereiche auf:

- **Haupteigenschaften**
- **Bandbreitenbeschränkung aktivieren**
- **MIME-Zuordnungen**

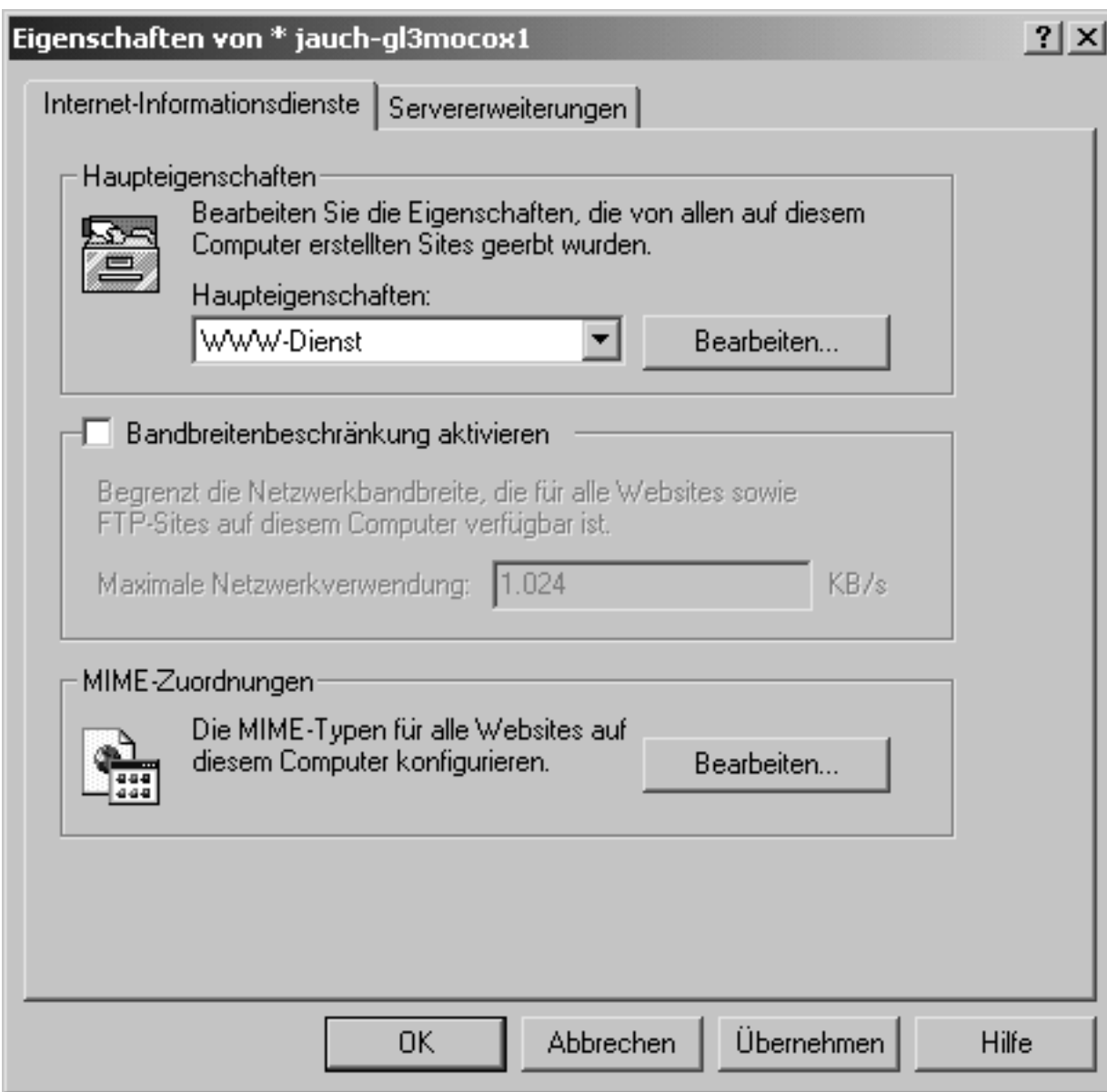


Abbildung 19.11: Definieren der wichtigsten Eigenschaften des IIS-Servers

Der Bereich **Haupteigenschaften** wird für die Festlegung der globalen Einstellungen auf eine Art und Weise verwendet, die nahezu identisch ist mit der, wie bestimmte Eigenschaften für jede Ihrer Websites und virtuellen Verzeichnisse definiert werden. So erscheint beispielsweise das Fenster für die Haupteigenschaften des WWW-Dienstes für **Computername*, wenn Sie links neben dem Dropdown-Listefeld auf die Schaltfläche **Bearbeiten** klicken. (Lassen Sie aus Gründen der Einfachheit die Standardoption **WWW-Dienste** im Listefeld stehen.)

Da außer einem der nachfolgenden Fenster alle gleich sind wie das, das für einzelne Websites verwendet wird, werden wir die gleichen Fenster überspringen und mit dem einen Fenster fortfahren, das sich von den anderen unterscheidet. (Die anderen Fenster werden kurz beschrieben, wenn wir eine Musterwebseite ändern.) Das Fenster öffnet sich, wobei die Registerkarte **Website** oben liegt. Daher müssen Sie auf die Registerkarte **Dienst** klicken, damit das Dialogfeld wie in Abbildung 19.12 erscheint.



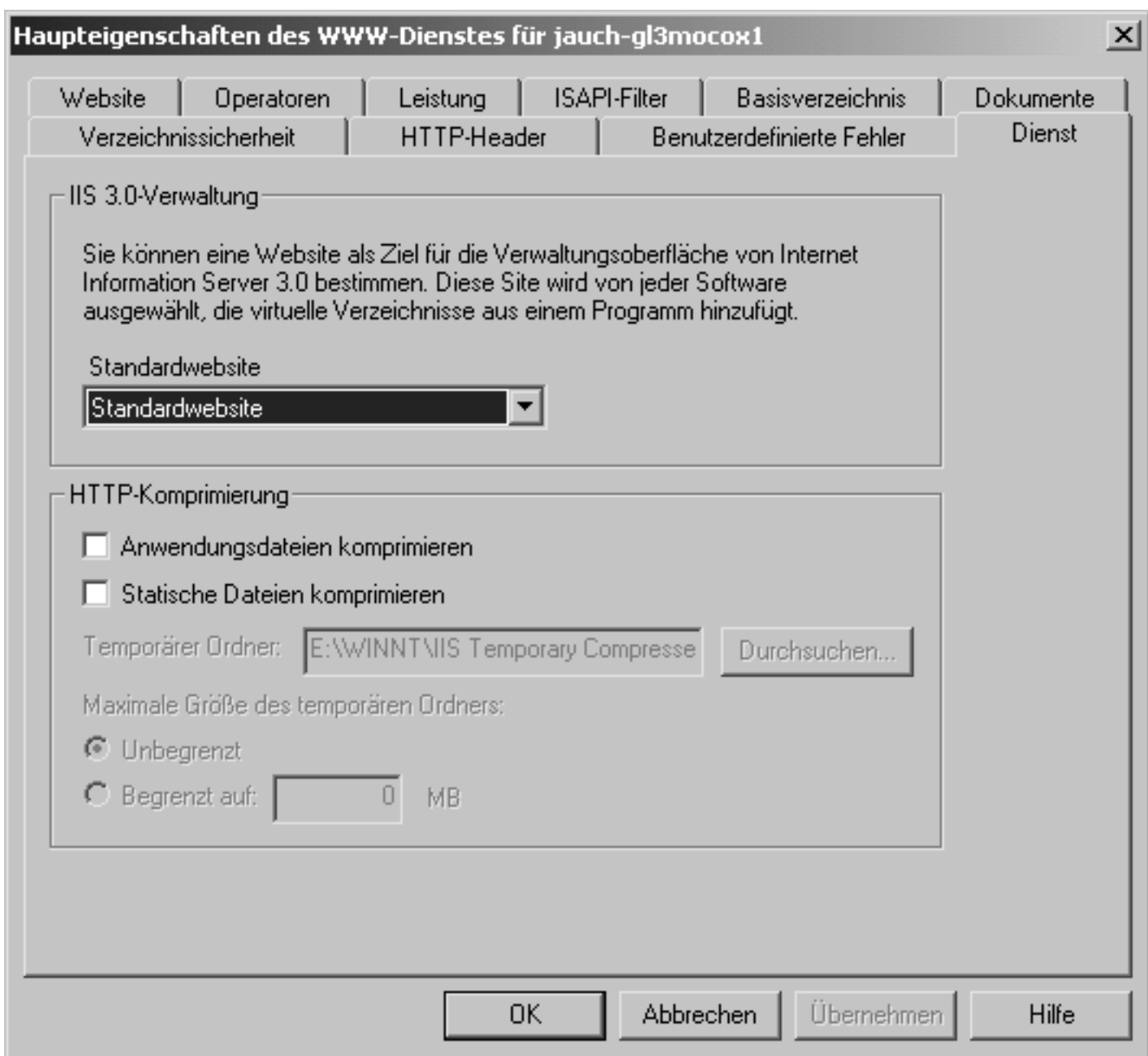


Abbildung 19.12: Aufrufen der Registerkarte Dienst zum Ändern der Haupteigenschaften einer Website

Sinn und Zweck dieses Fensters ist einfach: Anwendungen erstellen gelegentlich neue virtuelle Webverzeichnisse. Das bedeutet, dass Sie eine Standardwebsite als Ausgangspunkt für diese Verzeichnisse definieren sollten. Mit Hilfe dieses Fensters können Sie das tun. Wenn Sie IIS installieren, gibt es nur zwei Möglichkeiten: **Standardwebsite** und **Verwaltungswebsite**. Aus Gründen der Sicherheit und vielleicht auch der besseren Verwaltbarkeit sollten Sie eine neue Website erstellen und diese Site als Ausgangspunkt für sämtliche neu erstellten virtuellen Verzeichnisse verwenden. So können Sie beispielsweise die Standardsite *Standardprogrammsites* erstellen, von der aus automatisch alle neuen virtuellen Verzeichnisse installiert werden. Das müssen Sie natürlich nicht tun.

Wenn Sie aber erst einmal mehr als hundert virtuelle Verzeichnisse haben, dann werden Sie froh sein, wenn Sie es getan haben. (Ihre Meinung nachträglich zu ändern, ist praktisch nicht möglich.) Wenn die HTTP-Komprimierung auf Ihren Sites aktiviert ist, können Sie den momentan grau hinterlegten Bereich

unten in diesem Fenster ändern. Wenn Sie die gewünschten Änderungen vorgenommen haben, klicken Sie auf OK, um die Einstellungen zu bestätigen und zum Fenster **Internet-Informationdienste** zurückzukehren.



Die IIS-Software scheint einen Fehler zu enthalten. Statt zum Fenster **Eigenschaften** kehren Sie zum Fenster **Internet-Informationdienste** zurück. Das bedeutet, dass Sie im Kontextmenü von **Computernamen* wieder die Option **Eigenschaften** wählen müssen, wie Sie es zu Beginn dieses Abschnitts schon einmal getan haben.

Öffnen Sie also noch einmal das Fenster **Eigenschaften** für den Computer und sehen Sie sich den mittleren Bereich mit der Überschrift **Bandbreitenbeschränkung aktivieren** einmal näher an (siehe Abbildung 19.11). Die Bandbreite kann beschränkt werden, damit IIS Ihr physikalisches Netzwerk nicht zu stark beansprucht. Das ist besonders in einer Intranet-Umgebung recht nützlich. Um die Bandbreitenbeschränkung zu aktivieren, klicken Sie einfach auf dieses Kontrollkästchen, um dieses mit einem Häkchen zu versehen, wodurch die im Folgenden beschriebenen Optionen verfügbar werden. Wenn Sie diese Option zum ersten Mal aktivieren, werden standardmäßig 1 Mbyte (1.024 Kbit/s) angezeigt. Diese Einstellung können Sie ändern. Dabei sollten Sie jedoch sicherstellen, dass Sie keine Zahl wählen, die größer als die Ihrer gesamten Bandbreite ist. Bei einem 10Base-T-Netzwerk (10.240 Kbit/s) können Sie nicht 102.400 in das Feld eingeben. Dazu bräuchten Sie ein 100Base-T-Netzwerk.

Mit Hilfe des unteren Bereichs, **MIME-Zuordnungen**, können Sie die momentan für sämtliche Websites auf diesem IIS-Server installierten MIME-Typen ändern. Um die MIME-Typen zu ändern, klicken Sie auf die Schaltfläche **Bearbeiten**. Daraufhin erscheint das Dialogfeld **Dateitypen** (siehe Abbildung 19.13).



Abbildung 19.13: Registrierte Windows 2000 Server-Dateitypen

Erfahrenen Windows 9x- und Windows NT-Benutzern sollte dieses Fenster bekannt vorkommen. In diesem Dialogfeld können Sie die Dateitypen für diesen IIS-Server auf eine Art und Weise ändern, die der Art und Weise, wie Dateitypen für jedes 32-Bit-Betriebssystem von Microsoft geändert werden, sehr ähnlich ist. Um einen neuen Dateityp hinzuzufügen, klicken Sie auf die Schaltfläche **Neuer Typ**. Um einen Dateityp zu ändern, klicken Sie auf den entsprechenden Dateityp, um ihn zu markieren, klicken Sie dann auf die Schaltfläche **Bearbeiten**. Nachdem Sie die gewünschten Änderungen vorgenommen haben, klicken Sie auf die Schaltfläche **OK**, um die Einstellungen zu bestätigen und zum Dialogfeld **Eigenschaften** zurückzukehren.

Die letzte Option, an der Sie im Dialogfeld **Eigenschaften** möglicherweise Änderungen vornehmen möchten, befindet sich auf der Registerkarte **Servererweiterungen**. Klicken Sie auf diese Registerkarte, um diese wie in Abbildung 19.14 dargestellt aufzurufen.



Abbildung 19.14: Konfigurieren der Eigenschaften der Servererweiterungen

Diese Registerkarte besteht aus drei Bereichen:

- **Allgemein** - Sie verwenden diesen Bereich, um die Leistung zu konfigurieren sowie um festzulegen, welches Skript auf Seiten des Client verwendet werden soll (d.h. JavaScript oder VBScript).
- **Optionen** - Sie verwenden diesen Bereich, um die grundlegenden E-Mail-Einstellungen für Personen festzulegen, die Ihre Websites durchsuchen (diese können Sie jedoch natürlich auch für jede Website einzeln ändern).
- **Berechtigungen** - Sie verwenden diesen Bereich, um die wichtigsten Berechtigungen für die Veröffentlichung auf Ihren Websites zu konfigurieren und die Protokollierungsoptionen für Ihre Websites zu aktivieren.

Wenn Sie auf dieser Registerkarte auf die Schaltfläche **Einstellungen** klicken, erscheint das in Abbildung 19.15 dargestellte Dialogfeld **E-Mail-Einstellungen**.

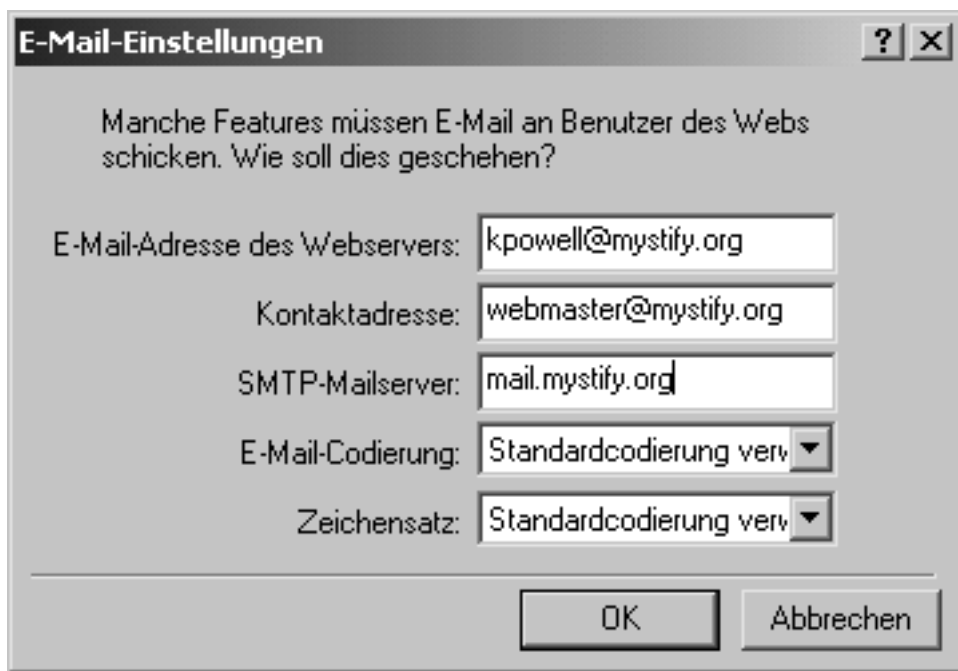


Abbildung 19.15: Definieren anwendbarer E-Mail-Einstellungen

In diesem Dialogfeld definieren Sie die E-Mail-Adressen für Ihre Websites, die Adresse des SMTP-Mailserver, die E-Mail-Kodierung sowie den Zeichensatz. Definieren Sie die gewünschten Einstellungen. Klicken Sie dann auf die Schaltfläche **OK**, um diese zu bestätigen und zum Fenster **Eigenschaften** zurückzukehren. Dort angekommen klicken Sie auf die Schaltfläche **OK**, um all Ihre Einstellungen und Änderungen zu speichern und zum Dialogfeld **Internet-Informationdienste** zurückzukehren.

Anonyme Benutzer

Anonyme Benutzer sind Personen oder Programme, die ohne Anmeldekennung und Kennwort auf Ihre Web- oder FTP-Sites zugreifen dürfen. Um anonymen Benutzern den Zugriff auf Ihre Websites zu gewähren oder zu verweigern, müssen Sie im Dialogfeld **Eigenschaften von Standardwebsite** die Registerkarte **Verzeichnissicherheit** aufrufen (siehe Abbildung 19.16).

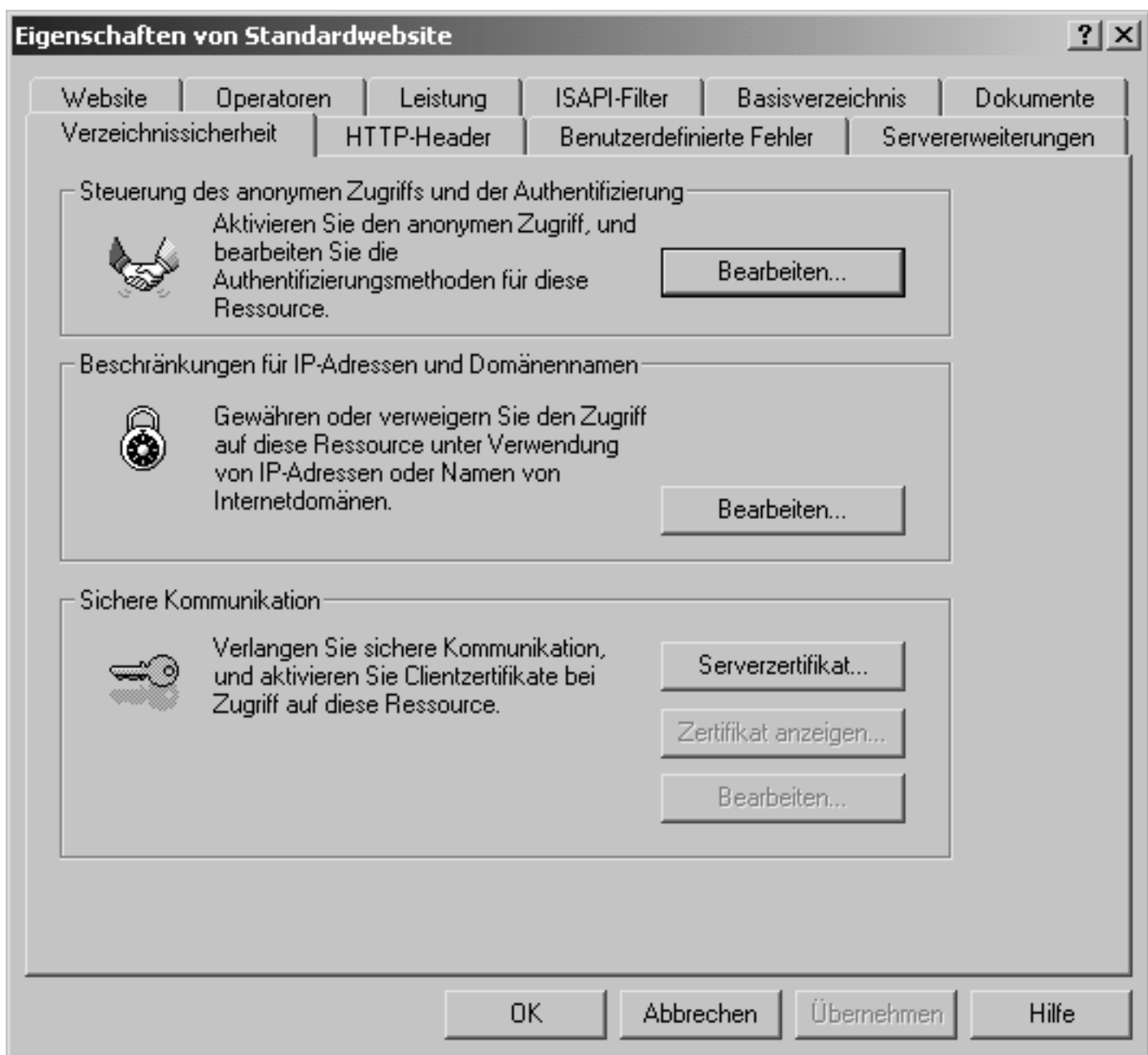


Abbildung 19.16: Definieren der Verzeichnissicherheit für eine Website

Um dasselbe für Ihre FTP-Sites zu tun, müssen Sie im Dialogfeld **Eigenschaften von Standard-FTP-Site** die Registerkarte **Sicherheitskonten** aufrufen (siehe Abbildung 19.17).

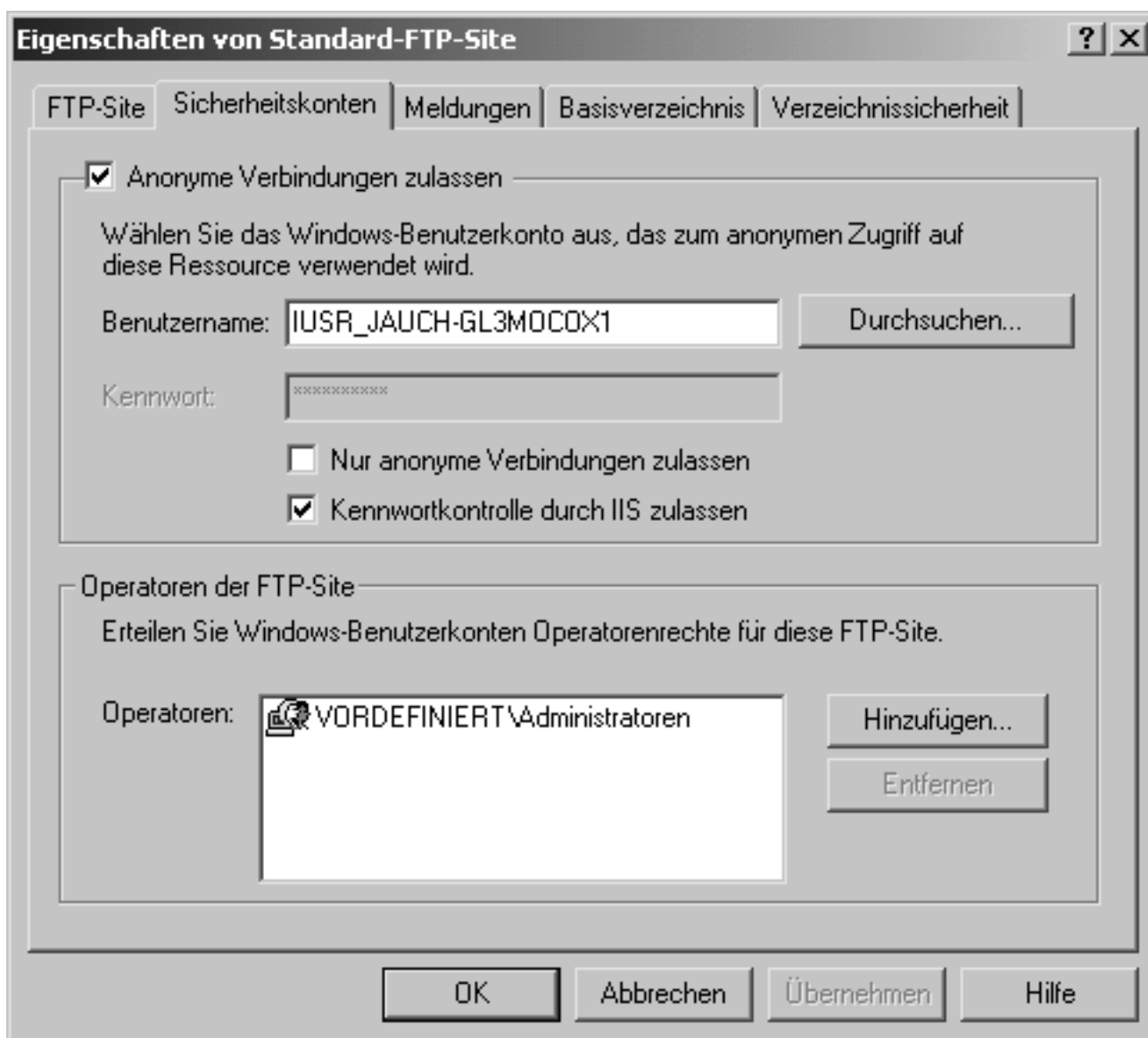


Abbildung 19.17: Konfigurieren der FTP-Sicherheitskonten

Um eines dieser Fenster aufzurufen, klicken Sie mit der rechten Maustaste entweder auf **Standardwebsite** oder auf **Standard-FTP-Site** (je nachdem, was Sie bearbeiten möchten). Daraufhin erscheint ein Kontextmenü. Klicken Sie in diesem Menü auf die Option **Eigenschaften**, um das Fenster für die allgemeinen Eigenschaften aufzurufen. Klicken Sie als Nächstes auf die Registerkarte, über die Sie die gewünschten Eigenschaften ändern können. Im Dialogfeld **Eigenschaften von Standardwebsite** müssen Sie auf die obere Schaltfläche **Bearbeiten** klicken, um die entsprechenden Änderungen vornehmen zu können. Im Dialogfeld **Eigenschaften von Standard-FTP-Site** müssen Sie das obere Kontrollkästchen (**Anonyme Verbindungen zulassen**) verwenden, wenn Sie festlegen möchten, ob Sie diese Funktion für Ihre FTP-Benutzer aktivieren möchten. Warum anonyme Benutzer so wichtig sein können, erfahren Sie später in diesem Kapitel.

Protokollierungsoptionen

Einem IIS-Administrator steht eine Vielzahl von Protokollierungsoptionen zur Verfügung. Wenn Sie beispielsweise das Dialogfeld **Eigenschaften von Standard-FTP-Site** oder das Dialogfeld **Eigenschaften von Standardwebsite** aufrufen, wird wie in Abbildung 19.18 als Erstes die Registerkarte

Website angezeigt.

Eigenschaften von Standardwebsite

Verzeichnissicherheit | HTTP-Header | Benutzerdefinierte Fehler | Servererweiterungen

Website | Operatoren | Leistung | ISAPI-Filter | Basisverzeichnis | Dokumente

Identifizierung der Website

Beschreibung: Standardwebsite

IP-Adresse: (Alle nicht zugeordnet) Weitere Optionen...

TCP-Anschluss: 80 SSL-Anschluss:

Verbindungen

☒ Unbegrenzt

☐ Begrenzt auf: 1.000 Verbindungen

Verbindungstimeout: 900 Sekunden

☒ HTTP-Verbindung aufrechterhalten (HTTP-Keep-Alive aktivieren)

☒ Protokollierung aktivieren

Aktives Protokollformat: W3C-erweitert Eigenschaften...

OK Abbrechen Übernehmen Hilfe

Abbildung 19.18: Konfigurieren der Optionen für die Standardwebsite

Mit Hilfe der untersten Option **Protokollierung aktivieren** können Sie die Protokollierungsfunktionen des IIS-Servers einschalten. Wenn die Option aktiviert worden ist, müssen Sie aus dem daraufhin erscheinenden Dropdown-Listenfeld das geeignete Protokollierungsformat wählen:

- **Microsoft IIS** - Dieses feste ASCII-Format ist das Standardformat für IIS, das Microsoft ursprünglich für seine erste Version von IIS entwickelt hat. Es ist das Format, das heute immer noch verwendet wird. In diesem Format werden mehr Informationen aufgezeichnet als im NCSA-Format (National Center for Supercomputing Applications), es kann jedoch bezüglich des Layouts nicht angepasst werden.
- **NCSA allgemein** - Wie das Protokollierungsformat Microsoft IIS kann auch das NCSA-Format nicht angepasst werden. Es handelt sich ebenso um eine Datei mit einer festen Länge, in der nur die elementaren Informationen in Bezug auf die Aktivitäten um den IIS-Dienst gespeichert

werden. Das NCSA-Format wurde an der Universität von Illinois in Urbana vom National Center for Supercomputing Applications als Teil des Internet-Entwicklungsprogramms des Instituts entwickelt. (Hier wurde auch Mosaic, der erste Internet-Webbrowser entwickelt.)

Beachten Sie, dass Sie dieses Dateiformat nicht für Ihre FTP-Sites verwenden können, da dessen Einsatz ausschließlich auf Websites beschränkt ist. (Daher erscheint dieser Dateityp im Dropdown-Listenfeld von FTP-Sites erst gar nicht.)

- **ODBC** - Mit Hilfe dieser Option können Sie die Protokolle Ihres IIS-Servers in einer Datenbank Ihrer Wahl speichern, vorausgesetzt, diese Datenbank unterstützt den ODBC-Standard (Open Database Connectivity) und kann in Bezug darauf, was aufgezeichnet wird, angepasst werden.
- **W3C-erweitert** - Hierbei handelt es sich um das Standardformat, das dem Standard des W3C (World Wide Web Consortium) entspricht, und dennoch ein ASCII-Format ist, das angepasst werden kann. Darüber hinaus werden im Gegensatz zu anderen Formaten Zeiteinträge nicht in lokaler Zeit, sondern in Greenwich-Zeit aufgezeichnet.

Nachdem Sie in dem Dropdown-Listenfeld ein Protokollierungsformat gewählt haben, klicken Sie auf die Schaltfläche **Eigenschaften**. Daraufhin erscheint das in Abbildung 19.19 dargestellte Dialogfeld **Erweiterte Protokollierungseigenschaften**.

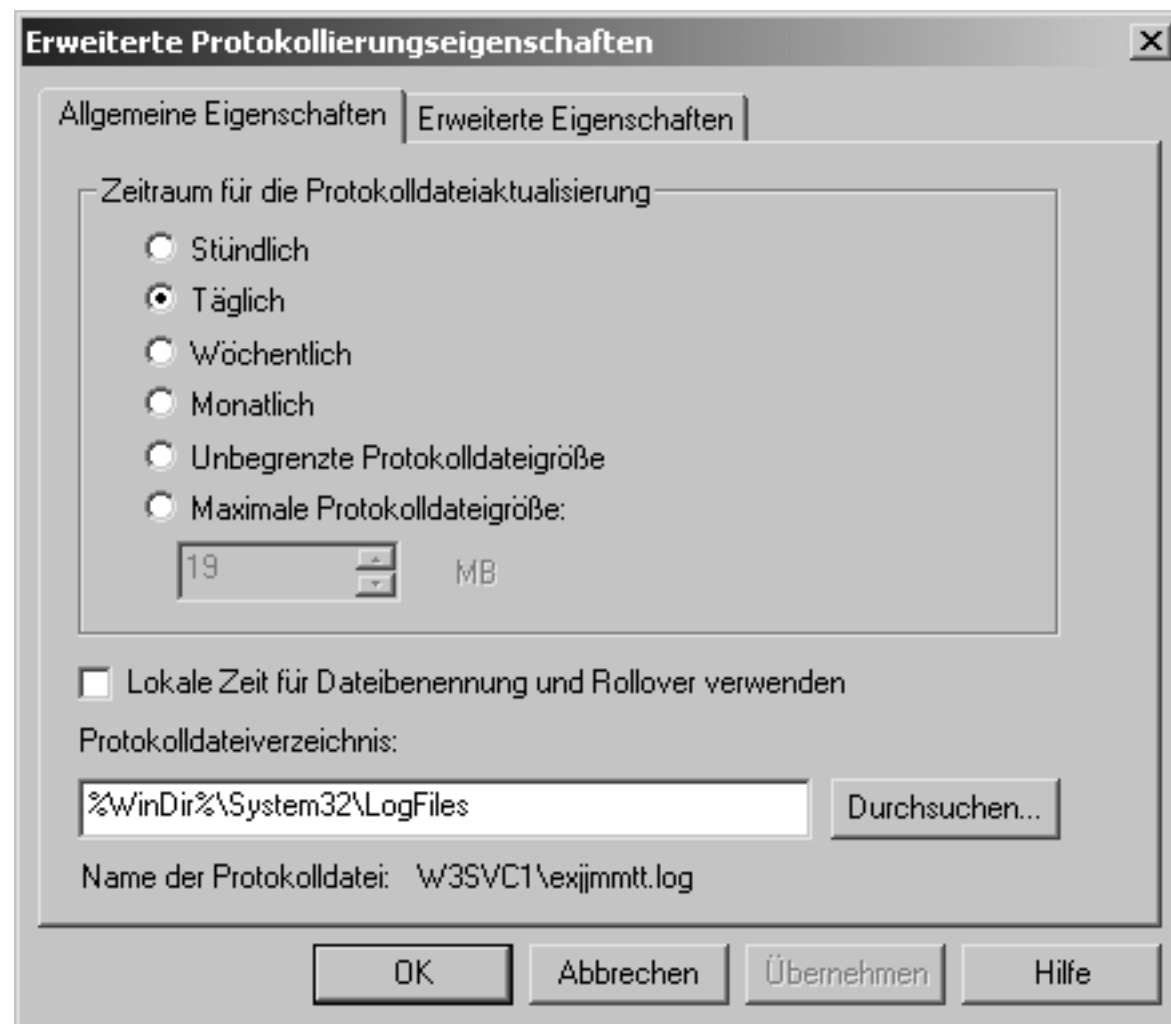


Abbildung 19.19: Festlegen der erweiterten Eigenschaften für Protokolldateien

Im Dialogfeld **Erweiterte Protokollierungseigenschaften** legen Sie den Zeitraum für die

Protokolldateiaktualisierung - stündlich, täglich, wöchentlich oder monatlich - sowie die maximale Größe und den Speicherort der Protokolldateien fest. Sie können auch festlegen, mit welcher Zeitmessung eine Protokolldatei auf Ihrem Computer gespeichert wird (lokale Zeit oder Greenwich-Zeit). Nachdem Sie die gewünschten Einstellungen vorgenommen haben, aktivieren Sie die Registerkarte **Erweiterte Eigenschaften** (siehe Abbildung 19.20).

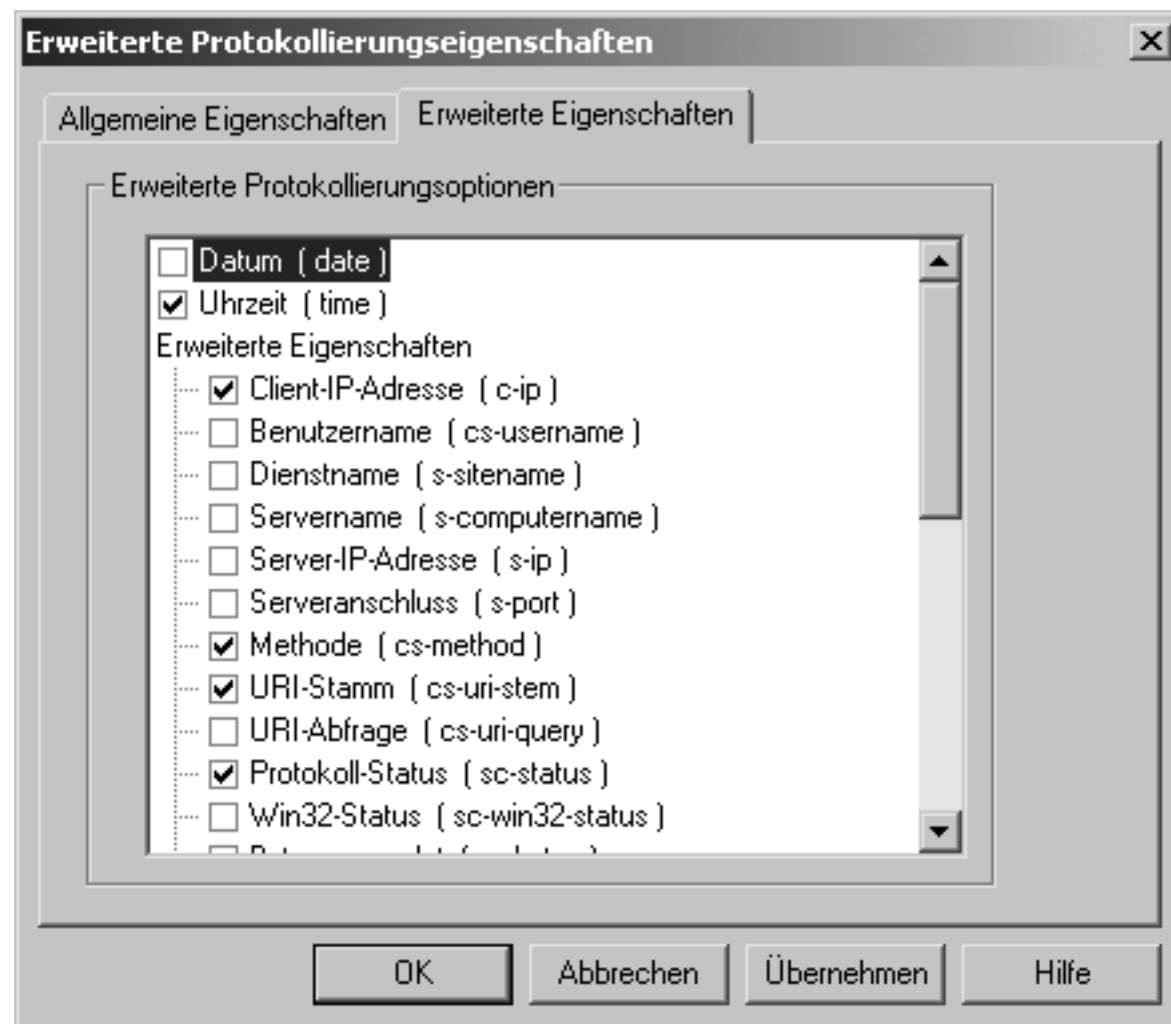


Abbildung 19.20: Konfigurieren der erweiterten Eigenschaften für erweiterte Protokolldateien

Mit Hilfe der Optionen dieses Fensters können Sie lediglich das Format der W3C-erweiterten Protokolldatei anpassen, da die anderen Dateiformate keine Anpassung zulassen. Aktivieren Sie die Kontrollkästchen neben jeder Option, die Sie in die Protokolldatei aufnehmen möchten, und deaktivieren Sie die Optionen, die Sie nicht aufnehmen möchten: Ein Häkchen im Kontrollkästchen bedeutet, dass die Option in der Protokolldatei aufgezeichnet wird, während ein leeres Kontrollkästchen bedeutet, dass die entsprechende Option nicht in die Protokolldatei aufgenommen wird. Wenn Sie alle gewünschten Optionen aktiviert haben, klicken Sie auf die Schaltfläche **OK**, um zum Dialogfeld **Eigenschaften von Standard-FTP-Site** oder zum Dialogfeld **Eigenschaften von Standardwebsite** zurückzukehren (je nachdem, ob Sie eine FTP-Site oder eine Website konfigurieren). Klicken Sie auf **OK**, um das Fenster **Eigenschaften** zu schließen.

Verzeichnisverwaltung

Die unterschiedlichen Verzeichnisse innerhalb Ihrer Web- und FTP-Sites zu verwalten, ist wohl eine der

wichtigsten Siteverwaltungsaufgaben überhaupt. Wenn Sie den Ausdruck *Verzeichnis* verwenden, bedeutet dieser wesentlich mehr als nur die Angabe der physikalischen Adresse Ihrer Web- oder FTP-Site. Verzeichnis impliziert immer den logischen Speicherort Ihrer Web- bzw. FTP-Site. Das Basisverzeichnis einer Website gibt beispielsweise an, ob sich eine Website physikalisch auf demselben Computer befindet, auf dem auch die IIS-Dienste ausgeführt werden, oder ob sie über eine Freigabe gespeichert wird, die ein anderer Computer zur Verfügung stellt, der ein 32-Bit-Betriebssystem von Microsoft ausführt, oder ob es sich um nichts anderes als um eine Umleitung an einen anderen URL handelt. (Diese letzte Option ist nur bei Websites möglich, da FTP-Sites keine URLs unterstützen.) Denken Sie also beim Lesen der nächsten Abschnitte daran, dass ein Verzeichnis mehr ist als nur eine statische Adresse, unter der Sie Ihre Dateien speichern können.

Verwalten von Verzeichnissen

Wenn Sie eine Website über eine Verzeichnisstruktur erstellen, erstellen Sie wahrscheinlich im Verzeichnis `\inetpub\wwwroot` einen Ordner auf Ihrem Server. Damit im Internetdienste-Manager unter dem Symbol **Standardwebsite** eine neue Websiteadresse erscheint, gehen Sie wie folgt vor:

1. Gehen Sie in Ihrem Webserver zum Ordner `\inetpub\wwwroot` und erstellen Sie einen neuen Ordner. (Geben Sie ihm einen beliebigen Namen ohne Leerzeichen. Verwenden Sie also beispielsweise statt *Genfer Schnee* den Begriff *GenferSchnee*.)
2. Starten Sie den Internetdienste-Manager, indem Sie auf **Start, Programme, Verwaltung** und dann auf **Internetdienste-Manager** klicken.
3. Öffnen Sie die Elemente unter dem Symbol **Standardwebsite**.
4. Sie werden nun sehen, dass die Website *GenferSchnee* (oder wie Sie Ihre Website auch immer genannt haben) auf wundersame Weise dort erscheint.

Das war doch nicht schwierig, oder? Natürlich müssen Sie noch einige Dinge tun, um Inhalte für die Website zu erstellen, aber Sie sehen, wie das Ganze funktioniert.

Um einige grundlegende Informationen bezüglich Ihrer Website zu ändern, rufen Sie im Dialogfeld **Eigenschaften von Standardwebsite** die Registerkarte **Basisverzeichnis** auf (siehe Abbildung 19.21).

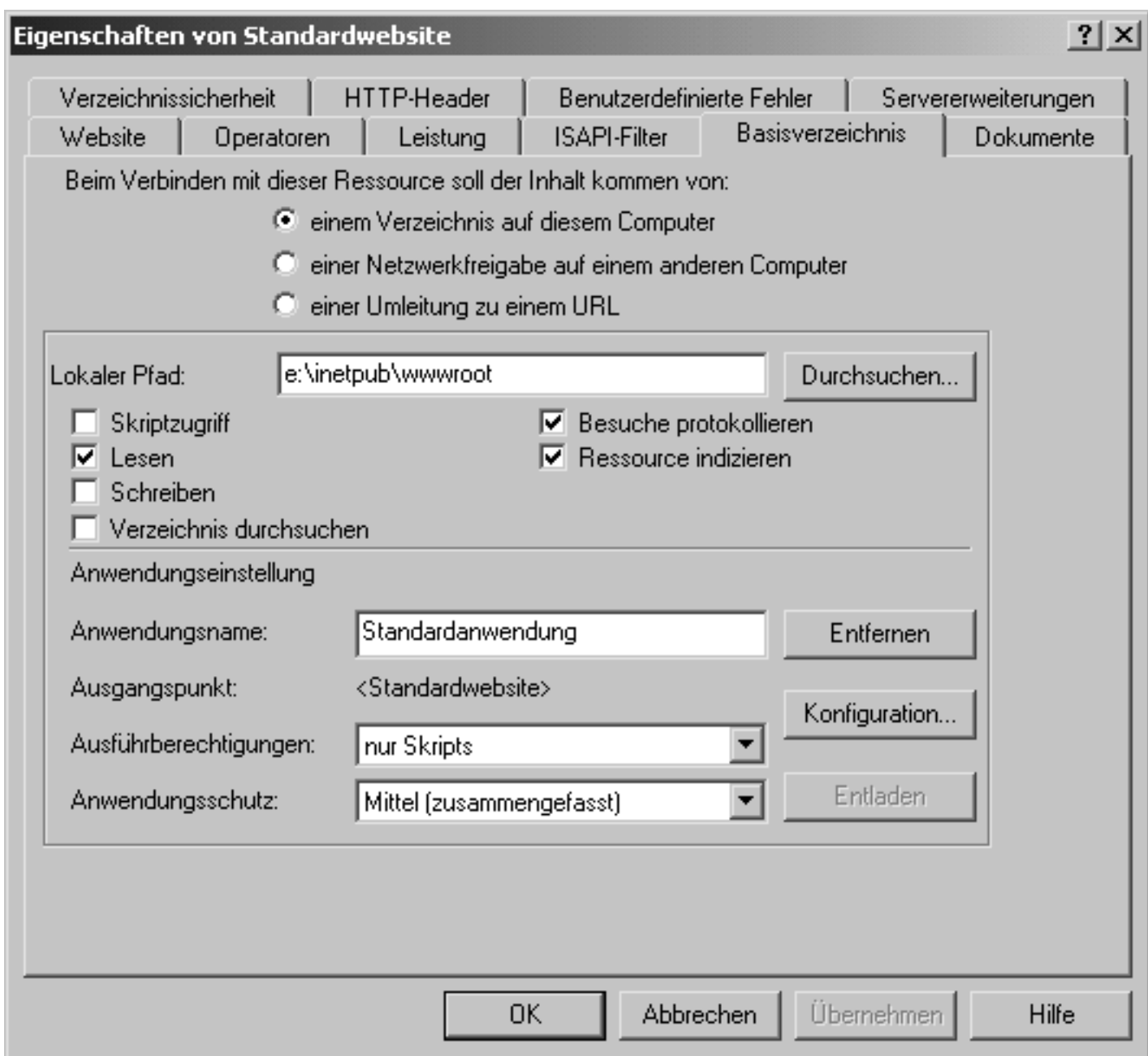


Abbildung 19.21: Festlegen der Eigenschaften für das Basisverzeichnis für die Standardwebsite

Auf dieser Registerkarte können Sie festlegen, von wo der Inhalt für Ihre Standardwebsite bezogen werden soll. Das bedeutet, dass Sie eine der folgenden drei Optionen wählen müssen:

- **Einem Verzeichnis auf diesem Computer**
- **Einer Netzwerkfreigabe auf einem anderen Computer**
- **Einer Umleitung zu einem URL**

Sie sollten sich die Zeit nehmen und sorgfältig prüfen, wie Ihre Organisation den Inhalt ihrer Website auf einer fortlaufenden Basis sowohl in Bezug auf die Verwaltbarkeit als auch in Bezug auf die Sicherheit am besten einsetzen soll. Denken Sie dabei daran, dass es generell am einfachsten ist, Websites zu verwalten und zu sichern, wenn diese sich physikalisch praktisch an derselben Stelle befinden.

Weitere Optionen, die Sie sorgfältig prüfen sollten, betreffen den Zugriff:

- **Skriptzugriff** - Mit dieser Option können Skripten auf Ihrem Webserver ausgeführt werden.

- **Lesen** - Mit dieser Option können Benutzer die Website lesen und Material kopieren, aber keine Änderungen vornehmen.
- **Schreiben** - Mit dieser Option können Benutzer nicht nur lesen, sondern auch Änderungen an der Website vornehmen. (Seien Sie mit dieser Option vorsichtig!)
- **Verzeichnis durchsuchen** - Dies ist eine der gefährlichsten Optionen bei einer offenen Website, da Benutzer nach Aktivieren dieser Option Ihre physikalische Verzeichnisstruktur durchsuchen können, was diese vielleicht tun werden, um nach einer Schwachstelle zu suchen, an der sie in Ihr System eindringen können. Mir fällt kein Grund ein, der dafür spricht, dass ein IIS-Administrator diese Option für eine Website aktiviert.
- **Besuche protokollieren** - Sie verwenden diese Option, um sicherzustellen, dass sämtliche Besuche der Website im Protokollierungsformat Ihres IIS-Servers protokolliert werden.
- **Ressource indizieren** - Wenn Sie diese Option aktivieren, wird der Inhalt dieser Website über den in IIS integrierten Indizierungsdienst indiziert.

Sie verwenden den Bereich **Anwendungseinstellung** im Dialogfeld **Eigenschaften von Standardwebsite**, um eine Anwendung zu definieren, die die Verwaltung oder die Verwendung Ihrer Standardwebsite (oder auch einer beliebigen anderen Website) unterstützt. Um eine zu verwendende Anwendung zu installieren, klicken Sie auf die Schaltfläche **Erstellen**. Dadurch werden die anderen, zuvor nicht anwendbaren Optionen in diesem Bereich aktiv. Wenn Sie auf die Schaltfläche **Konfiguration** klicken, können Sie die für Ihren Webserver zur Verfügung stehenden ISAPI-Tools (Internet Server Application Programming Interface) hinzufügen oder ändern. Dazu gehört das Zwischenspeichern von ISAPI-Anwendungen, das Festlegen von Sitzungszustand und Sitzungstimeout sowie das Festlegen einer ASP-Standardsprache, üblicherweise VBScript, und das Festlegen der unterschiedlichen Debug-Optionen für Anwendungen.

Das Dropdown-Listenfeld **Ausführberechtigung** ist sowohl für die Sicherheit als auch für die Verwendbarkeit von großer Bedeutung. Die Seite der Sicherheit ist einfach: Je mehr Flexibilität Sie zulassen, umso weniger sicher ist Ihre Website. Es hängt von der Anwendung ab, welches Verhältnis Sie anstreben, und Sie werden auch einfach ausprobieren müssen. (Daher konfigurieren Sie das Ganze auch erst einmal in einer Testumgebung und nicht gleich in einer Arbeitsumgebung.) Die Seite der Verwendbarkeit ist etwas vertrackter: Sie müssen ein Minimum an Verwendbarkeit festlegen um sicherzustellen, dass Ihre Anwendung richtig läuft.

Das Dropdown-Listenfeld **Anwendungsschutz** umfasst drei Ebenen des Schutzes:

- **Niedrig (IIS-Prozess)** - Die Anwendung wird (unter Verwendung der Datei *InetInfo.exe*) in demselben Prozess ausgeführt wie die Webdienste.
- **Mittel (zusammengefasst)** - Die Anwendung wird in einem zusammengefassten Prozess ausgeführt, was bedeutet, dass üblicherweise alle Anwendungen zusammen außerhalb jedes Webdienstes (unter Verwendung der Datei *DLLHost.exe*) ausgeführt werden.
- **Hoch (isoliert)** - Die Anwendung wird in ihrem eigenen, isolierten Raum abseits der Webdienste und anderer Anwendungen (unter Verwendung einer anderen Instanz der Datei *DLLHost.exe*) ausgeführt.

Wenn wir den Ausdruck *Schutz* im Sinne von IIS 5.0 verwenden, bedeutet das, dass dies der Prozess ist, in dem diese spezielle Anwendung ausgeführt wird. Wenn beispielsweise eine Anwendung im niedrigen

Modus ausgeführt wird und abstürzt, kann dies dazu führen, dass die Dienste des Webservers ebenfalls teilweise oder ganz mit abstürzen. Wenn Sie jedoch alle Anwendungen im isolierten Modus ausführen, kann das deutlich negative Auswirkungen auf die Leistung Ihres IIS-Servers haben. Aus diesem Grund empfiehlt Microsoft, dass Sie nicht mehr als zehn Anwendungen im isolierten Modus ausführen sollten.



Die Registerkarte **Basisverzeichnis** im Dialogfeld **Eigenschaften von Website** gibt es für jede Website. Es ist dieselbe Registerkarte wie im Dialogfeld **Eigenschaften von Standardwebsite**. Daher können Sie bei jeder auf Ihrem IIS-Server existierenden Website dieselben, wie für die Standardwebsite beschriebenen Schritte befolgen, um Änderungen vorzunehmen. Ebenso gibt es sämtliche andere Optionen in diesem Fenster für jede Ihrer anderen Websites ebenfalls. Notieren Sie sich also die Optionen, von denen Sie denken, dass Sie diese bei jeder über diesen IIS-Server verfügbaren Website ändern sollten.

Die beste Möglichkeit, eine Website innerhalb des Internetdienste-Managers zu erstellen, besteht darin, den von Microsoft zur Verfügung gestellten Assistenten zu verwenden. Um diesen Assistenten aufzurufen, klicken Sie mit der rechten Maustaste auf **Standardwebsite** (oder auf eine beliebige andere Website, nicht jedoch auf ein virtuelles Verzeichnis). Klicken Sie in dem daraufhin erscheinenden Kontextmenü auf die Option **Neu**. Nun erscheint rechts neben dem Kontextmenü ein weiteres Menü, in dem Sie auf die Option **Site** klicken. Daraufhin startet der **Assistent für neue Website**. Beantworten Sie die vom Assistenten gestellten Fragen und in etwa zwei Minuten werden Sie eine neue Website haben.

Schließlich müssen Sie noch daran denken, dass es einen Unterschied zwischen einer Website und einem virtuellen Webverzeichnis gibt. Eine Website umfasst den eigentlichen Inhalt, der vom Basisverzeichnis oder einem anderen Verzeichnis aus Ihrer Website stammt, während ein virtuelles Verzeichnis einen Alias verwendet, um dem Webbenutzer vorzutäuschen, dass dieses virtuelle Verzeichnis aus der Verzeichnisstruktur derselben Website stammt.

Verwalten von virtuellen Servern

Virtuelle Server sind nichts anderes als virtuelle Verzeichnisse, die sowohl für Web- als auch für FTP-Sites erstellt werden können. Um zu klären, was ein virtuelles Verzeichnis genau ist, sollten Sie einfach eines erstellen. Gehen Sie dazu wie folgt vor:

1. Klicken Sie mit der rechten Maustaste auf eine Ihrer Web- oder FTP-Sites auf Ihrem IIS-Server. Klicken Sie in dem daraufhin erscheinenden Kontextmenü auf die Option **Neu**.
2. Klicken Sie in dem rechts neben dem Kontextmenü erscheinenden Menü auf die Option **Virtuelles Verzeichnis**. Daraufhin öffnet sich das Fenster des **Assistenten zum Erstellen virtueller Verzeichnisse** (siehe Abbildung 19.22).
3. Klicken Sie auf die Schaltfläche **Weiter**, um zu dem in Abbildung 19.23 dargestellten Fenster zu gelangen.
4. Nun müssen Sie einen Alias erstellen, anhand dessen die Benutzer Ihrer Web- bzw. FTP-Site Ihr neues virtuelles Verzeichnis finden können. Wenn Sie beispielsweise den Alias KaVpConsulting (und vorausgesetzt, der Computername des Windows 2000-Servers ist z.B. Vanessa) eingeben, dann verwendet der Endbenutzer den URL `http://vanessa/kavpconsulting/`, um auf dieses neue virtuelle Webverzeichnis zuzugreifen.



Abbildung 19.22: Starten des Assistenten zum Erstellen virtueller Verzeichnisse

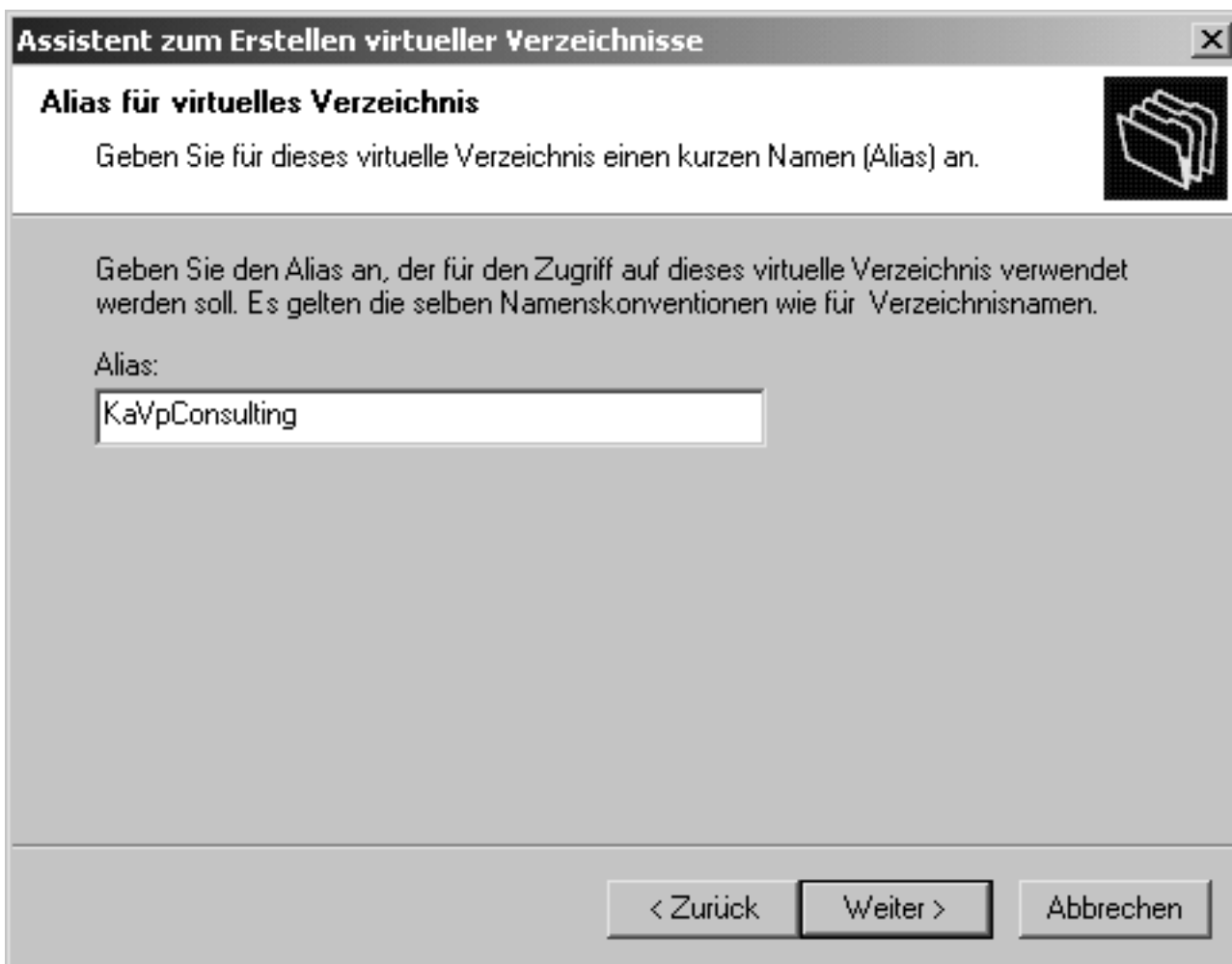


Abbildung 19.23: Erstellen des Alias für das virtuelle Verzeichnis

5. Wenn Sie Ihren neuen Alias eingegeben haben, klicken Sie auf die Schaltfläche **Weiter**, um das in Abbildung 19.24 dargestellte Fenster aufzurufen.

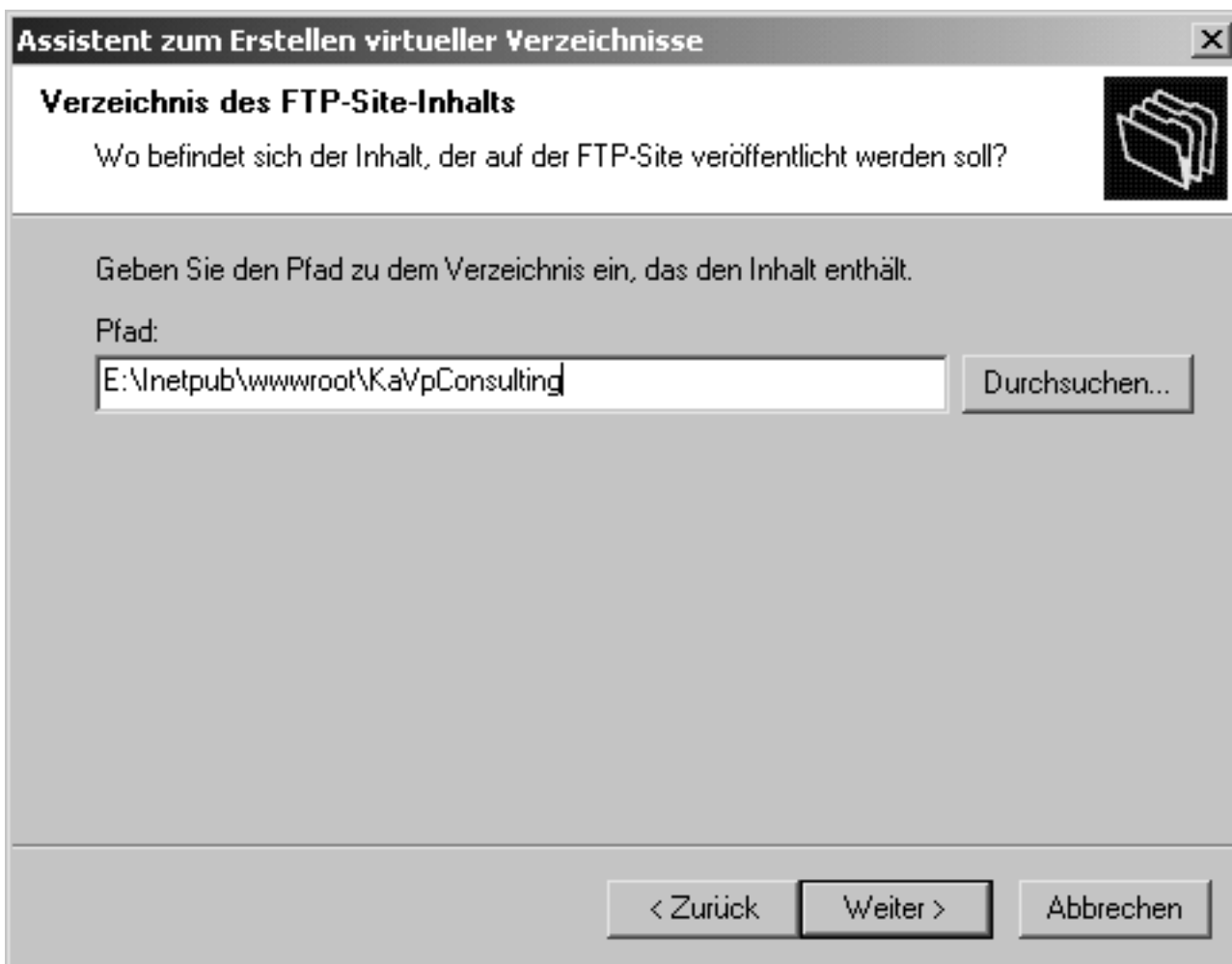


Abbildung 19.24: Erstellen des Verzeichnisses des FTP-Site-Inhalts

6. Nun, da Sie einen Alias für dieses neue virtuelle Verzeichnis haben, ist es an der Zeit festzulegen, von wo der Inhalt für diese neue Site bezogen werden soll. In der Regel speichern Sie den Inhalt für Ihr Webverzeichnis in derselben Ordnerstruktur wie Ihre anderen Websites. Nachdem Sie den Verzeichnispfad eingegeben haben, klicken Sie auf die Schaltfläche **Weiter**, um das in Abbildung 19.25 dargestellte Fenster aufzurufen.

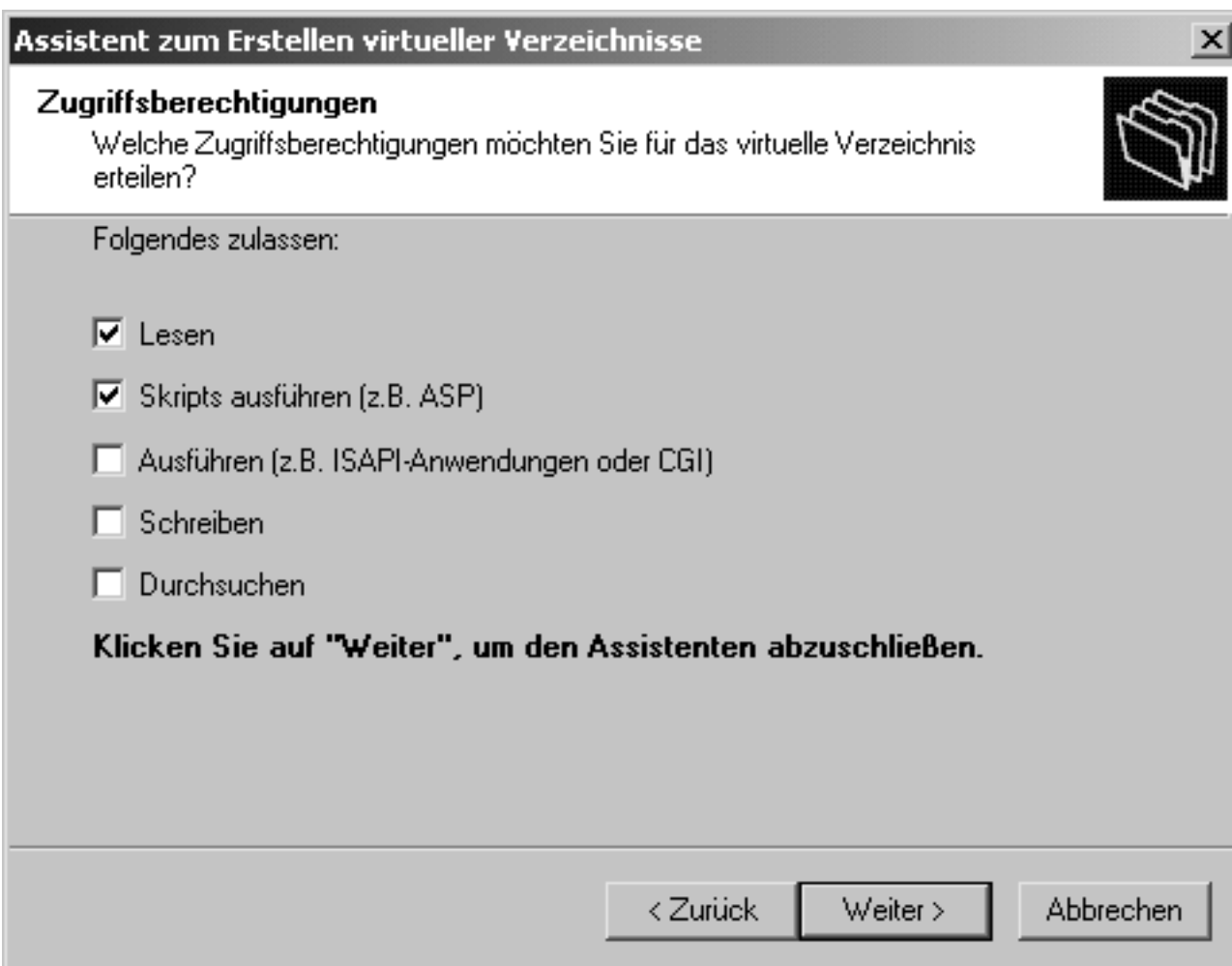


Abbildung 19.25: Festlegen von Zugriffsberechtigungen

7. Mit diesem Schritt werden die grundlegenden Berechtigungen festgelegt, die auf dieses neue virtuelle Verzeichnis angewendet werden. Im Abschnitt »Verwalten von Verzeichnissen« werden die einzelnen Optionen erläutert. Klicken Sie auf die Schaltfläche **Weiter**, um das abschließende Fenster des Assistenten aufzurufen.

8. Klicken Sie auf die Schaltfläche **Fertig stellen**. Daraufhin erscheint wieder das Fenster **Internet-Informationdienste**. Hier wird nun Ihr neues virtuelles Verzeichnis angezeigt (siehe Abbildung 19.26).

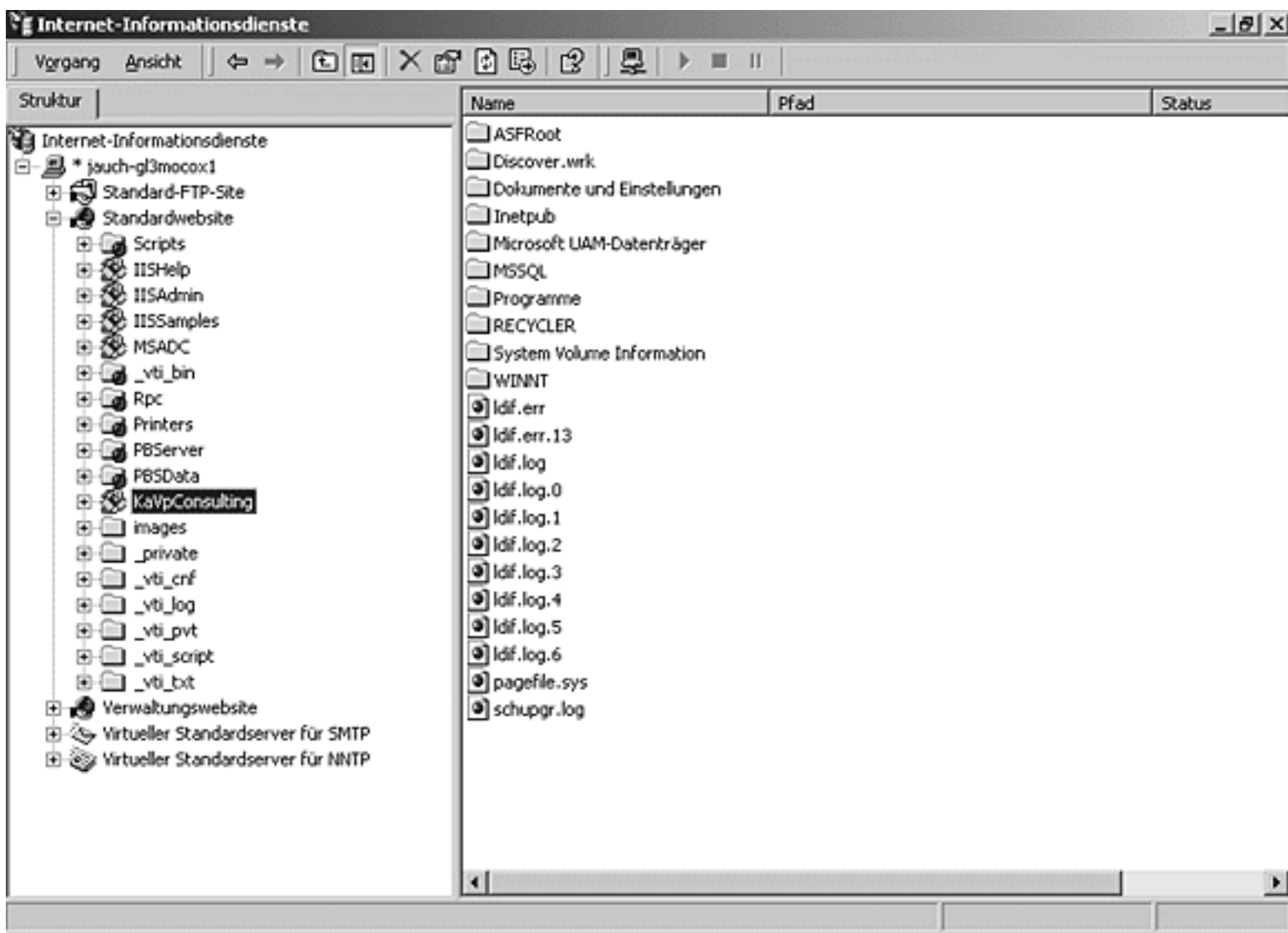


Abbildung 19.26: Das neu erstellte Verzeichnis im Fenster Internet-Informationssdienste

Wenn Ihr neues Verzeichnis nicht sofort erscheint, klicken Sie auf die Schaltfläche **Aktualisieren** (diese sieht aus wie ein kleines Stück Papier mit zwei kleinen kreisförmigen grünen Pfeilen darauf). Damit wird die Ansicht des Fensters **Internet-Informationssdienste** aktualisiert, woraufhin Ihr neu erstelltes virtuelles Verzeichnis angezeigt wird. Wenn Sie sich dieses Hauptfenster ansehen, sehen Sie, dass die virtuellen Verzeichnisse als Symbole dargestellt werden, die wie ein Ordner mit einem kleinen Globus in der Ecke aussehen (während das Symbol für eine Site wie ein Globus in einer ausgestreckten Hand aussieht). Sie werden nie eine Site innerhalb eines virtuellen Verzeichnisses sehen - nur umgekehrt.

Erweiterte Verwaltung

IIS 5.0 bietet Tausende Funktionen, von denen die meisten in diesem Kapitel nicht so ausführlich beschrieben werden können, wie sie es verdient hätten. Damit Sie jedoch nicht das Gefühl haben, etwas Wichtiges zu verpassen, sollen nun in diesem Abschnitt die erweiterten Funktionen von IIS 5.0 beschrieben werden, die nicht für die Verwendung durch die Allgemeinheit gedacht sind. Dazu gehört das Zusammenfassen von Site-Sockets ebenso wie Fragen bezüglich der Zugriffskontrolle und die Beschränkung der Anzahl gleichzeitiger Zugriffe.

Nähere Informationen über die unterschiedlichen Funktionen finden Sie im Windows 2000 Server

Resource Kit von Microsoft. Auch wenn die Abhandlungen über IIS 5.0 recht kurz sind, werden hier doch einige sehr technische Themen besprochen.

Zusammenfassen von Site-Sockets

Bei IIS 5.0 kann der Server-Administrator mehr als eine Website mit einem einzelnen IP-Adress-Socket verknüpfen. Dies stellt eine enorme Verbesserung gegenüber IIS 4.0 dar, denn bei dieser Version von IIS konnte eine Website einen IP-Socket nicht mit einer anderen Site gemeinsam nutzen. Das bedeutet, dass der Server-Administrator nicht ausgelagerten Speicher spart, da in der Vergangenheit jeder Socket diesen Speicher beanspruchte und ihn nicht mit anderen Sockets gemeinsam nutzen konnte. Bei der neuen Version von IIS können sämtliche Sites Sockets mit anderen gemeinsam nutzen. Das bedeutet, dass ein einzelner Webserver eine wesentlich größere Anzahl an zusätzlichen Websites verwalten kann als ein mit IIS 4.0 konfigurierter Server. Wenn Sie jedoch eine wichtige Website haben, die einen eigenen Socket erfordert, können Sie diese Funktion für das Zusammenfassen von Sockets bei Bedarf deaktivieren (Sie sollten dies dann auf der Ebene der Site und nicht auf globaler Ebene tun). Das Deaktivieren dieser Funktion kann jedoch leider nur mittels Skripten erfolgen, was bedeutet, dass es keine Möglichkeit gibt, diese Funktion über eine grafische Benutzeroberfläche zu deaktivieren.

Zugriffskontrolle

Zugriffskontrolle ist das Verfahren, mittels dessen Endbenutzern der Zugriff auf IIS-Ressourcen gewährt oder verweigert wird. Mit Hilfe der Zugriffskontrolle wird einem Endbenutzer die Berechtigung, auf Ihre vom IIS 5.0-Server zur Verfügung gestellten Web-, FTP-, SMTP- und NNTP-Sites zuzugreifen, gewährt oder verweigert. Es wird eine Zugriffskontroll- oder auch Zugriffssteuerungsliste (ACL) verwendet, um schnell festzustellen, welche Benutzer und/oder Gruppen auf ein Objekt innerhalb Ihrer IIS-Site zugreifen und/oder Änderungen vornehmen oder ein solches Objekt löschen dürfen.

Das Verfahren der Zugriffskontrolle ist nicht allzu kompliziert. Wenn jemand den Inhalt Ihrer Website einsehen oder nutzen möchte, führt der IIS-Server folgende Schritte aus:

1. Die IP-Adresse wird geprüft um zu sehen, ob sie für diese Website gültig ist. (Sie können den Zugriff für bestimmte IP-Adressen, Domänen oder DNS-Anfragen sperren.) Wenn der Benutzer hier erfolgreich ist, geht es mit dem nächsten Schritt weiter.
2. Die Zugriffsberechtigungen des Benutzers werden kontrolliert. Dabei werden ID und Kennwort des Benutzers geprüft. Wenn der Benutzer hier erfolgreich ist, geht es mit dem nächsten Schritt weiter.
3. Der Webserver bestätigt, dass die bei ihm festgelegten Berechtigungen den Zugriff auf die angeforderte(n) Ressource(n) zulassen. Wenn der Benutzer hier erfolgreich ist, geht es mit dem nächsten Schritt weiter.
4. Die NTFS 5.0-Berechtigungen werden daraufhin geprüft, ob der angestrebte Zugriff zulässig ist. Wenn die Berechtigungen gültig sind, wird dem Benutzer schließlich der Zugriff auf die gewünschte(n) Ressource(n) gewährt.

Wenn während dieses Vorgangs der Zugriff an einer Stelle verweigert wird, erscheint eine Fehlermeldung und dem Benutzer wird der Zugriff auf die Ressource verweigert. Darüber hinaus wird der Versuch des Benutzers in den Protokolldateien von IIS aufgezeichnet (vorausgesetzt, die Protokollierungsfunktionen sind aktiviert). Wenn ein Benutzer während der ersten drei Schritte abgewiesen wird, erscheint die Fehlermeldung 403 - Access Forbidden (Zugriff verboten) auf dem

Bildschirm des Benutzers. Wenn der Benutzer während des letzten Schrittes abgewiesen wird, erscheint die Fehlermeldung 401 - Access Denied (Zugriff verweigert) auf dem Bildschirm des Benutzers.

Ein weiterer Aspekt des Zugriffskontrollmechanismus ist die Authentifizierung. Mit Hilfe der *Authentifizierung* weisen Endbenutzer nach, dass sie über gültige Windows-Benutzerkonten und Kennwörter verfügen, um auf die gewünschten Ressourcen zuzugreifen. Es gibt mehrere Arten der Authentifizierung für Websites, aber nur zwei Arten der Authentifizierung für FTP-Sites. Entscheiden Sie anhand der folgenden Beschreibung, welches Verfahren für Ihre Organisation am besten geeignet ist:

Authentifizierungsmethoden für Websites

- **Anonyme Authentifizierung** - Benutzer können auf Ihre Website zugreifen, ohne anhand von Benutzernamen und Kennwort nachweisen zu müssen, dass sie berechtigte Benutzer Ihrer Website sind. Wenn jemand versucht, mit dieser Art der Authentifizierung auf den Webserver zuzugreifen, wird dieser Benutzer dem Windows-Benutzerkonto `IUSR_computername` zugewiesen, wobei *computername* in der Regel der Name des Servers ist, auf dem IIS 5.0 installiert ist.
- **Standardauthentifizierung** - Diese Methode der Authentifizierung ist eine Industriestandard entsprechende Methode für Webbrowser-basierte Authentifizierung bei einer Website, obwohl es sich gleichzeitig um die am wenigsten sichere Authentifizierungsmethode für den Zugriff auf Ressourcen auf Ihrem IIS-Server handelt. Bei der Standardauthentifizierung gibt ein Endbenutzer seinen Windows 2000 Server-Benutzernamen und sein Kennwort in das Anmeldefeld ein, das erscheint, wenn er auf Ihre Website zuzugreifen versucht. Diese Benutzerkennung wird in Klartext und das Kennwort mit einer Base64-Kodierung an den Webserver zur Authentifizierung gesendet. Wenn Sie die Möglichkeit haben, zwischen verschiedenen Authentifizierungsmethoden zu wählen, dann sollten Sie sich aus Gründen der Sicherheit niemals für diese Art der Authentifizierung entscheiden.
- **Digestauthentifizierung** - Diese Windows 2000-Version der Standardauthentifizierung sorgt dafür, dass die Anmeldeinformationen nicht so leicht entschlüsselt werden, wie das bei der Standardauthentifizierung der Fall ist. Dies wird durch einen nicht umkehrbaren Prozess erreicht, der häufig als *Hashing* bezeichnet wird. Die Digestauthentifizierung kann nur bei Windows 2000-Domänencontrollern in einer Windows 2000-Domäne verwendet werden.
- **Integrierte Windows-Authentifizierung** - Diese alte NTLM oder Authentifizierung mittels Windows NT-Herausforderung/Rückmeldung ist mit den in Windows 2000 integrierten Verschlüsselungstechnologien der Kerberos-Version 5.0 auf den neuesten Stand gebracht worden. (NTLM steht für NT LAN-Manager. Dabei handelt es sich um die ursprüngliche Form der Authentifizierung, die bei einem Windows NT-Server möglich ist. Diese Art der Authentifizierung kommt aus der Zeit von Windows NT 3.1.) Um diese Authentifizierungsmethode anwenden zu können, müssen sowohl der Client als auch der IIS-Server über vertraute Verbindungen zu einem KDC (Key Distribution Center) verfügen und mit den Verzeichnisdiensten kompatibel sein. Das bedeutet, dass Sie den vollen Einsatz von Windows 2000-Servern und zumindest einen teilweisen Einsatz des Active Directory mit mindestens einem KDC, einem globalen Katalog und einer Active Directory-Struktur (oder einer Active Directory-Gesamtstruktur) haben müssen.
- **Zertifikatauthentifizierung** - Hierbei handelt es sich um die Methode, bei der Clients über die SSL-Technologie (Secured Sockets Layer) für den Zugriff auf die Website authentifiziert werden. Die Authentifizierung erfolgt über eine verschlüsselte digitale 40-Bit-Identifizierung.

Authentifizierungsmethoden für FTP-Sites

- Anonyme FTP-Authentifizierung - Benutzer können auf die FTP-Site zugreifen, ohne anhand von Benutzernamen und Kennwort nachweisen zu müssen, dass sie berechtigte Benutzer der FTP-Site sind. Wenn jemand versucht, mit dieser Art der Authentifizierung auf den FTP-Server zuzugreifen, wird dieser Benutzer dem Windows-Benutzerkonto **IUSR_computername** zugewiesen, wobei *computername* in der Regel der Name des Servers ist, auf dem IIS 5.0 installiert ist. Diese Art der Authentifizierung funktioniert genau so wie die Web-Version der anonymen Authentifizierung.
- FTP-Standardauthentifizierung - Hierbei handelt es sich um die Klartextversion der Authentifizierung für FTP-Sites. Das bedeutet, dass ein Endbenutzer seinen Windows 2000 Server-Benutzernamen sowie sein Kennwort verwendet, um auf die FTP-Site zuzugreifen. Wenn Sie die Möglichkeit haben, zwischen verschiedenen Authentifizierungsmethoden zu wählen, dann sollten Sie sich aus Gründen der Sicherheit niemals für diese Art der Authentifizierung entscheiden, da Ihre Endbenutzer damit ihre ansonsten sicheren Windows 2000 Server-Benutzernamen und Kennwörter in Klartext und somit in einer für Sniffer lesbaren Form versenden.

Einschränken gleichzeitiger Verbindungen

Um einer Überlastung der Web- oder FTP-Site(s) Ihrer Organisation vorzubeugen, können Sie die Anzahl der gleichzeitigen Verbindungen zu diesen FTP- und/oder Websites einschränken. Rufen Sie dazu das Fenster **Internet-Informationdienste** auf, indem Sie auf **Start, Programme, Verwaltung** und schließlich auf **Internetdienste-Manager** klicken. Klicken Sie anschließend mit der rechten Maustaste auf das Symbol **Standardwebsite** (oder **Standard-FTP-Site**). Klicken Sie in dem daraufhin erscheinenden Menü unten auf **Eigenschaften**. Nun öffnet sich das Dialogfeld **Eigenschaften von Standardwebsite**, wobei die Registerkarte **Website** automatisch aktiviert ist (siehe Abbildung 19.27).

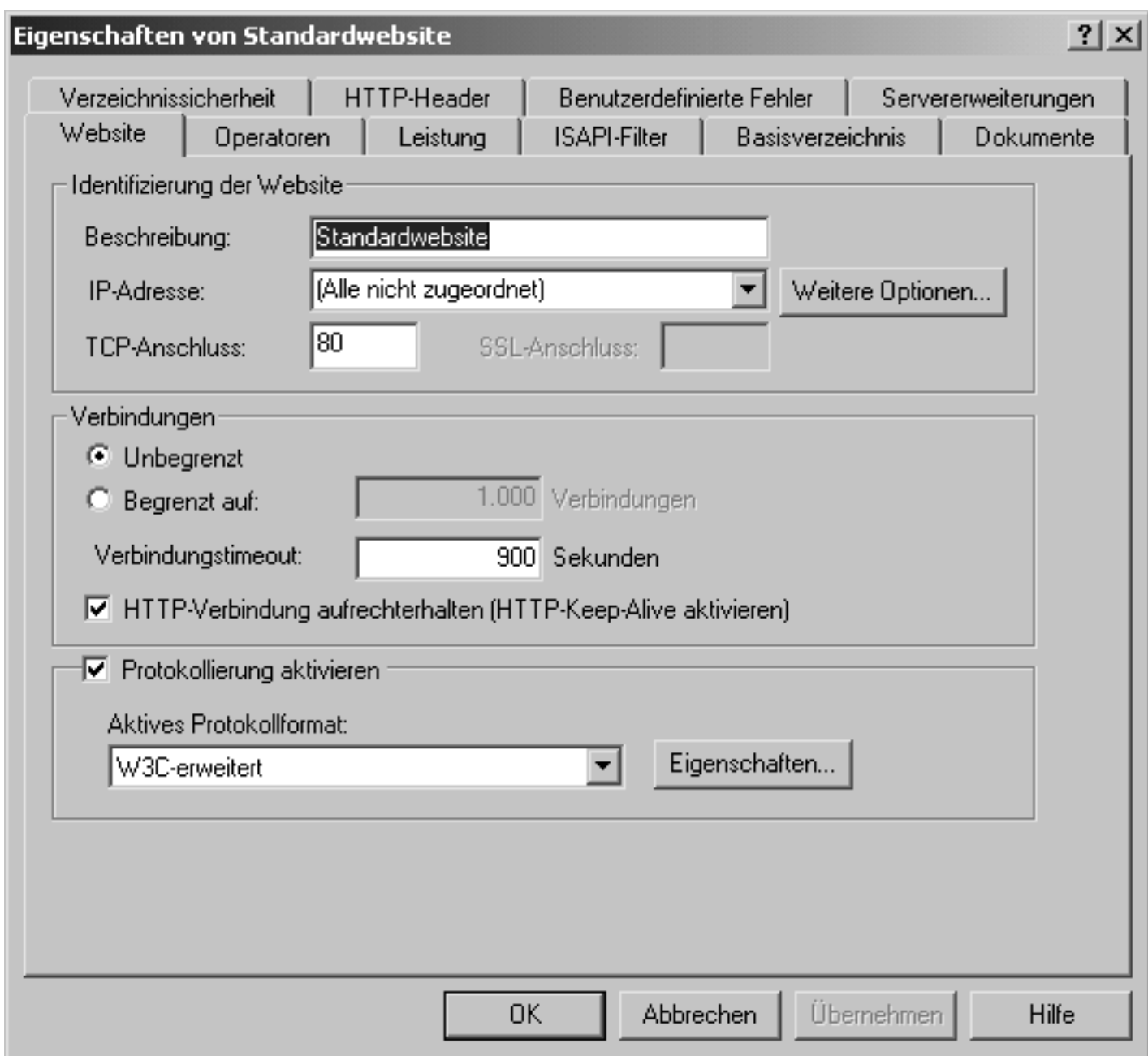


Abbildung 19.27: Websiteeigenschaften der Standardwebsite

Etwa in der Mitte dieses Dialogfeldes befindet sich der Bereich **Verbindungen**. Hier können Sie die Anzahl der gleichzeitigen Verbindungen einschränken, indem Sie eine maximale Anzahl an Verbindungen zu Ihrer Website eingeben. (Für die FTP-Site gibt es genau dieselbe Registerkarte im Dialogfeld **Standard-FTP-Site**.) Standardmäßig ist die Option **Unbegrenzt** aktiviert. Um dies zu ändern, klicken Sie in das Optionsfeld **Begrenzt auf** und geben eine Zahl ein, von der Sie meinen, dass diese die geeignete Anzahl darstellt. Wenn es sich beispielsweise um eine private Website handelt und Ihr Unternehmen nur 200 Angestellte hat, dann sollten Sie die Zahl 200 eingeben. Ihre Organisation sollte die Anzahl der Verbindungen für jede ihrer Web- und FTP-Sites festlegen, auch wenn die IT-Gruppe je nach Hardware, die für die Unterstützung dieser Web- und FTP-Server verwendet wird, wahrscheinlich einige Möglichkeiten hat. Nachdem Sie die gewünschten Einstellungen vorgenommen haben, klicken Sie auf **OK**, um diese zu bestätigen und zum Fenster **Internet-Informationdienste** zurückzukehren.

19.4.2 Verwalten der FTP-Site

Die FTP-Site (File Transfer Protocol) basiert ebenso wie die Webdienste und Telnet auf dem Netzwerkprotokoll TCP/IP. FTP dient dazu, Dateien von und zu nicht lokalen Computersystemen zu übertragen. Bei diesen Computersystemen kann es sich sowohl um Windows NT- oder um Windows 2000-Computer als auch um UNIX-, Macintosh- und NetWare-Computer handeln. Es gibt natürlich andere, effektivere Möglichkeiten, Dateien zwischen Windows-basierten Computern sowie zwischen NetWare-Systemen zu übertragen, aber das ist hier nicht der Punkt. Darüber hinaus ist es möglich, mittels FTP-Befehlen Datei- und Verzeichnislisten von diesen entfernten Computern zu erhalten, was (aus der Sicht des Windows-Clients) sehr hilfreich ist, wenn Sie mit UNIX-Systemen in einer Nicht-NTFS-Umgebung (Network File System) arbeiten.

Der größte Teil der Konfiguration von FTP-Sites wurde in diesem Kapitel bereits erläutert, da die Fenster für die Konfiguration und Verwaltung der FTP-Dienste genau so funktionieren wie die der meisten der von IIS 5.0 zur Verfügung gestellten Webdienste.

Konfigurieren von FTP-Meldungen

Um eine Begrüßungs- oder Beendigungsmeldung für Ihren FTP-Server hinzuzufügen, zu ändern oder zu löschen, klicken Sie auf **Start, Programme, Verwaltung** und schließlich auf **Internetdienste-Manager**. Klicken Sie anschließend mit der rechten Maustaste auf das Symbol **Standard-FTP-Site**. Klicken Sie in dem daraufhin erscheinenden Menü fast ganz unten auf **Eigenschaften**. Nun öffnet sich das Dialogfeld **Eigenschaften von Standard-FTP-Site**. Aktivieren Sie hier die Registerkarte **Meldungen** (siehe Abbildung 19.28).

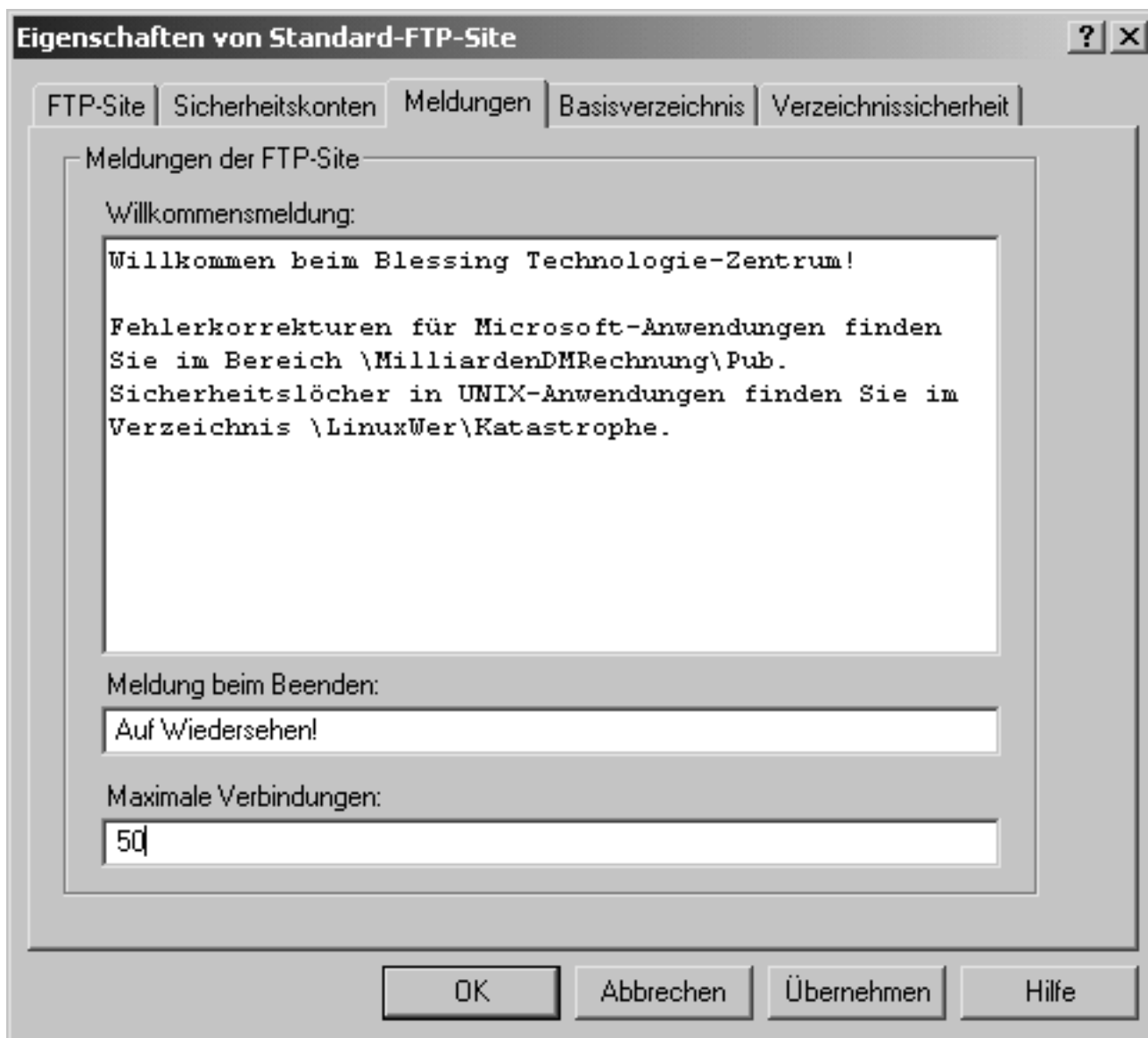


Abbildung 19.28: Festlegen der Begrüßungsmeldung für Ihre FTP-Site

Auf der Registerkarte **Meldungen** können Sie sowohl eine textbasierte Begrüßungs- als auch eine textbasierte Beendigungsmeldung konfigurieren, die die Benutzer sehen, wenn sie auf Ihre FTP-Site zugreifen bzw. die Sitzung beenden. Die Meldungen können nur im Textformat verfasst (ein Nachteil, der jedoch die Abwärtskompatibilität für DOS, UNIX, NetWare, OS/2 und andere Nicht-Windows-Clients und -Server ermöglicht) und sollten möglichst kurz gehalten werden. Wenn die Meldungen zu lang sind, werden die Benutzer nur verwirrt, da die Meldungen auf dem Bildschirm rasch vorüberziehen und es keine Möglichkeit gibt, diese anzuhalten. Die andere Option, die Sie sich etwas näher anschauen sollten, ist die unterste Option, die Ihnen die Möglichkeit gibt, die Anzahl der Benutzer zu begrenzen, die gleichzeitig auf Ihre FTP-Site zugreifen können. Geben Sie eine Zahl ein, die Ihnen sinnvoll erscheint (oder lassen Sie das Textfeld leer). Klicken Sie auf die Schaltfläche **OK**, um die Einstellungen zu bestätigen und zu sichern. Daraufhin erscheint wieder das Fenster **Internet-Informationdienste**.

19.4.3 Erweiterte Verwaltung der Website

Der WWW-Site-Dienst ist der wichtigste Bereich von IIS, der in das Betriebssystem Windows 2000 Server integriert ist. Dieser Webdienst hat eine weite Wegstrecke zurückgelegt, denn die erste Version von IIS unterstützte nicht einmal ASP (Active Server Pages), geschweige denn die neuen Tools für die Remoteverwaltung und die Funktionen für die sichere Authentifizierung. Die Websites, sowohl die realen als auch die virtuellen Verzeichnisse, werden über den Internetdienste-Manager verwaltet, den Sie über die Option **Verwaltung** aufrufen. Wenn Sie den Internetdienste-Manager aufrufen, öffnet sich das Fenster **Internet-Informationdienste**.

Eine allgemein nicht so bekannte Tatsache ist, dass bei der Installation von IIS automatisch eine beliebige Anschlussnummer zwischen 2000 und 9999 gewählt wird, die als Standardanschluss für die Verwaltungswebsite Ihrer Organisation dient. Dies ist wichtig für die allgemeine Sicherheit Ihrer IIS-Installation, da es dadurch für Unbefugte um so schwieriger herauszufinden wird, an welchem Anschluss sich Ihre Verwaltungswebsite befindet. (Ja, es ist möglich, dies mit Hilfe von Anschluss-Scannern herauszufinden. Die anderen in Ihrer Organisation für die Netzwerksicherheit verantwortlichen Tools sollten jedoch feststellen können, wer in Ihrem Netzwerk einen Anschluss-Scanner auf welchen Server ansetzt.) Um beispielsweise die Web-basierte Version der Verwaltungswebsite aufzurufen, müssen Sie den vollständigen URL für die Website Ihres Servers wie im folgenden Beispiel eingeben:

`http://localhost:2047/iis.asp`

Damit Sie über Ihren Webbrowser (Internet Explorer 5.0 ist der bevorzugte Webbrowser, da dies der Browser ist, der mit Windows 2000 Server ausgeliefert wird) auf die Verwaltungswebsite zugreifen können, müssen Sie die richtige Anschlussnummer für die Verwaltungswebsite Ihrer Organisation eingeben. Wenn Sie diese Nummer nicht kennen, geht der IIS-Server davon aus, dass Sie nicht berechtigt sind, auf diese Informationen zuzugreifen, und verweigert Ihnen somit die Remoteverwaltung dieser Site. Die Anschlussnummer ist der Teil der Webadresse direkt rechts neben dem Localhost oder dem Namen Ihres Computers. Sie ist am Doppelpunkt zu erkennen und besteht aus vier Ziffern. Wenn Sie versucht haben, Ihre Website ohne diese Anschlussnummer remote zu verwalten, werden Sie wohl ein Fenster wie das in Abbildung 19.29 dargestellte gesehen haben.

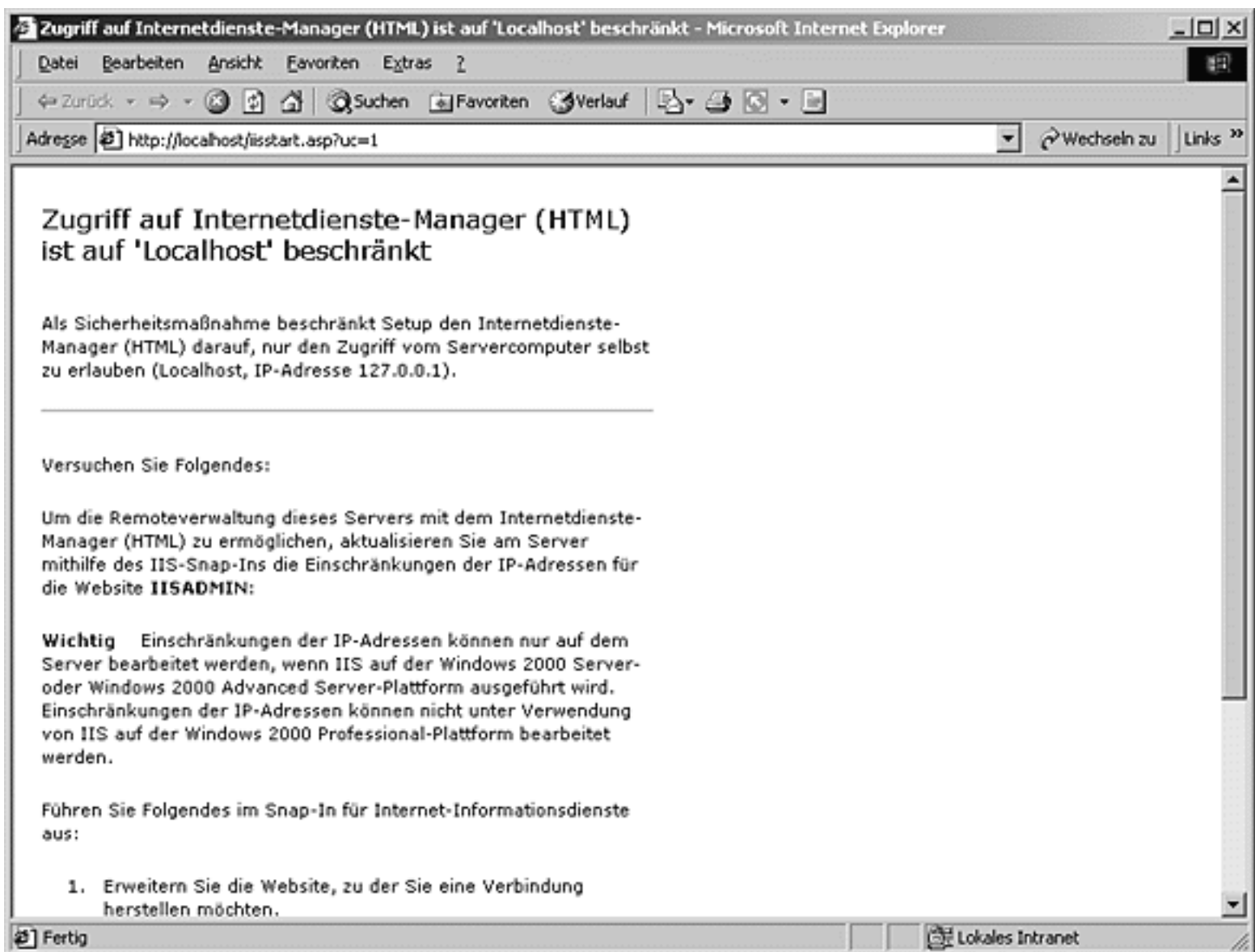


Abbildung 19.29: Fehlermeldung beim Versuch der Remoteverwaltung ohne Anschlussnummer

Denken Sie daran, dass nur Benutzer, die Mitglied der Gruppe der Windows 2000-Administratoren sind, auf die Verwaltungswebsite zugreifen dürfen. Jedem anderen wird der Zugriff verweigert.

Wahl einer Standard-Homepage

Wenn der IIS-Dienst installiert wird, wird nicht automatisch eine Standard-Homepage festgelegt, nicht einmal für die Standardwebsite. Wenn also ein Benutzer versucht, auf Ihre Standardwebsite zuzugreifen, erscheint eine Meldung wie die in Abbildung 19.30.

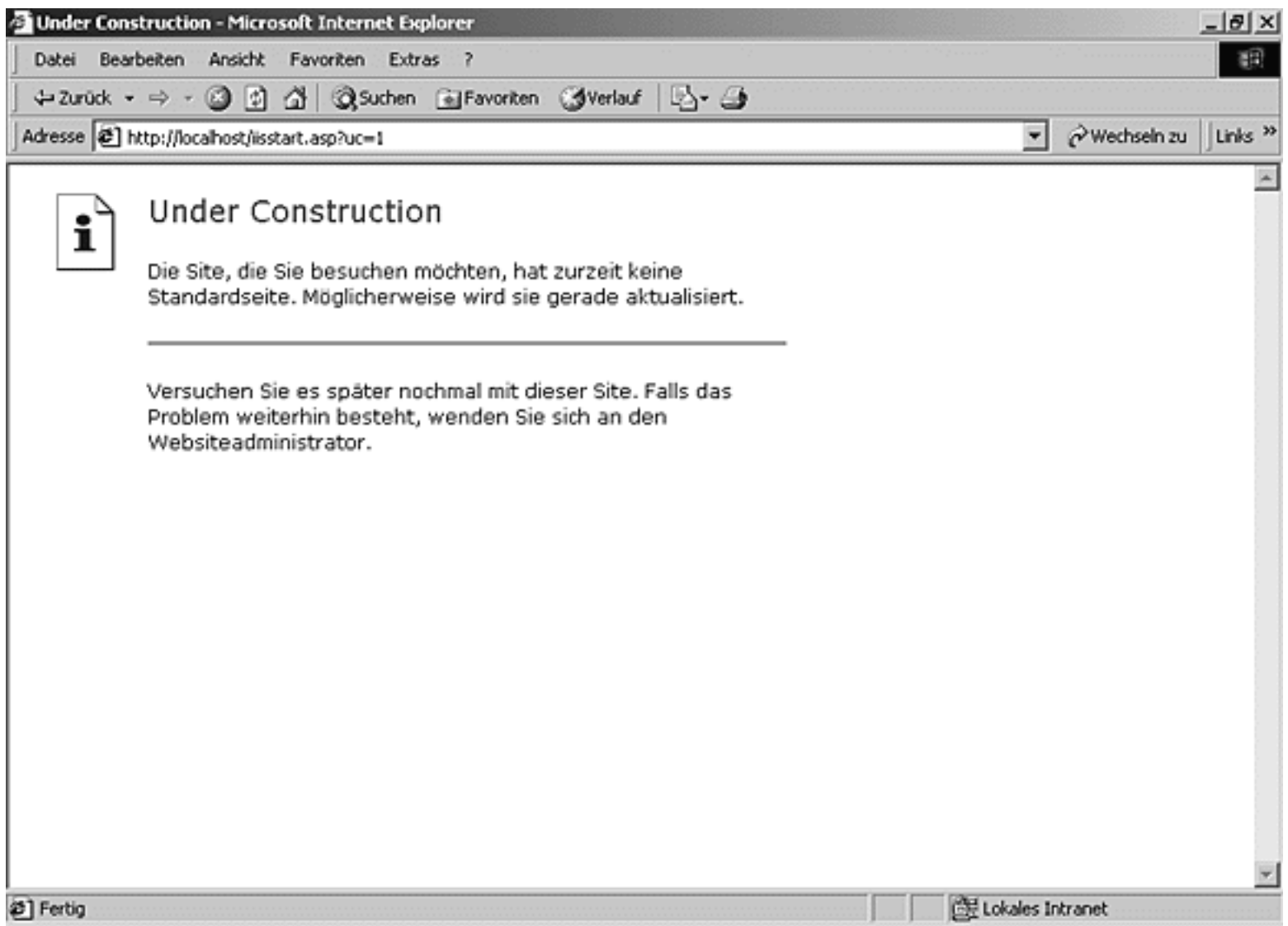


Abbildung 19.30: Das sehen Sie, wenn es keine Standard-Homepage gibt

Um eine Standard-Homepage zu definieren, klicken Sie auf **Start, Programme, Verwaltung** und schließlich auf **Internetdienste-Manager**. Klicken Sie dann mit der rechten Maustaste auf das Symbol **Standardwebsite**. Klicken Sie in dem daraufhin erscheinenden Menü fast ganz unten auf **Eigenschaften**. Nun öffnet sich das Dialogfeld **Eigenschaften von Standardwebsite**, wobei zunächst die Registerkarte **Website** aktiviert ist. Klicken Sie nun auf die Registerkarte **Dokumente** (siehe Abbildung 19.31).

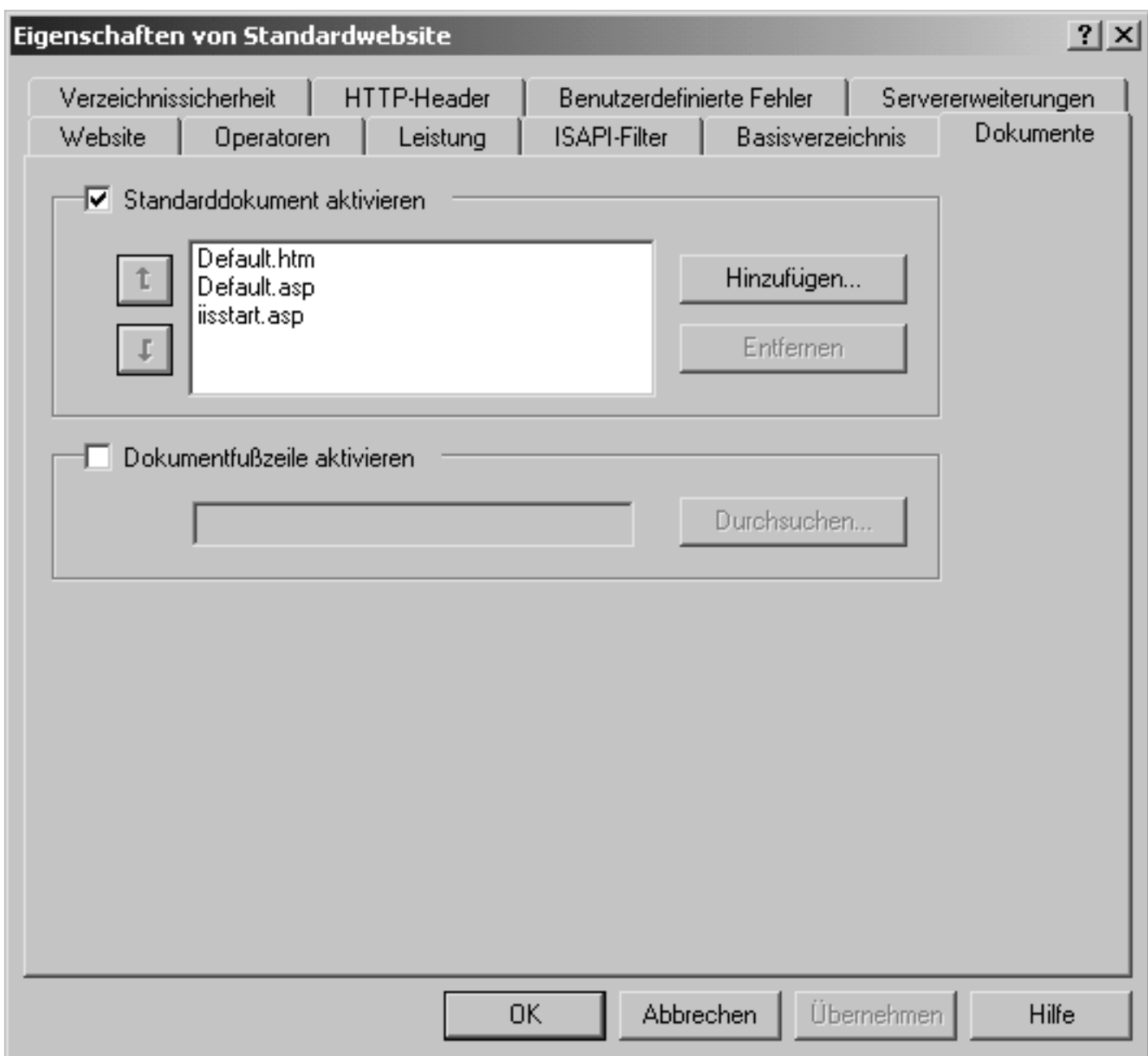


Abbildung 19.31: Aktivieren eines Standarddokumenttyps

Um eine Standard-Homepage zu definieren, wählen Sie oben auf der Registerkarte das Kontrollkästchen **Standarddokument aktivieren**. Sie können die Reihenfolge der Dokumenttypen (*Default.htm*, *Default.asp* und *iisstart.asp*) ändern, indem Sie einen davon durch Anklicken markieren und dann entweder auf die Schaltfläche mit dem nach oben oder mit dem nach unten zeigenden Pfeil klicken, um das Standarddokument in der Liste nach oben oder unten zu verschieben. Nachdem Sie die gewünschten Einstellungen vorgenommen haben, klicken Sie auf die Schaltfläche **OK**, um diese zu bestätigen und zum vorhergehenden Fenster zurückzukehren.

Wenn Sie diese Einstellungen bereits vorgenommen haben und immer noch keine Standardseite erscheint, wenn Sie auf Ihre Standard-Website zugreifen, dann kann dies daran liegen, dass es die physikalische Datei (*Default.htm*, *Default.asp* oder *iisstart.asp*) im Dateiordner Ihrer Webseite nicht gibt. Um dies zu prüfen, öffnen Sie diesen Ordner (wahrscheinlich `\inetpub\wwwroot`) und sehen nach, ob es hier eine dieser Dateien gibt. Wenn nicht, dann erstellen Sie eine und stellen sicher, dass Sie den Inhalt

für diese eine Datei richtig erstellt haben. Wie Sie dabei vorgehen, erfahren Sie in der Dokumentation zu Ihrem Web-Dokumenterstellungstool (wie z.B. Microsoft FrontPage 2000 oder Dreamweaver).

WebDAV (Web Distributed Authoring and Versioning)

WebDAV ist eine neue Technologie. Mit Hilfe von WebDAV können Web-Clients folgende Aufgaben auf dem IIS 5.0-Server ausführen:

- Manipulieren von Ressourcen - Benutzer können mit den entsprechenden Berechtigungen Ressourcen innerhalb eines WebDAV-Verzeichnisses kopieren und/oder verschieben.
- Ändern der Ressourceneigenschaften - Web-Benutzer können die Eigenschaften von Web-Ressourcen ändern, vorausgesetzt, sie verfügen über die entsprechenden Berechtigungen.
- Sichern von Ressourcen - Mehrere Benutzer können Ressourcen im Betrieb sperren oder die Sperrung aufheben, sodass viele Leute die Datei gleichzeitig lesen können, aber nur eine einzige Person Schreibzugriff auf die Datei hat.
- Durchsuchen - Benutzer können den Inhalt und die Eigenschaften ihrer Dateien innerhalb eines WebDAV-Verzeichnisses durchsuchen.

Das WebDAV-Veröffentlichungsverzeichnis zu konfigurieren, ist wesentlich einfacher, als Sie vielleicht denken. Sie müssen lediglich ein virtuelles WebDAV-Verzeichnis erstellen. Dazu gehen Sie wie folgt vor:

1. Erstellen Sie innerhalb des Ordners `\inetpub\wwwroot` einen physikalischen Ordner mit einem Namen wie z.B. WebDAV (in diesem Fall würde der vollständige Pfad `\inetpub\wwwroot\WebDAV` lauten).
2. Starten Sie den **Assistenten zum Erstellen virtueller Verzeichnisse** und geben Sie den Namen *WebDAV* als Alias ein. Wenn Sie sich nicht mehr sicher sind, wie Sie diesen Assistenten aufrufen, sehen Sie im Abschnitt über die Verwaltung virtueller Server nach.
3. Erteilen Sie die Berechtigungen Lesen, Schreiben und Durchsuchen, indem Sie in die Kontrollkästchen neben diesen Optionen klicken.
4. Nur wenn Sie die Berechtigung zum Ändern der Active Server Pages oder anderer skriptbasierter Dateien erteilen möchten, müssen Sie diesen letzten Schritt ausführen. Gewähren Sie Ihrem neu erstellten virtuellen *WebDAV*-Verzeichnis über die Registerkarte **Virtuelles Verzeichnis** im Dialogfeld **Eigenschaften von WebDAV** Zugriff auf die Skriptdatei.

Das ist alles, was Sie tun müssen, um Ihren Server für die WebDAV-Veröffentlichung zu konfigurieren. Es ist natürlich möglich, dass Sie Ihre gesamte Website als einen riesigen WebDAV-Prozess konfigurieren. Hinsichtlich der Sicherheit ist das jedoch nicht empfehlenswert. Wenn Ihre Organisation nicht sehr groß, vielleicht eine kleine Bildungseinrichtung oder eine gemeinnützige Organisation ist, dann können Sie in Erwägung ziehen, WebDAV in Ihrer gesamten Organisation zu verwenden.

19.4.4 Verwalten der Gopher-Site

Leider ist die textbasierte Datenbanktechnologie Gopher mit ihrer Suchfunktion VERONICA nicht mehr Bestandteil der IIS-Technologie von Microsoft. Für viele neue Benutzer im Internet ist das wohl kaum ein großer Verlust. Aber diejenigen, die schon die letzten zehn Jahre im Internet gesurft haben, ist es entmutigend zu sehen, wie einer der Gründer des Internet so schnell von der Bildfläche verschwindet.

19.4.5 Verwalten des Telnet-Dienstes

Der Telnet-Dienst ist eigentlich nicht Teil der IIS-Technologie. Aus rein technischer Sicht ist das WWW eine Art »Reiter« auf dem Rücken der Telnet-Technologie. Der Serverdienst ist jedoch nicht selbst in IIS integriert. Um entweder die Version mit der grafischen Benutzeroberfläche oder die befehlszeilenbasierte Version des Telnet-Dienstes mit einem Windows 2000-Server zu nutzen, klicken Sie einfach in Windows 2000 Server auf **Start** und dann auf **Ausführen**. Der Telnet-Dienst für Windows 2000 Server besteht nur aus wenigen Dateien:

- *telnet.chm* - Diese Datei befindet sich im Ordner %systemroot%\Help. Dabei handelt es sich um die kompilierte Hilfedatei mit grafischer Benutzeroberfläche für den Telnet-Dienst.
- *telnet.hlp* - Diese Datei befindet sich im Ordner %systemroot%\Help. Sie wird im Zusammenhang mit den befehlszeilenbasierten Telnet-Diensten verwendet.
- *telnet.exe* - Diese Datei befindet sich im Ordner %systemroot%\System32. Dabei handelt es sich um die befehlszeilenbasierte Telnet-Clientanwendung.
- *telnetc.exe* - Diese Datei befindet sich im Ordner %systemroot%\System32. Dabei handelt es sich um die Telnet-Clientanwendung mit grafischer Benutzeroberfläche.

19.4.6 Erweiterte Sicherheitskonzepte

Einen IIS-Server vor ungewollten und unbefugten Benutzern vollständig zu schützen, ist eine der schwierigsten, wenn nicht gänzlich unmöglichen Aufgaben. Um Ihre Web- und FTP-Serverdienste jedoch vor der großen Mehrzahl derjenigen im Internet zu schützen, die möglicherweise versuchen, Ihnen Schaden zuzufügen, ist nicht so schwierig, wie Sie es sich vielleicht vorstellen. Wie bei allem anderen im Computerbereich ist es ein schmaler Grad zwischen dem Sicherstellen, dass die Benutzer genügend Zugriffsrechte haben, und dem Sicherstellen, dass unbefugte Personen und Programme keinen Zugriff erlangen.

Zunächst einmal ein bisschen Terminologie. Die nicht befugten Personen, die möglicherweise Zugriff auf die Dienste Ihres IIS-Servers haben möchten, lassen sich in drei Hauptgruppen unterteilen:

- Script Kiddies - Dabei handelt es sich um Jugendliche, die denken, dass sie etwas Besseres sind, wenn sie in eine Website eindringen, einfach nur weil sie es geschafft haben, oder aber um ein paar unverschämte, derbe Sprüche und/oder pornografische Bilder auf Ihrer Website zu hinterlassen. Diese Jugendlichen werden als Script Kiddies bezeichnet, da sie bezüglich Netzwerk oder Programmieren keine echten Kenntnisse haben und nur das (üblicherweise mit einer grafischen Benutzeroberfläche ausgestattete) Hacker-Tool von jemand anderem verwenden, um sich unbefugten Zugriff auf Ihre Website zu verschaffen. Das Ergebnis? Wenn Sie sich bei der Konfiguration Ihrer Web- und FTP-Sites nur ein wenig Zeit nehmen, können Sie die große Mehrheit dieser Angriffe auf Ihre Organisation abwehren.
- Hacker - Ein Hacker ist jemand, der die Netzwerk- und Programmierfertigkeiten besitzt, um illegal in die Site Ihrer Organisation einzudringen. Hacker arbeiten häufig allein und sehen ihre Arbeit als eine Herausforderung. Es kommt sehr selten vor, dass ein Hacker wirklich Schaden an Ihrer Site anrichtet, wobei die Platzierung von pornografischem Material auf einer ansonsten normalen Geschäftssite jedoch einen beträchtlichen Schaden im öffentlichen Erscheinungsbild eines Unternehmens anrichten kann. Gehen Sie niemals davon aus, dass Ihre Organisation so

uninteressant ist, dass es sich für niemanden lohnt, hier einzudringen, denn es gibt so viele Hacker, dass es jeden einmal treffen kann.

- Cracker - Ein Cracker ist jemand, der über die Fertigkeiten eines Hackers verfügt und diese in böswilliger Absicht missbraucht. Cracker versuchen (und häufig mit Erfolg) nicht nur in Web- und FTP-Sites einzudringen, sondern sie tun das mit der Absicht, Ihnen Schaden zuzufügen. Häufig gibt sich ein Cracker damit zufrieden, wenn es ihm gelingt, allen ansonsten autorisierten Benutzern den Zugriff auf Ihre Sites zu verweigern. Diese Art des Angriffs wird als Denial-of-Service-Attacke bezeichnet. Leider handelt es sich dabei um eine relativ einfache und effektive Art des Angriffs gegen einen Windows NT- bzw. Windows 2000-Server. Cracker können das, was sie tun, sehr gut, und sind häufig auch bereit, ihre Arbeit gegen Bezahlung zu tun. (Möglicherweise hat Ihre Organisation einen äußerst skrupellosen Konkurrenten, der vielleicht ein paar Cracker dafür bezahlt, Ihr Internet-Geschäft zu ruinieren?) Sie sollten also besondere Vorsichtsmaßnahmen gegen Personen dieser Art ergreifen.

Es gibt einige einfache Dinge, die Sie tun können, um sich selbst vor Script Kiddies und manchen Hackern und Crackern zu schützen:

- Überwachen Sie Ihre IIS-Server. - Aktivieren Sie die umfassenden Überwachungsfunktionen von IIS. Dabei sollten sowohl alle erfolgreichen als auch alle fehlgeschlagenen Anmeldeversuche, sämtliche fehlgeschlagenen Versuche, unerlaubt auf Inhalt und/oder Ressourcen zuzugreifen, sowie sämtliche Versuche von nicht autorisierten Personen, Programme oder eingeschränkte Befehle auszuführen, aufgezeichnet werden.
- Schränken Sie die Verwendung von Domänencontrollern ein. - Surfen Sie niemals mit einem Windows 2000 Server-Domänencontroller, mit einem globalen Katalog oder mit einem KDC im Internet. Damit würden Sie Ihre wichtigsten Server grundlos den Gefahren des Internet preisgeben. Außerdem sollten Sie die IIS-Software niemals auf einem Domänencontroller, KDC oder globalen Katalog installieren, da dies nicht nur negative Auswirkungen auf die Reaktionszeit Ihrer Benutzer hat, sondern Sie auch unnötigerweise dem Internet aussetzt.
- Verwenden Sie Antiviren-Software. - Diesen Rat kann ich nicht oft genug geben. Führen Sie immer auf allen Servern sowie auf den Computern Ihrer Endbenutzer Antiviren-Software aus. Unglaublich viele Unternehmen setzen die Software nur entweder auf Seiten des Servers oder auf Seiten des Client ein.
- Verwenden Sie die sicherste mögliche Form der Authentifizierung. - Wenn Ihre Web- und FTP-Sites nur den internen Benutzern zur Verfügung stehen, wie das bei einem Intranet der Fall ist, dann sollten Sie keinen anonymen Zugriff zulassen und ausschließlich eine sichere Authentifizierung anwenden. Dasselbe gilt auch für Internet-basierten Zugriff. Gewöhnen Sie Ihre Endbenutzer daran, immer die sicherste mögliche Form der Authentifizierung anzuwenden. Verwenden Sie beispielsweise die integrierte Windows-Authentifizierung oder die Digestauthentifizierung in Ihrem Intranet und vielleicht die Zertifikatauthentifizierung auf der Seite des Internet für diejenigen Benutzer, die bekannt sind (beispielsweise Kunden, die Waren von Ihrer Organisation kaufen). Alle anderen Benutzer auf der Seite des Internet bleiben so lange anonyme Benutzer, bis sie die imaginäre Grenze überschreiten und echte Kunden werden. Ab dann können Sie die Zertifikatauthentifizierung einsetzen.
- Implementieren Sie physikalische Sicherheit. - Setzen Sie den physikalischen IIS-Server niemals der allgemeinen Öffentlichkeit oder womöglich den gewöhnlichen Angestellten aus, d.h. Sie

sollten den Web- oder FTP-Server niemals unter den Tisch von irgendjemandem oder in einem nicht gesicherten Datencenter (d.h. keine Türen oder Wände für das Datencenter, geschweige denn Schlösser an den Türen) aufstellen und in jedem Fall immer Kennwörter auf BIOS- und Bildschirmschonerebene für den IIS-Computer selbst verwenden. Darüber hinaus sollten Sie dafür sorgen, dass dieser Server nicht an die LANs oder WANs Ihrer Organisation angeschlossen ist, wenn nur über das Internet auf ihn zugegriffen werden soll. Wenn es sich jedoch um einen ausschließlich im Intranet verwendeten IIS-Server handelt, dann sollten Sie dafür sorgen, dass nicht über das Internet auf diesen Server zugegriffen werden kann.

- Implementieren Sie logische Sicherheit. - Sie sind gut beraten, wenn Sie getrennte Verwaltungskonten verwenden (es sollten niemals mehrere Personen dasselbe Konto verwenden, da Sie sonst nie feststellen können, wer was getan hat) und sichere Web- und Benutzerberechtigungen festlegen.
- Minimieren Sie die Anzahl der verwendeten IIS-Dienste. - Führen Sie auf diesem Server keine Dienste aus, die für den Betrieb Ihrer Web-, FTP-, SMTP- oder NNTP-Sites nicht unbedingt notwendig sind. D.h. Sie sollten den IIS-Server nicht für Datei- und Druckdienste, Anwendungsdienste u.ä. verwenden. Darüber hinaus sollten Sie die folgenden Windows 2000 Server-Dienste deaktivieren: Anwendungsverwaltung, Ablagemappe, Computersuchdienst, Faxdienste, Dateireplikation, Net Logon, Infrarotmonitor, Kerberos KDC (Key Distribution Center) (vorausgesetzt, Ihr IIS-Server ist kein Domänencontroller, KDC und kein globaler Katalog), Remotedesktop-Freigabefunktion von NetMeeting, Druck-Spooler, QoS (Quality of Service) RSVP, Dienst für die Remote-Registrierung, RRAS, Telnet, Terminaldienste, Windows Installer und Windows-Zeitdienst.
- Verwenden Sie auf allen IIS-Servern das Dateisystem NTFS. - Um strengere Sicherheitseinstellungen auf die Dateien anwenden zu können, müssen Sie das Format der Dateizuordnungstabelle von FAT oder FAT32 in NTFS 5.0 ändern (das ist neu bei Windows 2000). Beachten Sie, dass Sie aus einer FAT- oder FAT32-Partition, nachdem Sie diese auf NTFS aktualisiert haben, nur dann wieder eine FAT- bzw. FAT32-Partition machen können, wenn Sie diese Partition neu formatieren. (D.h. Sie müssen alles sichern und dann löschen.)
- Erzwingen Sie Kennwortsicherheit. - Lassen Sie nicht zu, dass Ihre Windows-autorisierten Benutzer sich angewöhnen, dasselbe Kennwort zum wiederholten Male verwenden. Definieren Sie die allgemeine Sicherheitsrichtlinie, dass Kennwörter mindestens acht Zeichen umfassen müssen, und halten Sie Ihre Benutzer dazu an, Sonderzeichen in ihre Kennwörter einzufügen. Außerdem sollten die Kennwörter für alle Benutzer und Administratoren in regelmäßigen Zeitabständen ablaufen: beispielsweise alle 90 - 120 Tage bei Endbenutzern und alle 30 Tage bei Administratoren.
- Arbeiten Sie mit einer Verschlüsselung. - Verwenden Sie für alle verwaltungstechnischen Aufgaben in Ihrer Website sowohl lokal als auch remote, auch für die Erstellung neuer Inhalte, die SSL-Verschlüsselung (Secure Sockets Layer).
- Verwenden Sie Benutzerkonten mit geringen Berechtigungen. - Wenn es ausreicht, dass die Benutzer Ihre Web- oder FTP-Sites nur lesen, dann sollten Sie den Benutzern keine weiteren Berechtigungen erteilen. Öffnen Sie Ihre Sicherheitsstruktur niemals mit dem Gedanken, sie jederzeit wieder verschärfen zu können. Gehen Sie lieber umgekehrt vor: Schränken Sie zunächst jeden Bereich Ihrer Site so gut wie möglich ein. Öffnen Sie dann die Zugriffsmöglichkeiten für die Benutzer Ihrer Organisation nach Bedarf. Das bedeutet, dass Sie zunächst einmal nur mit der

Berechtigung Lesen beginnen und die Berechtigungen dann allmählich auf Schreiben und vielleicht auf den Skriptzugriff ausweiten.

Es gibt Hunderte von Tipps und Tricks, wie Sie die IIS-Umgebung schützen können. Wir haben hier nur die Möglichkeit, an der Oberfläche zu kratzen. Im Internet finden Sie weitere Hinweise, wie Sie Ihren Server vor unerlaubtem Zugriff schützen können. Die folgende Adressliste kann Ihnen bei der Suche nach Informationen behilflich sein:

- <http://www.microsoft.com/security/>
- <http://www.l0pht.com/>
- <http://www.networkcomputing.com/netdesign/>
- http://windowsupdate.microsoft.com/nt5help/Enterprise/en/nt_frame.htm
- <http://www.rsa.com/>
- <http://www.nmrc.org/files/snt/index.html>

Viel Glück!

Zuweisen von Verzeichnisrechten für sichere Sites

Eine Website zu schützen, ist nicht einfach. Das kostet einiges an Zeit und Aufwand und auch dann wird eine Website nicht hundertprozentig sicher sein vor Schnüfflern. Gleichgültig, wie Sie es anstellen, nichts wird jemals hundertprozentig sicher sein vor Hackern und Crackern, wenn Ihre Website mit dem Internet verbunden ist. Dennoch gibt es einige Maßnahmen, die Sie ergreifen können, die meisten Leute davon abzuhalten, Ihre Sicherheitsgrenzen zu verletzen.

Berechtigungseinstellungen

Als Erstes müssen Sie Ihre Webberechtigungen definieren. Das ist eine relativ einfache Aufgabe. Es kann jedoch einige Zeit in Anspruch nehmen herauszufinden, wem Ihre Organisation den Zugriff worauf gewähren möchte. Es gibt im Wesentlichen vier Ebenen des Zugriffs, die dann mit der Funktion, Besuche zu protokollieren und Ressourcen zu indizieren gekoppelt werden. Es gibt folgende Berechtigungen:

- Leseberechtigung. - Hierbei handelt es sich um die Standardeinstellung für alle Websites, die dem Benutzer die Möglichkeit bietet, den Inhalt der Site zu lesen und zu kopieren.
- Schreibberechtigung. - Diese Berechtigung bietet Besuchern die Möglichkeit, den Inhalt und Eigenschaften der Website zu bearbeiten, d.h. auch Dateien zu löschen und Sicherheitsgrenzen festzulegen.
- Skriptzugriff. - Diese Art der Berechtigung ist etwas schwieriger anzuwenden als der Lese- und Schreibzugriff. Damit können Benutzer der Website auf den Quellcode Ihrer Skriptdateien wie z.B. auf ASP-basierte Anwendungen zugreifen, um diese zu lesen und/oder zu ändern. Wenn Sie den Lesezugriff zusammen mit dem Skriptzugriff aktiviert haben, können Ihre Webbenutzer diese Skripts verwenden. Wenn Sie jedoch den Schreibzugriff zusammen mit dem Skriptzugriff aktiviert haben, können Ihre Webbenutzer den Quellcode all Ihrer Skripten ändern.
- Berechtigung, das Verzeichnis zu durchsuchen. - Mit Hilfe dieser Berechtigung können Ihre Webbenutzer die Ordner Ebenen Ihres IIS-Servers durchsuchen. Das ist für jeden Webserver eine

gefährliche Einstellung. Für FTP-Server ist diese Einstellung dagegen normal, da FTP-Sites dazu gedacht sind, nach bestimmten Datei- und Ordnerinformationen durchsucht zu werden. Daher sollten in einer FTP-Site niemals sichere Daten gespeichert werden.

Nachdem Sie sich entschieden haben, welche Webberechtigungen angewendet werden sollen, müssen Sie die NTFS-Berechtigungen für Ihren IIS-Server definieren. (Dazu müssen Sie die Partitionsstruktur von FAT bzw. FAT32 in NTFS geändert haben.)

Einstellungen für die Zugriffskontrolle

Nachdem Sie Ihre Partitionsstruktur in NTFS geändert haben, können Sie die Berechtigungen, basierend auf folgenden Einstellungen, ändern:

- **Vollzugriff.** - Benutzer mit dieser Berechtigung können mit den Dateien und Ordnern, aus denen die betreffenden Sites bestehen, tun, was sie möchten.
- **Dateiinhalte anzeigen.** - Hierbei handelt es sich um eine der sichereren Berechtigungsebenen. Benutzer mit dieser Berechtigung können den Inhalt eines Ordners lesen, aber nicht darauf zugreifen.
- **Ändern.** - Mit dieser Berechtigung können Benutzer Dateien und Ordner sowie deren Eigenschaften ändern.
- **Kein Zugriff.** - Benutzer mit dieser Berechtigung haben keinerlei Zugriff auf Dateien oder Ordner auf dem IIS-Server Ihrer Organisation.
- **Lesen.** - Benutzer können Dateien und Ordner sowie deren Eigenschaften anzeigen, können aber deren Inhalte nicht ändern.
- **Lesen und Ausführen.** - Diese Berechtigung stellt eine Erweiterung der Leseberechtigung dar. Benutzer mit dieser Berechtigung können nicht nur Dateien und Ordner sowie deren Eigenschaften lesen, sondern auch Anwendungen und Skripten auf Ihrer Site ausführen.
- **Schreiben.** - Diese Berechtigung schließt die Lese- und Ausführberechtigung ein und umfasst darüber hinaus die Berechtigung, Dateien und Ordner zu ändern.

Durchsuchen von Verzeichnissen

Wie bereits erwähnt, ist die Berechtigung zum Durchsuchen von Verzeichnissen die gefährlichste, die Sie in einer offenen Website erteilen können. Bei Websites, die nur für die Intranetbenutzer Ihrer Organisation offen sind, gibt es einen Grund dafür, warum diese Berechtigung erteilt werden sollte: um WebDAV als Veröffentlichungsmechanismus zu verwenden.

Das Durchsuchen von Verzeichnissen von FTP-Sites ist dagegen etwas völlig anderes. Es wird natürlich vorausgesetzt, dass Sie niemals etwas anderes (Daten, Dienste oder was auch immer) auf dem IIS-Server installieren, der die FTP-Site(s) Ihrer Organisation ausführt, da dies eine enorme Sicherheitslücke darstellen würde. Das Durchsuchen von Verzeichnissen ist ein Vorgang, der von den meisten FTP-Sites üblicherweise zugelassen wird. Dabei sollten Sie natürlich für die privaten Bereiche Ihrer FTP-Site eine Kennwortauthentifizierung verwenden und erzwingen.

Sicherheitslücken suchen

Die Suche nach Sicherheitslücken in Web- oder FTP-Sites ist nicht so einfach, wie man sich das zunächst vorstellen mag. Bei der Suche nach Sicherheitslücken geht es nicht nur darum festzustellen, dass sich jemand unberechtigt Zugriff auf private Informationen verschafft hat. Vielmehr geht es dabei auch darum herauszufinden, wie diese Person sich den Zugriff auf diese Informationen verschafft hat. Denn wenn Sie das nicht herausfinden und diese Person aussperren, kommt diese an einer anderen Stelle wieder herein.

Bei der Suche nach Sicherheitslücken gibt es auch noch eine andere Seite. Es kann sein, dass Sie für eine bestimmte IIS-Server-basierte Ressource eine falsche Sicherheitsstufe definiert haben und jemand Ihre vermeintliche Sicherheitsgrenze unbewusst überschritten hat. In diesen Fällen ist es hilfreich, wenn Sie sich erst einmal klar machen, was Sie eigentlich schützen möchten, warum Sie das tun möchten und wie Sie Ihre Schutzmechanismen einsetzen möchten.

Nun, da Sie beide Seiten der Sicherheitslücken kennen, geht es darum, wie Sie damit umgehen. Wenn Berechtigungen nicht richtig definiert sind, müssen Sie die Web- und NTFS-Berechtigungen Ihrer Sites sowie die Zugriffsberechtigungen Ihrer Benutzer genau prüfen. Als Nächstes sollten Sie prüfen, wo Sie Ihr virtuelles WebDAV-Verzeichnis erstellt haben. Zeigt es auf eine Stelle weit oben in Ihrer Ordnerhierarchie? D.h. haben Sie die WebDAV-Berechtigungen festgelegt, um mit Ihrem Ordner `\inetpub\wwwroot` zu beginnen, oder haben Sie diese Berechtigungen weiter unten in Ihrer Ordnerhierarchie untergebracht? Je weiter oben Sie die Berechtigungen festlegen, umso wahrscheinlicher ist es, dass Ihr IIS-Server über den WebDAV-Bereich hinaus durchsucht werden kann. Es hat sich als praktisch erwiesen, den WebDAV-Ordner auf einem Computer zu speichern, der vom allgemeinen IIS-Server physikalisch getrennt ist, und auch dann sollten Sie diesen Ordner in einer NTFS-Partition speichern, die außer dem WebDAV-Inhalt sonst nichts enthält.

Ein weiterer potenzieller Fehler bzw. ein unbeabsichtigtes Sicherheitsproblem wird offensichtlich, wenn ein Webbrowser die Fehlermeldung 404 - Access Denied (Zugriff verweigert) sendet. Fehlermeldungen dieses Typs werden dann angezeigt, wenn einem Benutzer aufgrund der Zugriffssteuerungsliste der Zugriff gewährt, er aber dennoch nicht authentifiziert wird. Anonyme Web- und FTP-Benutzer erhalten diese Art der Fehlermeldung häufig. Wie bereits erwähnt, kann es vorkommen, dass übereifrige Administratoren, die das Kennwort oder die Richtlinien für das Konto `IUSR_computername` ändern, diese Art des Fehlers verursachen können. Mit diesem Konto wird der anonyme Zugriff für Benutzer von FTP- sowie Webdiensten kontrolliert. Wenn an diesem Konto Änderungen vorgenommen werden, kann dies dazu führen, dass sich der IIS-Server weigert, eine anonyme Verbindung für eine bestimmte, von diesem Server kontrollierte Ressource herzustellen.

Ein ähnlicher Fehler bzw. ein ähnliches Sicherheitsproblem wird durch die Fehlermeldung 403 - Access Forbidden (Zugriff verboten) angezeigt. Wenn Sie fälschlicherweise für die IP-Adressen Ihrer Benutzer den Zugriff auf den IIS-Server gesperrt haben, kann dies eine Fehlermeldung dieser Art zur Folge haben. Ebenso erscheint diese Fehlermeldung, wenn ein Benutzer kein gültiges Windows 2000 Server- bzw. Domänenkonto und Kennwort mehr hat. Bei einer Fehlermeldung wie dieser müssen Sie lediglich dafür sorgen, dass das Konto der Person aktiv und gültig ist.

Um festzustellen, ob sich unberechtigte Benutzer auf Ihrem Windows 2000-Server tummeln, sollten Sie die Computerverwaltung aufrufen. Klicken Sie dazu mit der rechten Maustaste auf dem Desktop auf das Symbol **Arbeitsplatz** und klicken Sie dann in dem daraufhin erscheinenden Kontextmenü auf die Option **Verwalten**. Nun öffnet sich das Fenster **Computerverwaltung** (siehe Abbildung 19.32).

Klicken Sie auf das Pluszeichen neben dem Symbol **System** und dann auf das Symbol **Freigegebene Ordner**. Klicken Sie anschließend auf den Ordner **Sitzungen**, um sämtliche aktiven Benutzer auf Ihrem Server im rechten Fensterbereich anzuzeigen. (Denken Sie daran, dass anonyme Benutzer hier nicht einzeln aufgeführt werden.) Es bleibt Ihnen, dem Systemadministrator, überlassen festzustellen, welche der hier aufgeführten Benutzer berechnete Benutzer sind. Das ist nicht immer einfach, ganz besonders dann nicht, wenn jemand mit einem ansonsten gültigen Benutzerkonto in Ihre Netzwerke eingedrungen ist.

Wenn Sie das Konto eines Hackers ausfindig gemacht haben, ist es relativ einfach, dieses aus dem System zu löschen. Klicken Sie dazu mit der rechten Maustaste auf das Konto dieses Benutzers. Daraufhin erscheint ein kleines Kontextmenü (siehe Abbildung 19.33).

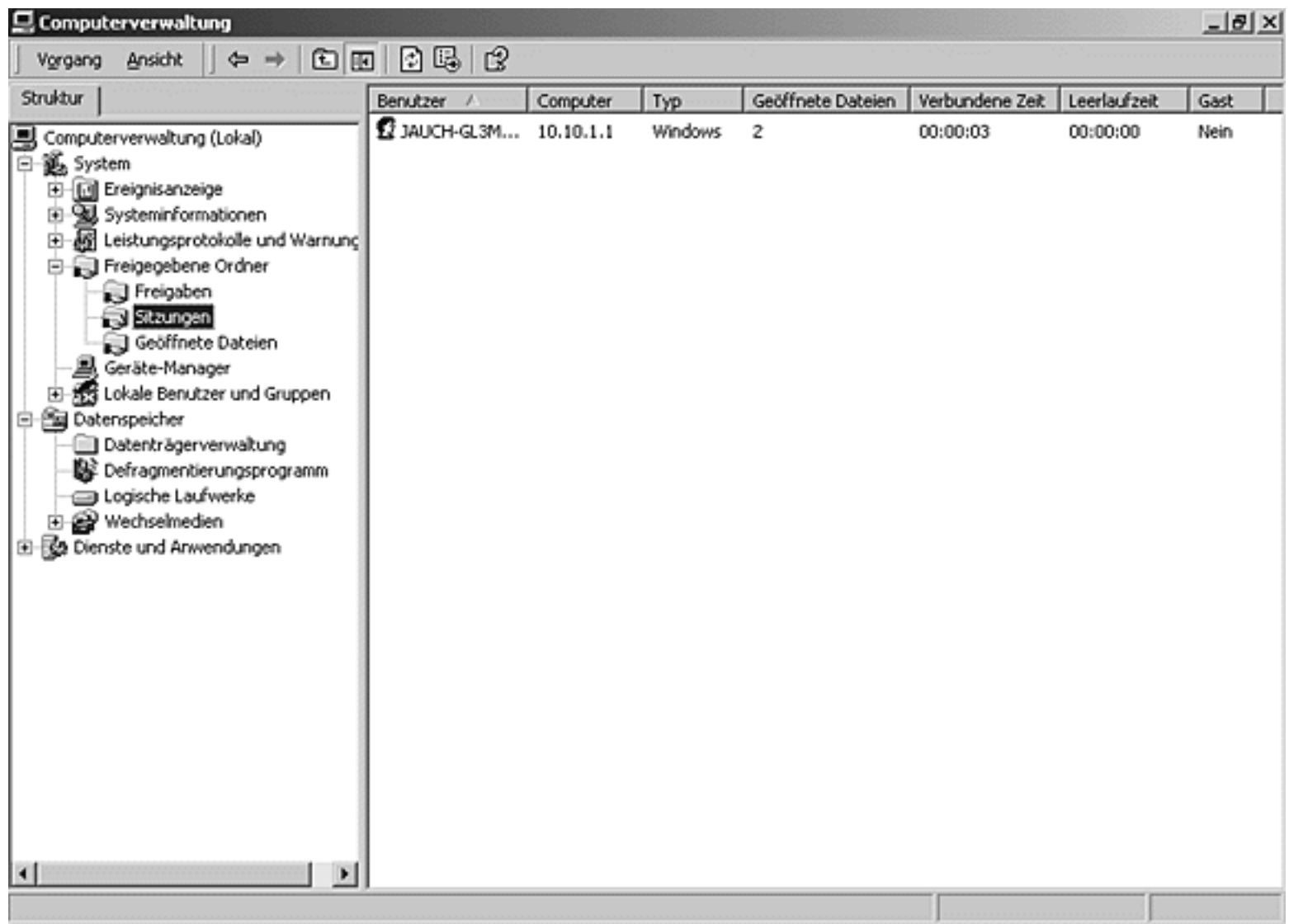


Abbildung 19.32: Anzeigen aktiver Sitzungen

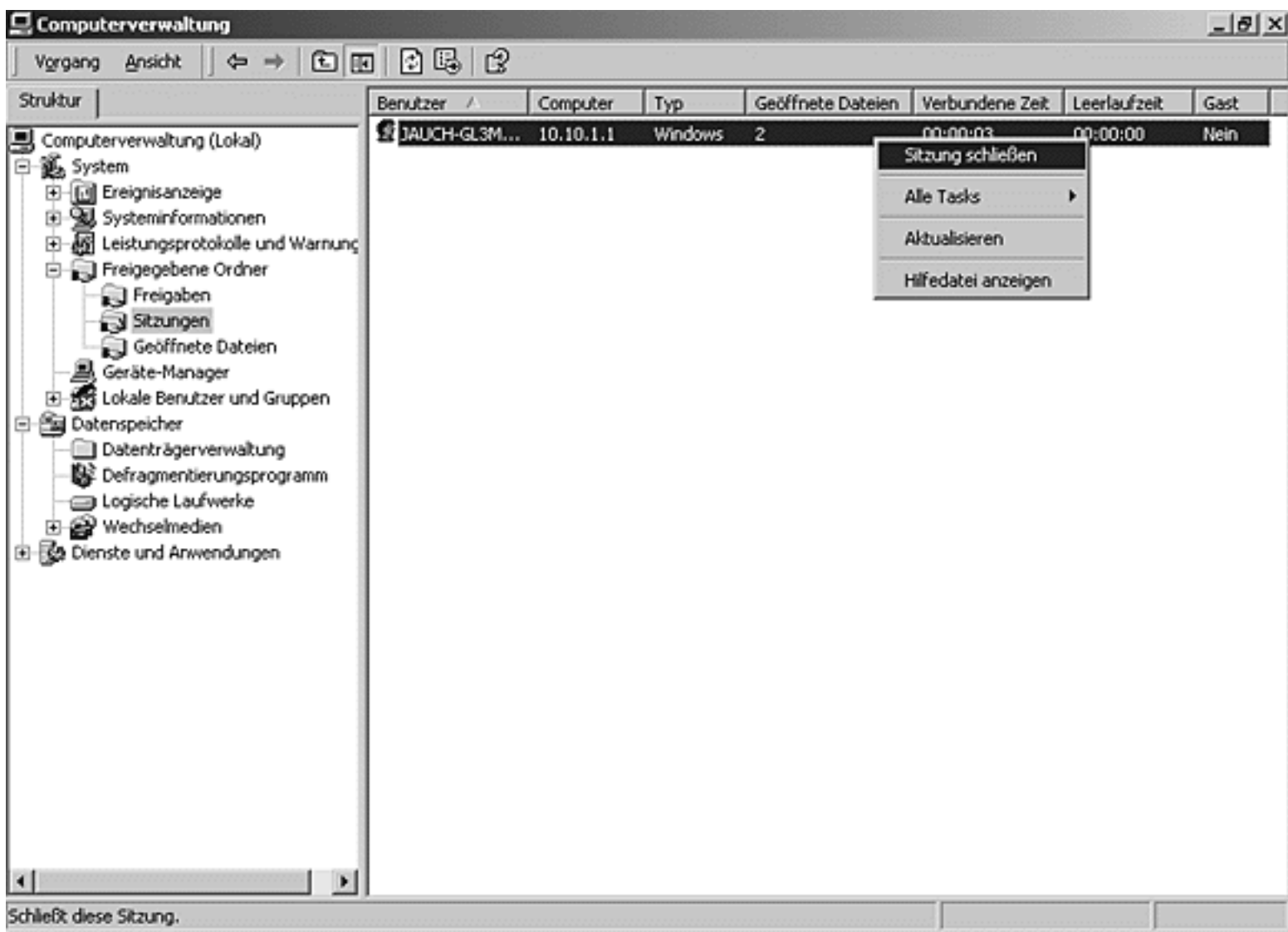


Abbildung 19.33: Um eine Benutzersitzung zu schließen, wählen Sie die Option Sitzung schliessen. Anschließend müssen Sie diese Entscheidung bestätigen.

Klicken Sie auf **OK**, sodass die unzulässige Sitzung dieses Benutzers von Ihrem Windows 2000-Server entfernt wird. Wenn Sie nicht herausfinden, wie sich der Benutzer Zugriff verschafft hat, besteht die Gefahr, dass der Benutzer innerhalb kürzester Zeit wieder in Ihrem System ist. Sie müssen die Ereignisprotokolle von Windows 2000 Server sorgfältig prüfen um festzustellen, welche Benutzer wiederholte Male versucht haben, auf Bereiche zuzugreifen, auf die diese Benutzer eigentlich nicht zugreifen sollten. Eine andere Möglichkeit besteht darin, Ihre IIS-Protokolle auf ungewöhnliche Aktivitäten zu prüfen. Wie Sie sich vielleicht schon vorstellen können, kann es für Sie und vielleicht auch für andere in Ihrer Organisation sehr zeitaufwändig sein, einem Script Kiddy, einem Hacker oder einem Cracker auf die Spur zu kommen. Eines schönen Tages kann es sein, dass vielleicht zig Versuche von nicht berechtigten Benutzern unternommen werden, um auf die Internet- und Intranet-basierten Server Ihrer Organisation zuzugreifen. Diese alle ausfindig zu machen, bevor sie größeren Schaden anrichten, kann ein Full-Time-Job sein.

Kapitel 20 Virtuelle private Netzwerke

Die Nutzung der VPNs (virtuelle private Netzwerke) im Internet wird heute immer gängiger. Die Unternehmen benötigen immer mehr Verbindungen und ihre Telekommunikationskosten steigen in schwindelnde Höhen. Filialbüros, Außendienstmitarbeiter und Telearbeiter brauchen den sicheren Zugriff auf Netzwerkressourcen, der gleichzeitig kostengünstig ist. Noch vor kurzer Zeit gab es keine andere Möglichkeit, als ein WAN (Wide Area Network = Weitbereichsnetz) über von Telefongesellschaften gemietete Leitungen zu nutzen. Der Vorteil dabei war, dass dies ihr ganz privates Netzwerk war - kein anderes Unternehmen konnte es nutzen. Das ist sehr sicher und die Bandbreite ist garantiert. Der Nachteil waren die Kosten: eine einzige T1-Leitung (1,54 Mbps) kostete bis zu 3.000 DM im Monat. Wenn man mehr Bandbreite brauchte, konnten T3-Leitungen (45 Mbps) gemietet werden, was aber - je nach Ortslage - mit einem Kostenaufwand zwischen 30.000 und 200.000 DM pro Monat verbunden war. Dabei handelte es sich zwar um eine relativ sichere, aber für das Budget mancher IT-Abteilungen nicht immer erschwingliche Lösung. Deshalb werden die VPNs so rege genutzt - sie füllen eine Lücke.

Das Konzept der VPNs ist vielen noch fremd, um nicht zu sagen »unheimlich«. Dieses Problem aber hat die Netzwerkindustrie selbst geschaffen. Der Begriff VPN wurde relativ freizügig genutzt, um alle möglichen Lösungen zu beschreiben, die für ein VPN nicht nötig sind. Dieses Kapitel will die Gerüchte in Bezug auf VPNs aus der Welt schaffen und zeigen, wie praktisch, kostengünstig und sicher diese Technologie ist.

Bevor wir weiter in das Thema einsteigen, hier ein Überblick über den Inhalt dieses Kapitels:

- Machen Sie das Internet zu Ihrem eigenen WAN!
- Was ist ein VPN, ein »Virtuelles privates Netzwerk«?
- Sicherheit und Verschlüsselung
- Tunnel-Server
- Microsoft VPN
- L2TP und IPSec
- Einrichtung eines grundlegenden VPN in Windows 2000
- RRAS-Verbesserungen

20.1 Machen Sie das Internet zu Ihrem eigenen WAN

Die Budgets der meisten IT-Abteilungen sind begrenzt und die Kosten müssen ausgeglichen werden. Angenommen, Sie brauchen eine Verbindung Ihres Büros in München mit dem Unternehmenssitz in Frankfurt. Sie rufen also bei Ihrer bevorzugten Telefongesellschaft an und beantragen eine T1-Leitung zwischen den beiden Büros. Bei der Überprüfung Ihrer Ausgaben erkennen Sie, dass Sie entweder Ihre existierende T1-Verbindung zum Internet loswerden müssen - oder den Sohn des Chefs feuern, der momentan der Systemadministrator ist. Weil das Letztere nicht wirklich in Betracht kommt, sollten Sie die erste Möglichkeit genauer betrachten - aber Sie können sich nicht leisten, Ihre Verbindung zum

Internet zu verlieren. Die Verkaufsabteilung nutzt diese Verbindung, um mit den Kunden zu kommunizieren, die Entwicklungsabteilung verschafft sich Informationen aus dem Web und Sie suchen damit nach Informationen, die Ihnen beim Betrieb Ihres Netzwerks weiterhelfen. Es muss noch eine andere Lösung geben. Wenn Sie das Problem genauer betrachten, erkennen Sie, dass Sie eine Lösung für 24 Stunden und 7 Tage die Woche haben, während Sie eigentlich nur 5 Prozent dieser Zeit nutzen.

Sie haben nämlich bereits eine WAN-Lösung. Schließlich senden Sie bereits E-Mail mit Hilfe des Internet zwischen den Büros hin und her. Warum sollten Sie also nicht auch alle anderen Dateien auf diese Weise übertragen? Was wäre, wenn Sie eine Verbindung hätten, die eine ähnliche Sicherheit und Zuverlässigkeit bietet wie Ihre private T1-Leitung, aber keine so hohen Kosten produziert? Und hier kommen die VPNs ins Spiel. VPNs bieten Ihnen die Möglichkeit, das Internet oder ein anderes öffentliches Netzwerk als WAN-Verbindung zu nutzen und dabei die Sicherheit einer privaten Verbindung aufrecht zu erhalten.

20.2 Was ist ein VPN, ein »Virtuelles privates Netzwerk«?

Ein *Virtuelles privates Netzwerk* ist eine private Verbindung zwischen zwei Computern oder Netzwerken, die private Daten über ein öffentliches oder freigegebenes Netzwerk sendet, beispielsweise das Internet. Die Verbindung zwischen den Computern oder Netzwerken wird so eingerichtet, dass eine private Verbindung simuliert wird, die ähnlich einer privaten, gemieteten Leitung zwischen diesen Geräten ist. Die Anwendungen sehen die Verbindung als private Verbindung und müssen nichts über die Anschlussmodalitäten an das Internet wissen. Das wird durch das Konzept des *Tunnelings* realisiert. Grundsätzlich können zwei IP-Geräte einen Tunnel zwischen sich anlegen, wobei Daten von einer Anwendung an einem Ende eingekapselt werden, am anderen ausgepackt und dort der Anwendung übergeben, die die Daten so empfängt, als ob es eine direkte Verbindung gäbe. Die Anwendungen müssen nichts über das Routing oder die verschiedenen Verbindungen über das Internet wissen. Die Daten werden verpackt, durch den Tunnel geschickt, am anderen Ende ausgepackt und der Anwendung übergeben.

Das Konzept des Tunnelings ist einem Protokoll ganz ähnlich, das Sie möglicherweise schon kennen: PPP (Punkt-zu-Punkt-Protokoll). Sie verwenden es bereits, wenn Sie über ein Modem eine Verbindung zum Internet einrichten. Neben einigen Konzepten von PPP bietet das Tunneling ähnliche Vorteile. Die beiden wichtigsten Vorteile sind Einfachheit und Transparenz. Durch das Tunneling bleibt es den VPNs erspart, unnötig die Funktionalität von Protokollen höherer Ebene zu implementieren; die Daten werden einfach verpackt und an das andere Ende geschickt, wo man sie weiterverarbeiten kann. Sie können sogar andere Protokolle transportieren, wie beispielsweise IPX und AppleTalk, indem Sie sie in ein IP-Paket einkapseln. Im Grunde genommen simulieren VPNs eine PPP-Verbindung über ein öffentliches Netzwerk.

Wo kommt die Verschlüsselung ins Spiel und was ist mit den ganzen anderen geheimnisvollen Konzepten, wie öffentlichen Schlüsseln, privaten Schlüsseln und Authentifizierung? Das alles ist für VPNs sehr wichtig und wird später in diesem Kapitel noch beschrieben. Hier aber soll deutlich gemacht werden, dass VPNs nicht unbedingt so kompliziert sein müssen. Sie können Ihre privaten Daten unverschlüsselt über das Internet übertragen, aber das ist eher unwahrscheinlich. Ihre

Entwicklungsabteilung würde laut aufschreien, wenn die Entwürfe der neuesten und besten Technologien im Klartext über das Internet geschickt würden, wo jeder sie lesen kann. Und hier erhalten die VPNs ihre Bedeutung. Wenn Sie das VPN-Tunneling und Verschlüsselungstechniken kombinieren, erhalten Sie eine sichere Verbindung, die vielleicht sogar sicherer ist als eine private gemietete Leitung. Die Daten werde nicht nur eingekapselt, sondern auch verschlüsselt, um sie geheim zu halten und die Integrität Ihrer Dateien zu bewahren.

20.3 Sicherheit und Verschlüsselung

Wir wissen nun, dass es weniger sinnvoll ist, die Datenpakete einfach zu verschnüren und über das Internet zu versenden, wo jeder sie sehen kann. Wer weiß schon, wer da draußen lauert? Es geht aber nicht nur darum, dass jemand zuhören könnte. Wie kann man wissen, ob die Datei, die Sie versenden, genau so ankommt, wie sie abgeschickt wurde? Wie können Sie sicher sein, dass die Leute, die sich über ein VPN an Ihrem Netzwerk anmelden, auch die sind, die sie zu sein vorgeben, und die Kennwörter und Zugriffsberechtigungen nicht irgendwo gestohlen haben? Wie können Sie unerwünschten Verkehr unterbinden? Die VPN-Technologie wird all diesen Aspekten gerecht, ohne für den Endbenutzer zu viel Komplexität einzuführen.

Momentan ist PPTP (Point-to-Point Tunneling Protocol) von Microsoft das gebräuchlichste Protokoll für VPNs. Es wurde von Microsoft und 3Com als offener Industriestandard entwickelt. Es ist in Windows NT Server 4.0, Windows 98 und als Komponente des DFÜ-Netzwerk 1.2 Upgrades für Windows 95 enthalten. Unter Windows 2000 wurden PPTP und die VPN-Dienste wesentlich verbessert und unterstützen jetzt unter anderem auch Zertifikate, L2TP (Layer 2 Tunneling Protocol) und IPsec (Internet Protocol Security). PPTP ist vor allem deshalb so beliebt, weil es so einfach ist. PPTP übernimmt sowohl die Kapselung der Daten als auch die Verschlüsselung des Datenstroms, selbst wenn andere, nicht-IP-basierte Protokolle transportiert werden.

Microsofts Implementierung von PPTP verwendet MPPE (Microsoft Point-to-Point Encryption) zur Verschlüsselung des VPN-Verkehrs. MPPE basiert auf dem RSA RC4-Verschlüsselungsalgorithmus und nutzt 40-Bit- oder 128-Bit-Schlüssel. PPTP erzeugt einen Tunnel zwischen der Client-Workstation und dem Server. Der Client einigt sich mit dem Server auf PPP, häufig auch als Tunnel-Terminator bezeichnet, und eine Verschlüsselungssitzung wird initiiert. MPPE verschlüsselt PPP-Pakete auf der Client-Seite, bevor sie in den PPTP-Tunnel gelangen. Der Tunnel-Terminator entschlüsselt die Pakete und gibt sie an ihr endgültiges Ziel weiter.

MPPE verwendet auch MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol), eine Authentifizierungsmethode für die Auswertung der Benutzerzugriffsberechtigungen in Hinblick auf Windows NT-Domänen. Wenn ein Server eine MS-CHAP-Authentifizierungsanforderung von einem Client erhält, sendet er eine Abfrage. Diese Abfrage beinhaltet eine beliebige Abfragezeichenkette sowie die Sitzungs-ID. Der Remote-Client gibt den Benutzernamen, einen aus der Abfragezeichenkette erzeugten Hashschlüssel, die Sitzungs-ID sowie ein ebenfalls mit dem Hashingalgorithmus verschlüsseltes Kennwort zurück.

Diese Art der Authentifizierung ist nicht nur für den Server wichtig, damit er den Benutzer auswerten kann, sondern auch für den Client. Es gibt einen Netzwerkangriff, der auch als »Mann in der Mitte« bezeichnet wird. Dabei platzieren sich die potenziellen Eindringlinge während einer Kommunikation

zwischen Server und Client, sodass sie den Benutzer täuschen und Information von ihm entgegennehmen können. Weil bei der Verbindung die Sitzungs-IDs und eine nach dem Hashalgorithmus verschlüsselte beliebige Abfragezeichenkette verwendet werden, kann der Client relativ sicher sein, dass er wirklich mit dem Server kommuniziert, den er gemeint hatte. Es ist also nicht nur wichtig, die Datenpakete zu verschlüsseln, bevor sie in ein öffentliches Netzwerk übertragen werden, sondern auch die Authentifizierung, nämlich die Möglichkeit, an beiden Enden des Tunnels sicherzustellen, dass der Gegenüber der ist, der er zu sein behauptet.

Diese ganze Verschlüsselung und Authentifizierung ist notwendig, bringt aber auch einen wesentlichen Zusatzaufwand mit sich. Die Verschlüsselung ist nichts für schwache Prozessoren. Mit jedem Datenpaket entsteht Datenoverhead, wodurch letztlich die Bandbreite geschmälert wird. Dann kommt die Verschlüsselung und Entschlüsselung. Auch dadurch entstehen Verzögerungen, was ebenfalls den Eindruck verringerter Bandbreite verursacht. Es ist direkt erstaunlich, dass wir überhaupt Informationen über diesen VPN-Tunnel erhalten. Wenn Sie nicht gerade den neuesten und den leistungsfähigsten Prozessor einsetzen, werden die Benutzer von VPN nicht besonders begeistert sein. Das kann jedoch durch den Einsatz von dedizierten VPN-Tunnel-Servern kompensiert werden.

20.4 Tunnel-Server

Wenn die Verschlüsselung die Computer Ihrer Benutzer zu langsam macht, haben Sie zwei Möglichkeiten. Sie können die Computer aufrüsten oder einen Teil des Verschlüsselungsaufwands auf einer Maschine verarbeiten, die genau für diesen Zweck abgestellt wird, den Tunnel-Server. Sie können Ihr gesamtes VPN ohne jegliche VPN-Software auf den Client-Workstations aufbauen. Wenn Sie zwei LANs verbinden wollen, richten Sie einen Tunnel-Server ein - den so genannten Tunnel-Initiator -, der den Tunnel zu dem Server auf dem anderen LAN einrichtet, einen terminierenden Tunnel-Server, und erlauben diesen Maschinen, die gesamte Verschlüsselung sowie den Aufbau des Tunnels zu übernehmen. Damit kommen wir zu zwei Konzepten, die Sie kennen sollten, bevor es weitergeht: freiwillige (voluntary) und erzwungene (compulsory) Tunnel.

Es gibt zwei Tunnelformen: freiwillige und erzwungene Tunnel. Um einen freiwilligen Tunnel anzulegen, muss der Client VPN-fähig sein, d.h. er braucht die Software und die Hardware, um selbst VPN-Tunnel anzulegen und ein VPN zu nutzen. Erzwungene Tunnel werden genutzt, wenn der Client einen VPN-fähigen Tunnel-Server anstatt einer Client-Workstation verwendet, um Tunnel einzurichten und die Verschlüsselung zu nutzen. Diese Clients haben keine Kontrolle über die Nutzung eines VPN; sie sind also gezwungen, ihn zu nutzen (daher auch der Name).

Vielleicht haben Sie gerade die Situation, in der der gesamte Verkehr aus München zu einem Tunnel-Initiator geleitet wird, wo der Tunnel angelegt und die Daten verschlüsselt werden. Diese Daten werden durch den Tunnel zum Büro in Frankfurt geschickt, wo sie am Tunnel-Terminator entschlüsselt und in das Netzwerk weitergegeben werden. Die Client-Workstations merken gar nicht, was passiert, und auf den Workstations entsteht kein zusätzlicher Aufwand. Das wäre ein Beispiel für einen erzwungenen Tunnel.

Ein gebräuchliches Beispiel für einen freiwilligen Tunnel ist eine einzelne Workstation, die sich in das Internet einwählt. Diese Workstation stimmt Tunnel und Verschlüsselung mit einem Server im LAN ab, mit dem sie kommunizieren will. Der Rechner übernimmt den Aufwand für die VPN-Verbindung selbst.

Diese Form von VPN wird häufig von einzelnen Remote-Benutzern verwendet, beispielsweise Außendienstmitarbeitern oder Telearbeitern.

Wir könnten das Ganze noch einen Schritt weiter führen und den Aufwand für die VPNs völlig jemand anderem übertragen. Viele ISPs und Netzwerkdienstanbieter stellen VPN-Dienste bereit, über die Sie Ihren Verkehr abwickeln; sie legen den VPN-Tunnel für Sie an. In dieser Situation verbinden Sie Ihr Netzwerk mit dem des ISP und übergeben den Verkehr, der an diesen geleitet werden soll. Anschließend werden die Daten verschlüsselt, über das Internet gesendet, am anderen Ende entschlüsselt und schließlich an Sie weitergegeben. Das kostet etwas mehr als eine einfache Internet-Verbindung, aber sehr viel weniger als eine gemietete Leitung.

20.5 VPN-Tunnel-Server und Firewalls

Die Nutzung eines dedizierten VPN-Tunnel-Servers mit irgendeiner Verschlüsselung muss Ihre Bedenken in Hinblick auf die Sicherheit der VPNs nicht unbedingt aus der Welt schaffen. Sie sollten jetzt überlegen, wo Sie Ihren Tunnel-Server unterbringen. Weil die meisten Netzwerke, die an das Internet angeschlossen sind, eine Art Firewall zum Schutz ihrer Netzwerke verwenden, muss überlegt werden, wo der Tunnel-Server platziert wird. Es gibt drei Möglichkeiten: innerhalb Ihres Netzwerks (hinter der Firewall), außerhalb Ihres Netzwerks (außerhalb der Firewall) oder in der Firewall. Alle diese Positionen haben ihre Vor- und Nachteile.

Zuerst überlegen Sie sicher, ob Sie den Tunnel-Server hinter der Firewall platzieren sollten. Schließlich wollen Sie mit der Firewall die meisten anderen Server schützen, indem Sie den Zugriff darauf beschränken. Größtenteils ist das eine vernünftige Maßnahme. Die Firewall schützt den Tunnel-Server vor Angriffen, falls dieser irgendwelche Schwächen aufweist - im Betriebssystem oder in Ihrer Implementierung. Sie könnten außerdem die Wahrscheinlichkeit eines DoS-Angriffs (Denial of Service) verringern. Ein solcher Angriff findet statt, wenn eine weniger freundliche Person im Internet Ihr System angreift, nicht um einzudringen, sondern um das System unbrauchbar zu machen. Dabei wird entweder ein Bug eingeschleust oder das System so mit Verkehr überhäuft, dass es auf nichts mehr reagieren kann. Eine Firewall schützt Sie vor solchen Angriffen, aber wenn Sie den Tunnel-Server innerhalb der Firewall platzieren, verlieren Sie zum Teil auch die wichtigste Funktionalität Ihrer Firewall - die Kontrolle, woher der Verkehr kommt, der in Ihr Netzwerk geschickt wird.

Wenn Verkehr, der für Ihren Tunnel-Server vorgesehen ist, durch die Firewall geht, werden die Datenpakete verschlüsselt. Die Firewall kann sie nicht daraufhin auswerten, wohin sie geschickt werden sollen. Der Verkehr kann also über den Tunnel-Server an jeden anderen Server gehen und die Firewall kann ihn nicht kontrollieren. Sie haben also mit der Firewall eine Maßnahme ergriffen, Ihren Mainframe vor unerlaubtem Verkehr zu schützen, und Ihr Tunnel-Server lässt unbeabsichtigt genau diesen Verkehr durch. Ihre Firewall kennt das Ziel des Pakets nicht, nachdem dieses den Tunnel-Server verlassen hat. Am besten platzieren Sie Ihren VPN-Tunnel-Server sicherheitshalber außerhalb der Firewall.

Wird der Tunnel-Server außerhalb der Firewall platziert, erfolgt der gesamte Verkehr, der nach innen gehen soll, verschlüsselt, bevor er an die Firewall geleitet wird. Die Firewall kann das Ziel für den Verkehr anhand ihres Regelsatzes steuern. Mit dem Tunnel-Server wird ein Tunnel angelegt; die Daten werden am anderen Ende des Tunnels verschlüsselt und am terminierenden Tunnel-Server entschlüsselt. Der terminierende Tunnel-Server versucht dann, die Daten in das Netzwerk zu reichen, aber erst,

nachdem die Firewall überprüft hat, ob die Verbindung erlaubt ist. Damit ist Ihr Tunnel-Server jedoch im Internet irgendwie preisgegeben. In diesem Fall sollten Sie einen Filter für den Tunnel-Server einführen.

20.6 Verkehr mit Hilfe eines Tunnel-Servers filtern

PPTP bietet die Möglichkeit zu filtern, welcher Verkehr akzeptiert werden soll. Dazu können unterschiedliche Methoden angewendet werden. Ist die Option aktiviert, wird der gesamte Nicht-PPTP-Verkehr ignoriert. Der Filter kann auch abhängig von dem Datenziel gefiltert werden. Warum sollte man Verkehr an Ihre Firewall weiterleiten, wenn man schon absehen kann, dass er sie nicht überwinden wird? Der Verkehr kann auch nach dem Client gefiltert werden, von dem er kommt. Ausgehender Verkehr dagegen kann nach dem Ziel gefiltert werden, an das er gerichtet wird.

Das Filtern im Tunnel-Server ist sehr praktisch. Wenn Sie für die Sicherheit im Netzwerk verantwortlich sind, sollten Sie mehrere Sicherheitsebenen einführen. Sie sollten nicht davon ausgehen, dass eine einzige Sicherheitsmaßnahme Ihr Netzwerk schützt. Wenn Sie Filter für Ihre VPN-Tunnel-Server einsetzen, haben Sie damit eine weitere Ebene in Ihrem Sicherheitsmodell eingeführt. Zuerst wird der Verkehr im Tunnel-Server kontrolliert oder gefiltert; wurde er von dieser Sicherheitsebene für gut befunden, wird er an die Firewall weitergegeben. Die Firewall untersucht den Verkehr entsprechend dem definierten Regelsatz. Sind die Regeln befolgt, übergibt sie den Verkehr an das interne Netzwerk. Schließlich überprüft Ihr internes Netzwerk die Berechtigungen für bestimmte Netzwerkressourcen. Sind für die Anforderung die entsprechenden Zugriffsberechtigungen vorhanden, wird die Ressource zur Verfügung gestellt. Weil die Sicherheitsrichtlinien viele Ebenen umfassen, sind Sie nicht von einer einzigen Ebene abhängig, um alle Aspekte des Netzwerks zu schützen. Verweigert eine Ebene aus irgendeinem Grund den Zugriff nicht, ist es sehr wahrscheinlich, dass die nächste Ebene greift und den Zugriff auf eine Netzwerkressource verbietet.

Es gibt noch eine Möglichkeit, den Tunnel-Server zu platzieren. In einigen Firewalls gibt es ein so genanntes DMZ-Netzwerk (analog zu einer »entmilitarisierten Zone«). Ein DMZ ist ein weiteres, an Ihre Firewall angeschlossenes Netzwerk mit eigener Schnittstelle zur Firewall, aber ohne direkten Anschluss an Ihr internes Netzwerk oder das Internet. Häufig werden Web-Server und Mail-Server im DMZ platziert, sodass sie durch die Firewall geschützt sind, aber das interne Netzwerk nicht direkt preisgeben. Sie könnten Ihren Tunnel-Server in einem DMZ platzieren. Damit ist der Tunnel-Server durch die Firewall geschützt, aber die Firewall kontrolliert dennoch das Ziel der Daten, nachdem der Tunnel-Server sie weitergegeben hat, weil die Daten zurück zur Firewall müssen, um ihr endgültiges Ziel zu erreichen. Auf diese Weise erhalten Sie das Beste aus beiden Welten. Der einzige Nachteil dieser Implementierung ist die zusätzliche Komplexität des Netzwerks. Außerdem besitzt Ihre Firewall möglicherweise keine zusätzliche Schnittstelle, um ein DMZ-Netzwerk einrichten zu können.

Ein letztes Wort zu Firewalls und der Platzierung von Tunnel-Servern. Viele Implementierungen von Firewalls nutzen die so genannte NAT (Network Address Translation). NAT wandelt IP-Adressen in der Firewall so um, dass ein Netzwerk seine eigentliche IP-Struktur verbergen oder private Netzwerkschemata verwenden und dennoch eine Verbindung zum Internet einrichten kann. Häufig unterstützen VPNs die NAT nicht ausreichend, weil das Datenpaket verschlüsselt ist. Sie bekommen vielleicht Probleme, wenn Sie beschließen, Ihren Tunnel-Server hinter einer Firewall anzulegen, der NAT implementiert.

Eine weitere Möglichkeit der VPN-Welt ist der FEP (Frontend-Prozessor). Ein FEP ist ein DFÜ-Server, der für seine DFÜ-Clients einen PPTP-Tunnel anlegt. Dieser Dienst ist wirklich praktisch, wenn er von einem Drittanbieter bereitgestellt wird. Ein anderer kann sich um Modempools kümmern und lokalen oder gebührenfreien Zugriff für die Benutzer bieten. Viele IPSs und NSPs stellen mehrere POPs (Points of Presence) für die Einwahl in FEPs bereit, die dann Daten an einen an Ihr lokales Netzwerk angeschlossenen terminierenden Tunnel-Server weitergeben. Beachten Sie, wo sich die POPs (Points of Presence) der ISPs befinden; sie sollten zum Ortstarif damit verbunden werden, um die Kommunikationskosten zu senken. Gegebenenfalls können Sie auch eigene FEP-Ausrüstung kaufen und Ihren eigenen DFÜ-Modempool einrichten.

20.7 Microsoft Windows 2000 VPN

Microsoft hat in Windows 2000 zahlreiche Funktionen und Sicherheitsverbesserungen von RRAS (Routing and Remote Access Services Server) und seine VPN-Implementierung aufgenommen. Die beiden wichtigsten Erweiterungen sind L2TP (Layer 2 Tunneling Protocol) und IPsec (IP Security Protocol). Mit der Implementierung dieser Protokolle gewährleistet Microsoft außerdem, dass Windows 2000 mit anderen Nicht-Microsoft-Geräten wie beispielsweise Routern oder Firewalls verbunden wird.

20.7.1 IPsec

IPsec ist ein Protokoll zur Gewährleistung von Datenintegrität und Authentifizierung. Außerdem sorgt es für Privatheit und Schutzmöglichkeiten für IP-Verkehr. Und weil es sich um ein offenes Protokoll handelt, das nicht Microsoft gehört, bietet es Interoperabilität mit anderen Systemen.

IPsec kann in zwei Protokolltypen unterteilt werden: IP-Protokoll 50 und IP-Protokoll 51. Das IP-Protokoll 50, auch als ESP-Format (Encapsulating Security Payload) bezeichnet, realisiert Privatheit, Authentifizierung und Datenintegrität. IP-Protokoll 51, das AH-Format (Authentication Header), bietet nur Integrität und Authentifizierung, aber keine Privatheit. IPsec wird in zwei Modi genutzt: Transportmodus und Tunnelmodus.

Der Transportmodus bietet Sicherheit für den IP-Verkehr von der Quelle zum Ziel zwischen zwei Systemen. Dieser Modus unterstützt Verschlüsselung zwischen den Verbindungsenden, aber keine wirkliche Tunnelingfunktion. Das Paket wird eingekapselt, verschlüsselt und an sein Ziel gesendet. Was passiert, wenn Sie dieses Paket durch ein komplexeres Netzwerk leiten wollen? Das Paket ist verschlüsselt und damit auch ein Teil der erforderlichen Routinginformation. Hier nun kommt der Tunnelmodus ins Spiel.

Der Tunnelmodus von IPsec legt ein existierendes IP-Paket innerhalb eines neuen Pakets ab, das zum Tunnelende geschickt wird. Der Tunnelmodus wird hauptsächlich für Zwischenknoten im Netzwerk bereitgestellt, beispielsweise Router, Gateways und Firewalls. Mit Hilfe von IPsec können diese Geräte einen Teil des IP-Pakets entschlüsseln, sodass die Routinginformation gelesen und das Paket sicher an sein Ziel geschickt werden kann. IPsec ist eigentlich nicht für den VPN-Zugriff von Remote-Usern vorgesehen, vielmehr soll es die Punkt-zu-Punkt-Sicherheit oder erzwungene Tunnel unterstützen. L2TP ist besser geeignet für eine Situation, wo ein einzelner Benutzer einen freiwilligen Tunnel zu einem Tunnel-Server über ein öffentliches Netzwerk anlegt.

20.7.2 L2TP (Layer 2 Tunneling Protocol)

Die erste Implementierung von PPTP, die in Windows DFÜ-Netzwerk Version 1.2 Upgrade enthalten war, war nicht vollständig ausgereift. Das von Cisco entwickelte Layer 2 Forwarding konnte einige der Funktionen bereitstellen, die in PPTP fehlten. Man erkannte schnell, dass es sinnvoll ist, diese beiden Protokolle zu kombinieren. Das Ergebnis war das Layer 2 Tunneling Protocol.

Das Layer 2 Tunneling Protocol wurde als IETF-Standardprotokoll (Internet Engineering Task Force) vorgeschlagen, das öffentliche Schlüssel für die Benutzerauthentifizierung benutzt und über sehr viel mehr Kommunikationsmedien eingesetzt werden kann als PPTP. L2TP unterstützt keine Verschlüsselung, wird aber genutzt, um Tunnel anzulegen, über die verschlüsselte Daten geschickt werden. Daten können über IP, X.25, Frame Relay und ATNs (Asynchronous Transfer Networks) geschickt werden. Wenn es für IP konfiguriert wird, kann L2TP über das Internet genutzt werden und sogar Nicht-Internet-Protokolle wie IPX und AppleTalk transportieren.

L2TP kapselt PPP-Frames ein und sendet sie unter Verwendung von UDP-Port 1701 an den terminierenden Tunnel-Server. Diese Kommunikation umfasst L2TP-Seuermeldungen für die Tunnelwartung sowie die gekapselten PPP-Frames. Diese Frames können komprimiert oder verschlüsselt werden. L2TP kann Authentifizierungsoptionen wie CHAP, MS-CHAP oder EAP (Extensible Authentication Protocol) verwenden. L2TP wurde sowohl für die Ende-Ende-Nutzung als auch für Client-Verbindungen für den Serverzugriff entwickelt. L2TP ist die natürliche Weiterentwicklung von PPTP; es führt Sicherheitsfunktionen ein und bietet eine größere Flexibilität in Hinblick auf die Medien. In Kombination mit IPSec stellt es einen offenen Standard zur Realisierung sehr sicherer und zuverlässiger VPNs dar.

20.8 Synchrone und asynchrone Schlüssel

Sowohl IPSec als auch L2TP verwenden IKE (Internet Key Exchange), das wiederum PKI-Zertifikate (Public Key Infrastructure) für die wechselseitige Authentifizierung benutzt. Sie können jetzt also asynchrone Schlüssel verwenden, die wesentlich sicherer sind als synchrone Schlüssel.

Ursprünglich wurden in PPTP synchrone Schlüssel verwendet. Beide Parteien mussten sich also auf einen Schlüssel einigen, um eine sichere Verbindung einrichten zu können. Dieser Schlüssel musste von einem System zum anderen transportiert werden. Beide Seiten verwendeten denselben Schlüssel. Wenn man wollte, dass ein anderes System diesen Schlüssel nutzte, musste man eine Kopie davon via E-Mail, Fax, Brief, Morsecode, Telefonanruf oder einen eingebauten Mechanismus in der VPN-Software übermitteln. Diese Kommunikation konnte abgehört und zur Entschlüsselung Ihrer Daten genutzt werden. Oder der Benutzer am anderen Ende konnte die Information anderen mitteilen, ohne dass Sie das kontrollieren konnten.

Asynchrone Schlüssel könnten Abhilfe schaffen. Jede Partei legt ein Schlüsselpaar an: einen öffentlichen Schlüssel und einen privaten Schlüssel. Diese Schlüssel sind nicht gleich, aber mathematisch ähnlich. Sie können Ihren öffentlichen Schlüssel beliebig weitergeben, halten aber Ihren privaten Schlüssel geheim. Wenn Ihnen jemand verschlüsselte Daten senden will, verschlüsselt er diese unter Verwendung Ihres öffentlichen Schlüssel. Dabei handelt es sich um eine Einwege-Verschlüsselung. Wenn also ein anderer Ihre Daten abfängt, kann er sie nicht entschlüsseln, selbst wenn er Ihren öffentlichen Schlüssel kennt.

Nur Sie können diese Daten mit Ihrem privaten Schlüssel entschlüsseln, weil nur Sie diesen Schlüssel besitzen. Analog können die von Ihnen mit Ihrem privaten Schlüssel verschlüsselten Daten mit Hilfe Ihres öffentlichen Schlüssels entschlüsselt werden. Damit ist keine Privatheit der Daten gewährleistet, weil jeder Ihren öffentlichen Schlüssel besitzen kann, aber Sie haben damit eine Methode zu garantieren, dass Ihre Daten von Ihnen kommen. Weil nur Sie den privaten Schlüssel besitzen, können die Daten nur von Ihnen stammen.

Mit IPSec verwenden beide Verbindungsenden einen öffentlichen und einen privaten Schlüssel, womit diese Form der Verschlüsselung möglich wird und die Datenintegrität sichergestellt ist. Empfängt ein Tunnel-Server Daten von Ihnen, kann er anhand Ihres öffentlichen Schlüssels sicherstellen, dass die Daten von Ihnen mit Ihrem privaten Schlüssel verschlüsselt wurden. Erhalten Sie Daten vom Tunnel-Server, die mit dessen privatem Schlüssel verschlüsselt wurden, können Sie die Integrität der Daten voraussetzen und sie mit dem öffentlichen Schlüssel des Servers entschlüsseln. Sie brauchen sich keine Gedanken über die Implementierung in Windows 2000 zu machen, aber Sie sollten das Konzept verstanden haben und wie praktisch die Verwendung von IPSec und L2TP gegenüber PPTP ist, was Privatheit und Integrität der Daten betrifft. Eine minimale zusätzliche Komplexität führt zu einer wesentlich verbesserten Sicherheit.

20.8.1 L2TP und IPSec

L2TP ist ein wohl durchdachtes Protokoll mit höherer Interoperabilität als IPSec. Es kompensiert die Defizite von IPSec in Hinblick auf freiwillige oder Client/Gateway-Anwendungen und wird von vielen anderen Anbietern unterstützt. Es unterstützt jedoch keine Verschlüsselung - nur das Anlegen von Tunneln. IPSec bietet ausgezeichnete Möglichkeiten für Verschlüsselung und Authentifizierung, unterstützt aber das freiwillige Tunneling nicht zufrieden stellend. Warum sollte man die beiden Protokolle nicht kombinieren und auf diese Weise verbesserte Sicherheit und Interoperabilität in Ihrem VPN gewährleisten?

Durch die Kombination von L2TP und IPSec können Sie ein VPN mit L2TP als Hauptprotokoll mit Nutzung verschlüsselter IPSec-Pakete anlegen. Diese Kombination wird häufig auch als L2TP/IPSec bezeichnet. Die Nutzung von L2TP in dieser Kombination bietet auch einige Vorteile von PPP, beispielsweise Verbindungen, Unterstützung mehrerer Protokolle (wie beispielsweise IPC) und Multicast.

Der einzige wirkliche Nachteil dieser Kombination ist die fehlende Zusammenarbeit mit NAT (Network Address Translation). Wie bereits erwähnt, können VPNs und NATs nicht immer kombiniert werden. Weil IPSec das IKE-Protokoll (Internet Key Exchange) nutzt, kann es nicht zusammen mit NAT eingesetzt werden. IKE verwendet Ihre IP-Adresse als Teil der Authentifizierung. Ihre IP-Adresse wird von NAT abgeändert und IKE kann Sie nicht erkennen. Wenn Sie also NAT in Ihrer Firewall einsetzen, müssen Sie Ihren Tunnel-Server außerhalb der Firewall platzieren. PPTP übernimmt das NAT und Sie können auch Clients mit älterer Software unterstützen, beispielsweise Windows 95, die kein L2TP/IPSec unterstützen; aus diesem Grund kann es erforderlich sein, dennoch PPTP zu implementieren.

20.9 Einrichtung eines grundlegenden VPN in Windows 2000

Bevor Sie anfangen, Ihr VPN einzurichten, brauchen Sie einige grundlegende Informationen. Als Erstes brauchen Sie die IP-Adressen Ihrer Endpunkt-Server. Sie können entweder über die IP-Adressen oder über einen DNS-Eintrag darauf verweisen. DNS ist hier möglicherweise die bessere Wahl, denn wenn sich irgendwann die IP-Adresse Ihrer Endpunkt-Server ändern sollte, ändern Sie sie nur in DNS und nicht auf allen Ihren Clients. Nachdem Sie die Platzierung Ihres VPN-Servers in Hinblick auf die Firewall festgelegt und einen Regelsatz für den Zugriff durch die Firewall eingerichtet haben, können Sie anfangen. Möglicherweise sollten Sie DHCP (Dynamic Host Configuration Protocol) einsetzen, sodass Ihre Clients gültige IP-Adressen in Ihrem Netzwerk erhalten.

Wir beginnen mit einem bei Bedarf eingerichteten VPN. Wie bereits erwähnt, übernimmt dabei der Client die Aufgabe, den VPN-Tunnel anzulegen und für die Verschlüsselung zu sorgen. Ein Beispiel dafür wäre ein Windows 98-Client, der das Internet nutzt, um eine Verbindung zu einer Domäne in Ihrem Netzwerk einzurichten. Im ersten Schritt richten Sie den RRAS-Server ein, um diese Verbindung zu ermöglichen.

Auf dem Windows 2000-Server wählen Sie in der Systemsteuerung **Netzwerk- und DFÜ-Verbindungen**. Mit **Neue Verbindung erstellen** richten Sie eine neue Verbindung ein. Sie erhalten einen Eröffnungsbildschirm angezeigt, der Ihnen kurz die Möglichkeiten mit diesem Assistenten erläutert. Wählen Sie **Weiter**. Im nächsten Bildschirm legen Sie den Netzwerkverbindungstyp fest. Hier können Sie die Einwahl in private Netzwerke, eine Verbindung zum Internet, eine Verbindung zu privaten Netzwerken über das Internet, die Entgegennahme ankommender Verbindungsanforderungen oder die direkte Verbindung zu einem anderen Computer einrichten. Wählen Sie **Eingehende Verbindungen akzeptieren** und klicken Sie auf **Weiter** (siehe Abbildung 20.1).

Netzwerkverbindungs-Assistent

Netzwerkverbindungstyp

Sie können den Typ der zu erstellenden Netzwerkverbindung wählen. Die Wahl sollte der Netzwerkkonfiguration und Ihren Bedürfnissen entsprechen.



- ☒ **In ein privates Netzwerk einwählen**
Stellt Verbindung über eine Telefonleitung (Modem oder ISDN) her.
- ☐ **In das Internet einwählen**
Stellt Internetanschluss über eine Telefonleitung (Modem oder ISDN) her.
- ☐ **Verbindung mit einem privaten Netzwerk über das Internet herstellen**
Stellt VPN-Verbindung oder Tunnel durch das Internet her.
- ☐ **Eingehende Verbindungen akzeptieren**
Andere Computer können über eine Telefonleitung, das Internet oder ein direktes Kabel eine Verbindung zu diesem Computer herstellen.
- ☐ **Direkt mit anderem Computer verbinden**
Stellt Verbindung über seriellen, parallelen oder Infrarotanschluss her.

< Zurück

Weiter >

Abbrechen

Abbildung 20.1: Der Bildschirm für die Auswahl des Netzwerkverbindungstyps. Wählen Sie die Option **Eingehende Verbindungen akzeptieren**, um ein freiwilliges VPN über das Internet einzurichten.

Der nächste Bildschirm beschreibt die eingehende virtuelle private Netzwerkverbindung. Hier wählen Sie **Virtuelle private Verbindungen zulassen** und klicken auf **Weiter** (siehe Abbildung 20.2).

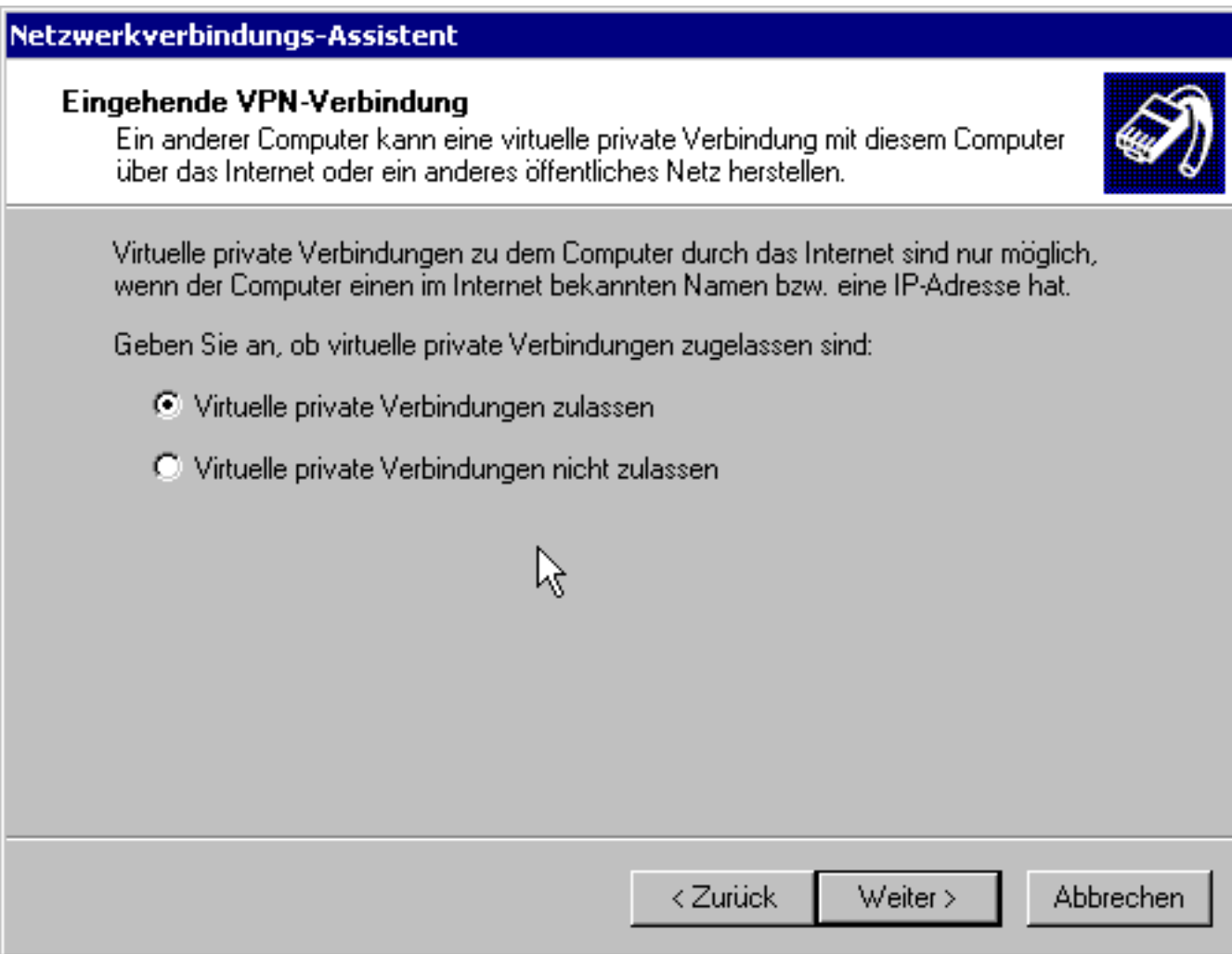


Abbildung 20.2: Über diesen Bildschirm lassen Sie eingehende virtuelle private Verbindungen zu

Im nächsten Bildschirm legen Sie fest, welche Benutzer über die VPN-Verbindung auf diese Maschine zugreifen dürfen. Hier sollten Sie nur die Benutzer angeben, die VPN nutzen, nicht einfach jedermann. Unnötig erteilte Benutzerrechte können zu Sicherheitslücken führen. Auf diesem Bildschirm fügen Sie Benutzer hinzu und ändern die Eigenschaften für die einzelnen Benutzer, beispielsweise Rückrufoptionen oder Kennwörter. Wählen Sie die betreffenden Benutzer aus und klicken Sie auf **Weiter** (siehe Abbildung 20.3).

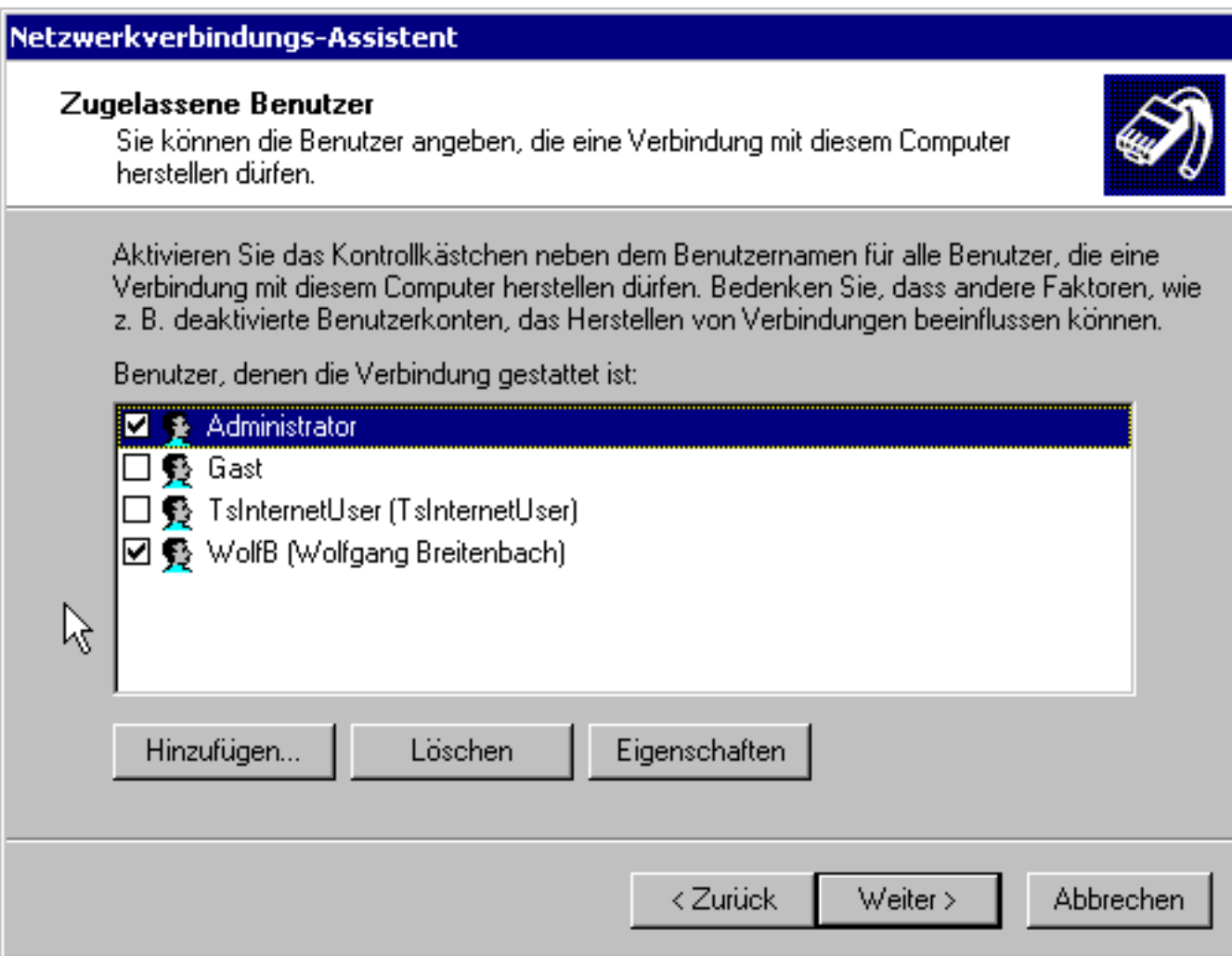


Abbildung 20.3: Über diesen Bildschirm legen Sie fest, welche Benutzer VPN-Zugriff erhalten

Im nächsten Bildschirm aktivieren oder deaktivieren Sie die Netzwerkkomponenten für Ihre VPN-Clients. Hier können Sie auch andere als die Internet-Standardprotokolle hinzufügen, beispielsweise IPX oder NetBEUI. Unter den Eigenschaften der einzelnen Protokolle legen Sie fest, ob die Benutzer mit diesem Protokoll Zugriff auf Ihr Netzwerk erhalten sollen. Für das Internet-Protokoll (TCP/IP) können Sie auch festlegen, ob Ihre VPN-Clients eine IP-Adresse über DHCP erhalten, oder ob ihnen direkt vom VPN-Server eine IP-Adresse zugeordnet wird. Sie können dem Benutzer auch erlauben, seine eigene IP-Adresse auszuwählen. Auch hier sollten Sie nur die Netzwerkkomponenten auswählen, die Ihre VPN-Clients wirklich brauchen. Klicken Sie auf **Weiter** (siehe Abbildung 20.4).

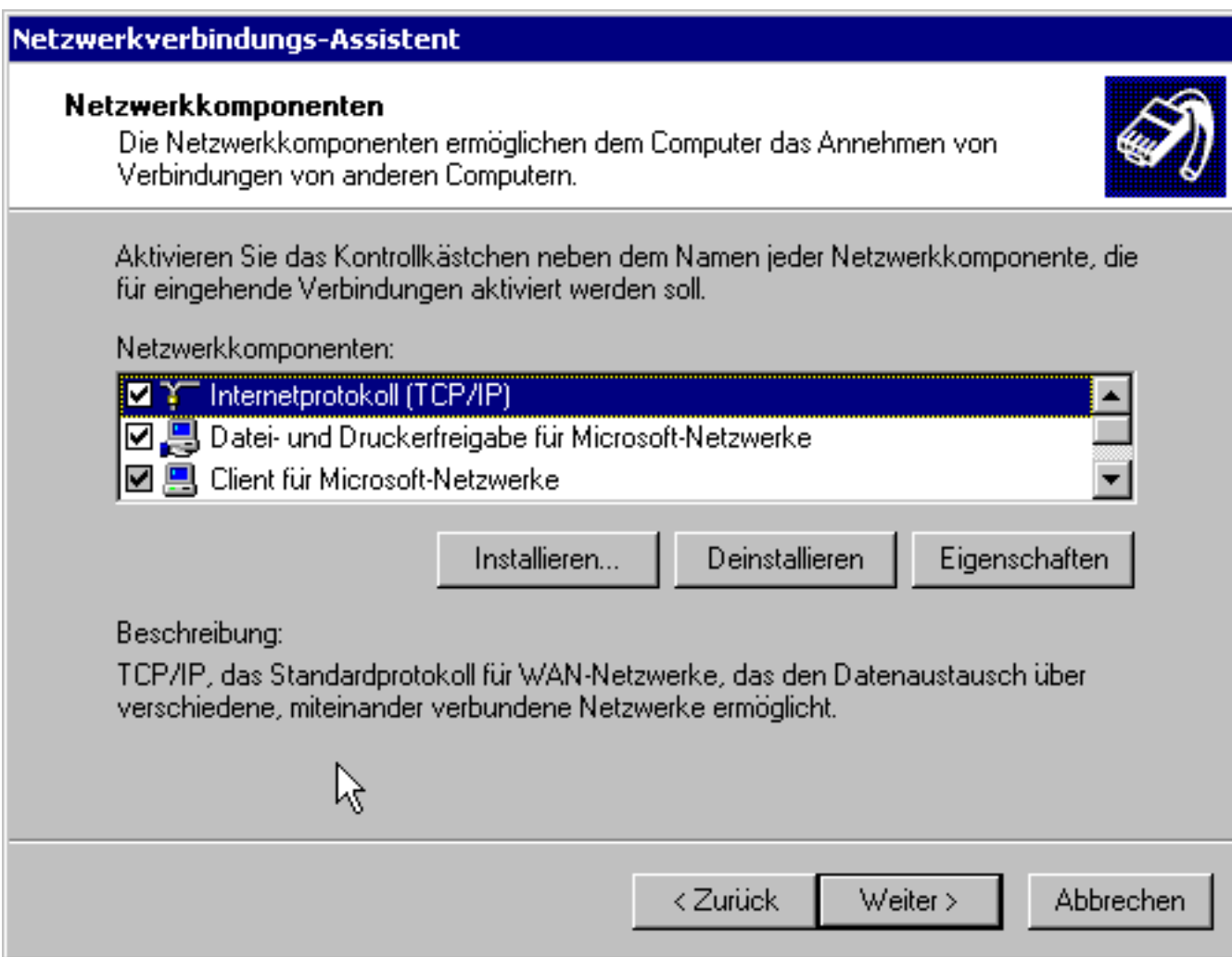


Abbildung 20.4: Der Bildschirm für die Auswahl der Netzwerkkomponenten erlaubt Ihnen die Auswahl, welche Netzwerkkomponenten über VPN zur Verfügung stehen

Damit sind Sie mit der Einrichtung Ihres VPN fertig. Klicken Sie auf **Fertig stellen** und betrachten Sie das Setup Ihres Windows 98-Clients. Doppelklicken Sie im **Arbeitsplatz** auf das Symbol **DFÜ-Netzwerk**. Dort wählen Sie **Neue Verbindung erstellen**. Sie werden nach einem Namen für diese Verbindung gefragt und müssen dann ein Gerät auswählen. Geben Sie einen beliebigen Namen ein und wählen Sie im Dropdown-Menü zur Geräteauswahl den **Microsoft VPN Adapter**. Klicken Sie auf **Weiter**. Im nächsten Bildschirm werden Sie nach dem Hostnamen oder der IP-Adresse gefragt. Weil Sie DNS zur Namensauflösung eingerichtet haben, können Sie hier einfach den Hostnamen eingeben und auf **Weiter** klicken. Damit sind Sie mit der Einrichtung der Windows 98-VPN-Verbindung fertig. Klicken Sie auf **Fertig stellen**.

Damit dieser Verbindungsaufbau im gesamten Internet genutzt werden kann, braucht der Windows 98-Client eine ISP-Verbindung über irgendein DFÜ-Medium zum Internet. Nachdem die Verbindung zum Internet eingerichtet ist, kann der Benutzer die von Ihnen angelegte VPN-Verbindung auswählen. Diese Verbindung löst den Hostnamen mit Hilfe Ihres öffentlichen DNS-Servers in eine IP-Adresse auf und stellt dann unter Verwendung eines VPN-Tunnels eine Verbindung zu dem Rechner her.



Viele nationale ISPs bieten mehrere POPs (Points of Presence) an. Größere nationale ISPs haben sehr viele POPs über das Land verstreut, sodass eine höhere Wahrscheinlichkeit besteht, dass Sie eine lokale DFÜ-Verbindung zum Internet einrichten können, auch wenn Ihre Clients sich »bewegen«. Damit verringern Sie Ihre Ausgaben für die Telekommunikation. Suchen Sie nach ISPs mit vielen POPs und einfacher Software, wenn Sie nach Einwahlmöglichkeiten für Ihre Benutzer Ausschau halten.

20.10 Einrichtung eines Tunnel-Server-VPN mit Windows 2000

Für unser nächstes Szenario wollen wir annehmen, dass Sie eine Filiale in Düsseldorf haben. In diesem Büro haben Sie DFÜ-ISDN-Zugriff auf das Internet und brauchen eine Verbindung zum Unternehmenshauptsitz in Frankfurt. Sie könnten nun jede Workstation als bedarfsgesteuerten VPN-Client einrichten, der die ISDN-Verbindung nutzt; Sie könnten aber auch einen Tunnel-Server einrichten und den Workstations diesen für die Verbindung zum Büro in Frankfurt zur Verfügung stellen.

Die Einrichtung eines Tunnel-Server-VPN (oder erzwungenen VPN) unter Windows 2000 erfolgt auf ähnliche Weise wie die Einrichtung des bedarfsgesteuerten Servers. Wählen Sie unter **Netzwerk- und DFÜ-Verbindungen** den Eintrag **Neue Verbindung erstellen**. Der Assistent zum Anlegen einer Netzwerkverbindung wird aufgerufen. Klicken Sie im Begrüßungsbildschirm auf **Weiter**. Sie gelangen zum Bildschirm zur Auswahl des Netzwerkverbindungstyps. Wählen Sie jetzt die Option **Verbindung mit einem privaten Netzwerk über das Internet herstellen**. Klicken Sie auf **Weiter**.

Falls Sie bereits eine DFÜ-Verbindung eingerichtet haben, erhalten Sie einen anderen Bildschirm. Dort werden Sie gefragt, ob Sie diese Verbindung automatisch einrichten wollen. Ist das nicht der Fall, deaktivieren Sie diese Möglichkeit und klicken auf **Weiter** (siehe Abbildung 20.5).

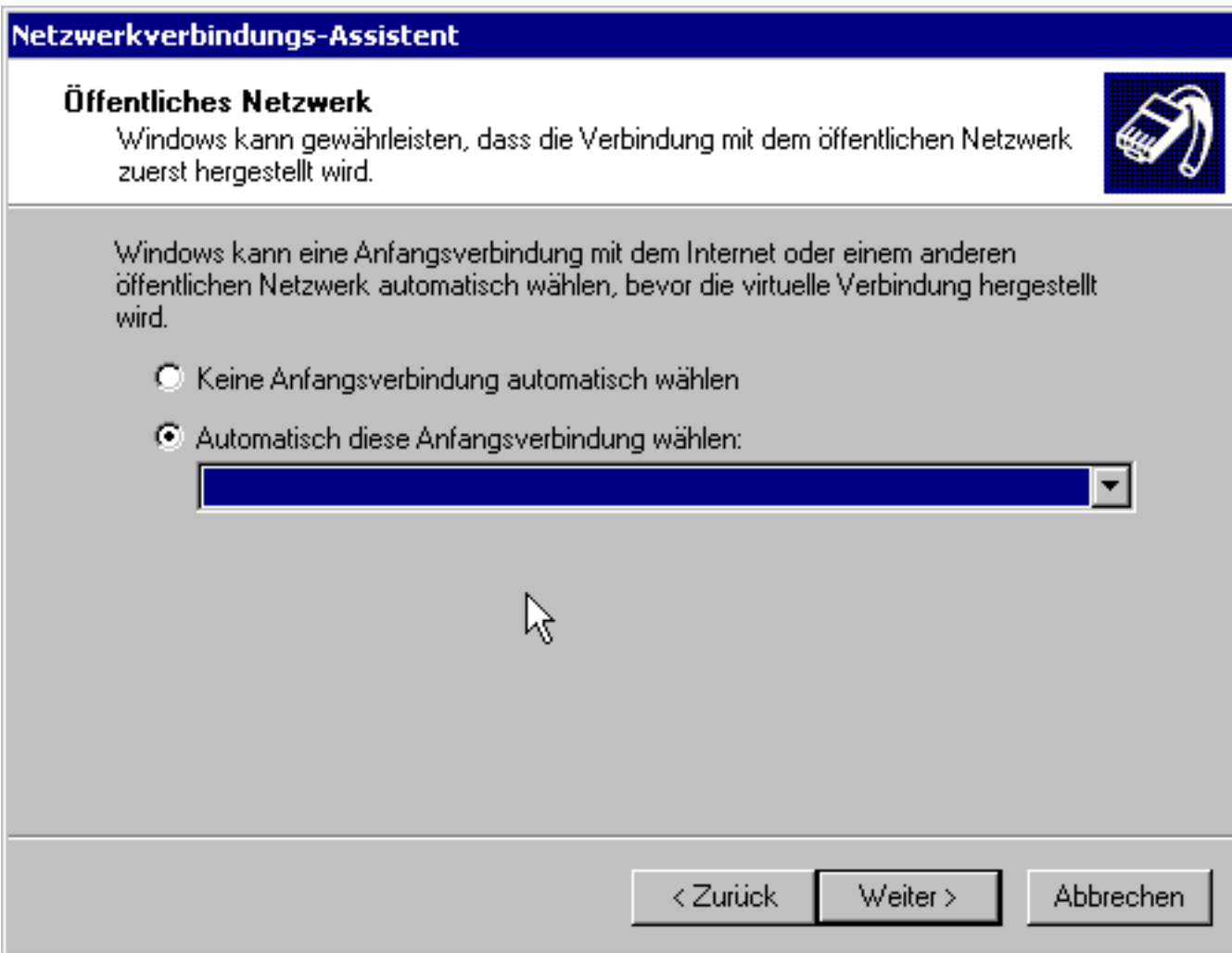


Abbildung 20.5: Der Bildschirm für die Auswahl des öffentlichen Netzwerks wird nur angezeigt, wenn Sie bereits eine DFÜ-Verbindung eingerichtet haben

Im nächsten Bildschirm legen Sie die Zieladresse fest. Geben Sie den Hostnamen des terminierenden VPN-Servers oder eine IP-Adresse ein und klicken Sie auf **Weiter** (siehe Abbildung 20.6).

Netzwerkverbindungs-Assistent

Zieladresse
Geben Sie den Namen oder die Adresse des Zielnetzwerks ein.

Geben Sie den Hostnamen oder die IP-Adresse des Computers oder Netzwerks ein, zu dem eine Verbindung hergestellt werden soll.

Hostname oder IP-Adresse (z.B. microsoft.com oder 123.45.6.78):

206.175.174.88

< Zurück Weiter > Abbrechen

Abbildung 20.6: Im Bildschirm zur Angabe der Zieladresse geben Sie den terminierenden Tunnel-Server als IP-Adresse oder als Hostnamen an



Weil Sie nur einen Server haben, der auf einen anderen verweist, und nicht viele Clients (wie es im Windows 98-Beispiel der Fall war), ist es möglicherweise nicht erforderlich, einen Hostnamen und DNS zu verwenden. Die Angabe der IP-Adresse könnte hier viel vorteilhafter sein. Wenn Ihr DNS aus irgendeinem Grund ausfällt, könnte es sein, dass Ihre VPN-Server keine Verbindung mehr einrichten können.

Im nächsten Bildschirm geht es um die verfügbaren Verbindungen. Hier legen Sie fest, ob andere Clients diesen Server als Tunnel-Server nutzen können, oder ob der Zugriff auf den Tunnel nur dem Server zur Verfügung stehen sollte. Wählen Sie **Diese Verbindung: für alle Benutzer verwenden** und klicken Sie auf **Weiter** (siehe Abbildung 20.7).



Abbildung 20.7: Auf dem Bildschirm zur Verfügbarkeit der Verbindung werden Sie gefragt, ob Sie Ihren VPN allen Benutzern oder nur dieser Maschine zur Verfügung stellen wollen. Falls Sie einen Tunnel-Server anlegen, sollten Sie die Option **Diese Verbindung: für alle Benutzer auswählen**.

Auf dem Bildschirm zur Freigabe der Internetverbindung werden Sie gefragt, ob Sie für diese Verbindung die Freigabe der Internetverbindung aktivieren wollen. Damit ist es allen Benutzern möglich, Ihren Rechner als Gateway zum Internet zu nutzen, während er als Tunnel-Server dient. In diesem Beispiel wollen wir diese Option nicht auswählen, klicken Sie also auf **Weiter**.



Wenn Sie die Freigabe der Internetverbindung aktivieren, müssen Sie den Server so einrichten, dass er die Umwandlung der Netzwerkadressen für Sie übernimmt. Weil der Server als Gateway zum Internet dient, braucht er korrekte Internet-Adressen, die er Ihren Benutzern zuweisen kann, wenn diese ins Internet gehen. Windows 2000 setzt die Internet-Adressen automatisch, wenn Sie das wirklich wollen. Falls Sie NAT nicht eingerichtet haben, weist er Ihrer internen Schnittstelle die IP-Adresse 192.168.0.1 zu und Sie müssen alle Ihre Workstations in diesem Netzwerk anlegen. Am besten deaktivieren Sie NAT, während Sie diese Option nutzen wollen.

Damit sind Sie fertig mit Ihrer Tunnel-Server-Verbindung; klicken Sie also auf **Fertig stellen**. Sie werden aufgefordert, die Verbindung anzulegen. Wenn Sie das nächste Mal eine automatische Anmeldung haben wollen, müssen Sie das Kennwort speichern. Wenn Sie die von Ihnen gewählten

Optionen ändern möchten, klicken Sie mit der rechten Maustaste auf das Symbol für diese Verbindung und wählen im Kontextmenü den Eintrag **Eigenschaften**.

20.11 RRAS-Erweiterungen

Microsoft hat RRAS (Routing and Remote Access Server) zunächst als Update des RAS (Remote Access Server) in Windows NT Server 4.0 bereitgestellt. Dieses Upgrade enthielt neue Funktionen wie beispielsweise PPTP/VPN-Unterstützung sowie mehr Routing-Unterstützung mit zusätzlichen Routingprotokollen, wie beispielsweise OSPF (Open Shortest Path First). In Windows 2000 wurden zusätzliche Erweiterungen eingeführt, die Ihnen ermöglichen, RRAS als nahezu vollfunktionale VPN-Lösung zu nutzen. Jetzt wollen wir diese Upgrades und ihre Implementierung betrachten.

RAS und RRAS unterstützten PPP Multilink, wobei mehrere physikalische Verbindungen (ISDN-, X.25- oder Modem-Verbindungen) zu einer einzigen logischen Verbindung kombiniert werden konnten, um eine größere Bandbreite zu realisieren. Unter Windows 2000 wurde diese Option durch die Einführung einer dynamischen Steuerung der DFÜ-Verbindungen erweitert. RRAS kann Bandbreite hinzufügen oder entfernen, indem nach Bedarf DFÜ-Verbindungen zugeschaltet oder entfernt werden. Damit erzielen Sie eine effizientere Nutzung Ihrer Kommunikationsressourcen, indem Sie Telefonleitungen freigeben, wenn diese nicht gebraucht werden. Außerdem wird damit die Ressourcenbelegung auf dem RRAS-Server vermindert.

Windows 2000 bietet außerdem Verbesserungen für das automatische Wählen. Beim automatischen Wählen werden IP-Adressen und Netzwerkverbindungen verwaltet, sodass diese nur gewählt werden, wenn sie benötigt werden. Damit können Sie den DFÜ-Prozess automatisieren, sodass ein Netzwerk bei Bedarf angewählt wird, ohne dass der Benutzer eingreifen muss.

Um diese Funktion nutzen zu können, öffnen Sie das Fenster **Netzwerk- und DFÜ-Verbindungen** und wählen im Menü **Erweitert** den Eintrag **DFÜ-Einstellungen**. Aktivieren Sie die Registerkarte **Automatisches Wählen**. Sie können das automatische Wählen je nach entsprechendem Standort festlegen. Entfernen Sie die Markierung im Kontrollkästchen für die Nachfrage vor der Einwahl, weil hier ein Tunnel-Server eingerichtet werden soll.

Wenn Sie jemals 90 Prozent einer 20 Mbyte großen Datei übertragen haben, um dann die Verbindung zu verlieren, werden Sie eine neue Möglichkeit von RRAS zu schätzen wissen: die direkte Fortsetzung einer abgebrochenen Datenübertragung. Diese Funktion setzt die Dateiübertragung automatisch fort, falls eine Leitung ausgefallen ist. Dabei wird aufgezeichnet, an welcher Stelle der Dateiübertragung die Leitung ausfiel, und Sie können die Übertragung nach der erneuten Einrichtung Ihrer Verbindung fortsetzen. Für diese Funktion müssen keine Attribute gesetzt werden. Genießen Sie diese Erweiterung einfach, wenn Sie beim nächsten Mal über das Telefonkabel stolpern und es aus der Wand reißen.

Wir haben in diesem Kapitel bereits über die Kombination von L2TP und IPSec gesprochen. Jetzt wollen wir einige der Aspekte betrachten, die bei der Implementierung dieser Verbesserung in Windows 2000 berücksichtigt werden müssen. Wie bereits erwähnt, verwenden Sie bei der Nutzung von L2TP für VPN in Windows 2000 automatisch auch IPSec. Es ist also keine eigentliche Konfiguration für IPSec erforderlich. Um L2TP nutzen zu können, legen Sie Zertifikate für beide Seiten an. Dazu verwenden Sie die Microsoft Management Console (MMC). Legen Sie für jeden Tunnel-Server ein Zertifikat an und tauschen Sie diese Zertifikate zwischen den Servern aus. Anschließend ändern Sie die Eigenschaften

Ihrer Verbindung ab.

Klicken Sie zuerst mit der rechten Maustaste auf die eben angelegte VPN-Verbindung und wählen Sie **Eigenschaften**. Aktivieren Sie die Registerkarte **Netzwerk**. Hier finden Sie ein Pulldown-Menü für die Auswahl des Typs des angerufenen VPN-Servers. Die Einstellung ist **Automatisch**. Um L2TP nutzen zu können, müssen Sie mindestens einen der Server auf L2TP setzen, aber am besten stellen Sie diesen Wert auf beiden Servern ein (siehe Abbildung 20.8).

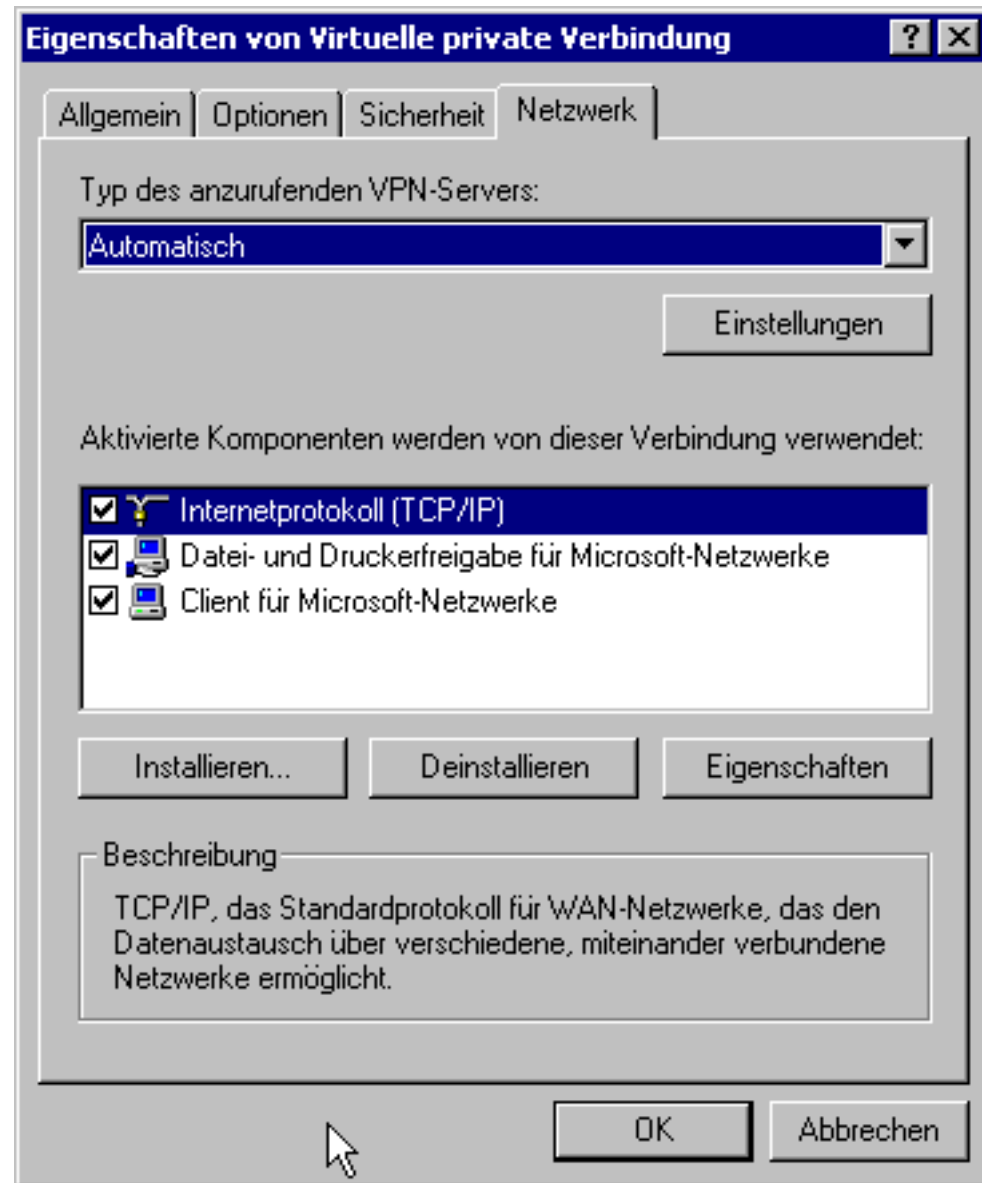
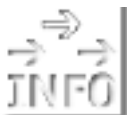


Abbildung 20.8: Die Eigenschaftsseite für die VPN-Verbindung. Hier ändern Sie Eigenschaften, wie beispielsweise den Typ des angewählten VPN-Servers.



RRAS richtet standardmäßig fünf PPTP- oder L2TP-Ports ein. Sie sollten diese Anzahl erhöhen. Dazu öffnen Sie **Routing und RAS**, klicken mit der rechten Maustaste auf **Anschlüsse** und wählen **Eigenschaften**. Hier konfigurieren Sie die Anzahl der Anschlüsse. Der maximale Wert beträgt 1.000.

Administration des Server

Teil VI

21. [Serververwaltung](#)

22. [Leistungsoptimierung und Tuning](#)

23. [Dienstprogramme zur Sicherung des Servers](#)

24. [Wiederherstellung nach Systemausfällen](#)

Kapitel 21 Serververwaltung

Die Administration eines Servers kann unterschiedliche Formen annehmen, aber in diesem Kapitel geht es hauptsächlich um die Verwaltung der Server-Hardware sowie der Hardware in der Server-Einheit. Mit anderen Worten: Wir wollen uns in diesem Kapitel nicht damit beschäftigen, Benutzerkonten anzulegen, Protokolle auszuwählen oder eine Verzeichnisstruktur zu erklären, weil das alles schon passiert ist.

Wir wollen Ihnen in diesem Kapitel demonstrieren, wie der eigentliche Server sowie die von Ihnen verwendeten Werkzeuge verwaltet werden. Unter anderem geht es dabei um:

- Die Microsoft Management Console
- Dienstprogramme zur Selbstverwaltung
- SNMP

21.1 Microsoft Management Console (MMC)

Die Serveroberfläche von Windows 2000 besitzt ein neues Frontend, die Microsoft Management Console, auch kurz als MMC bezeichnet. Selbst wenn Sie vielleicht schon den Spitznamen »Mickey Maus-Konsole« gehört haben, handelt es sich hierbei doch um ein sehr praktisches Werkzeug. Die Konsole ist eine benutzerdefinierbare Oberfläche, auf der der Administrator zentral alle Aufgaben für alle Server erledigen kann.

Zunächst ist dieses Werkzeug nichts als eine leere Seite, auf der der Administrator die Werkzeuge ablegen kann, die er für seine täglichen Arbeiten benötigt (siehe Abbildung 21.1). Man könnte die MMC also mit einem leeren Werkzeugkasten vergleichen, den der Administrator mit bestimmten Werkzeugen für bestimmte Aufgaben füllen kann.

Die Werkzeuge in der MMC werden Ihnen nach den letzten 20 Kapiteln dieses Buchs durchaus vertraut vorkommen - sie wurden bereits beschrieben. Sie können die Konsolenwerkzeuge auch separat nutzen; als Einzelwerkzeuge verhalten sie sich nicht anders. Einige Beispiele dafür wären etwa Active Directory-Benutzer und -Computer, Computerverwaltung oder die DHCP-Konsole.

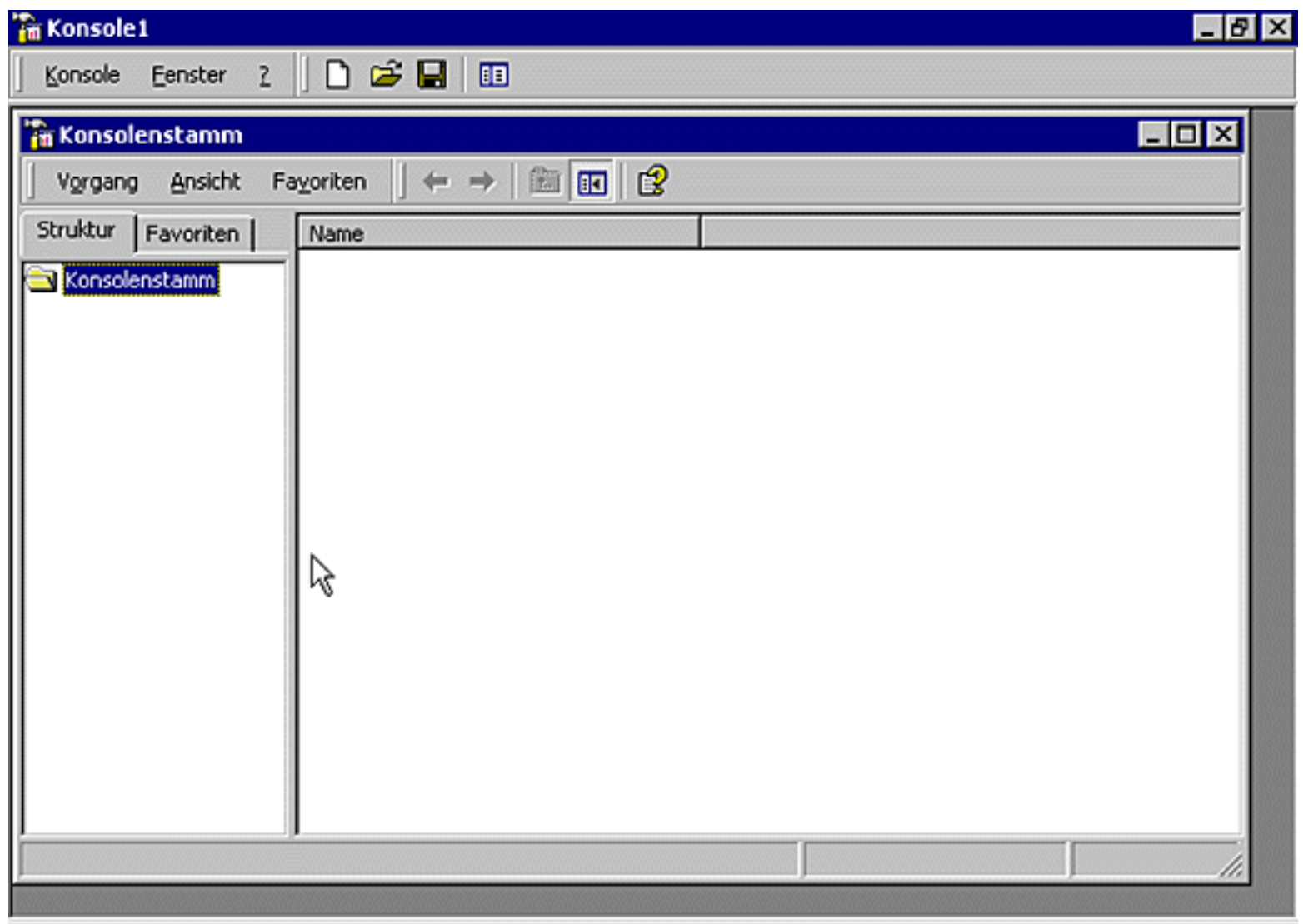


Abbildung 21.1: Eine leere MMC (Microsoft Management Console)

Alle der Konsole hinzugefügten Werkzeuge werden als »Snap-Ins« bezeichnet, weil sie in die Konsole eingeklinkt werden und als Teil von ihr auftreten. Der Administrator kann beliebig viele Snap-Ins in die Konsole einfügen und sogar unterschiedliche Konsolen anlegen, die er für unterschiedliche Aufgabenstellungen nutzt. Das Aussehen der Konsole erinnert etwas an den Windows-Explorer von Windows 95/98 und NT 4.0, aber hier werden Werkzeuge angezeigt. Abbildung 21.2 zeigt eine gefüllte Konsole mit geöffneten Werkzeugen.

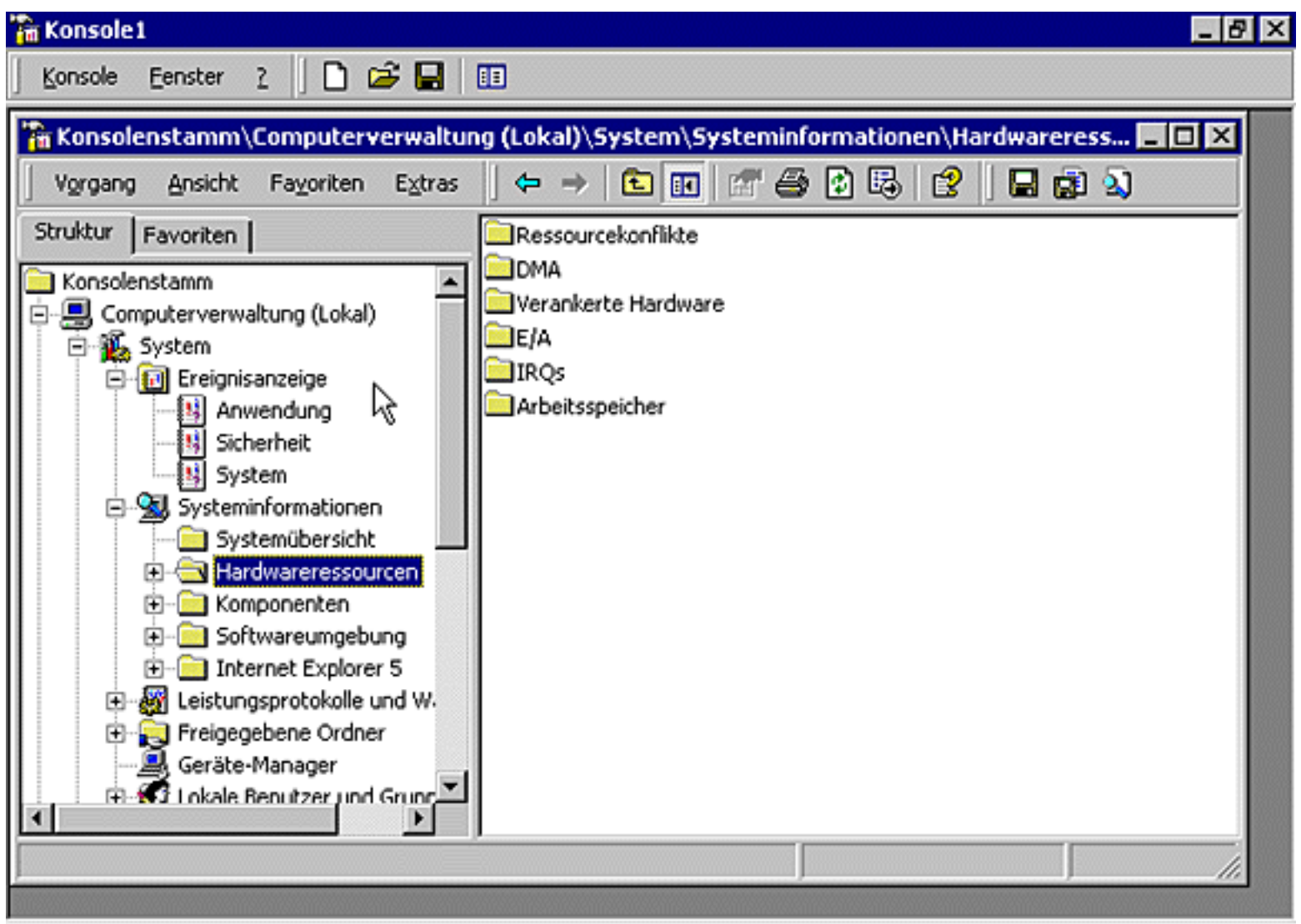


Abbildung 21.2: Eine gut gefüllte MMC-Konsole

Um als Administrator Einträge in einer Konsole vorzunehmen, gehen Sie wie folgt vor:

1. Öffnen Sie die MMC, indem Sie im Startmenü von Windows 2000 den Befehl **Ausführen** wählen.
2. Geben Sie MMC in das Textfeld ein und drücken Sie die (Enter)-Taste.
3. Wählen Sie im Menü **Konsole** den Eintrag **Snap-In hinzufügen/entfernen** und klicken Sie im gleichnamigen Dialogfeld auf **Hinzufügen**, um das in Abbildung 21.3 gezeigte Dialogfeld zu öffnen.



Abbildung 21.3: Der Bildschirm zum Hinzufügen eines eigenständigen Snap-Ins

4. Wählen Sie ein Snap-In in der Liste aus und klicken Sie noch einmal auf **Hinzufügen** (für einige Snap-Ins sind Konfigurationseinträge erforderlich).

5. Nachdem Sie alle gewünschten Snap-Ins ausgewählt haben, wählen Sie **Schliessen** und im nächsten Dialogfeld **OK**.

Nachdem Sie eine Konsole für die Ausführung bestimmter Aufgaben angepasst haben, sollten Sie sie speichern. Andernfalls muss die MMC bei jedem Öffnen neu angepasst werden. Um eine Konsole zu speichern, wählen Sie im Menü **Konsole** den Befehl **Speichern**. Nachdem die Konsole gespeichert wurde, öffnen Sie sie später, indem Sie auf das zugehörige Symbol doppelklicken. Sie können alle Arten von benutzerdefinierten Konsolen anlegen.

Darüber hinaus ist es möglich, Konsolen anzulegen und sie an remote befindliche Administratoren zu senden, um diese bei ihrer Arbeit zu unterstützen. Sie könnten beispielsweise eine Konsole mit **Active Directory-Benutzer und -Computer** und **Active Directory-Domänen und -Vertrauensstatus** für den Administrator der Verzeichnisstruktur anlegen. Eine andere Konsole könnte die Computerverwaltungsdienste enthalten und einem lokalen Hardwareadministrator Informationen bereitstellen. Wiederum eine andere Konsole könnte **DHCP** und **DNS** enthalten, um die Verwaltung des Domänennamenssystems des Unternehmens zu unterstützen.

Die MMC ist also kein eigenständiges Werkzeug, sondern stellt eine Möglichkeit dar, Werkzeugpakete

zu packen. Diese Werkzeuge können mobil eingesetzt werden - wenn Sie sie beispielsweise auf einer Diskette speichern. Sie können aber weitere Werkzeuge aufnehmen, sodass Sie einen Administrator nicht auf ein einziges Werkzeug beschränken.

21.2 Dienstprogramme zur Serververwaltung

Die früheren Versionen von Windows Server (NT) verwendeten den so genannten Server-Manager für viele der administrativen Aufgaben in der Domäne und auf den Servern. Windows 2000 unterstützt dieses Werkzeug zwar weiterhin (siehe Abbildung 21.4), ist aber nicht für die Nutzung in Windows 2000-Domänen vorgesehen. Der Server-Manager soll lediglich ältere Systeme unterstützen.

Um auf den Server-Manager zuzugreifen, gehen Sie wie folgt vor:

1. Wählen Sie im Startmenü den Befehl **Ausführen**.
2. Geben Sie SRVMGR in das Textfeld ein und drücken Sie die (Enter)-Taste.

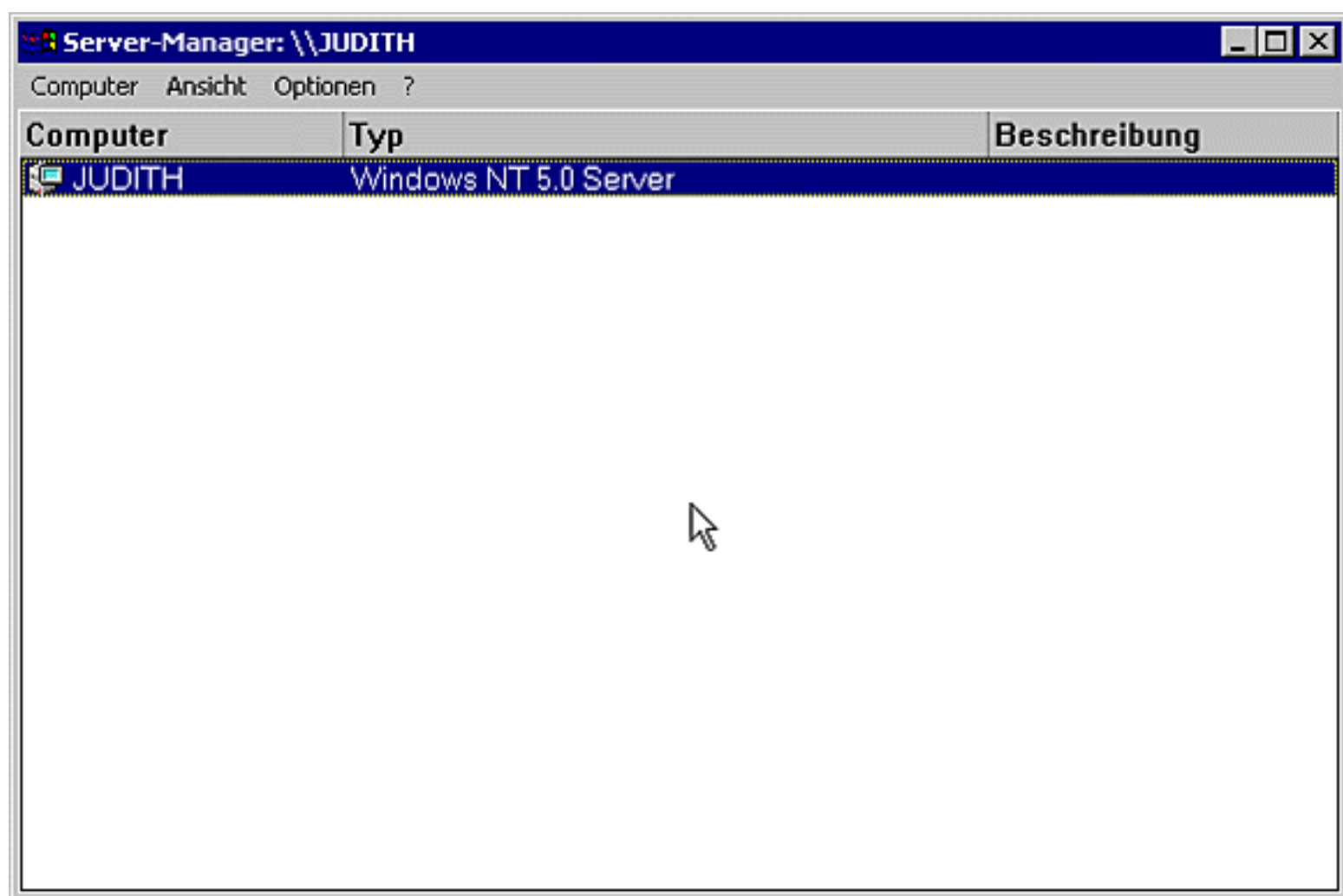


Abbildung 21.4: Der Server-Manager in Windows 2000

Der Server-Manager übernahm bei Windows NT die unterschiedlichsten Aufgaben. Die folgende Liste zeigt, welche Werkzeuge in Windows 2000 für diese Aufgaben genutzt werden können:

- Feststellen, welche Server in der Domäne eingesetzt werden:

Dazu verwenden Sie heute **Active Directory-Benutzer und -Computer**, indem Sie die Domäne dort einfach öffnen und in den Container **Domänencontroller** sehen.

- Feststellen, welche Ressourcen der Server freigibt:

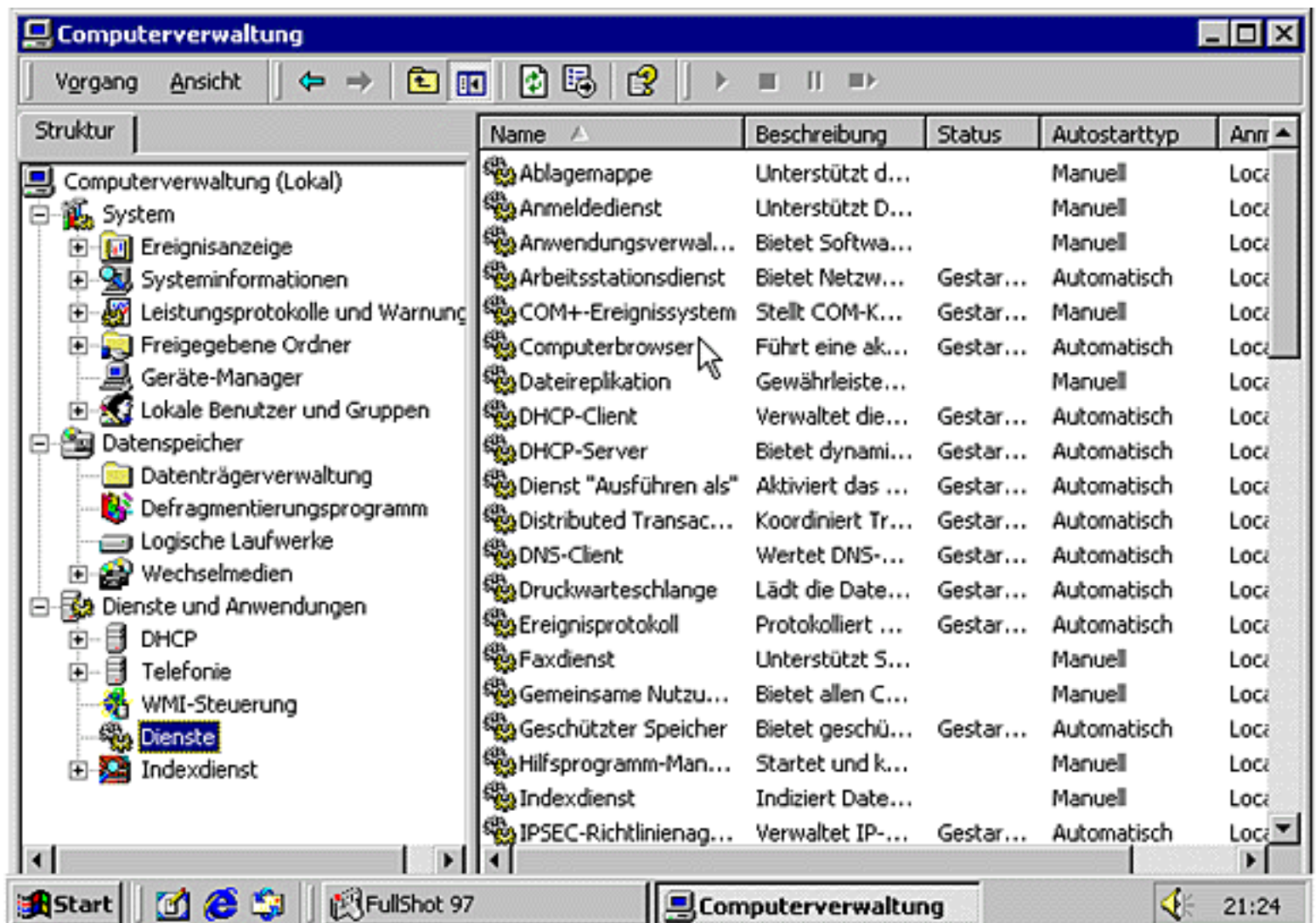
Freigaben werden im Snap-In **Computerverwaltung** angezeigt. Sie erreichen dieses Snap-In am einfachsten für jeden Computer unter **Active Directory-Benutzer und -Computer**. Suchen Sie dort nach dem Computer, den Sie verwalten wollen, klicken Sie mit der rechten Maustaste auf dessen Symbol und wählen Sie den Eintrag **Verwalten**.

- Steuerung der auf einem bestimmten Computer genutzten Dienste:

Dienste werden im Snap-In **Computerverwaltung** eingesehen.

Viele der Dienste aus dem Server-Manager werden heute in der **Computerverwaltung** bereitgestellt. Der Server-Manager hätte einfach auch in **Computerverwaltung** umbenannt werden können, weil das Werkzeug Ansichten der Workstations und Server bietet, die Windows 2000 oder Windows NT ausführen.

Die Computerverwaltungskonsole ist ein Werkzeug, das die einzelnen Komponenten des betreffenden Computers aufnimmt und dem Administrator erlaubt, sie zu überwachen oder zu steuern. Abbildung 21.5 zeigt die verschiedenen Komponenten.



21.2.1 Ereignisse anzeigen

Um die Ereignisanzeige unabhängig von der Computerverwaltung zu starten, wählen Sie im Startmenü nacheinander die Einträge **Programme/Verwaltung/Ereignisanzeige** (siehe Abbildung 21.6).

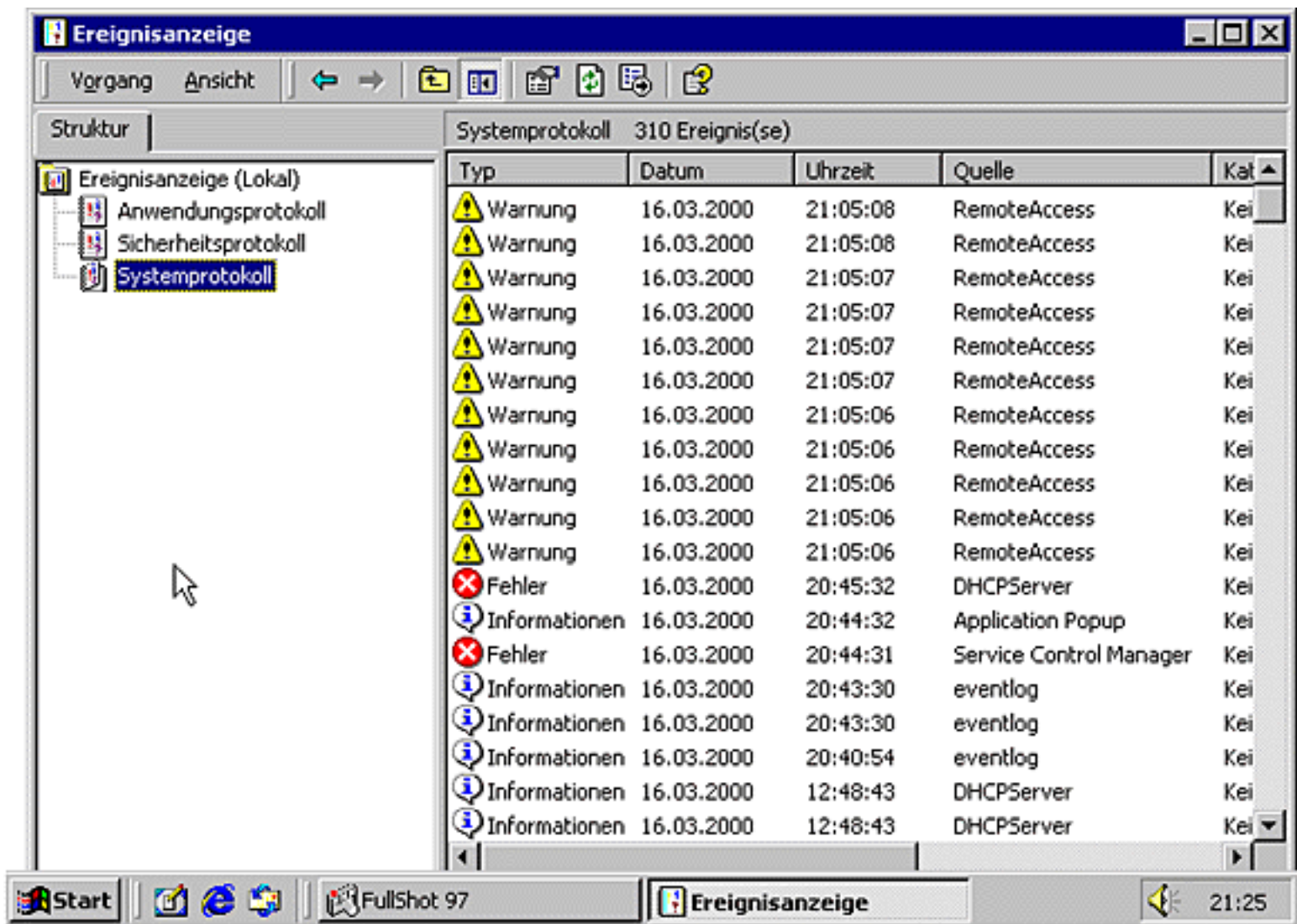


Abbildung 21.6: Die Ereignisanzeige

Innerhalb der Ereignisanzeige können - abhängig von der Konfiguration Ihres Systems - unterschiedliche Protokolle geführt werden. Eine Kernmenge an Ereignissen sowie die vom Standard abweichenden Ereignisse werden im Systemprotokoll, Anwendungsprotokoll und Sicherheitsprotokoll aufgezeichnet.

Im Systemprotokoll werden alle Ereignisse aufgezeichnet, die mit der Leistung oder der Funktionalität des Servers zu tun haben. Beim Starten des Systems wird ein Systemprotokoll geöffnet. Die Ereignisanzeige registriert ihren eigenen Beginn im Protokoll (siehe Abbildung 21.7). Jedes nachfolgend auftretende Ereignis wird aufgezeichnet und nach Typ und Dringlichkeit markiert.



Abbildung 21.7: Die geöffnete Ereignisanzeige

Das Anwendungsprotokoll wird nur von Anwendungen genutzt, die dafür konfiguriert wurden. Mit anderen Worten, das Betriebssystem protokolliert nicht alle Anwendungen und schreibt nicht alle ihre Ereignisse in das Anwendungsprotokoll. Ein Beispiel für eine Software, die das Anwendungsprotokoll nutzt, ist ein Groupware-Paket Exchange von Microsoft. Exchange schreibt viele Ereignisse in das Anwendungsprotokoll, die dem Administrator mitteilen, was in der Anwendung passiert ist.

Das Sicherheitsprotokoll zeichnet nichts auf, solange Sie nicht die Überwachung im Sicherheitssystem von Windows 2000 aktiviert haben. Das Starten dieser Überwachung kann von einer Änderung einer Gruppenrichtlinie abhängig gemacht werden und die Standardrichtlinie für die gesamte Domäne beinhalten.

Zur Einrichtung einer Überwachung gehen Sie wie folgt vor:

1. Öffnen Sie **Active Directory-Benutzer und -Computer**.
2. Klicken Sie in der Konsolenstruktur auf **Domain Controllers**.
3. Klicken Sie auf **Vorgang** und wählen Sie **Eigenschaften**.
4. Auf der Registerkarte **Gruppenrichtlinie** klicken Sie auf die Richtlinie, die geändert werden soll, und dann auf **Bearbeiten**.
5. Im Fenster **Gruppenrichtlinie** der Konsolenstruktur wählen Sie nacheinander die Symbole **Computerkonfiguration**, **Windows-Einstellungen**, **Sicherheitseinstellungen**, **Lo-kale Richtlinien**, **Überwachungsrichtlinien**.
6. Im Detailbereich klicken Sie auf das Attribut oder Ereignis, das überwacht werden soll.
7. Klicken Sie auf **Vorgang** und dann auf **Sicherheitseinstellungen**.
8. Ändern Sie die Konfigurationseinstellungen entsprechend ab.

Das Ereignis in Abbildung 21.7 hat mehrere Eigenschaften. Wenn Sie einen Vorfall auf einem Server beobachten, können die Elemente in diesem Ereignis zu einer Antwort führen, weil sie auf eine bestimmte Position verweisen. **Typ**, **Ereignis-ID**, **Quelle** und **Kategorie** sind nur Teile des Puzzles. Sie verschaffen Ihnen Informationen, die Sie zum Schuldigen führen.

Suchen Sie einmal anhand der folgenden Informationen im Microsoft TechNet (support.microsoft.com/search) nach Lösungen - Sie werden erstaunt sein, wie oft Sie eine Antwort finden, ohne den technischen Support anrufen zu müssen. Sie werden Erfolg haben, wenn Sie die folgenden Eigenschaften genauer betrachten:

- **Ereignis-ID:** Eine ID, die vom technischen Support bei Microsoft oder auf der Site support.microsoft.com genutzt wird, um einen bestimmten Vorfall nachzuschlagen. Falls Sie sonst keine Informationen für ein Ereignis finden, dann zumindest diese Nummer.
- **Typ:** Die Schwere des Ereignisses. Diese Typen beinhalten Information, Warnung und Fehler. Jeder Typ wird in der Ereignisanzeige durch ein Symbol dargestellt, wie in Abbildung 21.7 gezeigt.
- **Quelle:** Die Anwendung oder der Dienst, die das Ereignis verursacht oder das Ereignis im Protokoll aufgezeichnet haben. Weil es gute und schlechte Ereignisse gibt, bedeutet das nicht, dass die Quelle einen Fehler verursacht hat, sondern einfach, dass es eine Information an das System weitergegeben hat.
- **Kategorie:** Eine anwendungsspezifische Angabe, die im Allgemeinen nicht genutzt wird, außer in Hinblick auf die Sicherheit. Hier kann die Kategorie dabei helfen, eine Position für die Überwachungsdaten festzulegen.
- **Beschreibung:** Daten, die spezifische Informationen über den Fehler auf diesem Server bereitstellen. Im Allgemeinen legt der Entwickler einer Anwendung oder des Dienstes diese Beschreibung fest, die in das Ereignisprotokoll eingetragen wird, wenn ein bestimmter Fehler auftritt. Dieser Teil des Ereignisses ist der zweitwichtigste Aspekt, nach dem Sie suchen sollten.

Natürlich sind auch Zeit und Datum wichtig, aber ihre Bedeutung ist offensichtlich. Wenn beispielsweise genau jeden Donnerstag um 22:00 Uhr ein bestimmtes Ereignis auftritt, sollte der dienstbeflissene Administrator eben am nächsten Donnerstag um 22:00 Uhr anwesend sein. Es ist wichtig zu wissen, wann ein Fehler auftritt oder wie lang die Zeitspannen zwischen seinem Auftreten sind.

21.2.2 Protokolleinstellungen

Die Protokolle können gesteuert und manipuliert werden, um die Informationen aufzunehmen, die der Administrator braucht - zumindest in gewissem Maße. Wenn Probleme mit dem Server auftreten, stellen die Unternehmen oft sehr schnell fest, dass das Serverprotokoll voll ist. Das ist zwar ein berechtigter Hinweis darauf, dass zu viele Ereignisse auf diesem Server aufgezeichnet werden und etwas überprüft werden sollte, aber nicht die sinnvollste Methode, einen Server zu betreiben. Sie sollten die Protokolle und ihre Größe regelmäßig überprüfen. Ein volles Protokoll weist in der Regel auf eine volle Festplatte hin.

Die Einstellungen für die Protokolle werden in ihren Eigenschaftsseiten festgelegt. Klicken Sie mit der rechten Maustaste auf ein Protokoll und wählen Sie den Eintrag **Eigenschaften** (siehe Abbildung 21.8).

Als Erstes sehen Sie die Registerkarte **Allgemein**. Hier kann der Administrator festlegen, wie die

Protokolldatei gespeichert und ob sie geleert werden soll.

Die Einstellung **Maximale Protokollgrösse** legt genau das fest, was sie besagt. Die Protokolldatei ist standardmäßig 512 Kbyte groß. Das sollte genügend Platz bieten, um die normalen Ereignisse auf einem Windows 2000-Server zu protokollieren. Man kann diesen Wert aber auch ganz einfach vergrößern, um ein Ereignis über eine längere Zeitdauer zu beobachten. Tragen Sie dazu in das Textfeld den entsprechenden Wert in Kilobyte ein.

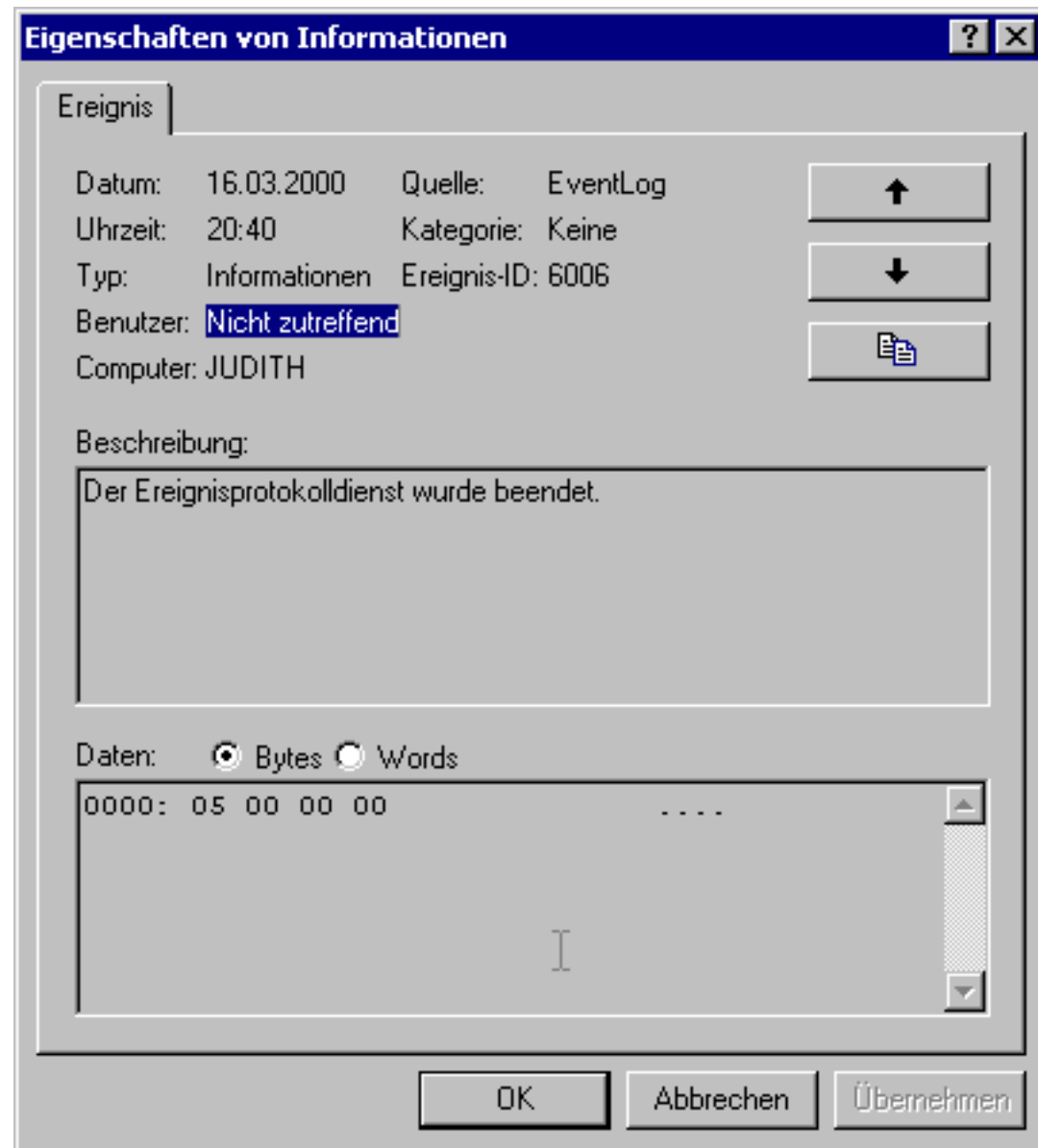


Abbildung 21.8: Eigenschaften eines Anwendungsprotokolls

Im Abschnitt **Protokollgrösse** werden die Größe und das Alter der Protokolldatei festgelegt. Dort gibt es die folgenden Optionen:

- **Ereignisse nach Bedarf überschreiben:** In das Protokoll werden so lange Ereignisse geschrieben, bis es voll ist (d.h. die maximale Größe erreicht wurde). Danach ersetzen die neuen Ereignisse die alten.
- **Ereignisse überschreiben, die älter als (X) Tage sind:** Ereignisse werden so lange in das Protokoll geschrieben, wie in dieser Option angegeben. Alle älteren Ereignisse werden aus der

Liste entfernt. Diese Einstellung gibt zurück, dass das Protokoll voll ist, wenn es seine maximale Größe erreicht hat, aber das Zeitlimit noch nicht erreicht wurde.

- **Ereignisse nie überschreiben (Protokoll manuell löschen):** Falls es ein Serverproblem gibt, das schwer zu überwachen ist, verhindert diese Einstellung, dass ein Protokoll gelöscht wird, bevor der Administrator es sieht. Diese Einstellung gibt zurück, dass das Protokoll voll ist, sobald es seine maximale Größe erreicht hat, aber noch nicht gelöscht wurde.

Es passiert selten, dass ein Administrator ein Protokoll auf diese Weise wartet. Manchmal ist die einzige Möglichkeit, ein Ereignis ab seiner Entstehung zu beobachten, das Ganze zu löschen und ganz von vorne zu beginnen. Im Allgemeinen ist es jedoch am besten, die Protokolldatei zu vergrößern, sodass das Protokoll nicht überschrieben werden kann. Nachdem Sie das Ereignis erkannt und korrigiert haben, können Sie die Einstellungen auf die alten Werte zurücksetzen.

Mit Hilfe von Filtern veranlassen Sie, dass nur die für Sie wichtigen Daten in das Protokoll aufgenommen werden. Die entsprechenden Optionen setzen Sie auf der Registerkarte **Filter** in den Protokolleigenschaften.

Mit Hilfe von Filtern steuern Sie auch die Zeitspanne für die Aufzeichnung von Daten. Tritt ein Ereignis jede Nacht zwischen Mitternacht und 1 Uhr auf, kann der Administrator das Protokoll so einstellen, dass genau dieser Zeitraum beobachtet wird. Dabei werden in der Regel auch detailliertere Daten für Sicherheit und Anwendung aufgezeichnet. Angenommen, ein Hacker meldet sich als Vorgesetzter an und Sie wollen detaillierte Informationen aufzeichnen, ohne dass dabei die normalen Ereignisse Ihres Systems berücksichtigt werden.

Sie können festlegen, welche Ereignistypen aufgezeichnet werden sollen. Typfilter erlauben dem Administrator, Meldungen zu verwerfen, die nur der Information dienen, oder Bestätigungsmeldungen, um auf diese Weise Platz für die Fehlerprotokollierung zu schaffen. In dem oben beschriebenen Szenario wäre es beispielsweise sinnvoll, nur Sicherheitsbestätigungsmeldungen aufzuzeichnen.



Sie sollten nicht ausschließlich bestimmte Ereignisse aufzeichnen, es sei denn, Sie sind ganz sicher, nach welchen Ereignissen Sie suchen. Selbst ein erfahrener Analytiker kann von der Ereignisanzeige überrascht werden. Wenn Sie einen Filter setzen, das problemschaffende Ereignis aber außerhalb dieses Bereichs liegt, vergeuden Sie nur Ihre Zeit.

21.2.3 Systeminformation

Der Abschnitt **Systeminformationen** in der Computerverwaltungskonsolle zeigt die enthaltene Information nur an. Sie können sie nicht ändern oder manipulieren, finden dort aber vielleicht Antworten, die Ihnen im Fehlerfall weiterhelfen (siehe Abbildung 21.9). Es ist nicht möglich, die Informationen an dieser Stelle zu ändern, Sie können sie aber ausdrucken.

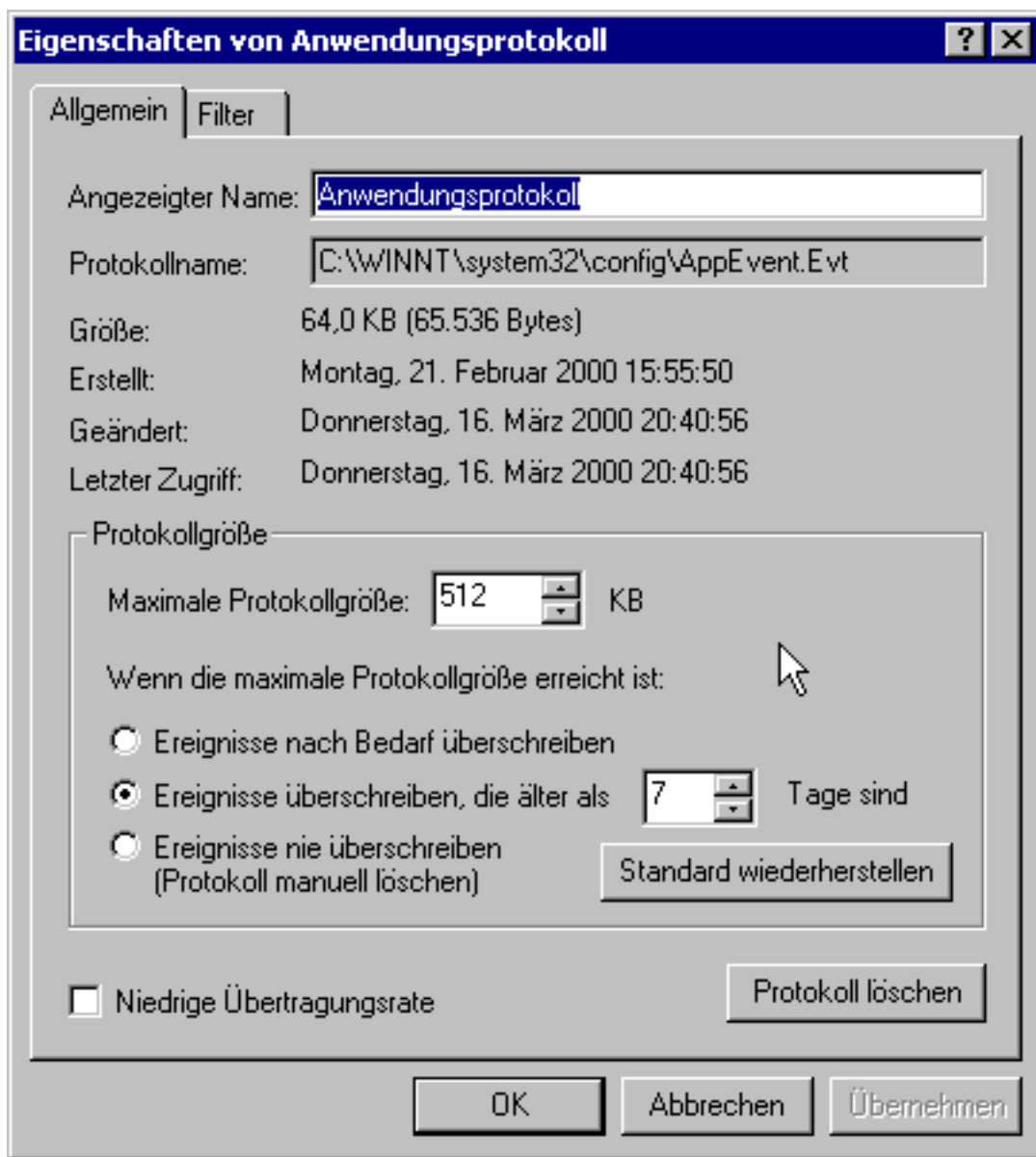


Abbildung 21.9: Der Bildschirm mit den Systeminformationen

21.2.4 Geräte-Manager

Dem Administrator, der bereits unter Windows 95/98 gearbeitet hat, ist der Geräte-Manager nicht neu. Er wurde unverändert in Windows 2000 übernommen und steht jetzt auch auf der Serverplattform zur Verfügung.

Sie öffnen den Geräte-Manager durch Anklicken seines Symbols in der Computerverwaltung. Die Oberfläche verhält sich wie der Windows-Explorer. Auf der obersten Ebene werden die allgemeinen Gerätetypen aufgelistet (Festplattenlaufwerke, Grafikkarten, Netzwerkkarten usw.). Neben jeder dieser Kategorien gibt es ein Pluszeichen. Es bedeutet, dass innerhalb dieser Kategorie ein Gerät vorhanden ist. Klicken Sie das Pluszeichen an, um die Einträge dieser Kategorie anzuzeigen.

Wie in Abbildung 21.10 gezeigt, erscheint ein Fragezeichen für Einträge, die vom Geräte-Manager nicht identifiziert oder fehlinterpretiert werden.



Dieses Fragezeichen ist ein Hinweis auf eine Neuheit in Windows 2000, die ebenfalls auf Windows 95/98 zurückzuführen ist - Plug&Play. Plug&Play ist dafür verantwortlich, dass der Geräte-Manager von Windows 2000 Hardware erkennen kann, die ihm nicht explizit bekannt gegeben wurde. Unter Windows NT war eine solche Erkennung nicht möglich, weil dort eine strenge Kontrolle über die Hardware im Betriebssystem geführt wurde. Nicht identifizierte Komponenten mussten manuell installiert werden oder wurden ignoriert.

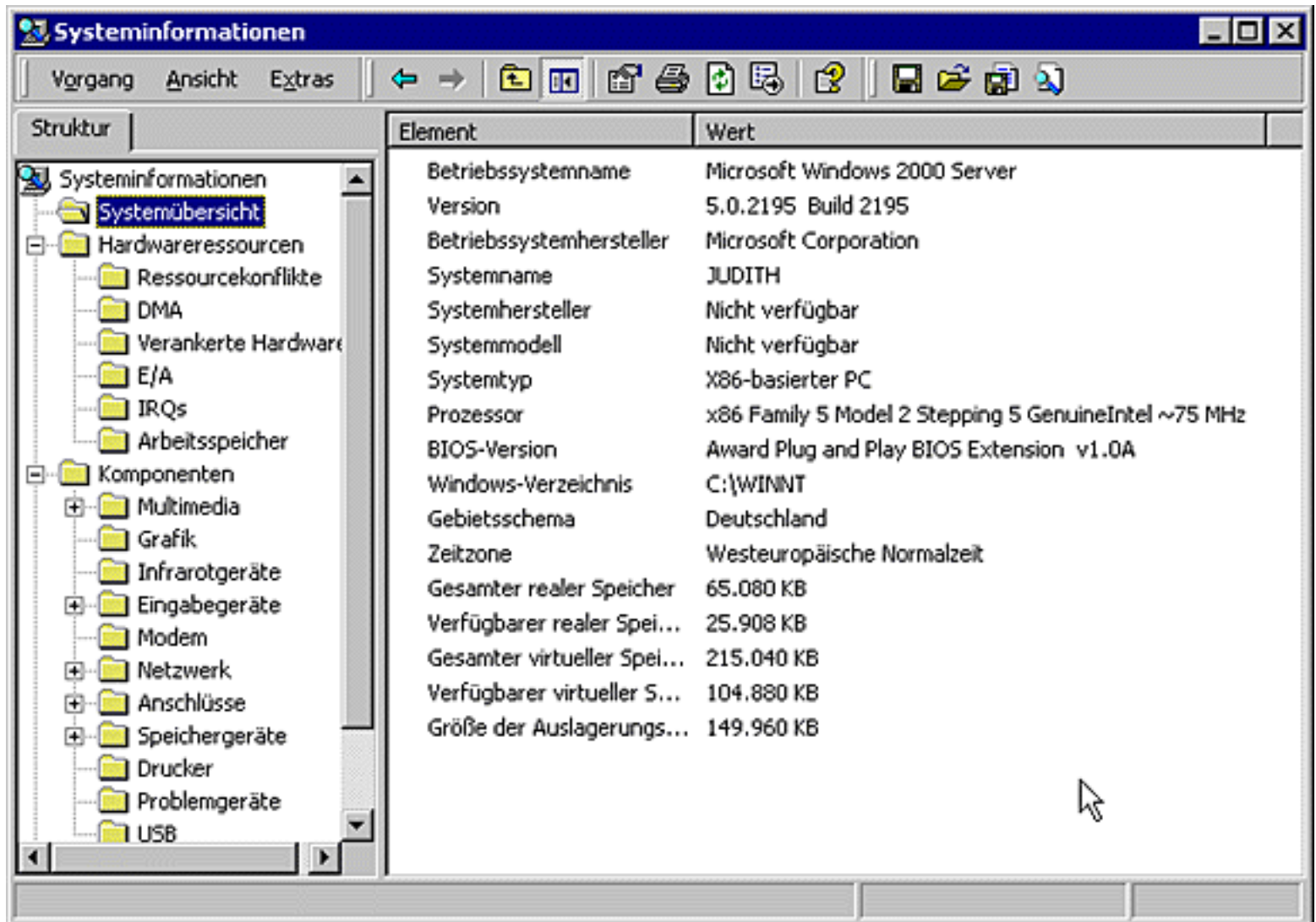


Abbildung 21.10: Der Geräte-Manager in der Computerverwaltungskonsolle

Um einen Eintrag im Geräte-Manager genauer anzusehen, klicken Sie auf das Pluszeichen neben der Kategorie und doppelklicken auf das betreffende Element. Nachdem Sie das Element geöffnet haben (siehe Abbildung 21.11), sehen Sie allgemeine und hardwarespezifische Optionen. Weil nicht jede Hardware dieselben Variablen benutzt, können Sie nicht alles auf einer einzigen Oberfläche verwalten.

In Abbildung 21.11 sehen Sie einen PCMCIA-Adapter, den das Betriebssystem erkannt hat, für den aber bei der Installation kein passender Treiber eingerichtet wurde. Das System weist darauf hin, dass der Treiber nicht gefunden wurde, und bietet die Möglichkeit, diesen nachträglich zu installieren. Dieses Beispiel zeigt, was auf dem Bildschirm für allgemeine Informationen angezeigt werden und wie Sie hier ein Problem unmittelbar lösen.

Auf der Registerkarte **Treiber** kann der Benutzer den Treiber ändern. Aber auch dieser Bildschirm sollte nur zur Information genutzt werden. Er enthält alle Informationen über den Treiber. Anhand der Version und des Datums erkennen Sie, ob der Treiber noch aktuell ist, auch wenn er scheinbar korrekt arbeitet. Durch einen Vergleich dieser Information mit den Informationen auf der Website des Herstellers oder mit technischen Unterlagen stellen Sie fest, ob das System auf dem neuesten Stand ist.

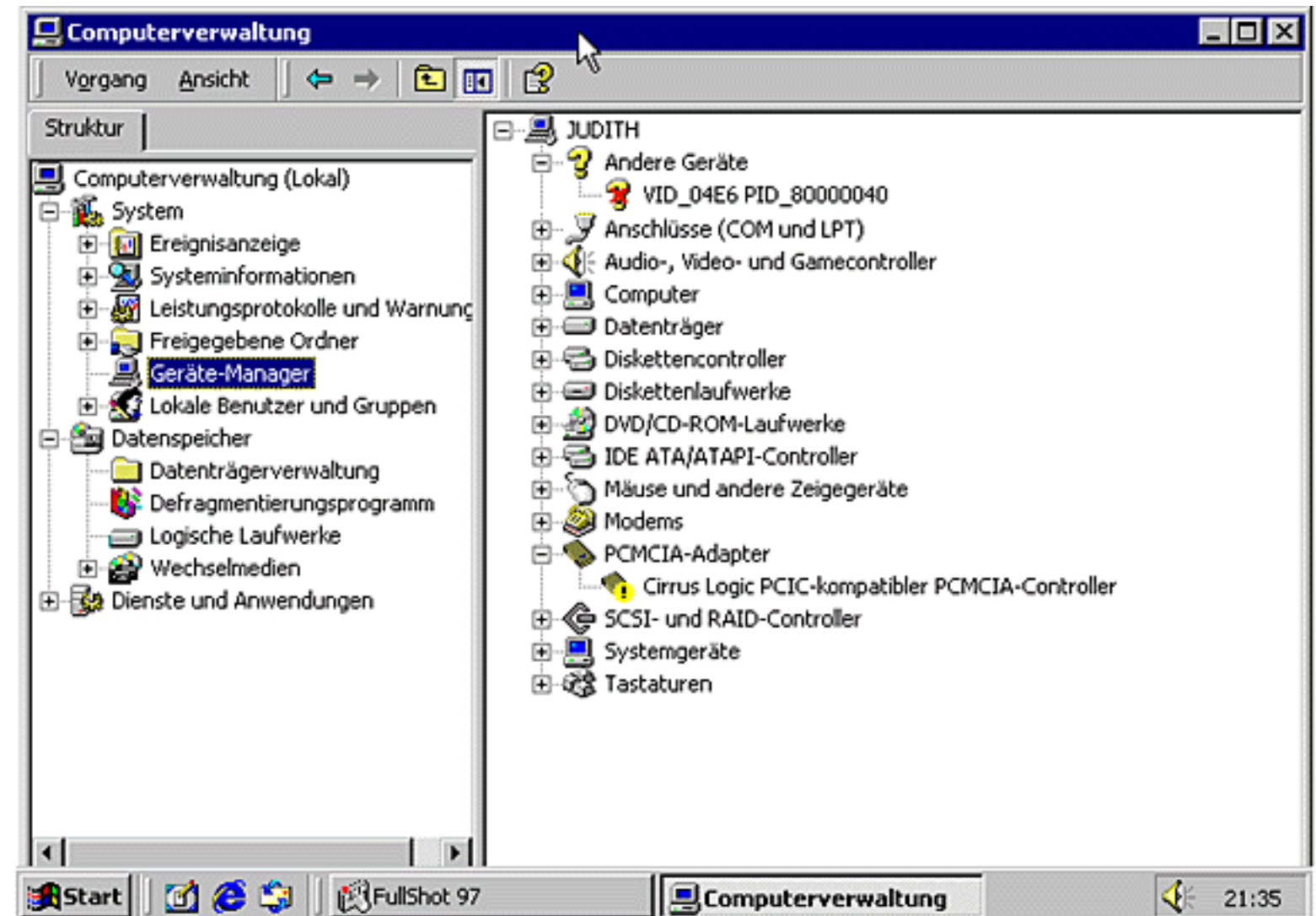


Abbildung 21.11: Die Anzeige des Geräte-Managers für ein nicht funktionierendes Gerät

Wenn Sie auf dieser Seite auf die Schaltfläche **Treiber aktualisieren** klicken, erscheint der Assistent zum Aktualisieren von Gerätetreibern. Dieser Assistent hilft Ihnen dabei, den neuesten Treiber zu finden und zu implementieren - falls er vorhanden ist.

Auf der Registerkarte **Ressourcen** kann der Administrator feststellen, welche Hardwareressourcen dem betreffenden Gerät zugeordnet sind, und ob diese Ressourcen ausreichend zur Verfügung stehen. Der Begriff *Hardwareressource* kann unterschiedliche Dinge bedeuten, abhängig von der jeweiligen Hardware. Das Konzept einer Hardwareressource ist die Gruppierung eindeutiger IDs, die der Prozessor als eindeutig erkennen muss. Stellen Sie sich das Ganze wie eine Auktion vor. Um Dinge ersteigern zu können, braucht der Käufer eine Nummer und er muss wissen, wie er sich zu verhalten hat. Dieses Verhalten und die Nummern sind die Ressourcen und müssen für jedes einzelne Stück eindeutig sein.

Hier eine Liste allgemeiner Ressourcen:

- Interrupt Request. Eine Interrupt- oder IRQ-Einstellung ist die eindeutige Nummer, unter der der Prozessor unterbrochen wird, sodass Dienste von ihm angefordert werden können.
- Speicherbereich: In den Speicherbereich schreibt das Hardwaregerät Informationen, die es für seinen Betrieb braucht. Unterschiedliche Hardwaregeräte haben unterschiedliche Speicheranforderungen und brauchen unterschiedliche Bereiche.
- I/O-Adresse: Die I/O-Adresse wird von dem Gerät und den damit kommunizierenden Geräten benötigt.
- DMA-Kanal: Anstatt bei jedem Speicherbedarf auf den Prozessor zuzugreifen, können einige Geräte direkt auf den Speicher zugreifen (DMA, Direct Memory Access). Dazu brauchen sie einen eindeutigen oder verfügbaren DMA-Kanal.

Ressourcenkonflikte für ein Gerät werden im Geräte-Manager mit einem Ausrufezeichen markiert. Durch Doppelklick auf das Gerät zeigt der Administrator auf der Registerkarte **Ressourcen** mögliche Ressourcenkonflikte an.



In unserer PCI-Welt treten immer seltener Hardwareressourcenkonflikte auf. Häufig gibt es jedoch Probleme, wenn das PCI-Plug&Play-BIOS mehrere Hardwaregeräte mit derselben IRQ- Einstellung einfügt. Weil der PCI-Bus jedoch eine gemeinsame Nutzung von IRQs erlaubt, ist das nicht immer ein Problem. Manchmal haben neu installierte Geräte sporadische Probleme oder verursachen den Ausfall bereits existierender Geräte. Am besten setzen Sie für diese Geräte manuell einen eigenen IRQ fest.

Für einige Hardwaregeräte kann der Benutzer im Geräte-Manager Einstellungen ändern. Das bedeutet nicht, dass die Hardwareeinstellungen geändert werden. Sie ändern die Einstellungen in Windows und irgendwann später an der Hardware. Auf diese Weise erkennt der Benutzer, ob durch die Änderung ein Hardwarekonflikt auftritt, bevor er irgendwelche Änderungen an der Hardware vornimmt. Gehen Sie wie folgt vor, wenn Sie eine Änderung vornehmen wollen:

1. Doppelklicken Sie im Geräte-Manager auf das betreffende Gerät und aktivieren Sie die Registerkarte **Ressourcen**.
2. Heben Sie die Markierung für **Automatisch konfigurieren** auf.
3. Markieren Sie die betreffende Einstellung und klicken Sie auf die Schaltfläche **Einstellung ändern**.
4. Geben Sie den gewünschten Wert ein und klicken Sie auf **OK**. Das Feld **Gerätekonflikt** unten im Dialogfeld hilft Ihnen, einen sinnvollen Ressourcenwert auszuwählen.

Nachdem Sie die Ressourcen geändert haben, müssen Sie das System neu starten, damit diese Änderungen in Kraft treten. Das ist einer der Bereiche, den Microsoft nicht steuern kann - wie oft Sie Ihr System neu starten müssen. Hardwareeinstellungen können meist nicht bei laufender Hardware in Kraft treten.

Denken Sie daran, die Änderungen auch an der Hardware vorzunehmen. Wenn Sie einen Wert im Geräte-Manager geändert haben, bedeutet das nicht, dass die Hardwareänderung damit auch erfolgt ist.

21.3 SNMP

Die Remote-Verwaltung von Windows-Servern wurde mit den Verbesserungen durch MMC und Computerverwaltung sehr viel einfacher. Diese Werkzeuge erlauben dem Administrator, Windows-Einstellungen von beliebiger Stelle in der Domäne aus zu ändern. Die Remote-Verwaltung eines Servers ist keine Zauberei mehr. Sie ist jedoch von einem intakten und wohl konfigurierten Betriebssystem abhängig.

Bei einer Beschreibung der Serververwaltung sollte die Verwaltung der Hardwareintegrität nicht vergessen werden. SNMP (Simple Network Management Protocol) ist ein von vielen Hardwareherstellern verwendetes Protokoll, mit dem ständig Informationen über die Hardware- und Softwareintegrität an ein überwachendes Gerät geschickt werden. Anhand dieses Protokolls kann der Administrator viele Probleme erkennen, noch bevor sie auftreten.

Unternehmen wie Compaq, Hewlett-Packard und IBM haben eigene Softwaredienste, die unter Windows 2000 laufen, um die Integrität des Servers zu gewährleisten. Der Compaq Insight Manager und Hewlett-Packard Open View installieren SNMP-Agenten auf ihren Servern, die die Hardware beobachten und Tendenzen und Fehler aufzeigen.

Durch Beobachtung der Hardware, die sie über mehrere Jahre unterstützen, haben diese Unternehmen gelernt, wodurch Hardware ausfällt. Außerdem wissen sie, was in den Tagen vor dem Ausfall passiert. Dieses Wissen, das von einem Gerät zur Aufzeichnung von SNMP-Daten bereitgestellt wird, kann dem Administrator von größtem Nutzen sein.

Dabei kann entweder die Oberfläche des Herstellers benutzt werden oder ein Programm von Drittanbietern, das mehrere Hardwareformen unterstützt. Beispiele für solche Produkte sind Hewlett-Packard Open View oder Computer Associates NetManageIT. Sie überwachen nicht nur Server, sondern alle Geräte, die SNMP-Verkehr verursachen.

SNMP-Daten, die von Geräten erzeugt werden, sollen aufgezeichnet und in einer MIB (Management Information Base) angezeigt werden. Durch Sammlung dieser MIBs und Hinzufügen zu offenen SNMP-Managern kann ein Administrator das Serverbetriebssystem verwalten und außerdem Router, Schalter, Drucker und alle anderen SNMP-fähigen Geräte kontrollieren.

Kapitel 22 Leistungsoptimierung und Tuning

Die Installation von Windows 2000 Server ist mit geringstem Aufwand Ihrerseits verbunden. Es gibt zahlreiche Werkzeuge, mit denen Sie Ihren Server auf maximale Leistung und allgemeine Sicherheit trimmen können. Ein pflichtbewusster Windows 2000-Systemadministrator muss sich jedoch zuerst einen Überblick verschaffen, welche Leistung sein Windows 2000 Server bringt, damit er ihn richtig optimieren kann. Die dazu notwendigen Informationen finden Sie in diesem Kapitel. Es beschreibt, was auf dem Server passiert und wie Sie ihn optimieren.

22.1 Windows 2000 Supporttools

Microsoft hat ein zusätzliches Paket mit Dienstprogrammen geschaffen, das so genannte *Resource Kit*. Seit der Windows-Version 3.0 gibt es für jede Version der Windows-GUI-Shells und -Betriebssysteme ein eigenes Windows Resource Kit (das war Mitte der neunziger Jahre). Das Windows 2000 Resource Kit enthält wie alle seine Vorgänger zahlreiche Werkzeuge und Betriebssystemressourcen, die ein Systemadministrator unbedingt haben sollte. Im Betriebssystem Windows-2000-Server ist eine Untermenge des formaleren Windows 2000 Resource Kit enthalten, die *Windows 2000 Supporttools*.

Sie erhalten von Microsoft eine kostenlose Version der Windows 2000 Supporttools (sehen Sie auf der Windows 2000 Server-CD nach), aber der Windows 2000 Resource Kit muss bei Microsoft Press erworben werden. Zusammen mit der Software erhalten Sie jedoch auch ein detailliertes, sehr technisch orientiertes Buch zum Microsoft Windows 2000 Resource Kit, in dem viele der »Leistungsmerkmale« beschrieben sind, die an keiner anderen Stelle dokumentiert wurden.

Weil das Windows 2000 Resource Kit ein Add-On des Windows 2000-Betriebssystems ist und nur die Supporttools im eigentlichen Paket enthalten sind, werden wir uns hier auf die Windows 2000 Supporttools konzentrieren. Sie finden dort zahlreiche Dienstprogramme und Hilfedateien, die einem Systemadministrator bei der Wartung eines Windows 2000-Servers wichtige Unterstützung bieten können (siehe Tabelle 22.1).

Werkzeugname	Beschreibung
Active Directory Administration	Dieses Werkzeug erlaubt den Administratoren von Windows-2000-Server, die Implementierung ihres Active Directory anzupassen.
Active Directory Replication Monitor	Dieses Überwachungswerkzeug zeigt die Replikationstopologie der Verbindungen zwischen den Servern am selben Standort innerhalb der Active Directory-Struktur eines Unternehmens an. Außerdem können Sie damit Active Directory-Abfragen optimieren.

ADSI Edit	Dieses Werkzeug unterstützt den Systemadministrator bei der Low-Level-Bearbeitung der Active Directory-Struktur des Unternehmens.
Command Prompt	Ein Standard-Fenster für die Windows 2000 Server-Befehlsshell.
Dependency Walker	Dieses Werkzeug baut ein hierarchisches Baumdiagramm der abhängigen Module auf, die beim Durchsuchen eines beliebigen Win32-Moduls erkannt wurden.
Deployment Planning Guide	Diese kompilierte Hilfedatei enthält den vollständigen Windows 2000 Server Resource Kit Deployment Planning Guide, ein Dokument, das Ihnen hilft, Windows-2000-Server unternehmensübergreifend zu planen.
DiskProbe	Dieses Werkzeug erlaubt dem Administrator, innerhalb von Windows 2000 Server Sektoren einer Festplatte zu bearbeiten.
Error and Event Messages	Diese Windows 2000-Hilfedatei enthält enorm viele Daten, die den Administratoren die Optimierung ihrer Windows 2000 Server-Installationen wesentlich vereinfachen.
Global Flags Editor	Erlaubt den Administratoren, die NtGlobalFlag-Einstellungen für einen Windows-2000-Server mit Hilfe eines GUI-Bildschirms zu bearbeiten.
Process Viewer	Dieses Werkzeug zeigt Daten über einen bestimmten aktiven Prozess an, unter anderem auch einen sehr detaillierten Bildschirm mit Informationen über die Speichernutzung.
Release Notes	Enthält aktualisierte Tipps und Hinweise, die unmittelbar vor der Veröffentlichung des Betriebssystems Windows 2000 noch festgehalten wurden.
Security Administration Tools	Die Systemadministratoren nutzen dieses Werkzeug, um die verschiedenen Zugriffssteuerungsrichtlinien auf einem Windows-2000-Server zu verwalten.
SNMP Query Utility	Windows-2000-Server-Administratoren können SNMP-Abfragen für verschiedene andere SNMP-fähige TCP/IP-Geräte in den Netzwerken des Unternehmens ausführen.
Tools Help	Bietet Hilfe zu den Windows 2000-Supporttools. Beschreibt die erforderlichen Dateien, die Syntax und andere Details zur Nutzung, ebenso wie Beispiele für den Einsatz dieser Werkzeuge.
WinDiff	Ein Werkzeug zum Vergleichen von Dateien und Verzeichnissen.

Windows Installer Cleanup -Utility	Dieses Dienstprogramm entfernt alle oder einige der Anwendungen auf einem Windows 2000 Server-System, die unter Verwendung der Windows Installer-Technologie installiert wurden.

Tabelle 22.1: Windows 2000-Supporttools

Zur Installation der Supporttools brauchen Sie die Installations-CD von Windows 2000 Server sowie möglicherweise Administratorrechte für den Server (das ist nicht zwingend erforderlich, aber aus offensichtlichen Gründen höchst empfehlenswert). Nachdem Sie die CD in das Laufwerk eingelegt haben, wechseln Sie in den Ordner \SUPPORT\TOOLS auf der CD. Unter anderem finden Sie dort auch eine ausführbare Setup-Datei.

Um den Installationsprozess zu initiieren, doppelklicken Sie auf die Datei Setup.exe. Nachdem der Prozess begonnen hat, sehen Sie den ersten Bildschirm für den Assistenten zur Einrichtung der Windows 2000 Server-Supporttools.

Im ersten Bildschirm werden lediglich Informationen angezeigt und es sind keine Eingaben von Ihnen erforderlich. Um die Installation der Supporttools fortzusetzen, klicken Sie auf die Schaltfläche **Next**. Dadurch gelangen Sie zum Fenster **User Information**, das Sie in Abbildung 22.1 sehen.

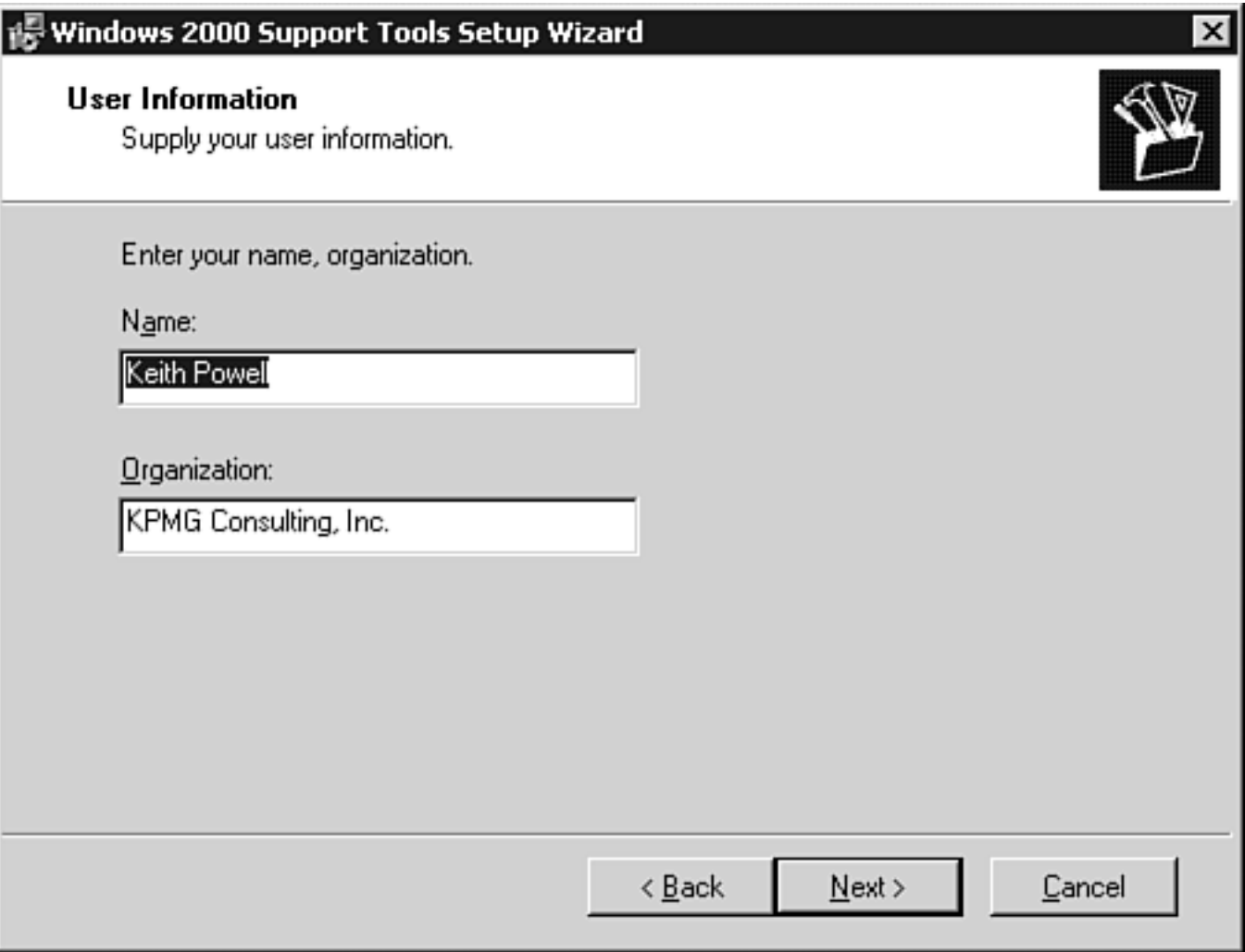


Abbildung 22.1: Eingabe Ihrer Benutzerinformation

Geben Sie Ihren Namen und das Unternehmen ein, für das diese Version von Windows 2000 Server registriert ist. Weil es für Microsoft keine Möglichkeit gibt, diese Informationen zu überprüfen, können Sie - wenn Sie möchten - als Namen auch »Mickey Maus« eingeben und als Unternehmen »Andromeda«. Nachdem Sie Ihre Einträge vorgenommen haben, klicken Sie auf **Next**, um in das Fenster zur Auswahl eines Installationstyps zu gelangen, das Sie in Abbildung 22.2 sehen.

Im Fenster zur Auswahl des Installationstyps legen Sie fest, welche dieser Werkzeuge Sie auf Ihrem Windows 2000 Server einsetzen wollen. Standardmäßig werden 16 der Windows 2000 Supporttools installiert. Weil die gesamte Anzahl der Tools nur 18 Mbyte Festplattenspeicher belegt, sollten Sie die Option **Custom** wählen, sodass Sie die zu installierenden Tools manuell markieren können. Nachdem Sie entschieden haben, welche Installation Sie ausführen wollen, klicken Sie auf das entsprechende Optionsfeld. Anschließend gelangen Sie mit der Schaltfläche **Next** zum Fenster für die benutzerdefinierte Installation, das Sie in Abbildung 22.3 sehen (falls Sie die Option **Typical** gewählt haben, sehen Sie natürlich nicht den Bildschirm aus Abbildung 22.3, sondern den Bildschirm aus Abbildung 22.4).



Abbildung 22.2: Auswahl eines Installationstyps

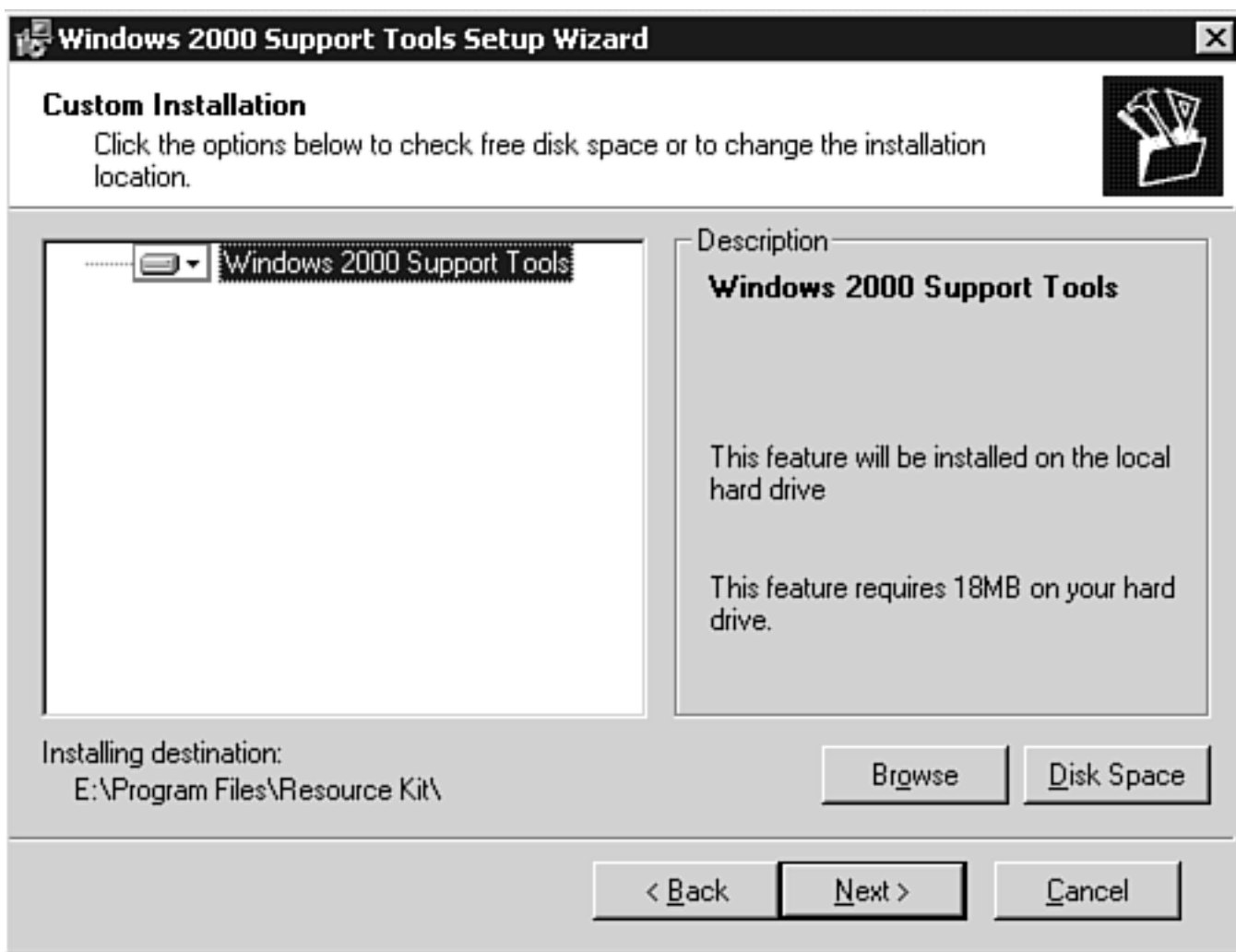


Abbildung 22.3: Auswahl der Installationsoptionen

Im Fenster für die benutzerdefinierte Installation legen Sie fest, welche Supporttools implementiert werden sollen. Falls Sie alle Tools brauchen, klicken Sie in das Dropdown-Feld (das ist das kleine weiße Feld mit dem Symbol einer Festplatte und einem Pfeil nach unten), um ein Kontextmenü aufzurufen (beachten Sie, dass Sie hier ausnahmsweise die linke anstelle der rechten Maustaste benutzen). In diesem Menü gibt es drei Auswahlmöglichkeiten:

- Installation auf der lokalen Festplatte.
- Gesamten Funktionsumfang auf die lokale Festplatte installieren.
- Gesamter Funktionsumfang steht nicht zur Verfügung.

Momentan implementiert Microsoft für dieses Windows 2000-Leistungsmerkmal den Alles-oder-Nichts-Ansatz, d.h. die beiden ersten Optionen führen zum selben Ergebnis: das gesamte Windows 2000 Supporttools Kit wird installiert.

Für die letztere Option wird überhaupt nichts installiert. Die beiden Schaltflächen unten im Fenster, **Browse** und **Disk Space**, sollen Ihnen bei der Entscheidung helfen, wo Sie die Windows 2000 Supporttools installieren wollen, und ob genügend Speicherplatz für die Installation zur Verfügung steht. Nachdem Sie Ihre Auswahl getroffen haben, klicken Sie auf die Schaltfläche **Next**, um mit der Installation zu beginnen. Sie sehen das Fenster des Assistenten in Abbildung 22.4.

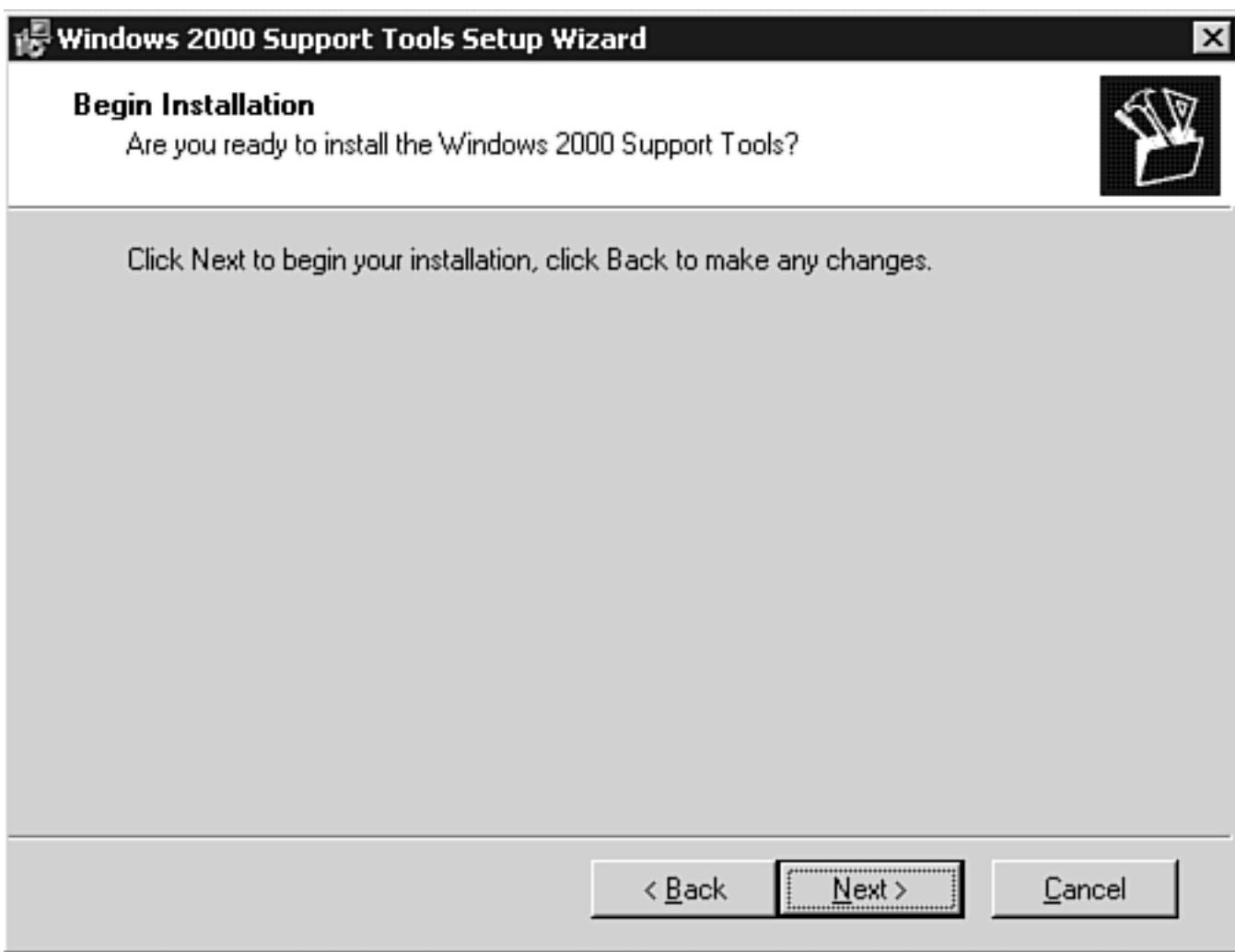


Abbildung 22.4: Hier starten Sie die Installation der Dateien

Dies ist ebenfalls ein Informationsbildschirm, der Sie lediglich darauf hinweist, dass Sie nun mit der Installation beginnen können. Klicken Sie auf die Schaltfläche **Next**, wenn Sie bereit sind.

Sie sehen eine Fortschrittsanzeige mit Informationen darüber, an welcher Stelle des Installationsprozesses Sie sich befinden. Nachdem der Prozess abgeschlossen ist, erscheint der in Abbildung 22.5 gezeigte Bildschirm.



Abbildung 22.5: Der Installationsprozess wurde erfolgreich abgeschlossen

Der letzte Bildschirm des Installations-Assistenten informiert Sie darüber, ob die Windows 2000 Supporttools korrekt eingerichtet werden konnten. Klicken Sie auf die Schaltfläche **Finish**, um die Installation abzuschließen und den Assistenten zu verlassen.

Sie finden die Windows 2000 Supporttools jetzt im Startmenü unter **Programme/Windows 2000 Support Tools**. Wählen Sie im entsprechenden Untermenü das Dienstprogramm aus, das Sie für Ihre Arbeit benötigen.

22.2 Automatische Optimierung

Die Optimierung der Windows-2000-Server-Betriebsumgebung ist einfach und zugleich kompliziert. Microsoft macht es Ihnen ziemlich einfach, mit Hilfe mehrerer Verwaltungskonsolen per grafischer Benutzeroberfläche eine grundlegende Leistungsoptimierung seines neuesten Betriebssystems vorzunehmen. Lassen Sie sich von diesen MMCs (Microsoft Management Console) jedoch nicht täuschen, sie führen nicht alle zu einer Optimierung Ihres Windows-2000-Servers. Es braucht viele Schritte, um die zahlreichen Aspekte der Windows 2000-Betriebsumgebung Ihres Unternehmens zu optimieren. Die Systemadministratoren des Unternehmens stellen eine optimale Windows-2000-Server-Betriebsumgebung sicher, indem sie den Optimierungsprozess sorgfältig überwachen und einige der dabei anfallenden Aufgaben automatisieren.

22.2.1 Vermeiden von Fragmentierung

Achten Sie darauf, dass Ihre Festplattenlaufwerke möglichst wenig fragmentiert sind, weil Sie damit die Systemleistung steigern können. Eine Fragmentierung kann auf allen Festplattenlaufwerken auftreten (EIDE, SCSI usw.), ebenso auf Systemen mit einer einzigen Festplatte oder RAID-fähigen Systemen. Je fragmentierter ein Festplattenlaufwerk ist, desto schwieriger wird es für Betriebssystem und Anwendungen, die Dateien für bestimmte Operationen zu finden. Verständlicherweise dauert es länger, eine über mehrere Festplatten verteilte Datei zu finden, und die Gesamtgeschwindigkeit bzw. die erkennbare Geschwindigkeit des Betriebssystems und/oder der Anwendung sinkt. Im Betriebssystem Windows-2000-Server gibt es ein Werkzeug namens *Defragmentierung*, das Ihnen hilft, fragmentierte Festplattenbereiche zu erkennen und die betreffenden Festplatten zu defragmentieren.

Um dieses Dienstprogramm in Windows 2000 zu öffnen, klicken Sie auf **Start/Programme/Zubehör/Systemprogramme/Defragmentierung**. Die Abbildung 22.6 zeigt den Startbildschirm.

Nachdem Sie die Defragmentierung aufgerufen haben, sehen Sie in der oberen Bildschirmhälfte eine Auflistung der verfügbaren Festplattenlaufwerke. Die untere Bildschirmhälfte zeigt die Überprüfungs- und Defragmentierungsprozesse, falls Sie eine oder beide dieser Funktionen ausgewählt haben. Für jedes Laufwerk gibt es sechs Spalten mit Informationen:

- *Datenträger*. Das logische Festplattenlaufwerk, das analysiert und/oder defragmentiert werden kann (falls eine Defragmentierung erforderlich ist).
- *Status*. In dieser Spalte sehen Sie den Status eines bestimmten Laufwerkdatenträgers. Während Sie beispielsweise die Überprüfung ausführen, sehen Sie den Begriff *Überprüfung...*, während der Defragmentierung sehen Sie *Defragmentierung...* Der Status *Beendet* oder *Angehalten* bedeutet, dass Sie die Defragmentierung während der Ausführung beendet oder angehalten haben.
- *Dateisystem*. Gibt den Formattyp des auf dem Laufwerk installierten Dateisystems an. Der Begriff FAT bedeutet, dass ein 16-Bit Windows 9x FAT-Format installiert wurde, während FAT32 die Windows 98 32-Bit-Version des FAT-Formats anzeigt. NTFS bedeutet, dass das Windows NT FAT-Format verwendet wurde. Es gibt noch mehr Dateisystemtypen, die hier angezeigt werden können, aber die drei genannten sind die gebräuchlichsten. Falls ein anderes Format angezeigt wird, sollten Sie keine Defragmentierung ausführen, weil ein Nicht-Microsoft-Betriebssystem dadurch beschädigt werden könnte (beispielsweise Red Hat Linux, OS/2, Sun Solaris usw.).
- *Kapazität*. Die formatierte Gesamtgröße des Laufwerkdatenträgers.
- *Freier Speicherplatz*. Der nicht genutzte Speicher auf dem Laufwerk.
- *% freier Speicherplatz*. Der verbleibende freie Speicher auf einem Laufwerk, angegeben in Prozent.

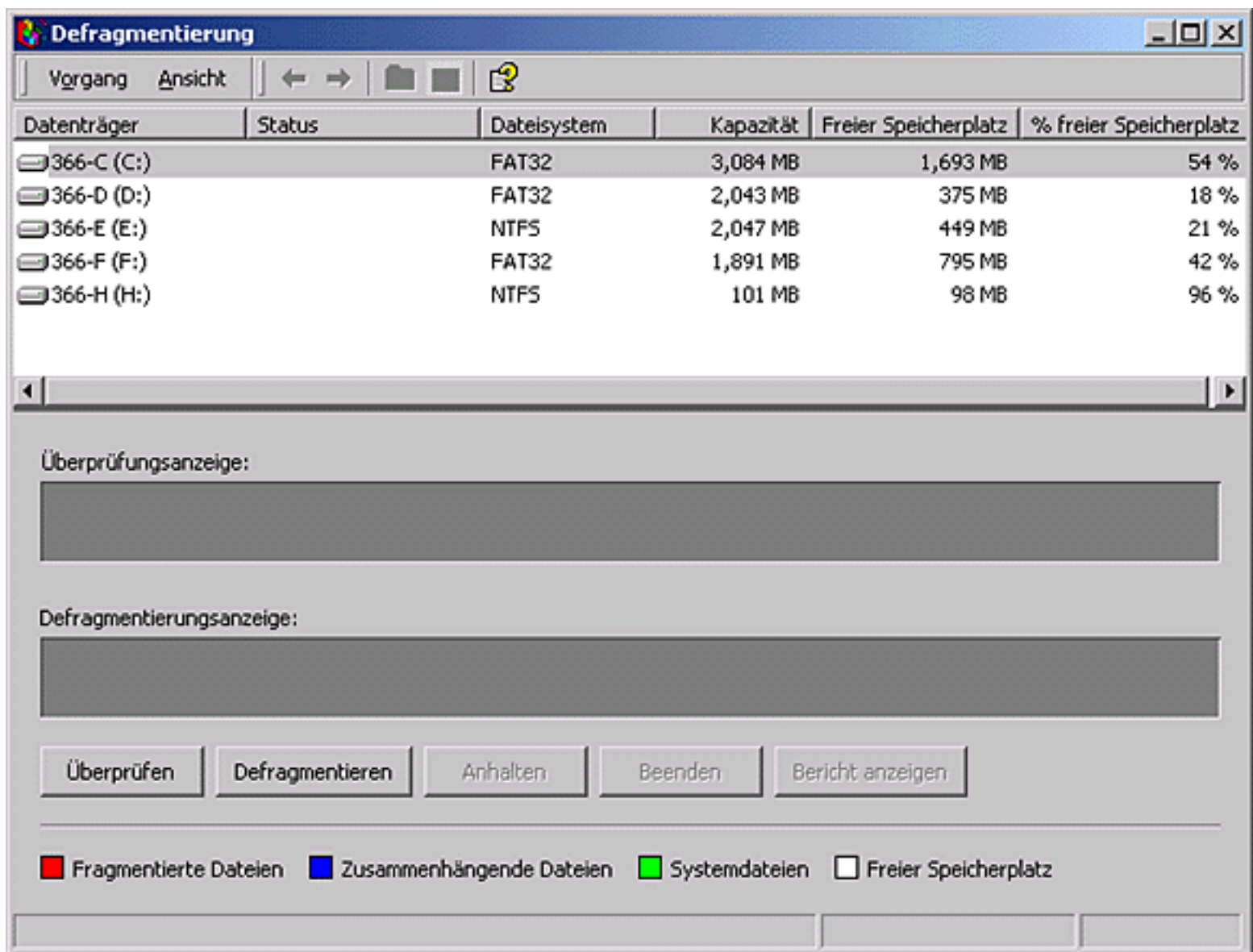


Abbildung 22.6: Anzeige des Hauptbildschirms für die Defragmentierung

Wählen Sie im Menü **Ansicht** den Befehl **Anpassen**, um die Optionen für die Anzeige der Defragmentierung zu ändern, wie in Abbildung 22.7 gezeigt.



Abbildung 22.7: Anpassen der MMC-Ansicht für die Defragmentierung

Im oberen Bereich dieses Optionsfensters, **MMC**, fügen Sie die verschiedenen Menü- und Navigationsleisten für die eigentliche MMC (Microsoft Management Console) ein bzw. entfernen sie. Beachten Sie, dass die Defragmentierung ein MMC-Snap-In ist, dessen Navigation ähnlich funktioniert wie in den anderen MMC-Snap-In-Werkzeugen von Windows-2000-Server. In der unteren Hälfte des Dialogfeldes **Ansicht anpassen** geben Sie an, ob Sie auch die Snap-In-Symbolleisten und -Menüs verwenden wollen. Aktivieren Sie die gewünschten Einstellungen und klicken Sie auf **OK**, um diese zu bestätigen und zu sichern.

Anschließend wählen Sie ein Laufwerk zur Überprüfung aus. Dazu klicken Sie auf ein Laufwerk, sodass es hervorgehoben dargestellt wird (das bedeutet, Sie werden die nachfolgenden Operationen für dieses Laufwerk ausführen; in diesem Beispiel ist es das Laufwerk C:). Jetzt klicken Sie auf die Schaltfläche **Überprüfen** (sie befindet sich unten links im Bildschirm) oder verwenden den Menübefehl **Vorgang/Überprüfen** (beides bewirkt dasselbe), um den Überprüfungsprozess der Defragmentierung zu starten.

Zunächst sehen Sie im Überprüfungsanzeigebereich des Bildschirms einen mehrfarbigen Balken (in der unteren Bildschirmhälfte). Anhand der Farbkodierung erkennen Sie, was auf Ihrem Datenträger gerade passiert. Wenn Sie die Defragmentierung für Ihren Datenträger noch nie ausgeführt haben, sehen Sie jetzt sehr viele fragmentierte Bereiche auf Ihrem Laufwerk. Nachdem die Überprüfung abgeschlossen ist, erscheint ein kleines Dialogfeld, wie in Abbildung 22.8 gezeigt.

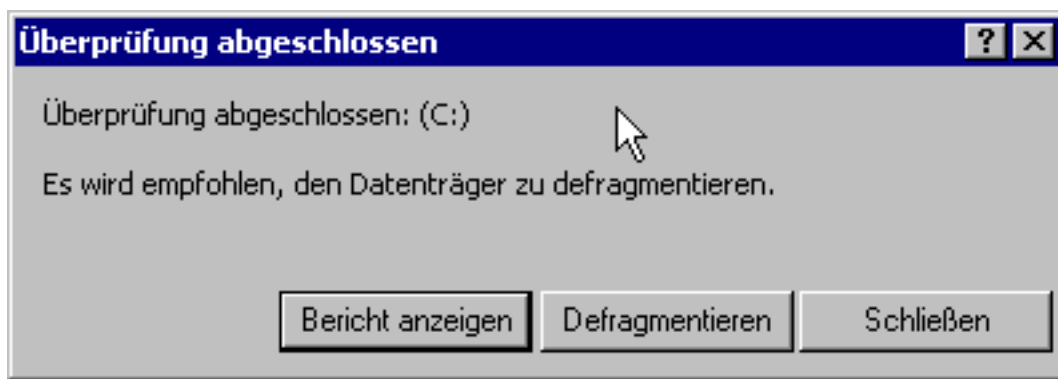


Abbildung 22.8: Nachdem die Überprüfung abgeschlossen ist, entscheiden Sie, was zu tun ist

Das Fenster **Überprüfung abgeschlossen** enthält eine Empfehlung für den betreffenden Datenträger. Sehr wahrscheinlich braucht Ihre Festplatte eine Defragmentierung, insbesondere dann, wenn sie in einem Datenbank- oder Dateiserver eingesetzt wird oder wenn Sie die Defragmentierung nie zuvor ausgeführt haben. Bevor Sie mit der Defragmentierung beginnen, sollten Sie auf die Schaltfläche **Bericht anzeigen** klicken, um den bei der Analyse automatisch erstellten Bericht einzusehen. Die Abbildung 22.9 zeigt beispielhaft einen solchen Überprüfungsbericht.

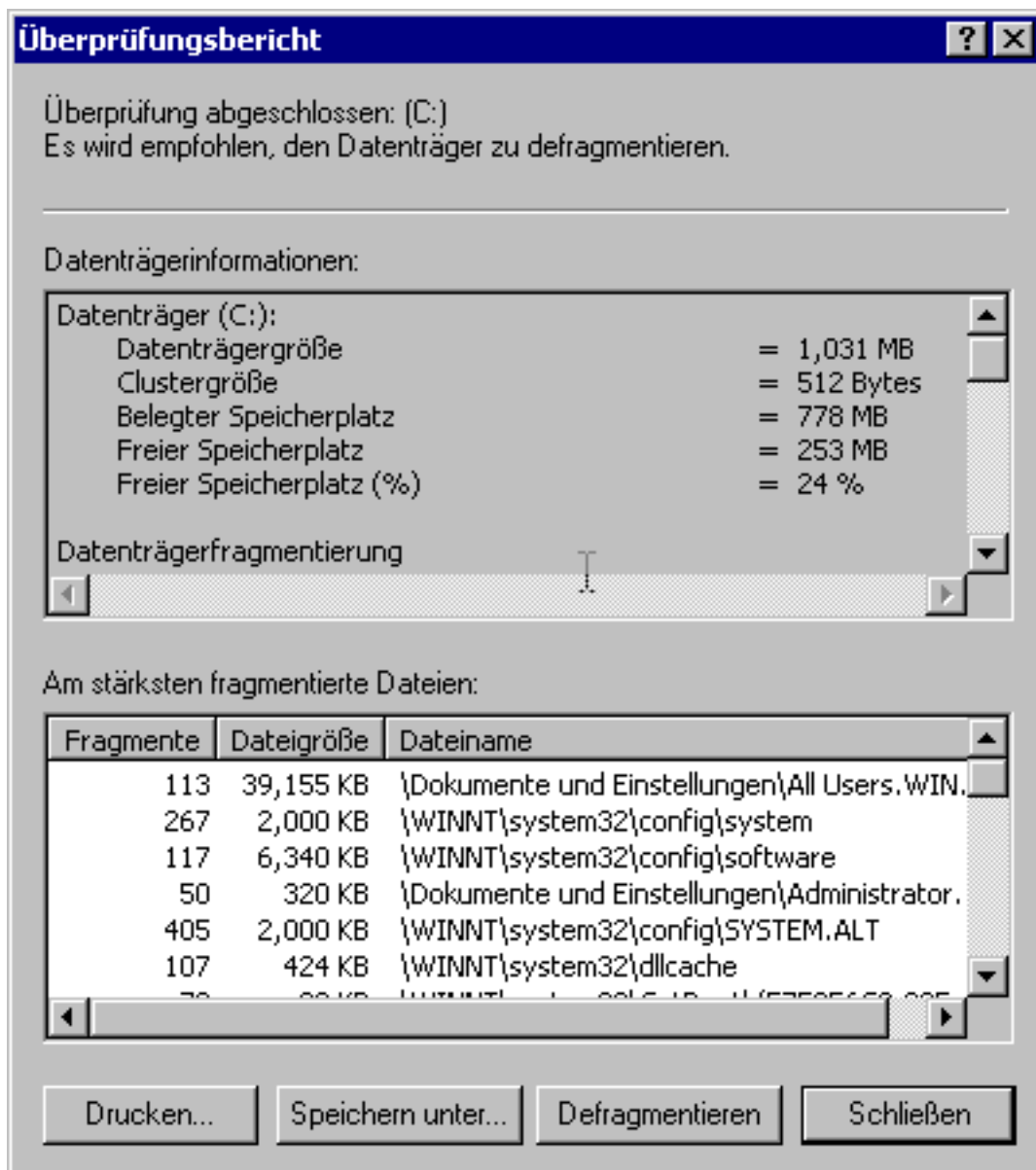


Abbildung 22.9: Online-Anzeige des Überprüfungsberichts

Beachten Sie, dass das Dialogfeld mit der Abschlussmeldung der Überprüfung verschwindet, sobald der Überprüfungsbericht angezeigt wird. Im Bereich *Datenträgerinformationen* finden Sie viele wertvolle Hinweise zu den Datenträgern in Ihrem Windows-2000-Server-Rechner. Mit Hilfe der Bildlaufleiste rechts bewegen Sie sich in diesem Teil des Dialogfeldes, dessen Anzeige nur zu Ihrer Information dient. Im Bereich *Am stärksten fragmentierte Dateien* des Dialogfeldes finden Sie eine Liste aller Dateien, die stärker fragmentiert sind, als es dem Durchschnitt für diesen Datenträger entspricht (den Durchschnitt sehen Sie in der Datenträgerinformation). Nachdem Sie den Bericht angesehen haben, verlassen Sie das Dialogfeld mit Hilfe der Schaltfläche **Schliessen**. Sie können die Defragmentierung natürlich auch aus dem Überprüfungsbericht heraus starten, indem Sie auf die Schaltfläche **Defragmentieren** klicken. Die Schaltfläche **Speichern unter** verwenden Sie, um Defragmentierungsberichte irgendwo auf dem Server abzulegen, um sie später noch einmal genauer auszuwerten.

Nehmen wir weiterhin an, Sie haben den Überprüfungsbericht mit der Schaltfläche **Schliessen** verlassen und wollen jetzt die Defragmentierung beginnen, ohne die Überprüfung erneut starten zu müssen. Dazu klicken Sie im Hauptfenster der Defragmentierung auf die Schaltfläche **Defragmentieren**.

Wie Sie sehen, wird in der Spalte **Status** für den betreffenden Datenträger im oberen Bildschirmabschnitt jetzt »Defragmentierung« angezeigt, d.h. die Defragmentierung hat wirklich begonnen. Außerdem sind in der Defragmentierungsanzeige des Hauptfensters Aktivitäten zu beobachten. Zunächst wird hier ein Abbild des Datenträgers angezeigt, das in der Überprüfungsanzeige zu sehen war. Nachdem die Defragmentierung für einen Datenträger beendet ist, wählen Sie ein weiteres Laufwerk zur Defragmentierung aus oder verlassen das Dienstprogramm. Um die Defragmentierung zu beenden, klicken Sie auf die Schaltfläche **Schliessen**. Um zuvor einen Bericht einzusehen, klicken Sie auf die Schaltfläche **Bericht anzeigen**.

22.2.2 Multiprocessing

Das Betriebssystem Windows-2000-Server unterstützt Computer mit einem oder mehreren Prozessoren (auch als *CPUs* bezeichnet). Für das Betriebssystem Windows 2000 DataCenter gibt es keine konkrete Begrenzung, was die theoretische Anzahl der Intel-basierten Prozessoren betrifft, aber die Obergrenze ist etwa bei 32 Prozessoren anzusetzen. In der Server-Version des Betriebssystems Windows 2000 werden jedoch maximal vier CPUs unterstützt. Es gibt zwei Kategorien von Multiprocessing-Computersystemen: asymmetrische und symmetrische.

Beim asymmetrischen Multiprocessing weist das Betriebssystem automatisch die Befehle einer bestimmten CPU zu. Die einer CPU zugeordneten Befehle können also nicht dynamisch an die zweite CPU weitergegeben werden, wenn die erste CPU überlastet ist. Glücklicherweise verwendet Windows-2000-Server nicht die asymmetrische Vorgehensweise - es handelt sich dabei um ein symmetrisches Multiprocessing-System (SMP).

Die symmetrische Verarbeitungsstruktur des Betriebssystems Windows 2000 erlaubt dem Computersystem, Systemprozesse oder Anwendungen dynamisch auf den jeweils verfügbaren CPUs auszuführen. Diese Funktionalität macht diese neueste Version von Windows NT in Kombination mit den Multitasking-Fähigkeiten von Windows-2000-Server zu einem sehr leistungsfähigen und skalierbaren Betriebssystem. Diese neu geschaffene Leistung und Skalierbarkeit bedeutet jedoch

gleichzeitig, dass Verwaltung, Überwachung und Leistungsoptimierung noch komplizierter werden. Im restlichen Kapitel erhalten Sie die Grundlagen, wie Sie die Datenverarbeitungsinfrastruktur Ihres Unternehmens noch besser darauf vorbereiten, in einer komplexen Welt von Windows-2000-Server eine optimale Leistung zu erzielen.

22.2.3 Priorisierte Prozesse und Threads

Wie im alten Windows NT Server 4.0 ist es auch unter Windows-2000-Server möglich, den verschiedenen Systemprozessen und Threads Prioritäten zuzuordnen. Natürlich sollte man dazu wissen, worum es sich bei Prozessen und Threads handelt. Deshalb wollen wir diese beiden Begriffe hier kurz erklären und dann über die dazugehörige Verwaltung sprechen. Anschließend werden wir beschreiben, wie und warum Sie die Prioritäten ändern sollten, um die Leistung eines bestimmten Prozesses oder Threads zu optimieren.

Was ist ein Prozess? Ein *Prozess* ist ein Programm, das unter Einhaltung einer bestimmten Schrittfolge ausgeführt wird. Dieses Programm besteht neben den verfügbaren Windows-2000-Server- und Systemressourcen aus dem grundlegenden Quellcode und Daten sowie einem privaten Speicheradressbereich (im Betriebssystem Windows-2000-Server) und einem oder mehreren Threads.

Ein *Thread* ist nichts anderes als eine präzise Anordnung von Anweisungen innerhalb eines Programms. Der Windows-2000-Server-Kernel steuert die Ausführung aller Threads. Ein Thread in einem Microsoft Word-Programm könnte beispielsweise Befehle enthalten, die die Druckvorschau initiieren. Vielleicht haben Sie schon einmal von »multi-threaded Prozessen« gehört - das bedeutet, ein einziger Prozess ist in der Lage, mehrere Threads gleichzeitig zu verarbeiten. Das ist bei Programmen wie beispielsweise dem Editor sehr praktisch, der in Windows-2000-Server enthalten ist. Der Editor nimmt gleichzeitig Eingaben von der Tastatur und der Maus des Benutzers entgegen, während außerdem beispielsweise ein Dokument ausgedruckt werden kann. Bei einem Single-threaded-Prozess müssten diese drei Aufgaben sequenziell ausgeführt werden (d.h. Schritt 2 könnte erst beginnen, nachdem Schritt 1 abgeschlossen ist usw.).

Dieses multi-threaded Processing wird auch als *Multitasking* bezeichnet. Beinhaltet Ihr Server nur eine einzige CPU, kann er leider die Vorteile des Multitaskings nicht wirklich nutzen, weil er jeweils nur einen Thread gleichzeitig verarbeiten kann. Das Betriebssystem Windows-2000-Server ist jedoch in der Lage, einen Multitaskingprozess zu nutzen, die so genannte *Kontextumschaltung*, wodurch es den Benutzern vorgaukelt, mehrere Threads gleichzeitig auszuführen (und hier kommt die Magie in den Computer). Die Kontextumschaltung funktioniert ganz einfach: Ein Thread wird ausgeführt und fortgesetzt, bis er entweder von selbst stehen bleibt (d.h. er muss auf andere System- oder Betriebssystemressourcen warten) oder bis das Betriebssystem ihm mitteilt, dass er warten muss (d.h. die Verarbeitung wird unterbrochen). In diesem Fall speichert das Betriebssystem den Kontext des Threads. Sobald dieses Ereignis auftritt, lädt das Betriebssystem den Kontext eines anderen Threads, sodass dieser weiter verarbeitet werden kann. Wie Sie sehen, wechselt das System die Threads einfach, bis auf diese Weise alle Threads verarbeitet wurden.

Es wäre natürlich zu einfach, Threads und Prozesse zu verstehen, hätte Microsoft das auf genau diese Weise realisiert. Deshalb müssen Sie noch ein Konzept verstehen: präemptives Multitasking. Beim präemptiven Multitasking steuert Windows-2000-Server den Zugriff auf alle CPUs des Computersystems. Das bedeutet, Windows kann die Ausführung von Threads aus einem von zwei Gründen unterbrechen (»Präemption«):

- *Quantum*. Dies ist ein Thread, der eine bestimmte Zeit lang ausgeführt wird. Nach Ablauf dieser Zeit unterbricht das Betriebssystem diesen Thread und erlaubt einem anderen Thread den Zugriff auf die CPU.
- *Priorität*. Falls ein Thread auftritt, der eine höhere Priorität als der aktuell ausgeführte Thread hat, unterbricht das Betriebssystem den aktuell ausgeführten Thread und führt statt dessen den Thread mit der höheren Priorität aus.

In Windows-2000-Server gibt es 32 verschiedene Prioritätsstufen, die von 0 bis 31 nummeriert sind (logisch, oder?). Diese Prioritätsstufen können in zwei Ebenen unterteilt werden:

- *Benutzermodus-Komponenten*. Diese Prioritätsstufen liegen im Bereich zwischen 0 und 15 und haben nur mit den verschiedenen Teilsystemen von Windows-2000-Server zu tun (POSIX, Win32, OS/2 und das Integral Subsystem) sowie mit den verschiedenen Anwendungen, die auf einem Windows 2000-Server ausgeführt werden können.
- *Kernelmodus-Komponenten*. Diese Prioritätsstufen liegen im Bereich zwischen 16 und 31 und umfassen alle Komponenten von Windows 2000, die mit der Ausführung zu tun haben, unter anderem alle Systemdaten und Hardwaregeräte sowie den direkten Speicherzugriff (DMA) und den Prozessmanager (der alle Systemprozesse und Threads erzeugt und beendet).

Alle von Windows-2000-Server verarbeiteten Threads haben eine Grundpriorität. Diese Grundpriorität eines Threads erscheint in einer von sechs Prioritätsebenen (von der niedrigsten oben bis zur höchsten unten), die beispielsweise in Werkzeugen wie dem Windows 2000 Task-Manager angezeigt werden:

- *Leerlauf*. Von 1 bis 6.
- *Normal*. Von 6 bis 10.
- *Hoch*. Von 10 bis 15.
- *Echtzeit*. Von 16 bis 31.

Beachten Sie, dass es für diese Prioritätsklassenebenen zusätzliche dynamische Einstellungen für die Prioritätsebene geben kann, beispielsweise Niedrig, Niedriger als Normal, Normal, Höher als Normal, Hoch und Echtzeit. Die dynamischen Prioritätsebenen werden vom Windows Server-Kernel verwaltet, der die Systemadministratoren davor bewahrt, dass sie ihr System in irgendeinen irreparablen Zustand versetzen. Deshalb gibt es innerhalb jeder Ebene eine weitere Ebene, die hilft, die jeweilige Prioritätsebene eines Threads in Windows-2000-Server festzulegen.

Wie Sie aus der obigen Auflistung erkennen, umfasst jede dieser Ebenen einen bestimmten Nummernbereich (obwohl Sie eigentlich nur den Namen zu kennen brauchen). Wenn Sie Ihre Prozesse im Windows-2000-Server Task-Manager betrachten (dieses Dienstprogramm wird später in diesem Kapitel noch erklärt), sehen Sie genau diese Ebenennamen, und nicht bestimmte Prioritätsnummern.

Weisen Sie nie einer Anwendung, einem Dienstprogramm, einem Thread oder etwas anderem die Echtzeitpriorität zu. Falls Sie es dennoch versehentlich tun, wird Ihr Windows 2000 Server- System innerhalb kürzester Zeit einen schnellen und qualvollen Tod erleiden. Alle Prozesse, denen Sie diesen Schwellenwert zuordnen, übernehmen einfach das gesamte Betriebssystem. Die Einstellung Echtzeit darf deshalb nur vom Betriebssystem verwaltet, nicht aber vom Administrator erteilt werden.



Die Basispriorität für einen Thread darf nie um mehr als zwei Ebenen höher als die Basis werden, und auch nicht tiefer als zwei Ebenen unterhalb der Basis. Beispielsweise beginnt die Anwendung Microsoft Imaging mit einer Basispriorität von Normal, mit einem tatsächlichen Wert von 8, wird also letztlich immer im Bereich zwischen 6 und 10 liegen.

Um zu sehen, welche Prozesse aktuell auf Ihrem Windows 2000-Server aktiv sind, drücken Sie (Strg)+(Alt)+(Entf), um das Fenster **Windows-Sicherheit** zu öffnen. Klicken Sie hier auf die Schaltfläche **Task-Manager** und aktivieren Sie im Task-Manager die Registerkarte **Prozesse**. Sie sehen das in Abbildung 22.10 gezeigte Dialogfeld.

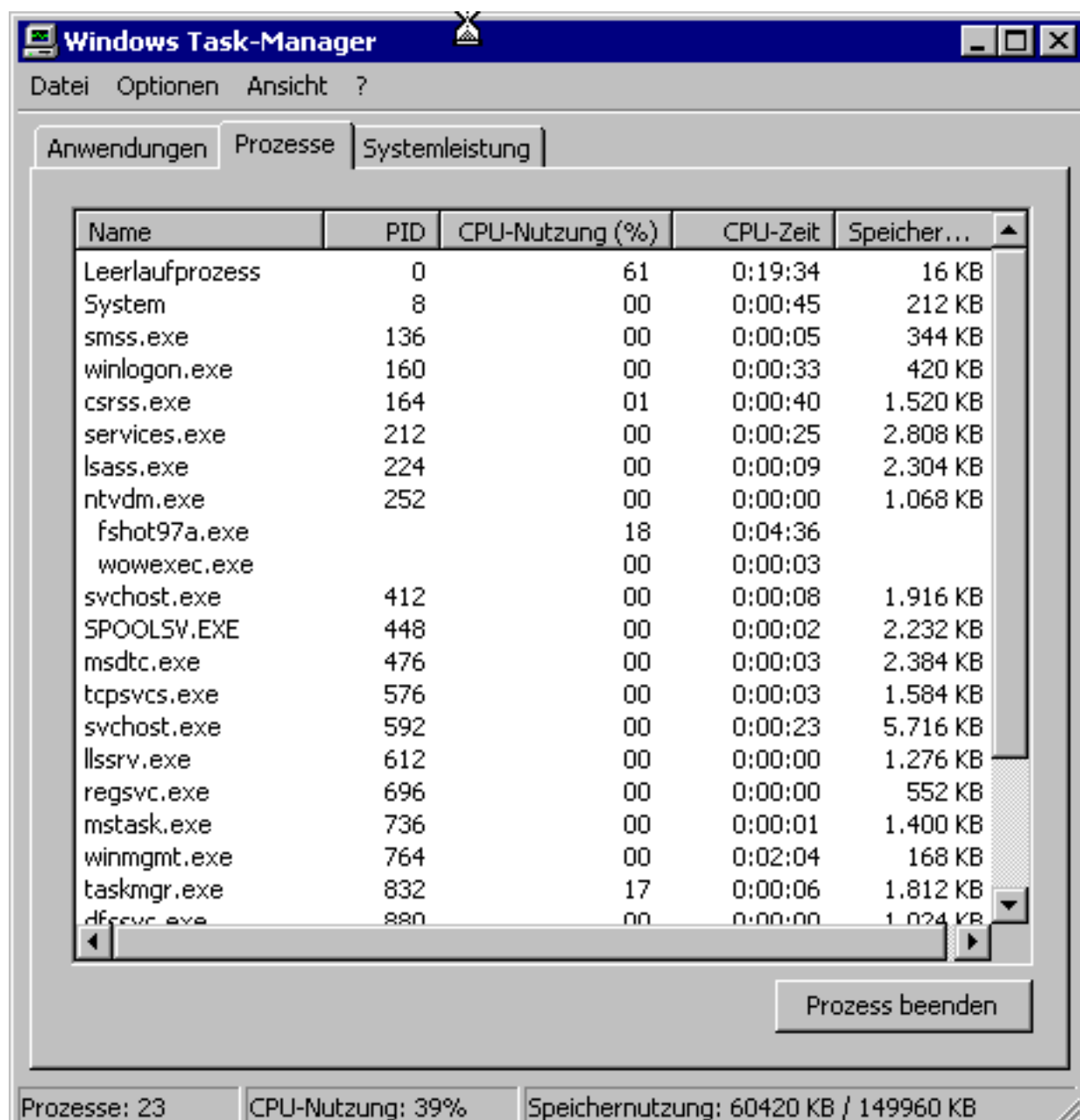


Abbildung 22.10: Anzeige der Prozesse im Task-Manager

Auf der Registerkarte **Prozesse** sehen Sie standardmäßig fünf Spalten:

- *Name*. Dies ist der dem Prozess zugeordnete Name.
- *PID*. Die Prozess-ID.

- *CPU-Nutzung (%)*. Die Prozessorzeit (angegeben in Prozent), die die Threads für diesen Prozess seit der letzten Aktualisierung verbraucht haben.
- *CPU-Zeit*. Die Gesamt-Prozessorzeit, die von einem Prozess verbraucht wurde, angegeben im Format »Stunden:Minuten:Sekunden«.
- *Speichernutzung*. Der vom Prozess belegte primäre Systemspeicher, angegeben in Kilobyte (1.024 Byte = 1 Kbyte).

Wenn Sie im Fenster des Task-Managers nach unten blättern (immer noch auf der Registerkarte **Prozesse**), sehen Sie einige Einträge, die gegenüber der restlichen Prozessliste eingerückt erscheinen, wie in Abbildung 22.11 gezeigt.

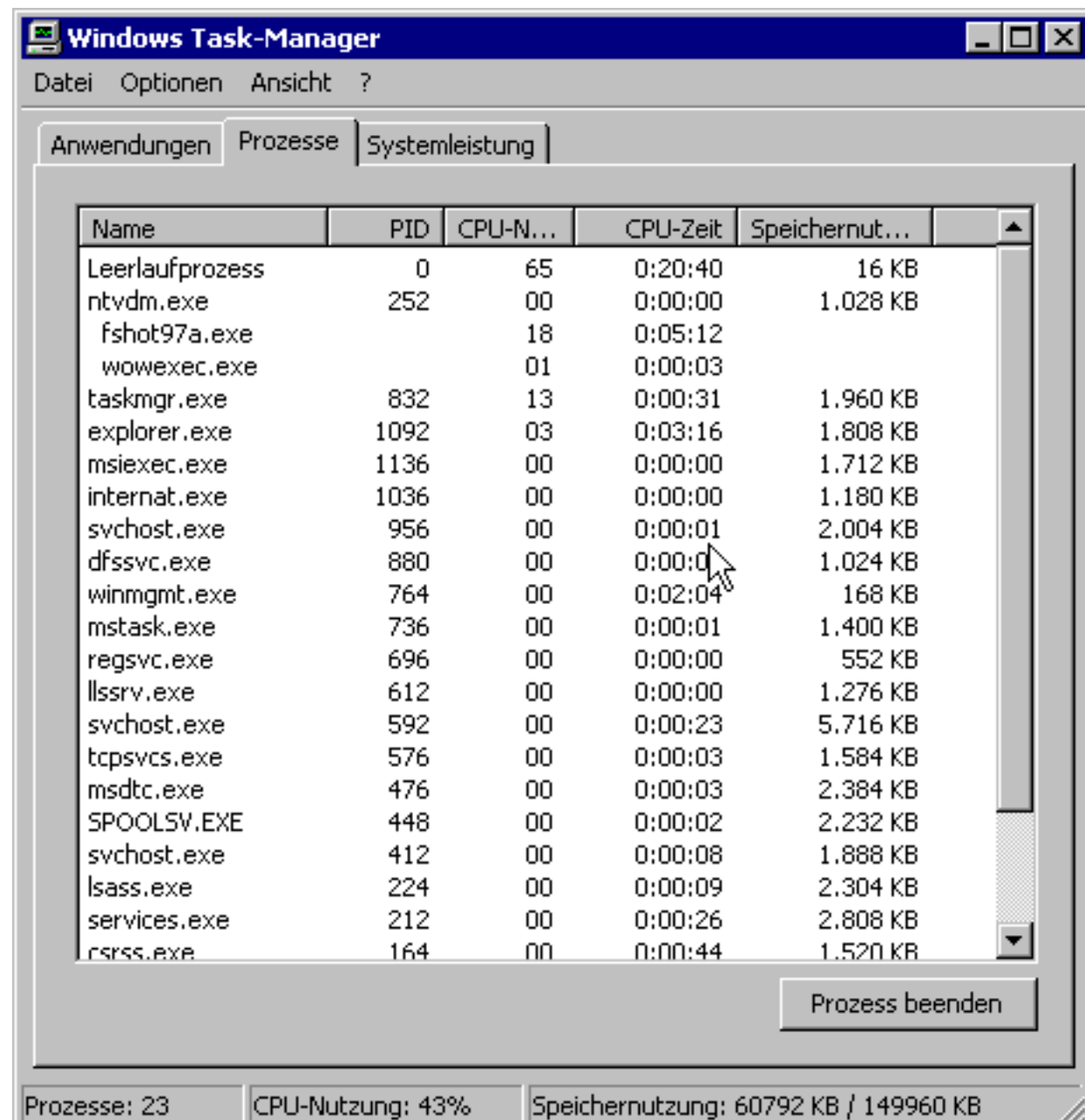


Abbildung 22.11: Analyse eines Windows 2000-Prozesses

Diese eingerückten Einträge bezeichnen Prozesse, die innerhalb der NTVDM (NT Virtual DOS Machine; beachten Sie, dass hier immer noch der Windows NT 4.0-Name »NT« statt der aktuelleren

Abkürzung »Win2k« verwendet wird) ausgeführt werden.



Die NT Virtual DOS Machine ist eines der Untersysteme, die das Betriebssystem Windows 2000 unterstützt. Windows 2000 emuliert eine geschützte Umgebung, in der die älteren MS- DOS- und 16-Bit-Windows-Anwendungen sicher ausgeführt werden können. Beachten Sie jedoch, dass nicht alle MS-DOS- und 16-Bit-Windows-Anwendungen unter Windows 2000 korrekt - wenn überhaupt - ausgeführt werden können, weil dieser Bereich unmittelbar erzeugt wird, wenn Sie versuchen, eines dieser älteren Programme auszuführen.

Um einen Prozess direkt auf der Registerkarte **Prozesse** zu beenden (vorausgesetzt, das ist möglich), markieren Sie diesen durch Anklicken. Anschließend klicken Sie einfach nur auf die Schaltfläche **Prozess beenden**, um diesen Prozess sofort zu beenden.

Um die Registerkarte **Prozesse** so anzupassen, dass Sie alle möglichen Spalten mit relevanten Prozessorinformationen sehen, rufen Sie im **Ansicht**-Menü den Befehl **Spalten auswählen** auf. Das daraufhin geöffnete Dialogfeld sehen Sie in Abbildung 22.12.

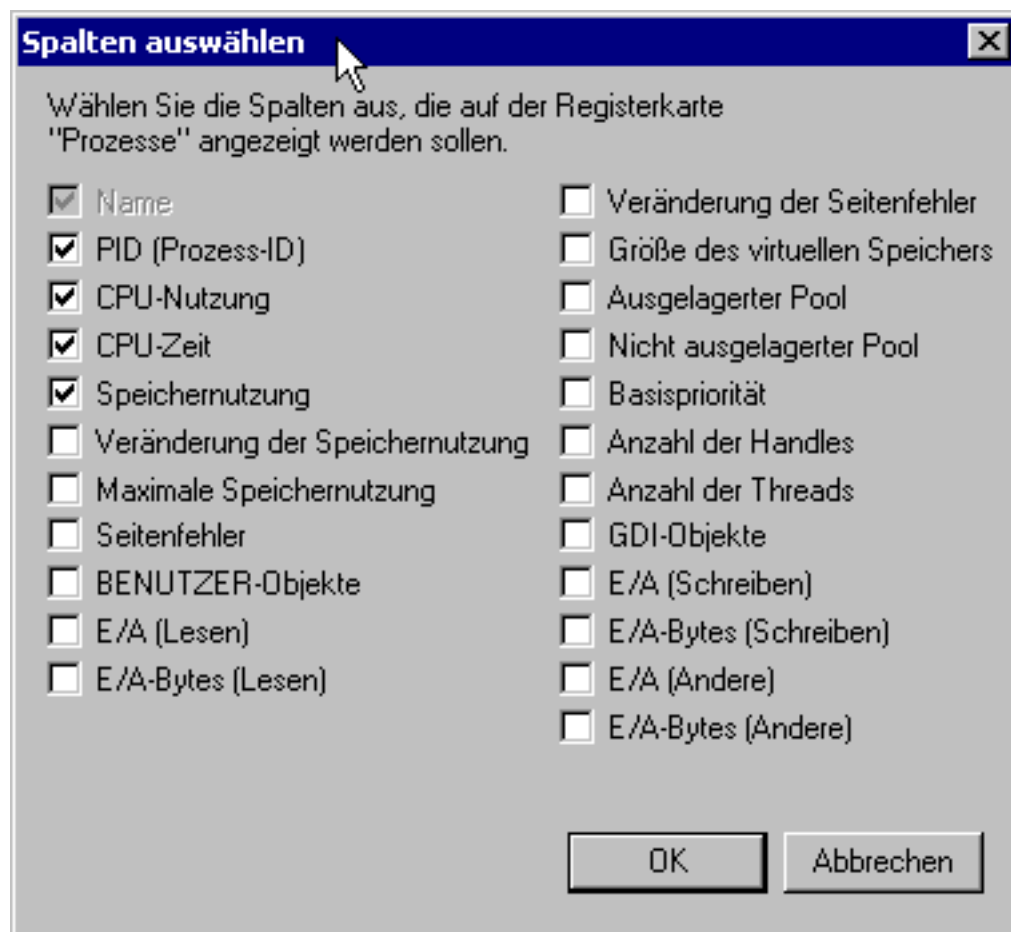


Abbildung 22.12: Auswahl der angezeigten Prozessinformation

Hier können neun Spalten mehr zur Anzeige ausgewählt werden (inklusive aller I/O-Objekte, Spitzenspeichernutzung, den USER-Objekten und den GDI-Objekten), als in den älteren Windows NT 4.0-Betriebssystemen zur Verfügung standen. Diese Spalten beinhalten die folgenden Informationen:

- *Name*. Der dem Prozess zugeordnete Name.

- *PID*. Die Prozess-ID, die einen Prozess von anderen Prozessen an anderen Positionen im gesamten Betriebssystem Windows-2000-Server unterscheidet.
- *CPU-Nutzung*. Die Prozessorzeit (angegeben in Prozent), die die Threads für diesen Prozess seit der letzten Aktualisierung verbraucht haben.
- *CPU-Zeit*. Die Gesamt-Prozessorzeit, die von einem Prozess verbraucht wurde, angegeben im Format »Stunden:Minuten:Sekunden«.
- *Speichernutzung*. Der vom Prozess belegte primäre Systemspeicher, angegeben in Kilobyte (1.024 Byte = 1 Kbyte).
- *Veränderung der Speichernutzung*. Die Differenz zwischen dem aktuell für den Prozess genutzten Speicher und dem bei der letzten Aktualisierung des Task-Managers genutzten Speicher.
- *Maximale Speichernutzung*. Der höchste Wert für den Arbeitsspeicher, der von einem Prozess seit seinem Beginn verbraucht wurde.
- *Seitenfehler*. Gibt an, wie oft das System Informationen für einen Prozess direkt von einer Festplatte außerhalb des Systemspeichers oder der zugehörigen Auslagerungsdatei von Windows-2000-Server holen musste. Dieser Wert wird für den betreffenden Prozess von dessen Beginn an akkumuliert.
- *BENUTZER-Objekte*. Die Gesamtzahl der (internen) BENUTZER-Objekte, die momentan von einem Prozess verwendet werden. Diese Objekte beinhalten Fenster, Menüs, Cursor, Monitore usw.
- *E/A (Lesen)*. Gibt an, wie oft ein Prozess versucht hat, Information von der Speicheradresse zu lesen, die die CPU nutzt, um Daten zu speichern und zu laden.
- *E/A-Bytes (Lesen)*. Die Gesamtzahl der Bytes, die ein Prozess versucht hat, von der Speicheradresse zu lesen, die die CPU nutzt, um Daten zu speichern und zu laden.
- *Veränderung der Seitenfehler*. Die Differenz zwischen der aktuell für einen Prozess aufgezeichneten Anzahl der Seitenfehler und der zuvor aufgezeichneten Gesamtzahl seit der letzten Aktualisierung des Task-Managers.
- *Größe des virtuellen Speichers*. Die Gesamtgröße der Auslagerungsdatei für einen Prozess.
- *Ausgelagerter Pool*. Der Speicher, der für die Auslagerung auf einem Plattenstapel zur Verfügung steht; ein Betrag, der nur BENUTZER-Speicher beinhaltet (Nicht-Kernelmodus-Speicher), den ein Prozess belegt. Dieser Wert wird in Kilobyte angegeben.
- *Nicht ausgelagerter Pool*. Der Betrag des nicht-ausgelagerten Speichers, der von einem Prozess belegt wird, d.h. der Systemspeicher (also Nicht-BENUTZER-Speicher).
- *Basispriorität*. Der Prioritätsklassenebenenbereich, der für einen Prozess eingerichtet wurde. Beachten Sie, dass diese Prioritätsebene durch die Anwendung festgelegt wird, die den Prozess erzeugt, und nicht vom Betriebssystem Windows-2000-Server. Beachten Sie außerdem, dass Windows 2000 die dynamische Prioritätsebene innerhalb dieser grundlegenden Einstellung setzt und/oder ändert.
- *Anzahl der Handles*. Die Gesamtzahl der Objekthandles für einen Prozess in seiner Objekttabelle.
- *Anzahl der Threads*. Die Gesamtzahl aller Objekt-Threads für einen Prozess.
- *GDI-Objekte*. Die Gesamtzahl der GDI-Objekte, die momentan von einem Prozess verwendet werden.

- *E/A (Schreiben)*. Gibt an, wie oft ein Prozess versucht hat, Informationen an die Speicheradresse zu schreiben, die die CPU zum Speichern und Laden von Daten benutzt.
- *E/A-Bytes (Schreiben)*. Die Gesamtzahl der Bytes, die ein Prozess versucht hat, an die Speicheradresse zu schreiben, die die CPU zum Speichern und Laden von Daten benutzt.
- *E/A (Andere)*. Gibt an, wie oft ein Prozess Information aus dem Speicheradressbereich genutzt hat, den die CPU zum Speichern und Laden von Daten benutzt.
- *E/A-Bytes (Andere)*. Die Gesamtzahl der Bytes, die ein Prozess in dem Speicheradressbereich genutzt hat, den die CPU zum Speichern und Laden von Daten benutzt.

Um eine oder mehrere Spalten auszuwählen, klicken Sie einfach auf das zugehörige Kontrollkästchen neben dem Eintrag. Ist ein Kontrollkästchen markiert, erscheint der Eintrag im Inhaltsbereich der Registerkarte **Prozesse**. Ist ein Kontrollkästchen nicht markiert, erscheint der Eintrag nicht in der Liste. Nachdem Sie alle gewünschten Markierungen vorgenommen haben, klicken Sie auf die Schaltfläche **OK**, um Ihre Auswahl zu bestätigen und zur Registerkarte **Prozesse** zurückzukehren. Sie zeigt jetzt alle von Ihnen ausgewählten Informationen an, wie in Abbildung 22.13 gezeigt.

Sie können das Fenster vergrößern, um alle Spalten in einem riesigen Fenster anzuzeigen, vorausgesetzt, Ihr Bildschirm ist groß genug. Darüber hinaus kann es sinnvoll sein, die Spalten zu verbreitern. Doppelklicken Sie dazu auf die Trennlinie (die dünne schwarze Linie) zwischen den Spaltenüberschriften, ähnlich wie in Tabellenkalkulationsprogrammen wie beispielsweise Microsoft Excel. Eine weitere Möglichkeit, die Prozessdaten noch aussagekräftiger anzuzeigen, ist es, die Spalten zu sortieren, indem Sie einmal auf die betreffenden Überschriften klicken. Sie können auch auf eine Spaltenüberschrift klicken, die Maustaste gedrückt halten und die Spalte nach links oder rechts an eine andere Position verschieben.

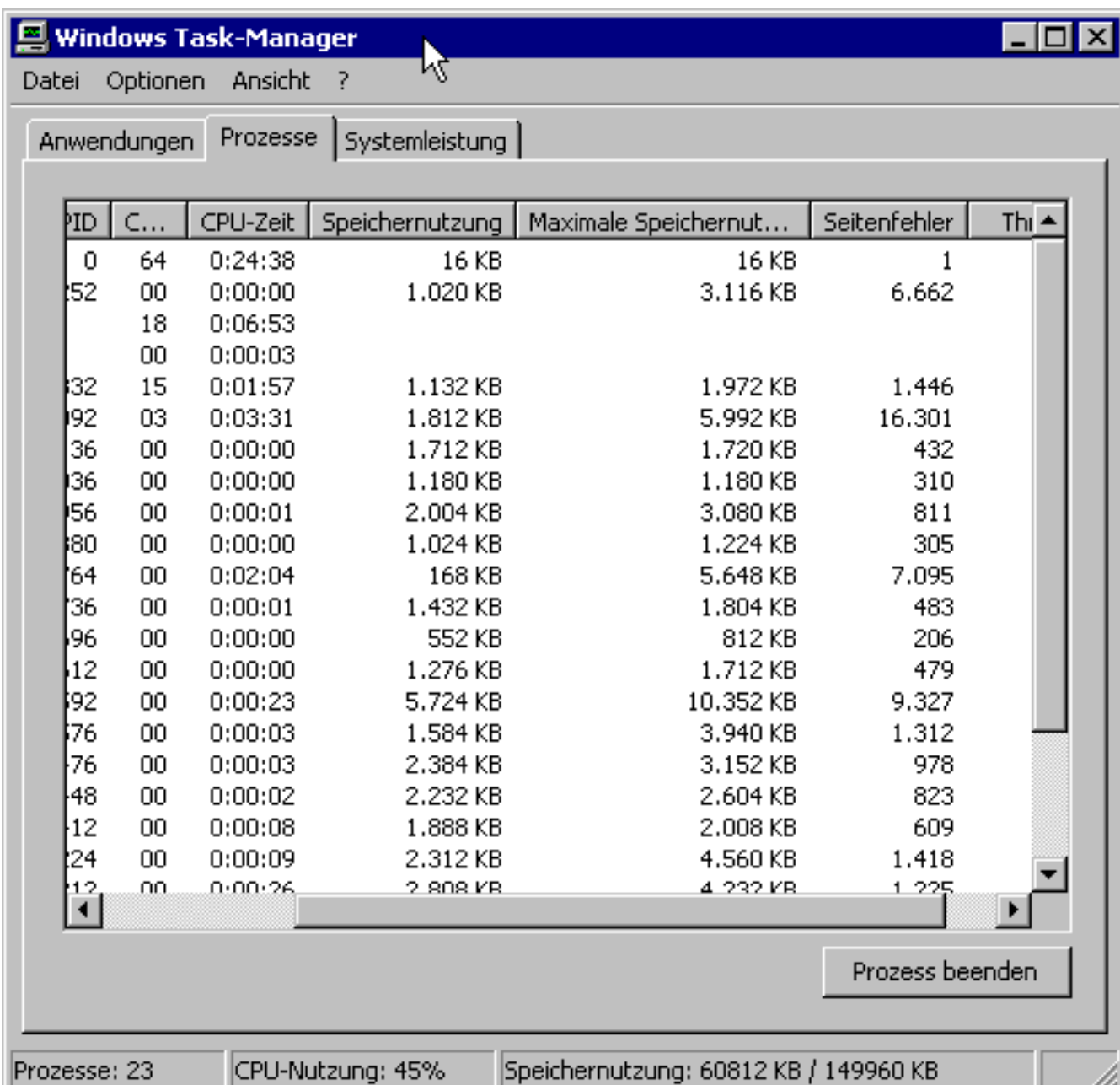


Abbildung 22.13: Anzeige der neu hinzugekommenen Informationsspalten

Wechseln Sie jetzt zur Registerkarte **Systemleistung** (siehe Abbildung 22.14).

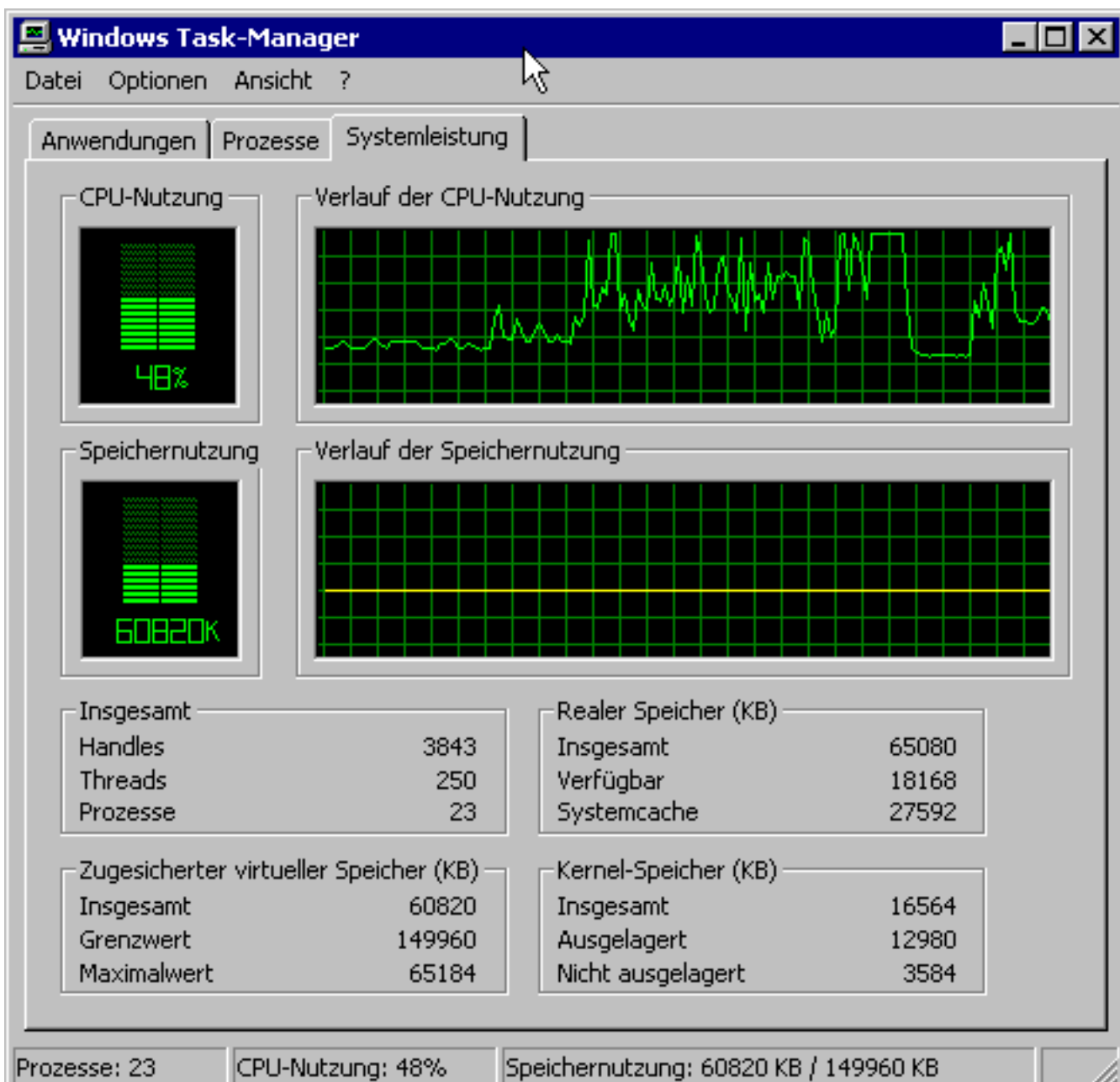


Abbildung 22.14: Anzeige der Systemleistung mit Hilfe des Task-Managers

Auf dieser Registerkarte können Sie schnell den »Gesundheitszustand« Ihres Windows 2000-Servers feststellen. Die vier Felder in der unteren Fensterhälfte enthalten statistische Werte zum »gesamten« und »verfügbaren« Speicher, wodurch die Verwaltung Ihres Systems sehr viel einfacher wird. Betrachten Sie den Abschnitt *Insgesamt*. Sie sehen die Gesamtzahl der aktuell auf Ihrer Windows-2000-Server-Maschine aktiven Prozesse und Threads. Analog zeigt der Abschnitt *Realer Speicher (KB)* den Gesamtbetrag des installierten und vom Betriebssystem erkannten Arbeitsspeichers an, ebenso wie den Speicher, der für das System und die Anwendungen zur Verfügung steht. Beachten Sie, dass diese Werte in Kilobyte angegeben sind; beispielsweise würde ein Wert von 196148 für 192 Mbyte stehen (1 Mbyte = 1.024 Kbyte).

Die Balken- und Liniendiagramme in der oberen Hälfte des Bildschirms sind grafische Darstellungen der CPU- und Speicherkomponenten Ihrer Windows-2000-Server-Maschine. Um diesen Bildschirmen noch mehr Informationen entnehmen zu können, könnten Sie die Anzeige von Kerndaten aktivieren oder die Diagramme auf eine einzige CPU beschränken (auf Systemen, in denen nur eine einzige CPU eingesetzt

ist, steht diese zweite Option nicht zur Verfügung). Um diese Optionen zu aktivieren, öffnen Sie das Menü **Ansicht** und wählen den Eintrag **Kernel-Zeiten anzeigen** aus.

Für die Anzeige der Kernelzeiten wird eine rote Linie in das Liniendiagramm eingefügt und der Teil des Balkendiagramms, der den Kernel darstellt, rot angezeigt. Beide Darstellungen sind praktisch, wenn Sie versuchen, ein nicht zufrieden stellend arbeitendes System zu diagnostizieren. Wenn ein System beispielsweise seinen Kernel ständig mit 100 Prozent auslastet, sehen Sie, dass in Ihrem Server nicht genügend Arbeitsspeicher vorhanden ist.

Um Ihre Diagramme so zu ändern, dass sie jeweils nur eine einzige CPU darstellen, aktivieren Sie im Menü **Ansicht** die Option **CPU-Verlauf/Ein Diagramm pro CPU**. Können Sie sich noch an die Beschreibung der Support Tools in diesem Kapitel erinnern? Hier können Sie zumindest eines dieser Werkzeuge sinnvoll einsetzen: den **Process Viewer**. Klicken Sie im Startmenü auf **Programme/Windows 2000 Support Tools/Tools/Process Viewer**. Sie sehen die Prozessanzeige (siehe Abbildung 22.15).

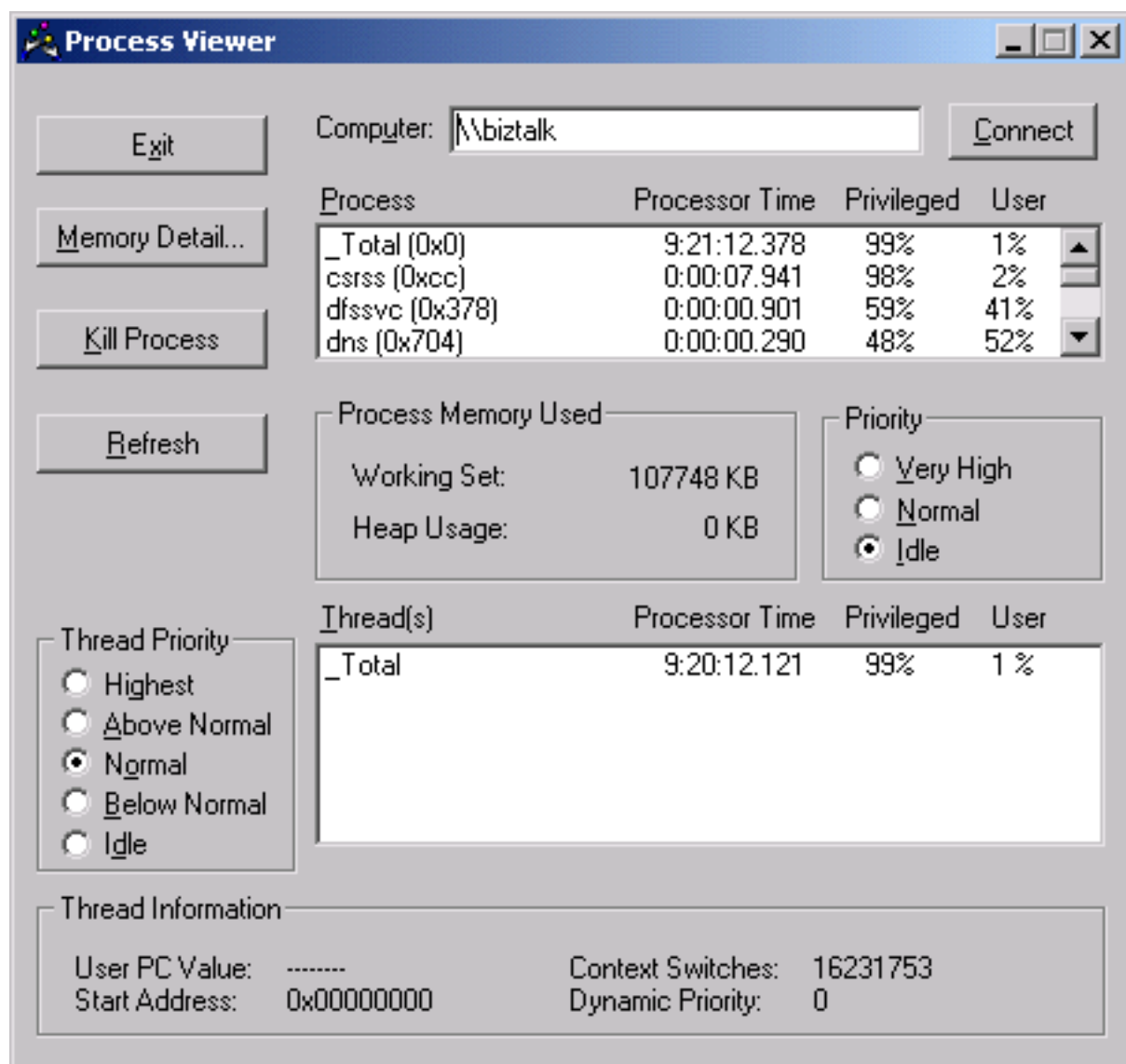


Abbildung 22.15: Der Hauptbildschirm des Process Viewers

Die Anzeige des Process Viewers ist kompliziert und manchmal etwas verwirrend. Die Nutzung dieses Dienstprogramms kann fast mit der Bearbeitung der Windows 2000 Server-Registrierung verglichen

werden: Sie können Ihre Arbeit als Administrator sehr viel besser erledigen, wenn Sie diese beiden Werkzeuge beherrschen. Aber der Weg dorthin ist voller Gefahren und ein einziger Fehler kann das gesamte System unbrauchbar machen (was momentan nicht korrigierbar ist). Sie werden sehr schnell feststellen, dass es in diesem Dienstprogramm keine Hilfe gibt, und dass auch die Online-Hilfe von Windows-2000-Server kaum Unterstützung bietet. Erwarten Sie auch nicht, Informationen aus den Handbüchern von Microsoft Press zu erhalten, weil die Konzepte für die Nutzung der Prozessanzeige über das Wissen der meisten Systemadministratoren hinausgehen und nur von wirklich fortgeschrittenen Administratoren genutzt werden können.

Der Hauptbildschirm des Process Viewers ist in zwei Abschnitte unterteilt: oben die Prozessverwaltung, unten die Threadverwaltung. Das Feld ganz oben zeigt den Computer an, auf dem diese Prozesse ausgeführt werden. Um einen anderen als den aktuell verwendeten Computer zu verwalten, vorausgesetzt, Sie besitzen die entsprechenden Berechtigungen, geben Sie den UNC-Pfad (Universal Naming Convention) (mit dem Format \\Servername) für diesen Server ein und klicken auf die Schaltfläche **Connect**. Im zweiten Feld sehen Sie Informationen zu den auf Ihrem Server aktiven Prozessen.

- *Process*. Der Name des Prozesses, wobei in Klammern die Anfangsspeicheradresse angezeigt wird.
- *Processor Time*. Die gesamte CPU-Zeit, wie lange ein Prozess aktiv war, angegeben in »Stunden:Minuten:Sekunden:Tausendstelsekunden«.
- *Privileged*. Manchmal auch als *Kernelmodus* bezeichnet, ist dies der Prozentsatz der Zeit, den ein bestimmter Prozess im privilegierten Modus im Gegensatz zum Benutzermodus ausgeführt wurde.
- *User*. Der Prozentsatz der Zeit, während der ein bestimmter Prozess im Benutzermodus im Gegensatz zum privilegierten Modus ausgeführt wurde. Beachten Sie, dass die Prozentsätze für *User* und *Privileged* zusammen immer 100 Prozent ergeben.



Der Privilegierte oder Kernelmodus ist eine Ebene der Hardware- und Speicheroperation, die von normalen Anwendungen nicht erreicht werden kann, d.h. es handelt sich um einen geschützten Bereich. Manchmal spricht man hier auch vom Protected Mode, vom Supervisor-Modus oder Ring 0. Prozesse, die im privilegierten Modus ausgeführt werden, haben Zugriff auf alle erweiterten CPU-Funktionen für I/O- und Speicherverwaltung, sodass sie sehr viel effizienter werden.

Im dritten Abschnitt dieses Bildschirms, Process Memory Used, erhalten Sie einen schnellen Überblick darüber, wie viel Speicher ein Prozess verbraucht hat. Dazu klicken Sie auf einen Prozessnamen im Feld Process. Sie sehen, wie sich die Werte für Working Set und Heap Usage entsprechend ändern.

Rechts neben dem Abschnitt Process Memory Used sehen Sie den Bereich Priority, wo Sie die Priorität für einen bestimmten Prozess ablesen. In der Regel wird hier die Einstellung Normal angezeigt, aber Sie können die Priorität für einen Prozess auch ändern, indem Sie einfach auf das entsprechende Optionsfeld klicken. Wollen Sie etwa in diesem Beispiel eine höhere Priorität zuweisen, klicken Sie auf das Optionsfeld für Very High. Wenn Sie nicht genau wissen, was das für Ihre Maschine für Konsequenzen hat, sollten Sie keinesfalls mit diesen Einstellungen experimentieren, es sei denn, Sie arbeiten in einer Testumgebung (eine falsche Einstellung könnte den Server zum Absturz bringen).

In der unteren Bildschirmhälfte der Prozessanzeige geht es um die Threadverwaltung. Ganz links sehen Sie den Bereich für die Threadpriorität, wo Sie die Prioritätsebene für einen einzelnen Thread eines

bestimmten Prozesses festlegen können. Auch mit dieser Einstellung sollten Sie nicht experimentieren, wenn Sie die Konsequenzen nicht absehen können. Die meisten Prozesse verwenden Threads mit der Priorität Normal, aber viele der Systemprozesse (d.h. Programme auf Betriebssystemebene) können eine etwas höhere Einstellung besitzen, beispielsweise Above Normal. Problematisch beim Versuch, Threadprioritäten zu manipulieren, ist es, zu erkennen, welche geändert werden sollen. Mit anderen Worten, Threads haben in der Regel keine aussagekräftigen Namen (betrachten Sie das Beispiel in Abbildung 22.15, wo die Threads einfach nur ihrer numerischen Reihenfolge nach bezeichnet sind). D.h. Sie erkennen sehr wahrscheinlich nicht, welcher Thread geändert werden soll, es sei denn, Sie haben die betreffende Anwendung selbst entwickelt.

Auch im Threadbereich gibt es einen Abschnitt für die aktiven Threads, rechts neben dem Bereich für die Threadpriorität. In diesem Feld erkennen Sie schnell, wie lang ein Thread für einen bestimmten Prozess ausgeführt wurde. Es scheint, als könne die Priorität eines Threads hier geändert werden, aber diese Optionsfelder sind nur Dekoration - die Threadpriorität kann im Process Viewer nicht geändert werden. Unterhalb dieses Felds sehen Sie die Threadinformationen. Hier können Sie den Status eines Threads ablesen. Sie erhalten die folgenden Informationen:

- *Start Address*. Die virtuelle Startadresse für einen Thread.
- *User PC Value*. Die virtuelle Adresse für den Wert des Benutzermodus.
- *Context Switches*. Ein Kontextwechsel tritt auf, wenn der Mikrokern den Prozessor von einem Thread an einen anderen Thread weitergibt; dieser Wert gibt die Anzahl dieser Wechsel für einen bestimmten Prozess auf Ihrem Windows 2000-Server an. Beachten Sie, dass dieser Wert auf einem System mit einem einzigen Prozessor nicht so relevant ist wie für einen Multiprozessor-Server.
- *Dynamic Priority*. Die Prioritätsebene, die Windows 2000 einem Thread automatisch zuweist, während er auf die Verarbeitung wartet. Sie können diese Einstellung für einige Prozesse ändern, beispielsweise wenn Sie die Leistungsebene für die Anwendungsreaktion ändern, indem Sie auf der Registerkarte **Erweitert** im Eigenschaftenfenster der Computerverwaltung (lokal) auf die Schaltfläche **Leistungsoptionen** klicken.

Auf der linken Seite des Process Viewers sehen Sie vier Schaltflächen, die diverse wichtige Aktivitäten der Prozessanzeige steuern:

- *Exit*. Hiermit verlassen Sie den Process Viewer.
- *Memory Detail*. Diese Schaltfläche zeigt einen detaillierteren Bildschirm mit Informationen zur Speichernutzung eines bestimmten Prozesses an.
- *Kill Process*. Diese Schaltfläche beendet die Ausführung eines Prozesses.
- *Refresh*. Diese Schaltfläche aktualisiert den Inhalt des Prozessinformationsfensters.

Damit Sie dieses Dienstprogramm für Ihre Aufgaben bestmöglich nutzen können, betrachten wir hier ein Beispiel und durchlaufen den gesamten Prozess, wobei alle Bereiche der Prozessanzeige genutzt werden sollen. Um das Beispiel so einfach wie möglich zu halten, betrachten wir hier das Spiel *Minesweeper*, das in Windows-2000-Server enthalten ist. Starten Sie die Prozessanzeige und dann das Spiel auf Ihrem Windows-2000-Server-Computer. Sie finden das Spiel im Startmenü unter

Programme/Zubehör/Spiele/Minesweeper. Wenn Sie im Prozessinformationsfeld nach unten blättern (das ist das größere Feld in der oberen Hälfte der Prozessanzeige), sollten Sie den Prozess für das Spiel *Minesweeper* sehen, wie in Abbildung 22.16 gezeigt.

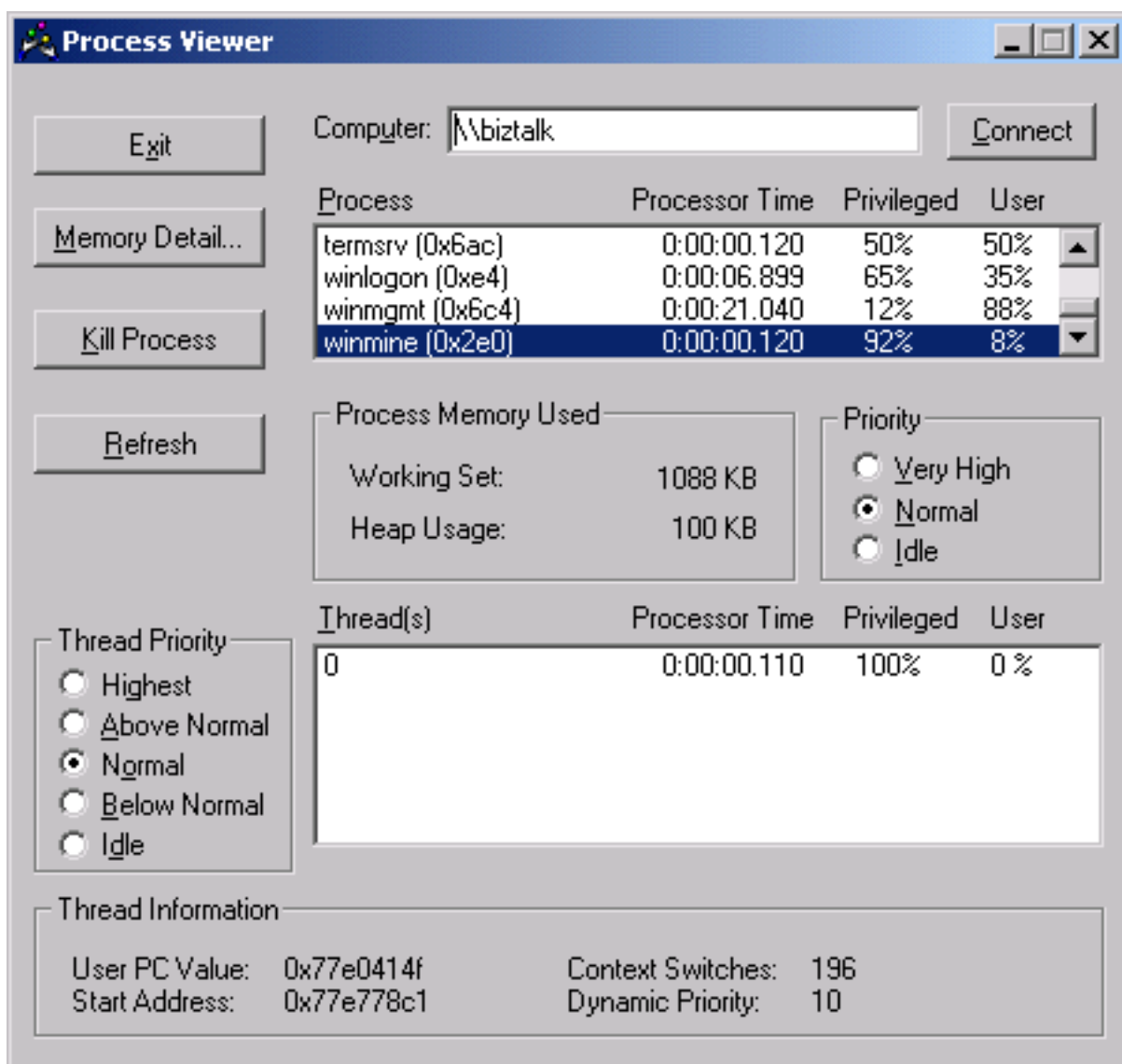


Abbildung 22.16: Anzeige der Eigenschaften eines bestimmten Prozesses

Es hat den Prozessnamen *winmine* (weil das der Name der Programmdatei für das Spiel Minesweeper ist). Wenn Sie diesen Prozess in Ihrer Prozessanzeige nicht sehen, klicken Sie auf die Schaltfläche **Refresh**, um den Inhalt des Prozessinformationsfelds zu aktualisieren. Jetzt sehen Sie den Prozess, vorausgesetzt, Sie haben den Minesweeper erfolgreich gestartet. Sehen Sie sich die verschiedenen Informationen für dieses Spiel in der Prozessanzeige genau an. Beachten Sie zum Beispiel, dass für dieses Spiel nur ein Thread ausgeführt wird, aber seine Ressourcen gleichmäßig zwischen privilegiertem und Benutzermodus aufgeteilt sind. Auch wenn es sich hier um ein sehr einfaches Spiel handelt, verbraucht es relativ viel Arbeitsspeicher und Heap-Prozessspeicher.

Nachdem Sie den Ressourcenbedarf für das Spiel ermittelt haben, beenden Sie es. Dazu gehen Sie aber nicht nach der normalen Methode vor (nämlich im Spiel selbst), sondern Sie beenden das Spiel mit Hilfe des Process Viewers. Dazu klicken Sie auf den Prozess *winmine* und dann auf die Schaltfläche **Kill Process**. Ein Popup-Feld wird angezeigt, das die genaue Speicherposition des zu beendenden Prozesses enthält.

In diesen Popup-Fenstern gibt es zwei Schaltflächen: **OK** und **Abbrechen**. Wenn Sie auf die Schaltfläche **Abbrechen** klicken, passiert nichts und der betreffende Prozess wird fortgesetzt (d.h. das

Spiel läuft weiter). Klicken Sie dagegen auf **OK**, wird das Spiel sofort beendet, ebenso der Prozess. Und jetzt wird es interessant: Der Process Viewer zeigt den Prozess *winmine* immer noch als aktiv an. Er wird nämlich nicht in regelmäßigen Abständen automatisch aktiviert. Klicken Sie auf die Schaltfläche **Refresh**, um die Anzeige zu aktualisieren.

Jetzt wollen wir noch den Bereich mit den Speicherdetails des Process Viewers genauer betrachten. Dazu klicken Sie auf einen beliebigen Prozess, beispielsweise *explorer* (das ist der Shell-Prozess für Windows-2000-Server), und dann auf die Schaltfläche **Memory Detail**. Das in Abbildung 22.17 gezeigte Dialogfeld **Memory Details** wird geöffnet.

Das Dialogfeld **Memory Details** zeigt verschiedene statistische Werte für den Prozess *explorer* an, der im Hauptfenster des Process Viewers ausgewählt wurde. Die hier gezeigten Speicherdetails werden im einzigen Dropdown-Listefeld des Bildschirms festgelegt: **User Address Space for**. In unserem Beispiel haben wir **Total Commit** ausgewählt, d.h. es werden die Speicherdetails für alle aktiven DLL-Dateien (Dynamic Link Libraries) für diesen Prozess angezeigt. Wenn Sie die Speicherdetails für eine bestimmte DLL-Datei anzeigen wollen, beispielsweise für die Dokumenteigenschaften (*docprop2.dll*), klicken Sie einfach in das Dropdown-Listefeld und wählen diese hier aus.

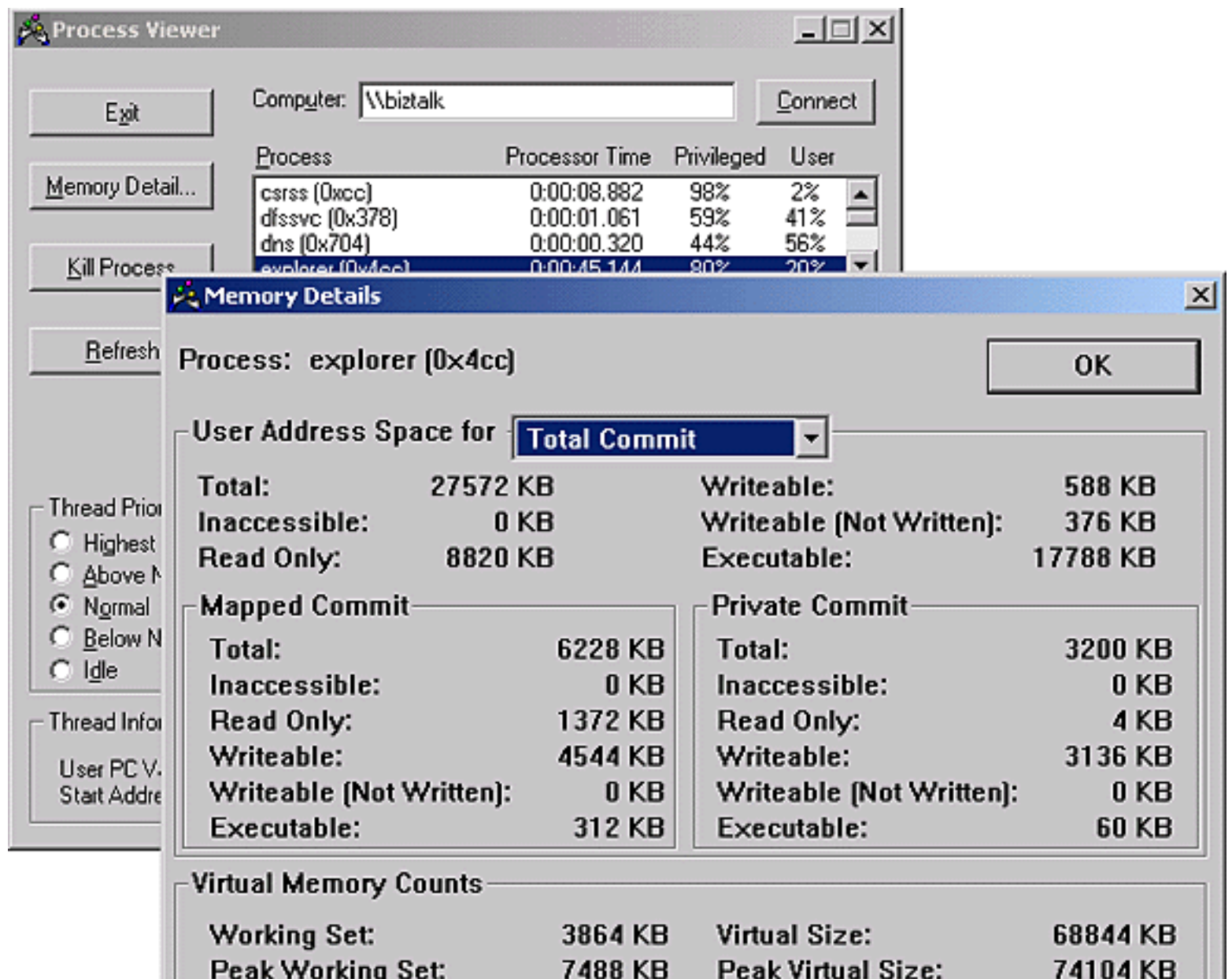


Abbildung 22.17: Anzeige der Speicherdetails für einen Prozess

Nachdem die DLL-Datei angeklickt wurde, erscheinen die zugehörigen Speicherdetails dafür im Dialogfeld. Nachdem Sie alle für Sie wichtigen Informationen angesehen haben, schließen Sie das Fenster mit **OK**. Damit gelangen Sie zum Hauptfenster des Process Viewers zurück. Um den Process Viewer endgültig zu verlassen, klicken Sie in diesem Fenster auf die Schaltfläche **Exit**.

22.2.4 Festplattenanforderung in den Cache stellen

Eine weitere Möglichkeit, die Leistung der Windows-2000-Server-Umgebung des Unternehmens zu steigern, ist das so genannte *Caching*. Genauer gesagt handelt es sich um das Caching der Festplattenanforderungen, wodurch eine Windows-2000-Server-Anwendung ihre Gesamtleistung verbessern kann. Leider kommt es vor, dass die Anwendungsentwickler ihre Programme nicht sorgfältig genug entwickeln. Dies bedeutet: Sie können die allerneueste Serverhardware einsetzen, was Speicher und Plattenlaufwerke/Controller betrifft, und die Anwendungen belegen trotzdem beliebig Speicher und bieten eine unzureichende Leistung. Am besten präsentieren Sie den Entwicklern innerhalb Ihres Unternehmens den belegten Beweis, dass ihre Anwendungen nicht so sind, wie sie sein sollten. Dazu brauchen Sie das Werkzeug »Systemmonitor«. Dieses Werkzeug ist die Aktualisierung des alten Systemmonitors von Windows NT 4.0. Die Verwendung des Werkzeugs wird später in diesem Kapitel genauer beschrieben.

Wenn Sie bereits wissen, wie man dieses Überwachungswerkzeug benutzt, können Sie es jetzt aufrufen. Wählen Sie im Startmenü die Einträge **Programme/Verwaltung/Systemmonitor**. Damit starten Sie die MMC *Leistung*, von wo aus Sie Ihre Diagnose ausführen können. Tabelle 22.2 zeigt einige der wichtigsten Leistungsindikatoren, die Sie überwachen können, und die Ihnen helfen, eine fehlerhafte Anwendung zu ermitteln (als Beweis für die Entwickler im Unternehmen).

Objekt	Leistungsindikator
Speicher	Datenzuordnungstreffer
Speicher	Cachefehler/Sek.
Speicher	Seitenfehler/ Sek.
Speicher	Seitenlesevorgänge/ Sek.
Cache	Kopieren Lesevorgänge/ Sek.
Cache	Datenleerungen/ Sek.
Cache	Kopieren Lesetreffer (%)
Cache	Schnelllesen nicht möglich/ Sek.
Cache	Vorauslesevorgänge/ Sek.
Logischer Datenträger	Datenträger lesen/Sek.

Tabelle 22.2: Überwachung von Problemen mit dem Festplattencache

22.3 Stripesets und Auslagerungsdateien im virtuellen Speicher

Die Leistung Ihres Windows 2000-Servers wird durch zwei wichtige Faktoren beeinflusst: den Typ des Festplattenspeichers und des Controllers im System sowie den Arbeitsspeicher (RAM), der dem Betriebssystem zur Verfügung steht. Um eine bestmögliche Systemleistung in Hinblick auf die Festplatte zu gewährleisten, sollten Sie die so genannte *RAID-Technologie (Redundant Array of Inexpensive Disks)* einsetzen, wobei *Stripesets* verwendet werden. Diese Technologie wird im nächsten Abschnitt genauer beschrieben. Mit der Stripeset-Methode erzielen Sie die beste Festplattenleistung unter Windows-2000-Server. Auch hier müssen Kompromisse getroffen werden, deshalb sollten Sie den nächsten Abschnitt sehr sorgfältig lesen.

Um die Systemleistung in Hinblick auf den Speicher zu optimieren, sollten Sie *Auslagerungsdateien im virtuellen Speicher* nutzen. Auch dieses Konzept wird hier noch genauer beschrieben. Dabei wird das so genannte *Demand Paging* genutzt, um Daten zwischen dem RAM Ihrer Windows 2000 Server-Maschine und den Auslagerungsdateien des Servers zu transportieren. Wenn in Ihrem Unternehmen die virtuelle Speicherkonfiguration von Windows 2000 vollständig genutzt wird, ist eine maximale Serverleistung möglich. Eine umfassende Beschreibung der Auslagerungsdateien im virtuellen Speicher für einen Windows 2000-Server finden Sie nach dem Abschnitt über die Stripeset-Datenträger.

22.3.1 Stripeset-Datenträger

Sie können die Leistung Ihres Betriebssystems für Windows-2000-Server in Ihrem Unternehmen optimieren, indem Sie so genannte *Stripeset-Datenträger* einsetzen. Ein Stripeset-Datenträger verbessert die Leistung für Lese- und Schreibvorgänge auf der Festplatte, weil dabei mehrere Festplatten beteiligt sind und ein besserer Datenschutz in Hinblick auf die Fehlertoleranz gewährleistet wird. Unter Windows 2000 gibt es wie im alten Windows NT 4.0 zwei Arten von Stripeset-Datenträgern: ohne Parität und mit Parität, jetzt als RAID-5-Datenträger bezeichnet. Nur ein RAID-5-Datenträger bietet Redundanz, ein Stripeset-Datenträger ohne Parität dagegen nicht.

Bevor wir diese Beschreibung fortsetzen, müssen Sie die Unterschiede zwischen den beiden Speicherarten im Betriebssystem Windows 2000 verstehen. Können Sie sich noch an Windows NT 4.0 erinnern, wo man die herkömmliche Version der Festplattenlaufwerke mit primären und erweiterten Partitionen hatte? Die Plattenlaufwerke mit den erweiterten Partitionen enthielten ein oder mehrere logische Laufwerke. Diese Art des Plattenspeichers wird in der Windows 2000-Welt jetzt als *Basisspeicher* bezeichnet. Es ist zwar weiterhin möglich, das Basisspeicherkonzept zu nutzen - insbesondere, weil es sich dabei um das Standardplattenformat handelt -, aber der Leistung und der Datenredundanz halber sollten Sie davon absehen. Die mit Windows 2000 neu eingeführte Methode ist der *dynamische Speicher*. Der dynamische Speicher erlaubt Ihnen, bis zu fünf verschiedene Speicherformate für Ihre Windows-2000-Server-Maschine zu verwenden:

- *Einfacher Datenträger*. Dieses einzelne Festplattenlaufwerk enthält eine einzige Partition, die das gesamte Festplattenlaufwerk beinhaltet. Ein einfacher Datenträger kann jedoch gespiegelt werden, wodurch in Ihrem Windows 2000-System eine gewisse Fehlertoleranz eingeführt wird.
- *Übergreifender Datenträger*. Diese Form des Festplattenspeichers verwendet mehrere Festplattenlaufwerke (bis zu 32 Laufwerke) als einzelne Partition, wodurch sehr große Partitionen angelegt werden können, ohne ein einziges, großes Laufwerk kaufen zu müssen. Ein offensichtlicher Nachteil bei den übergreifenden Datenträgern ist, dass beim Ausfall eines einzigen Laufwerks alle Daten auf allen Laufwerken verloren gehen.
- *Gespigelter Datenträger*. Ein gespiegelter Datenträger ist eine fehlertolerante Methode, Informationen auf Ihrer Windows-2000-Server-Maschine abzulegen. Dazu brauchen Sie mindestens zwei Festplattenlaufwerke, die zunächst als einfache Datenträger angelegt werden. Ein Vorteil bei gespiegelten Datenträgern ist, dass alle Systeminformationen und Daten vollständig geschützt sind, mit dem offensichtlichen Nachteil, dass Sie nur 50 Prozent Ihres gesamten Festplattenspeichers nutzen können (aufgrund der Spiegelung).
- *Stripeset-Datenträger*. Ein Stripeset-Datenträger ist die schnellste Form des Festplattenspeichers in der Windows 2000-Welt, weil dabei Lese- und Schreibvorgänge optimiert werden, weil über alle Festplatten mit derselben Geschwindigkeit geschrieben wird. Um einen Stripeset-Datenträger anzulegen, brauchen Sie mindestens zwei (aber nicht mehr als 32) Festplattenlaufwerke. Beachten Sie jedoch, dass ein Stripeset-Datenträger keine Fehlertoleranz für Computersysteme Ihres Unternehmens bietet.
- *RAID-5-Datenträger*. Ein RAID-5-Datenträger ist die fehlertolerante Version des Stripeset-Datenträgers. Dabei werden Lesevorgänge optimiert, die Schreibvorgänge jedoch wesentlich langsamer. Für RAID-5 brauchen Sie mindestens drei Festplattenlaufwerke (höchstens 32) und verwenden eine Parität-Striping-Funktion, um Daten über die Laufwerke zu speichern, ähnlich einer Bereitstellung von Fehlertoleranz für die Daten des Unternehmens.

Der *dynamische Speicher* unter Windows 2000 bietet etwas, wovon die Systemadministratoren unter Windows NT 4.0 nur träumen konnten: die Möglichkeit, einen Festplattendatenträger dynamisch zu vergrößern oder zu verkleinern, ohne das Betriebssystem neu starten zu müssen. Wie in der Windows NT 4.0-Welt ist es jedoch nicht möglich, Systempartitionen auf einem RAID-5-Datenträger anzulegen (sehr wohl jedoch auf einem Stripeset-Datenträger).

In Hinblick auf die Fehlertoleranz bedeutet ein RAID-5-Datenträger (Stripeset-Datenträger mit Parität) geringere Kosten pro Byte Information und außergewöhnlich hohe Leseleistung, benötigt aber mehr Systemspeicher als RAID-1-Datenträger (gespiegelter Datenträger). Darüber hinaus kann ein RAID-1-Datenträger die Boot- und Systempartitionen schützen, ein RAID-5-Datenträger dagegen nicht. Falls in Ihrem Unternehmen hauptsächlich Systemleistung gefordert wird (d.h. Sie können damit leben, wenn die Fehlertoleranz nur durch Ihre Sicherungskopien realisiert wird), sollten Sie hier einen Stripeset-Datenträger als dynamischen Speicher verwenden.

Es gibt ein MMC-Snap-In, mit dem Sie Ihre Festplattenkonfiguration ändern können, nachdem Sie Windows-2000-Server installiert haben: Datenspeicher. Es ist Teil der Computerverwaltung (aber Sie können damit Ihr eigenes, »spezielles« MMC-Format anlegen, falls Sie das möchten). Sie finden die Computerverwaltung von Windows-2000-Server im Startmenü unter **Programme/Verwaltung/Computerverwaltung**. Sie sehen den in Abbildung 22.18 gezeigten Bildschirm.

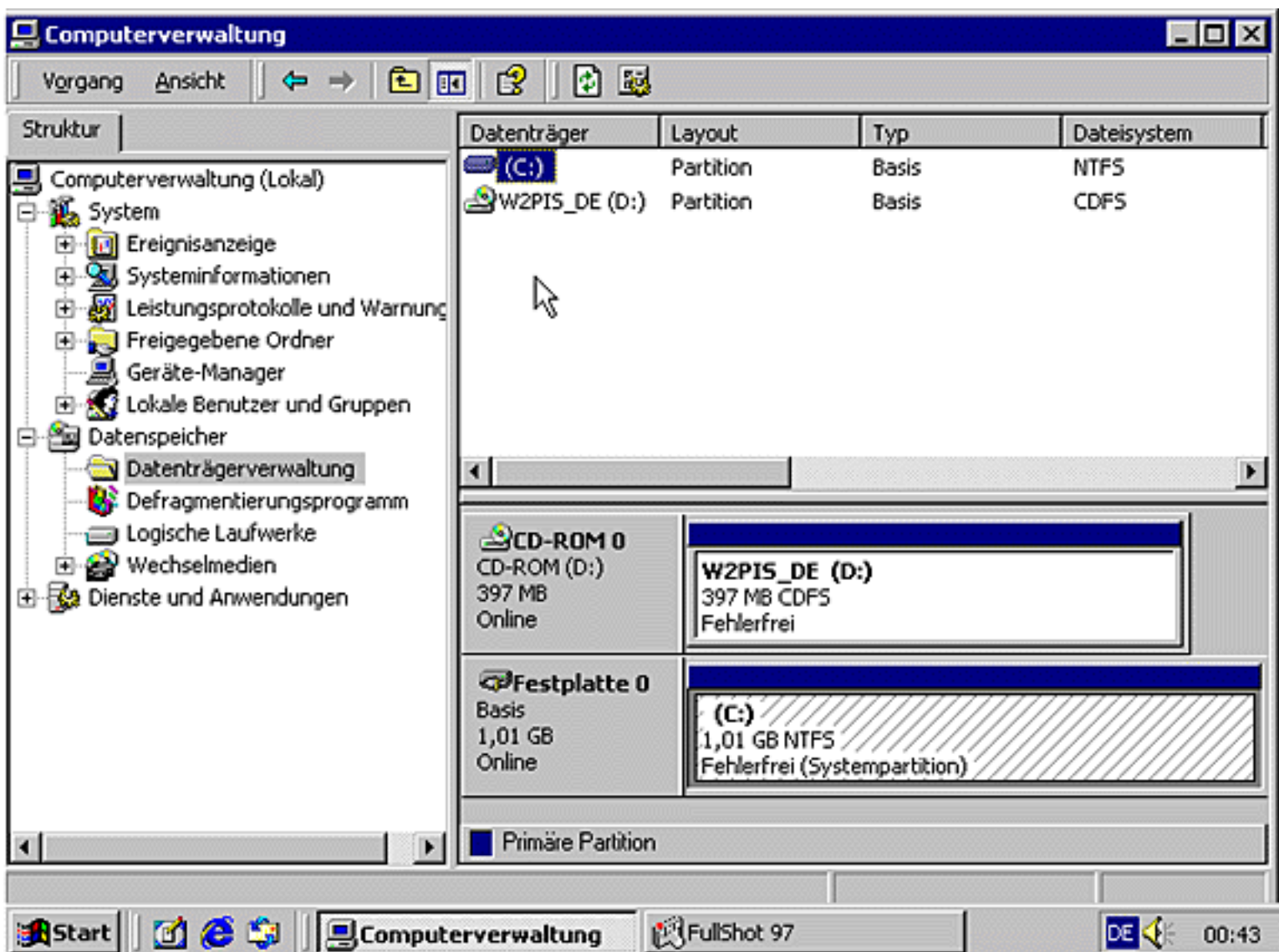


Abbildung 22.18: Die Datenträgerverwaltung in der Windows-2000-Server-Computerverwaltung

Als weitere Methode, dieses Werkzeug aufzurufen (die außerdem noch sehr viel schneller ist), klicken Sie mit der rechten Maustaste auf das Symbol **Arbeitsplatz** auf dem Windows 2000-Desktop und dann auf die Menüauswahl **Verwalten**. Damit sind Sie im Hauptmenü der Computerverwaltung angekommen und können anfangen. Klicken Sie auf das Plusymbol (+) links von der Option **Datenspeicher**, sodass dieser Bereich aufgeklappt wird. Hier finden Sie den Ordner **Datenträgerverwaltung**. Klicken Sie den Ordner an, um im rechten Feld eine Liste aller Datenträger des Systems anzuzeigen.

Wie Sie sehen, gibt es in diesem Beispiel mehrere Datenträger, die bereits angelegt sind und genutzt werden. Wenn Sie vorhaben, ein Multiboot-System anzulegen, wie das hier gezeigte (dieser Computer bootet auch Red Hat Linux, Windows NT 4.0 Server und Windows Millennium), dürfen Sie Ihr System nicht als dynamischen Windows 2000-Datenträger mit dem Dateisystem NTFS 5.0 formatieren. Wollen Sie dagegen nur Windows-2000-Server auf dem System ausführen (das ist die empfohlene Vorgehensweise, außer auf Testsystemen), können Sie die dynamische Datenträgerstruktur von Windows 2000 mit dem Dateisystem NTFS 5.0 nutzen. Um die Formatstruktur eines Datenträgers zu ändern, klicken Sie diesen in der unteren Hälfte des rechten Felds an, um ihn zu markieren, und klicken dann mit der rechten Maustaste auf denselben Datenträger, um das in Abbildung 22.19 gezeigte Kontextmenü aufzurufen.

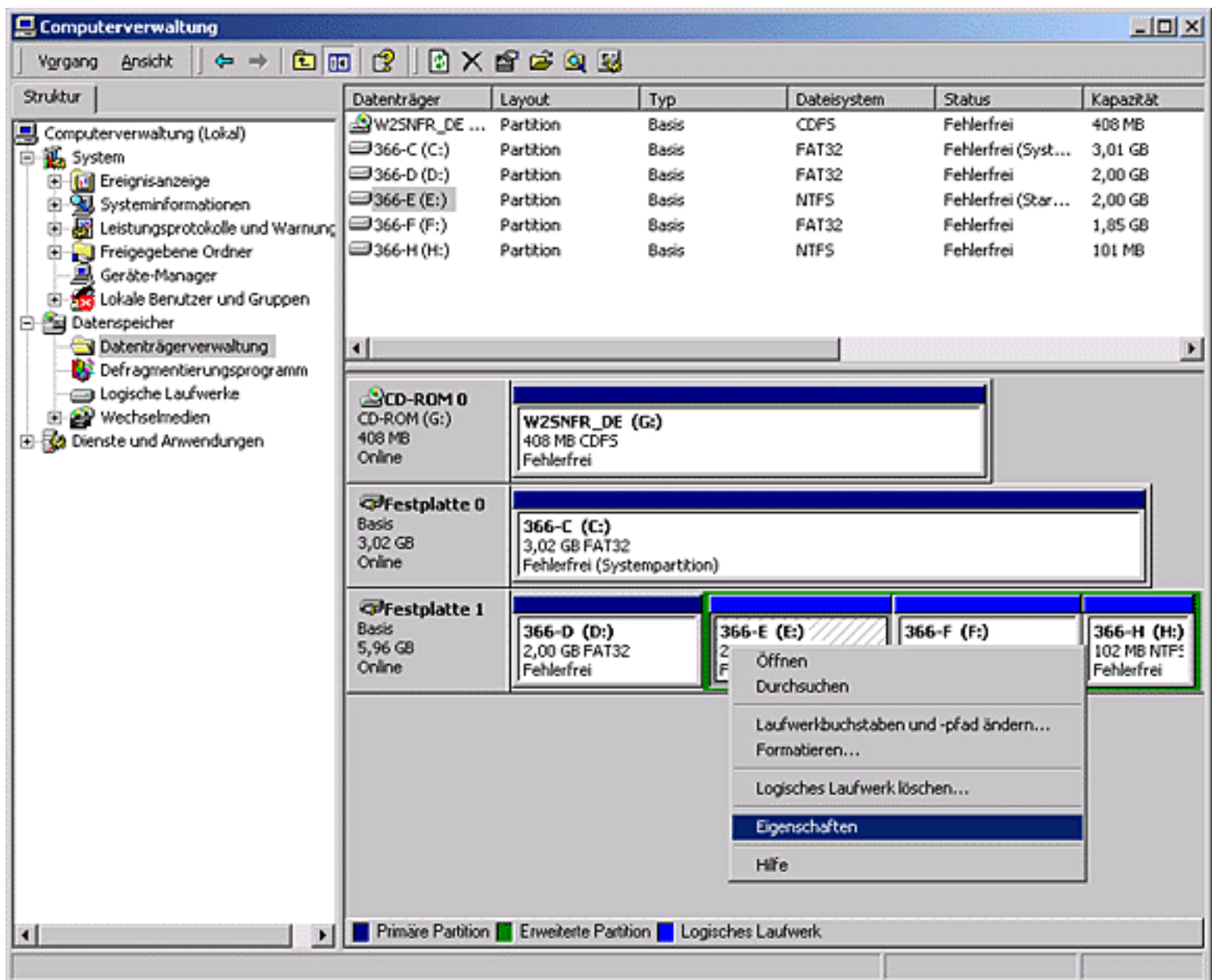


Abbildung 22.19: Das Kontextmenü der Datenträgerverwaltung

Die Menüauswahlen ermöglichen die Ausführung einfacher Aufgaben der Datenträgerverwaltung, beispielsweise den Wechsel des zugeordneten Laufwerksbuchstaben. Um mit Hilfe der Datenträgerverwaltung eine bessere Systemleistung zu erzielen, klicken Sie zunächst im Kontextmenü auf die Menüauswahl **Eigenschaften**. Dadurch wird das Fenster **Eigenschaften von Laufwerkname** angezeigt, wie in Abbildung 22.20 gezeigt.

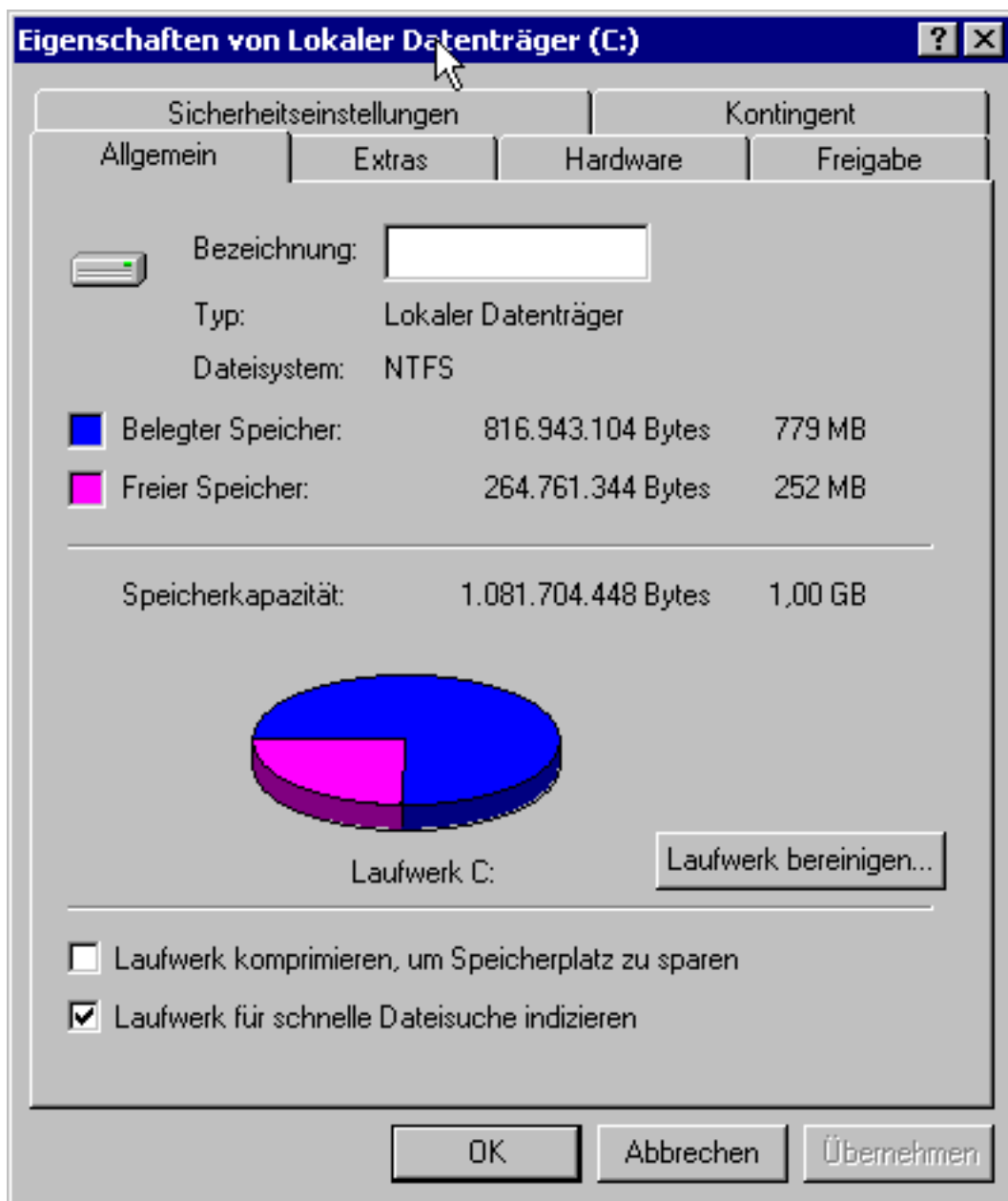


Abbildung 22.20: Das Eigenschaftenfenster für ein Festplattenlaufwerk

Im Eigenschaftenfenster gelangen Sie zunächst zur Registerkarte **Allgemein**, wo Sie einige wichtige Informationen finden. Die beiden Kontrollkästchen unten auf der Registerkarte haben wesentlichen Einfluss auf Ihre Windows-2000-Server-Maschine. Durch die Festplattenkomprimierung steht Ihnen mehr Plattenspeicher zur Verfügung, gleichzeitig wird aber die Leistung Ihres Datenträgers verringert. Durch die Aktivierung des Indexdienstes verbessern Sie die Leistung beim Suchen von Dateien für Ihre Benutzer, aber Sie verringern damit die Gesamtleistung der Maschine, insbesondere, wenn dieser Windows 2000 Server ein Anwendungs- oder Datenbankserver und kein Dateiserver ist. Durch Anklicken werden die Kontrollkästchen markiert, d.h. die jeweilige Funktion wird für den betreffenden Datenträger aktiviert. Mit Hilfe der Schaltfläche **Laufwerk bereinigen** finden Sie nicht genutzte oder unerwünschte Dateien auf dieser Windows-2000-Server-Maschine und Sie verbessern die Gesamtleistung des Systems, indem Sie diese Dateien löschen.

Wechseln Sie zur Registerkarte **Extras**, wie in Abbildung 22.21 gezeigt.



Abbildung 22.21: Auswahl eines Systemwerkzeugs für Ihren Windows-2000-Server

Durch häufige Nutzung dieses Dialogfeldes verbessern Sie die Leistung Ihrer Windows 2000-Installation, weil ein defragmentierter und fehlerfreier Datenträger immer eine bessere Leistung bringt als ein fragmentierter und fehlerhafter Datenträger. Klicken Sie auf die Schaltfläche **Jetzt prüfen**, um das Dienstprogramm ScanDisc von Windows 2000 auszuführen, mit dem Festplattenprobleme erkannt und korrigiert werden. Klicken Sie auf die Schaltfläche **Jetzt defragmentieren**, um die Defragmentierung von Windows 2000 auszuführen, womit eventuell fragmentierte Laufwerke auf einem Windows 2000-Server defragmentiert werden. Nachdem Sie alle für die Festplattenverwaltung erforderlichen Aufgaben ausgeführt haben, wechseln Sie zur Registerkarte **Freigabe**.

Je weniger Datenträger Sie freigeben, desto besser ist die Gesamtleistung Ihres Systems. Offensichtlich bedarf es hier aber einer genauen Abwägung, weil die Computerbenutzer in Ihrem Unternehmen bei ihrer Arbeit auf freigegebene Datenträger angewiesen sind. Die Funktion, die auf diesem Bildschirm die eigentliche Leistung bringt, ist die Schaltfläche **Zwischenspeicher**, mit der der Administrator von Windows-2000-Server die Konfiguration des Cachings für die Benutzer im Unternehmen für den Zugriff

auf Offlinedateien festlegt. Klicken Sie auf die Schaltfläche **Zwischenspeichern**, um den in Abbildung 22.22 gezeigten Bildschirm aufzurufen.

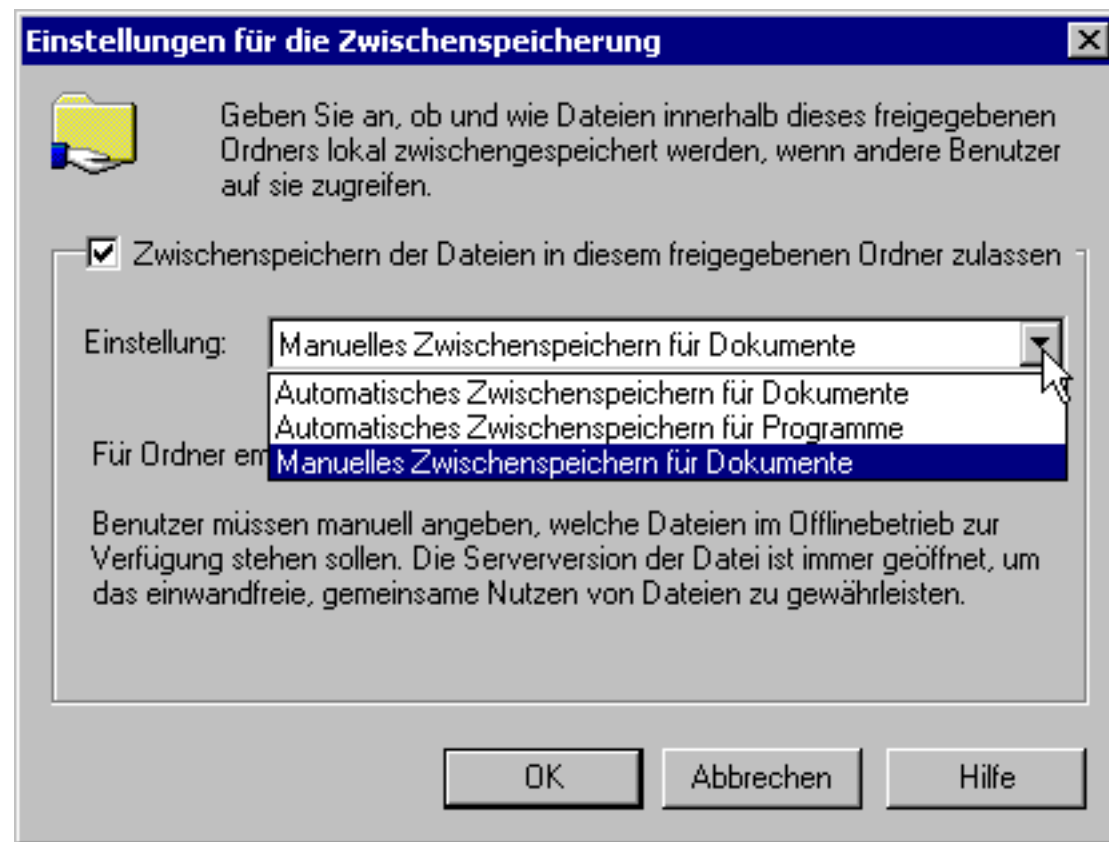


Abbildung 22.22: Bestätigen der Zwischenspeichereinstellungen für Ihren Windows 2000-Server

Im Dialogfeld für die Zwischenspeichereinstellungen müssen Sie entscheiden, ob Sie Dateien und Ordner für diesen lokalen Datenträger in den Cache stellen wollen. Angenommen, Sie wollen das, sollten Sie das obere Kontrollkästchen markieren (**Zwischenspeichern der Dateien in diesem freigegebenen Ordner zulassen**), indem Sie es anklicken. Jetzt wählen Sie eine Standard-Zwischenspeichereinstellung für diesen Datenträger aus. Öffnen Sie das Dropdown-Listefeld **Einstellung**. Die Auswahlmöglichkeiten sind selbsterklärend. Treffen Sie eine Wahl und klicken Sie auf **OK**, um die Einstellungen zu speichern. Damit gelangen Sie zum Hauptbildschirm der Eigenschaften von **Laufwerkname** zurück. Nachdem Sie die Optionen des Ordners **Computerverwaltung/Datenspeicher** betrachtet haben, klicken Sie auf das Schließen-Symbol (X) in der oberen rechten Ecke der Microsoft Management Console, um diese zu schließen.

22.3.2 Optimieren virtueller Speicherseiten

Die Optionen für den Windows-2000-Server VMM (Virtual Memory Manager) werden über das Dialogfeld **Virtueller Arbeitsspeicher** verwaltet. Bevor Sie das tun, sollten Sie einige grundlegende Konzepte verstanden haben. Die Optionen für die Speicherverwaltung unter Windows 2000 sind von der Hardwarekonfiguration Ihres Servers abhängig, aber es gibt einige Methoden, wie Sie die Leistung Ihrer Windows-2000-Server-Maschine maximieren:

- Legen Sie für jede auf Ihrem Windows 2000-System installierte physische Festplatte eine Auslagerungsdatei an. Damit kann Ihr Server die Informationen aus der Auslagerungsdatei von mehreren Positionen gleichzeitig lesen, sodass die Zugriffszeit für die Daten verringert wird. Wenn

Ihr System Informationen in die Auslagerungsdatei schreiben will, kann es auf diese Weise theoretisch das am wenigsten ausgelastete Laufwerk dafür verwenden.

- Setzen Sie die Auslagerungsdatei zunächst auf die maximale Größe, sodass Ihr System keine Zeit darauf verwenden muss, sie irgendwann später zu vergrößern (das bedeutet keine wesentliche Leistungssteigerung, aber man sollte nichts unversucht lassen).
- Legen Sie die Windows-2000-Server-Auslagerungsdatei auf einem anderen Datenträger an, als auf jenem, auf dem auch der Windows 2000-Ordner %systemroot% abgelegt ist (er heißt wahrscheinlich \WinNT oder \Win2000, abhängig von Ihrer Systemkonfiguration). Damit vermeiden Sie Kollisionen bei Datenanforderungen, die daraus resultieren, wenn sich die Auslagerungsdatei und die Systembootpartition auf demselben physischen Laufwerk befinden.

Um die verschiedenen Optionen für den Windows-2000-Server VMM (Virtual Memory Manager) zu ändern, der im Dialogfeld **Virtueller Arbeitsspeicher** verwaltet wird, gehen Sie in die Computerverwaltung. Dazu wählen Sie im Startmenü die Befehlsfolge **Programme/Verwaltung/Computerverwaltung**. Der Hauptbildschirm der Computerverwaltung wird angezeigt.

Dort klicken Sie mit der rechten Maustaste auf die Option **Computerverwaltung (lokal)**, die ganz oben in der Menüstruktur im rechten Feld angezeigt wird. Ein Kontextmenü mit nur einigen wenigen Optionen erscheint: **Verbindung zu anderem Computer herstellen...**, **Alle Tasks**, **Ansicht**, **Liste exportieren**, **Eigenschaften** und **Hilfe**.

Unten im Menü sehen Sie die Auswahl **Eigenschaften**. Klicken Sie darauf, um den in Abbildung 22.23 gezeigten Bildschirm aufzurufen.

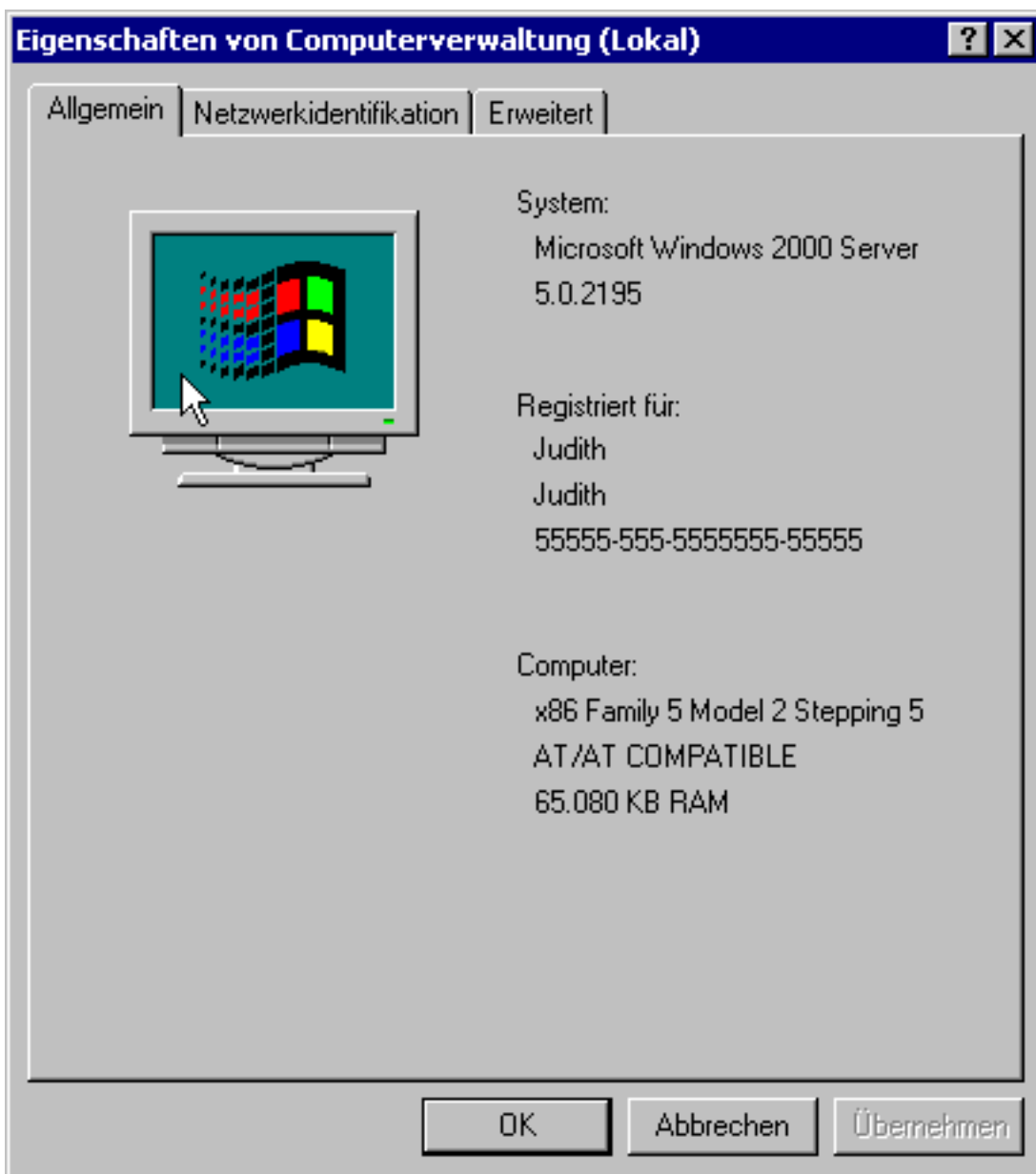


Abbildung 22.23: Ansicht der Basiskonfiguration für einen Windows 2000-Server

Im Eigenschaftfenster für *Computerverwaltung (lokal)* gelangen Sie standardmäßig auf die Registerkarte **Allgemein**. Die wichtigsten Daten finden Sie ganz unten auf diesem Bildschirm: den Gesamtarbeitsspeicher (RAM). Wechseln Sie zur Registerkarte **Erweitert**, die Sie in Abbildung 22.24 sehen.



Abbildung 22.24: Anzeige der erweiterten Eigenschaften für die Verwaltung Ihres Servers

Das Betriebssystem Windows 2000 wurde ähnlich aufgebaut wie die Betriebssysteme Windows NT und Windows 9x: in allen gibt es unzählige undokumentierte Funktionen. Was Sie eben in drei separaten Schritten unternommen haben, um das Eigenschaftensfenster für Computerverwaltung (lokal) anzuzeigen, erzielen Sie auch viel schneller mit einem einzigen Mausklick und einer Tastenkombination. Halten Sie die (Alt)-Taste auf der Tastatur gedrückt und doppelklicken Sie im Windows 2000-Desktop auf das Symbol **Arbeitsplatz**. Damit gelangen Sie direkt zur Registerkarte **Allgemein** im Systemeigenschaftensfenster. Interessant dabei ist, dass die Informationen, auf den beiden Registerkarten für Eigenschaften **Computerverwaltung (lokal)** als auch für Systemeigenschaften gleich sind. Wie Sie später selbst ausprobieren können, funktioniert diese Abkürzung auch in Windows NT und Windows 9x in vielen Bereichen.



In den drei Bereichen auf der Registerkarte **Erweitert** wollen wir uns hier auf den obersten konzentrieren. Im Bereich **Systemleistung** können Sie auf den Windows 2000 VMM (Virtual Memory

Manager) zugreifen, um auf die verschiedenen Verwaltungsaufgaben für Speicher und Auslagerungsdatei zuzugreifen. Dazu klicken Sie auf die Schaltfläche **Systemleistungsoptionen**, womit das Dialogfeld **Leistungsmerkmale** angezeigt wird, wie in Abbildung 22.25 gezeigt.

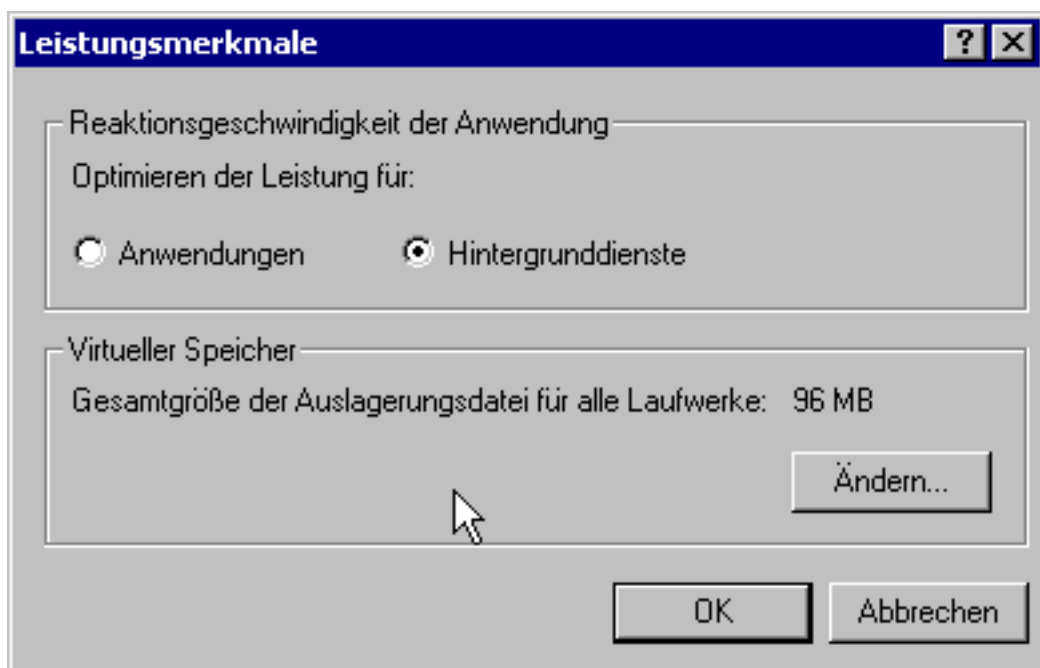


Abbildung 22.25: Änderung der Systemleistungsoptionen für einen Windows 2000-Server

Über das Dialogfeld **Leistungsmerkmale** können Sie Ihren Windows 2000-Server entweder für die darauf ausgeführten Anwendungen oder für seine Hintergrunddienste optimieren. Mit der Auswahl des Optionsfeldes **Anwendungen** teilen Sie Ihrem Windows 2000-Server mit, dass er die meisten CPU-Ressourcen an die im Vordergrund ausgeführten Anwendungen abgeben soll (d.h. an die aktive Anwendung). Das bedeutet, die aktive Anwendung (die im Vordergrund ausgeführte Anwendung) reagiert auf die Eingaben eines oder mehrerer Benutzer. Wählen Sie das Optionsfeld **Hintergrunddienste** aus, teilen Sie Ihrem Windows 2000-Server mit, allen darauf installierten Programmen gleich viel Systemressourcen zuzugestehen, unabhängig davon, ob eine davon gerade im Vordergrund ausgeführt wird. Nachdem Sie Ihre Auswahl in Bezug auf die Leistungsoptimierung getroffen haben, schließen Sie den Bildschirm mit **OK** und kehren zum Eigenschaftenbildschirm für die **Computerverwaltung (lokal)** zurück oder Sie klicken auf die Schaltfläche **Ändern** im Abschnitt **Virtueller Speicher**, um den in Abbildung 22.26 gezeigten Bildschirm aufzurufen.

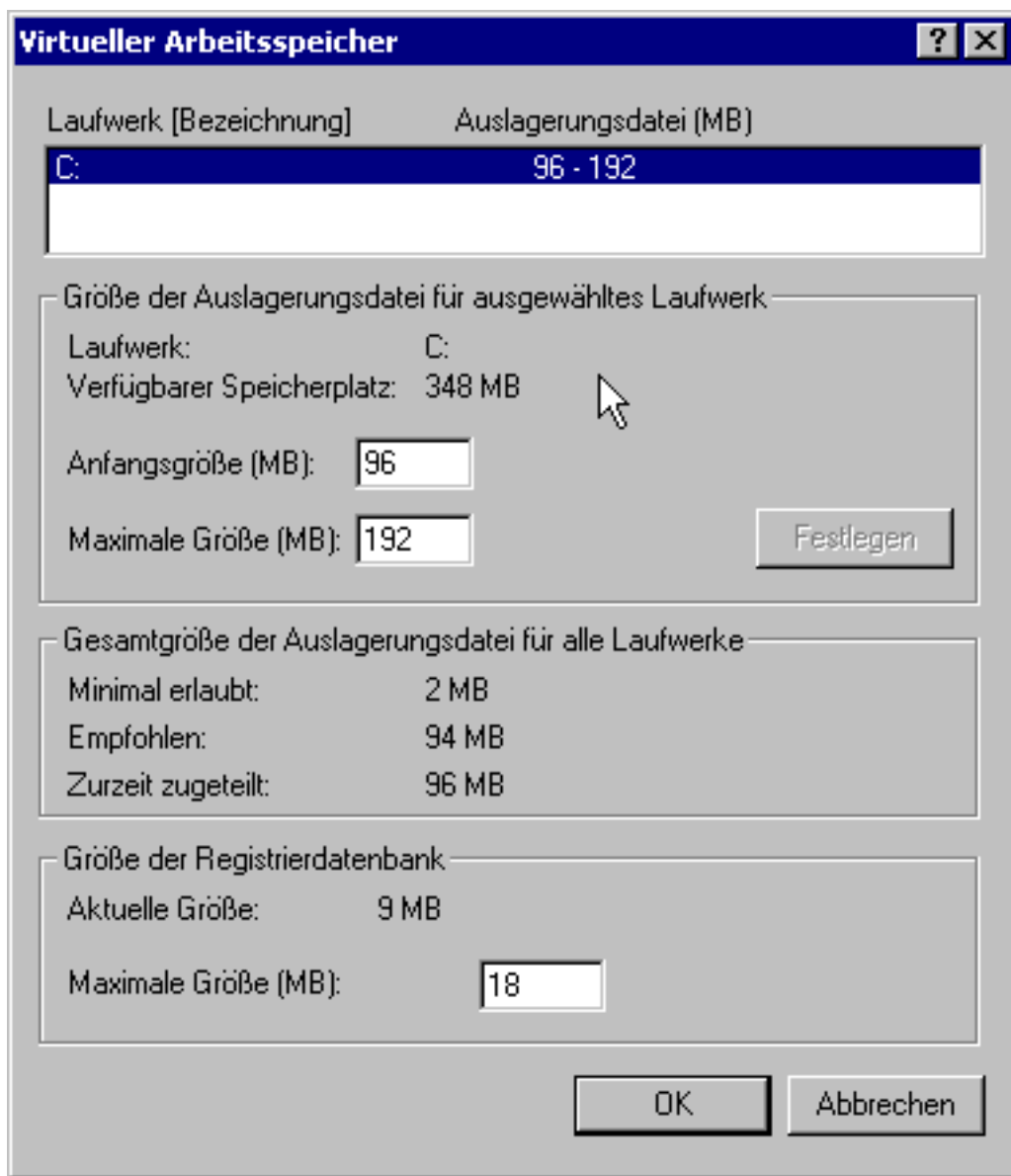


Abbildung 22.26: Anzeigen/Ändern der Konfigurationen für den virtuellen Speicher

Im Dialogfeld **Virtueller Arbeitsspeicher** sehen Sie die Gesamtgröße der vorhandenen Auslagerungsdatei sowie die Größe der Registrierungsdatenbank. Beachten Sie, dass die Windows-2000-Server-Auslagerungsdatei die Speicherseiten aufnimmt, die nicht mehr im RAM Ihres Servers behalten werden. Das bedeutet, dass diese Speicherseiten vom Betriebssystem in bestimmte verborgene Dateien auf der Festplatte »ausgelagert« wurden. Dieser Prozess kann von dem im nächsten Abschnitt des Kapitels beschriebenen Systemmonitor überwacht werden.

Um die Ausgangs- oder die maximale Größe Ihrer Auslagerungsdatei für den Windows 2000-Server zu ändern, klicken Sie auf das Laufwerk, auf dem die Auslagerungsdatei angelegt ist. Dort sehen Sie, dass die Schaltfläche **Festlegen** grau dargestellt ist. Das bedeutet nur, dass noch keine Änderungen angefordert wurden, es also keinen Grund gibt, sie zu »setzen«, d.h. sie in der Registrierung Ihres Windows 2000-Servers zu speichern. Nachdem Sie eine Änderung vorgenommen haben, beispielsweise für die Ausgangsgröße der Auslagerungsdatei, wird die Schaltfläche **Festlegen** nicht mehr grau dargestellt.

In diesem Dialogfeld können Sie auch festlegen, dass Ihre Auslagerungsdatei über mehrere Festplatten

verteilt werden soll, indem Sie einfach weitere Laufwerke anklicken, minimale und maximale Größen für die Auslagerungsdatei angeben und dann auf die Schaltfläche **Festlegen** klicken, um die Einträge zu bestätigen. Während Sie Ihre Einträge vornehmen, sehen Sie im Abschnitt **Gesamtgröße der Auslagerungsdateien für alle Laufwerke**, dass sich die Gesamtgröße der Auslagerungsdatei ändert. Beobachten Sie diesen Abschnitt, um die Größe und Position(en) Ihrer Auslagerungsdatei korrekt zu verwalten.

Auch der letzte Abschnitt **Größe der Registrierdatenbank** in diesem Dialogfeld ist sehr wichtig. Wenn Sie nicht genügend Plattenspeicher für die Registrierungsdateien Ihres Windows 2000-Servers bereitstellen, wird Ihr System irgendwann nicht mehr in der Lage sein, alle Informationen zu speichern, die es für einen fehlerfreien Betrieb benötigt. Wenn die Registrierung nicht entsprechend ihrem Bedarf anwachsen kann, erhalten Sie Fehlermeldungen, sobald Sie versuchen, zusätzliche Programme und Anwendungen auf Ihrem Windows 2000-Server zu installieren.

Nachdem Sie alle Auswahlen im Dialogfeld **Virtueller Arbeitsspeicher** getroffen haben, klicken Sie auf die Schaltfläche **OK**, um Ihre Eingaben zu bestätigen und das Dialogfeld zu verlassen. Sie gelangen zum Dialogfeld **Leistungsmerkmale** zurück. Klicken Sie auf **OK**, um Ihre Eingaben zu bestätigen, womit Sie auch diesen Bildschirm verlassen und zurück in den Eigenschaftenbildschirm für die Computerverwaltung (lokal) gelangen. Hier gibt es noch eine Option, die Sie genauer betrachten sollten: den Bereich **Starten und Wiederherstellen**. Klicken Sie unten im Dialogfeld **Eigenschaften von Computerverwaltung (lokal)** auf die Schaltfläche **Starten und Wiederherstellen**, um den in Abbildung 22.27 gezeigten Bildschirm aufzurufen.

Im Dialogfeld **Autostart und Wiederherstellung** legen Sie die Optionen für die Wiederherstellung des Systems fest. Normalerweise sollten diese Optionen nicht als Operationen zur Leistungssteigerung bezeichnet werden, aber an diesem Bereich muss Microsoft noch arbeiten: die Abtrennung vom Speichern der System-Debugginginformation und der Festlegung von Position/Größe der Auslagerungsdateien für das System.

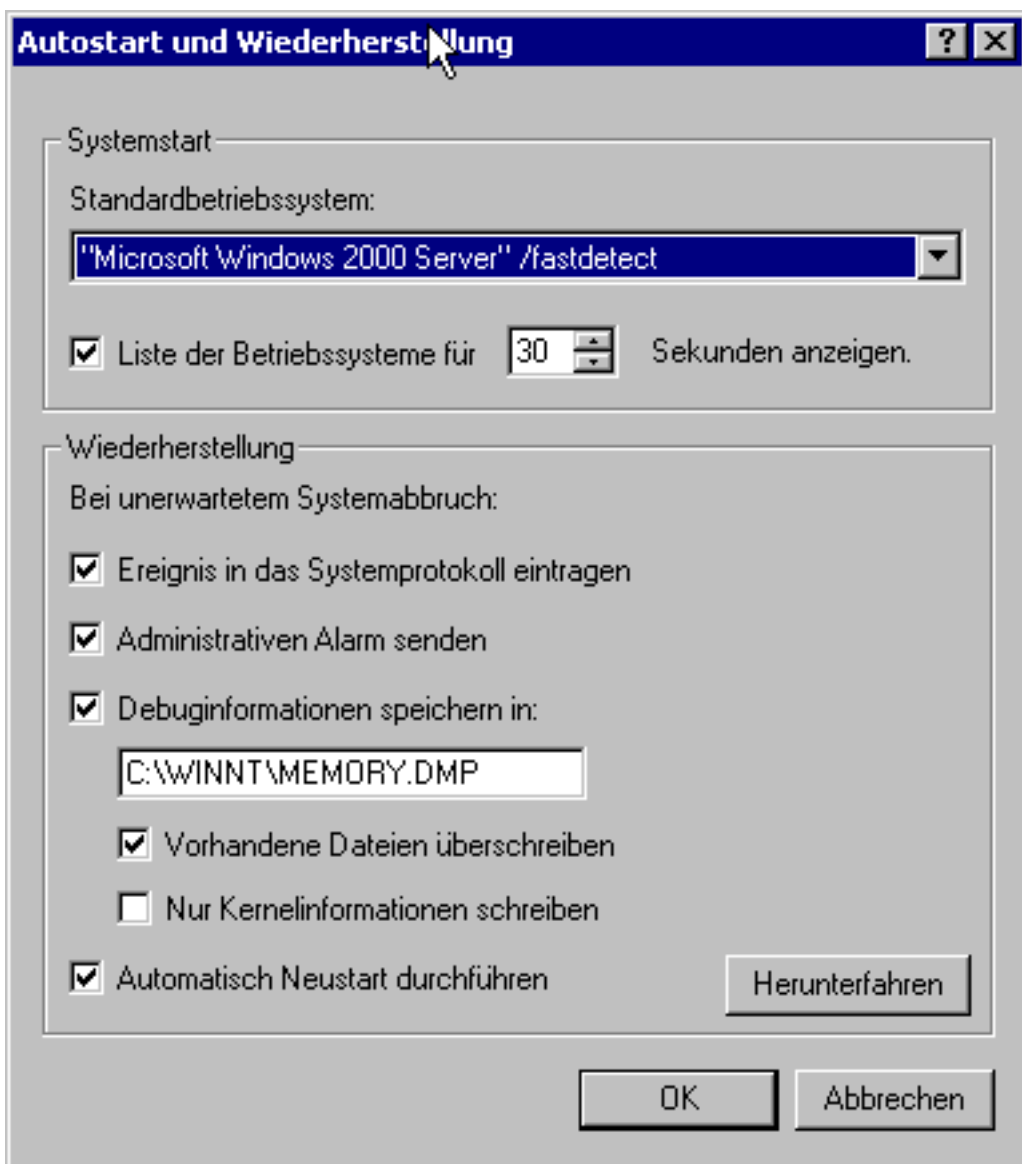


Abbildung 22.27: Anzeige Ihrer Optionen für Starten und Wiederherstellung

Mit anderen Worten, wenn Sie die Auslagerungsdatei für Ihr Windows 2000-System über mehrere Festplattenlaufwerke verteilen wollen, verzichten Sie auf die Möglichkeit, Debugginginformation für das System aufzuzeichnen - für den unwahrscheinlichen Fall eines Systemfehlers, wie etwa beim Auftreten der absoluten Lieblinge aller Systemadministratoren für Windows NT oder Windows 2000: die blauen Bildschirme (BSOD = Blue Screen of Death). Hier treten zweierlei Probleme auf: Die Auslagerungsdatei muss sich auf derselben Festplattenpartition befinden, auf der auch der Ordner %systemroot% abgelegt ist, und die Auslagerungsdatei muss mindestens um ein Megabyte größer sein, als insgesamt physisches RAM auf Ihrem Computer vorhanden ist. Das bedeutet für die unerfahrenen Systemadministratoren, dass Microsoft diese zwingt, zwischen einer verbesserten Leistung ihres Windows-2000-Server-Systems und der Möglichkeit, korrekte Wiederherstellungsinformationen bei Systemausfällen zu erhalten, zu wählen. Gutes Angebot! Weil es für beide Seiten gleich gute Argumente gibt, überlasse ich die Entscheidung Ihnen. Nur noch ein Wort: Wenn Sie eine sinnvolle Strategie für Sicherungen/Wiederherstellungen in Ihrem Unternehmen einsetzen und Sie vorausschauend genug waren, sich einige der guten Werkzeuge von Winternals Software Inc. gekauft zu haben (beispielsweise den Administrator's Pak, der das Werkzeug Blue-Save enthält), sollten Sie hier auf die Systemleistung setzen. Nur ein Gedanke ...

Um das Dialogfeld **Autostart und Wiederherstellung** zu verlassen, klicken Sie auf die Schaltfläche **OK**. Sie gelangen zurück zum Eigenschaften-Dialogfeld für die Computerverwaltung (lokal). Falls Sie Änderungen an der Konfiguration der Auslagerungsdatei von Windows 2000 oder für den Autostart und die Wiederherstellung vorgenommen haben, werden Sie in einem kleinen Meldungsfeld aufgefordert, Ihr Windows-2000-Server-System neu zu starten.

Nachdem Sie die Informationen in diesem Meldungsfeld gelesen haben, klicken Sie auf **OK** und schließen es. Ein weiteres Meldungsfeld wird angezeigt. Hier werden Sie gefragt, ob das System sofort neu gestartet werden soll.

Klicken Sie auf die Schaltfläche **Ja**, um den Neustart automatisch auszuführen, oder auf **Nein**, wenn Sie den Systemstart selbst vornehmen wollen. Nachdem das System neu gestartet wurde, treten alle Ihre Änderungen in Kraft.

22.4 Der Systemmonitor

Das Dienstprogramm *Leistung* in Windows-2000-Server ermöglicht Ihnen, die Leistung der Systemhardware Ihres Servers sowie des Betriebssystems und der darauf installierten Anwendungssoftware zu überwachen. Dieses Werkzeug ist sehr praktisch, aber Sie sollten es nicht überstrapazieren, weil sich dies negativ auf die Serverleistung auswirken könnte. Das bedeutet, Sie sollten sich genau überlegen, wie Sie Ihr System überwachen, insbesondere wenn in Ihrer Windows 2000 Server-Umgebung Webseiten oder eCommerce-Anwendungen angeboten werden.

Wenn Sie noch nie einen Server oder ein Netzwerk überwacht haben, könnten Sie die Vorgehensweise einhalten, die Microsoft in einer Checkliste der Hilfedatei von Windows-2000-Server empfiehlt:

- Lesen Sie die Informationen über die wichtigsten Konzepte bei der Systemleistungsüberwachung. Sie müssen also Ihre Hausaufgaben machen, bevor Sie die verschiedenen Netzwerk- und Servermonitore in der Produktionsserverumgebung Ihres Unternehmens einsetzen können.
- Stellen Sie sicher, dass Sie für den zu überwachenden Computer die erforderlichen Berechtigungen besitzen. Für die Überwachung in Windows-2000-Server brauchen Sie Administratorrechte für die verschiedenen Komponenten Ihres Windows 2000-Netzwerks.
- Installieren Sie den Netzwerkmonitor-Treiber, um die Leistungsindikatoren für das Netzwerk zu überwachen. Es gibt einen speziellen Windows-2000-Server Netzwerkmonitor-Treiber, der dafür installiert werden muss. Nehmen Sie den Installationsprozess mit Hilfe des Symbols **Netzwerk- und DFÜ-Verbindungen** in der Systemsteuerung von Windows-2000-Server vor. Installieren Sie das Netzwerkmonitor-Treiber-Protokoll, um die wichtigsten Überwachungen im Netzwerk vornehmen zu können.
- Richten Sie eine Überwachungskonfiguration ein. In diesem Schritt stellen Sie sicher, dass Sie einen separaten Windows 2000-Mitgliedsserver-Computer haben, von dem aus die Überwachung gesteuert wird. Sie sollten beachten, dass zu viel Überwachung negative Auswirkungen auf die Leistung haben kann, die andernfalls zu Lasten Ihrer Produktionsserverumgebung geht.
- Werten Sie die Überwachungsergebnisse aus und schaffen Sie Vergleichswerte. Nachdem Sie festgelegt haben, was wie überwacht werden soll, halten Sie Ausgangswerte fest, mit denen Sie zukünftige Ergebnisse vergleichen. Anhand der Unterschiede erkennen Sie, ob Ihre Systemleistung besser oder schlechter ist als zuvor. Falls Sie keine Vergleichswerte schaffen, vergeuden Sie nur

Ihre Zeit bei der Überwachung Ihrer Windows-2000-Server-Umgebung.

- Untersuchen Sie Abweichungen der Leistungsdaten und optimieren oder aktualisieren Sie die Komponenten nach Bedarf. Wenn Sie Leistungsunterschiede feststellen, insbesondere negative, sollten Sie wieder zu Ihrer allgemeinen Windows-2000-Server-Einstellung zurückkehren und die Hardware- und Softwareanwendungen entsprechend einrichten. Andernfalls vergeuden Sie nur Ihre Zeit bei der Überwachung Ihrer Windows-2000-Server-Umgebung.
- Archivieren Sie die Überwachungsdaten und nutzen Sie die Archive, um Trends zu beobachten. Die Trendanalyse für die Leistung Ihrer Windows-2000-Server-Umgebung ist äußerst wichtig. Sie wissen nie, wann in der Zukunft ein Leistungsproblem auftritt. Wenn Sie allerdings Daten aus der Vergangenheit besitzen, können Sie möglicherweise damit zukünftige Probleme lösen.

Nachdem Sie auf die Überwachung Ihres Systems vorbereitet sind, sollten Sie sicherstellen, dass alle Administratoren für Ihren Windows-2000-Server ausreichend geschult und vorbereitet sind, um die Ergebnisse des Überwachungsprozesses auswerten zu können. Mit anderen Worten, Sie brauchen unternehmensübergreifende Richtlinien und Prozeduren, um zu erzwingen, dass die von der Überwachung vorgeschlagenen Änderungen in Ihrer Windows-2000-Server-Umgebung korrekt implementiert werden. Darüber hinaus muss zwischen den Systemadministratoren Übereinstimmung herrschen. Fehlende Konsistenz würde Ihrer Windows-Server-Umgebung mehr schaden, als wenn Sie überhaupt keine Überwachung ausführen. Und noch etwas: Bei der Implementierung der durch die Überwachung vorgeschlagenen Änderungen sollten Sie schrittweise vorgehen, um Ihre Probleme nicht zu vertiefen, indem Sie eines lösen und ein paar neue damit schaffen.

Jetzt wollen wir mit der Überwachung beginnen. Dazu brauchen Sie das Dienstprogramm **Leistung** von Windows-2000-Server. Rufen Sie im Startmenü die Befehlsfolge **Programme/Verwaltung/Systemmonitor** auf. Sie sehen den in Abbildung 22.28 gezeigten Bildschirm.

Der Hauptbildschirm von **Leistung** ist in zwei Bereiche aufgeteilt. Der linke enthält die Menüstruktur mit dem eigentlichen Systemmonitor sowie darunter die Ordner mit den Leistungsprotokollen und den Warnungen. Im rechten Bereich sehen Sie die Anzeige des Systemmonitors (sie ist Ihnen vielleicht schon vertraut, wenn Sie bereits mit dem PerfMon-Werkzeug von Windows NT 4.0 gearbeitet haben). Oben in der Anzeige sehen Sie 16 Symbolschaltflächen, mit denen die Operationen des Monitors gesteuert werden. Es handelt sich von links nach rechts um:

- Neuer Leistungsindikatorensatz
- Anzeige löschen
- Aktuellen Vorgang anzeigen
- Protokolldaten anzeigen
- Diagramm anzeigen
- Histogramm anzeigen
- Bericht anzeigen
- Hinzufügen
- Löschen
- Markierung
- Eigenschaften kopieren

- Leistungsindikatorenliste einfügen
- Eigenschaften
- Anzeige fixieren
- Aktualisierungsdaten
- Hilfe

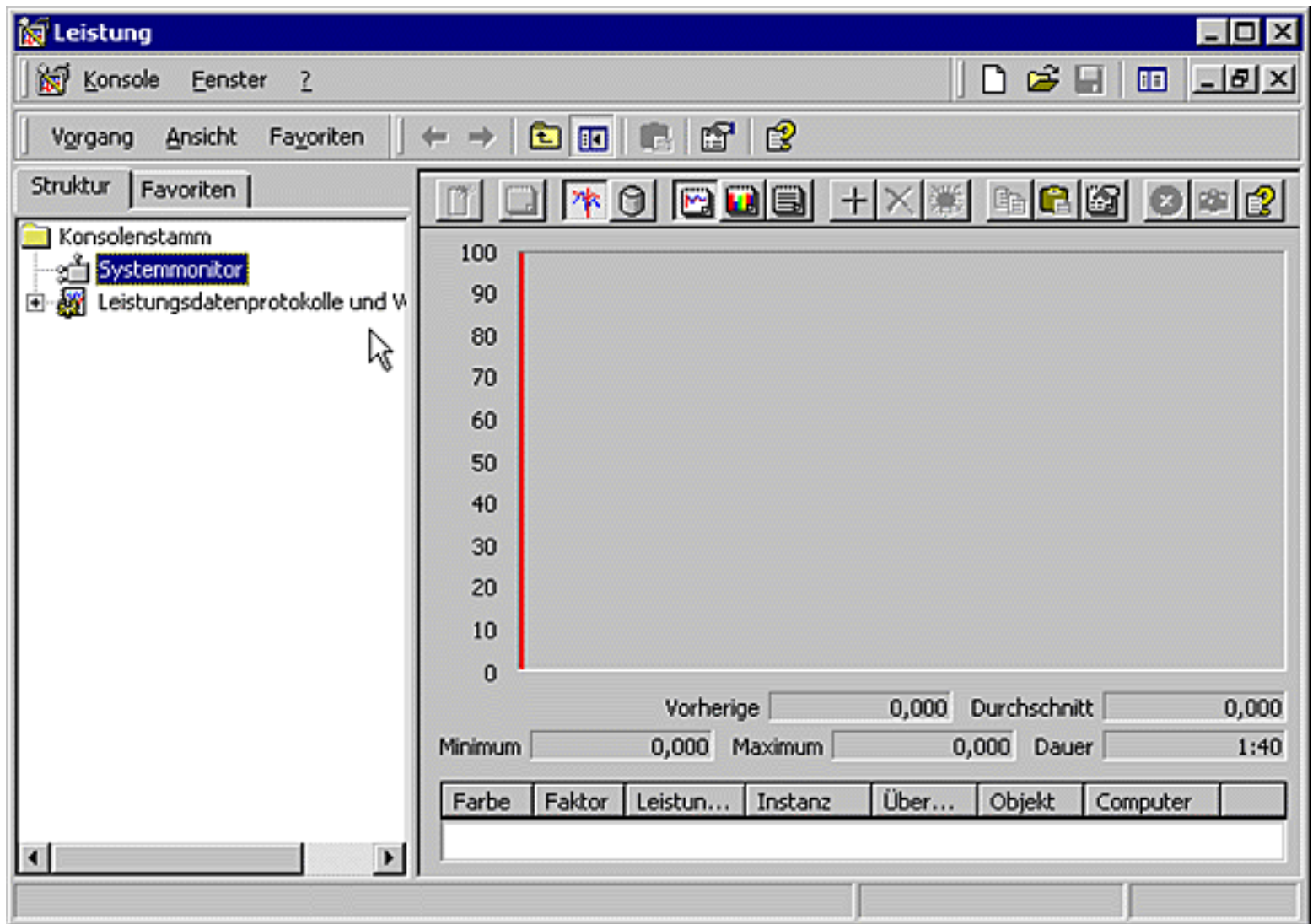


Abbildung 22.28: Der Hauptbildschirm für die Leistungsüberwachung in der Microsoft Management Console

Größtenteils sind diese Schaltflächen selbsterklärend. Wir werden sie jedoch in den nächsten Abschnitten noch genauer erklären. Zunächst aber wollen wir Ihnen einen Überblick über die verwendeten Objekte und Leistungsindikatoren geben. Anschließend werden wir der Anzeige einige zusätzliche Leistungsindikatoren hinzufügen und dann zeigen, wie Diagramme, Berichte, Protokolle usw. angelegt und interpretiert werden.

22.4.1 Objekte und Objektleistungsindikatoren

Sie brauchen mindestens einen Leistungsindikator, um eine Überwachung im Systemmonitor ausführen zu können. Dazu klicken Sie auf die Schaltfläche **Hinzufügen** (das ist die Schaltfläche mit dem kleinen Plussymbol). Das Dialogfeld **Leistungsindikatoren hinzufügen** wird aufgerufen.

Das Werkzeug **Leistung** beinhaltet eine sehr praktische Funktion, weil Sie damit nämlich entweder Ihren lokalen Server (d.h. auf dem das Werkzeug **Leistung** ausgeführt wird), aber auch einen anderen Windows 2000-Server irgendwo im Netzwerk Ihres Unternehmens überwachen können. Klicken Sie auf das entsprechende Optionsfeld, um das lokale oder ein Remote-System zu überwachen. Für die Überwachung eines Remote-Systems geben Sie den UNC-Pfad ein. Dem Dropdown-Listenfeld werden automatisch alle Computer hinzugefügt, zu denen Sie in der Vergangenheit eine Verbindung eingerichtet haben, sodass Sie den UNC-Pfad nicht jedes Mal neu eingeben müssen.

Unterhalb der Serverauswahl finden Sie das Dropdown-Listenfeld **Datenobjekt**. Ein *Datenobjekt* beinhaltet eine Kombination aus Leistungsindikatoren, die den Systemressourcen und Diensten zugeordnet sind, die zur Überwachung bereitstehen. Beispielsweise enthält das Datenobjekt **Speicher** diverse Leistungsindikatoren zur Überwachung, etwa **Verfügbare Bytes**, **Seitenfehler/s**, **Seiten/s** usw. Es gibt Dutzende von Leistungsindikatoren innerhalb dieser 38 Leistungsobjekte im Dropdown-Listenfeld, unter anderem:

- *ACS/RSVP-Dienst*. Zur Überwachung von QoS-Zugangssteuerungsaktivitäten.
- *Active Server Pages*. Zur Überwachung aller Aktivitäten zu IIS-basierten ASP-Seiten.
- *Cache*. Dateisystem-RAM-Cache-Aktivitäten.
- *Distributed Transaction Coordinator*. Transaktionsüberwachung.
- *HTTP-Indexdienst*. Überwachung des Indexdienstes.
- *IAS-Kontoführungsclients*. Überwachung eines IAS-Konten-Clients.
- *IAS-Kontoführungsserver*. Überwachung eines IAS-Konten-Servers.
- *IAS-Authentifizierungsclients*. Überwachung eines IAS-Authentifizierungs-Clients.
- *IAS-Authentifizierungsserver*. Überwachung eines IAS-Authentifizierungs-Servers.
- *ICMP*. Zur Überwachung von TCP/IP.
- *Indexdienst*. Überwachung des Indexdienstes.
- *Indexdienstfilter*. Überwachung des Indexdienstes.
- *Internet Informationsdienste Global*. Überwachung des IIS-Servers.
- *IP*. Überwachung von TCP/IP.
- *Auftragsobjekt*. Zur Überwachung bestimmter Aspekte eines Auftragsobjekts.
- *Auftragsobjektdetails*. Zur Überwachung bestimmter Aspekte eines Auftragsobjekts zu einem bestimmten Zeitpunkt (beispielsweise nur aktuelle Aktivitäten).
- *Speicher*. RAM-Überwachung.
- *NBT-Verbindung*. Zur Überwachung von TCP/IP.
- *Auslagerungsdatei*. Überwachung der Auslagerungsdatei.
- *Druckerwarteschlange*. Zur Überwachung verfügbarer Druckerwarteschlangen.

- *Prozess*. Zur Überwachung eines Anwendungsprozesses.
- *Prozessor*. Zur Überwachung der verfügbaren Prozessoren (CPUs).
- *RAS-Port*. Zur Überwachung verfügbarer RAS-Kommunikationsports.
- *RAS insgesamt*. Zur Überwachung der Gesamtaktivität der RAS-Ports, beispielsweise alle empfangenen Bytes, alle pro Sekunde übertragenen Bytes usw.
- *Redirectordienst*. Zur Überwachung des Netzwerk-Redirectors.
- *Server*. Zur Überwachung spezifischer Serveraktivitäten.
- *Serverwarteschlangen*. Zur Überwachung verschiedener Aspekte der Arbeitswarteschlangen in einem bestimmten Server.
- *System*. Zur Überwachung systemübergreifender Objekte, beispielsweise aktive Threads, Systemlaufzeit usw.
- *TCP*. Zur Überwachung von TCP/IP.
- *Telefonie*. Zur Überwachung von Telefonieaktivitäten des Windows-2000-Servers.
- *Thread*. Zur Überwachung der Aktivitäten eines oder mehrerer spezifischer Threads auf einem Server.
- *UDP*. Zur Überwachung von TCP/IP.

Die meisten dieser Datenobjekte sind selbst erklärend. Für die anderen finden Sie eine Hilfestellung in der Online-Hilfe von Microsoft für die Systemleistung. Sie sollten unbedingt die Hilfedateien lesen, falls Sie noch keine Erfahrung mit der Überwachung besitzen. Größtenteils sind die Hilfedateien von Windows-2000-Server sehr viel ausführlicher als unter Windows NT. Darüber hinaus brauchen Sie für die Systemüberwachung ein fundiertes Hintergrundwissen in Hinblick auf Systementwicklung und Netzwerk-Engineering. Außerdem sollten Sie über ausreichende logistische Fähigkeiten verfügen und ein Talent für die Fehlersuche mitbringen. Sie sollten also immer versuchen, Ihre Informationen über die Leistungsüberwachung aus allen verfügbaren Quellen zu erweitern.

Nachdem Sie das zu überwachende Datenobjekt bestimmt haben, wählen Sie einen oder mehrere der Leistungsindikatoren in der Liste unterhalb des Dropdown-Listenfelds **Datenobjekt** aus (diese Liste befindet sich im Feld unterhalb des Optionsfelds **Leistungsindikatoren wählen**). Wenn Sie das Optionsfeld **Alle Leistungsindikatoren** anklicken, werden Ihrem Diagramm alle Leistungsindikatoren für dieses Leistungsobjekt hinzugefügt. Das sollten Sie jedoch keinesfalls tun, weil Sie damit sehr schnell einen Informationsüberfluss erzeugen und außerdem Ihren Server mit der Überwachung überlasten.

Für mehrere der Leistungsindikatoren der Überwachung gibt es noch eine dritte Option: *Instanz*. Für den Leistungsindikator **Prozessorzeit (%)** gibt es mehrere Instanzen. Falls Sie eine Instanz auswählen wollen, klicken Sie beispielsweise auf das obere Optionsfeld (**Alle Instanzen**), um alle verfügbaren Instanzen für diesen Leistungsindikator auszuwählen. Die meisten Leistungsindikatoren haben nur ein paar wenige Instanzen. Wenn Sie jedoch sorgfältig sein wollen, klicken Sie auf das Optionsfeld **Instanzen wählen**. Damit können Sie eine oder mehrere Instanzen aus der nachfolgenden Liste auswählen. Um mehrere Leistungsindikatoren oder Instanzen auszuwählen, halten Sie bei der Auswahl die (Strg)-Taste gedrückt. Damit treffen Sie eine Mehrfachauswahl für alle Leistungsindikatoren und Instanzen.

Falls Sie nicht genau wissen, wofür die einzelnen Leistungsindikatoren verwendet werden, klicken Sie

auf den betreffenden Leistungsindikator und dann auf die Schaltfläche **Erklärung**. Unterhalb des Dialogfeldes **Leistungsindikatoren hinzufügen** wird ein Textfeld mit einer Erklärung angezeigt, wie in Abbildung 22.29 gezeigt.

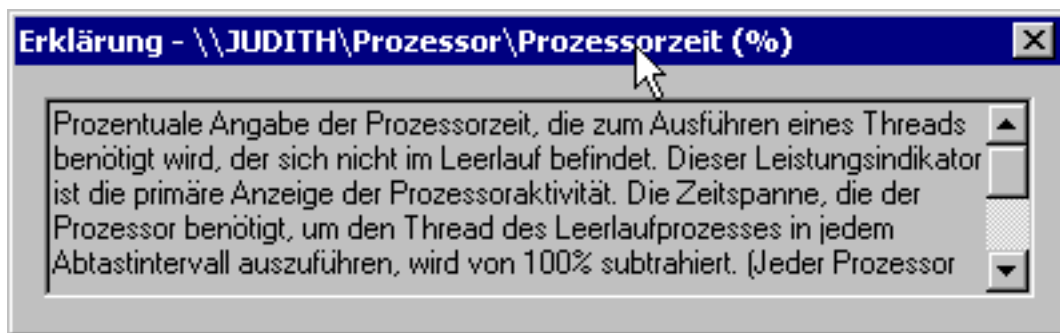


Abbildung 22.29: Anzeige einer Erklärung für einen bestimmten Leistungsindikator in der Leistungsüberwachung

Die Erklärung für die einzelnen Leistungsindikatoren ist größtenteils ausreichend. Es gibt jedoch Situationen, in denen die Erklärung verwirrend ist. In diesen Fällen sollten Sie andere Quellen nutzen, beispielsweise die Dokumentation der Hardware oder Software in Ihrem System. Falls Sie keine solche Dokumentation besitzen, sollten Sie vielleicht einen anderen Leistungsindikator verwenden oder sich an den technischen Support von Microsoft (der kostenpflichtig ist) wenden.

Ein weiterer Aspekt, den Sie beachten sollten, ist die Nutzung von Leistungsindikatoren und Instanzen für sehr spezifische Zwecke. In dem in Abbildung 22.30 gezeigten Beispiel sollten Sie sicherstellen, dass Sie die korrekte Instanz für die zu überwachende Web-Site auswählen.

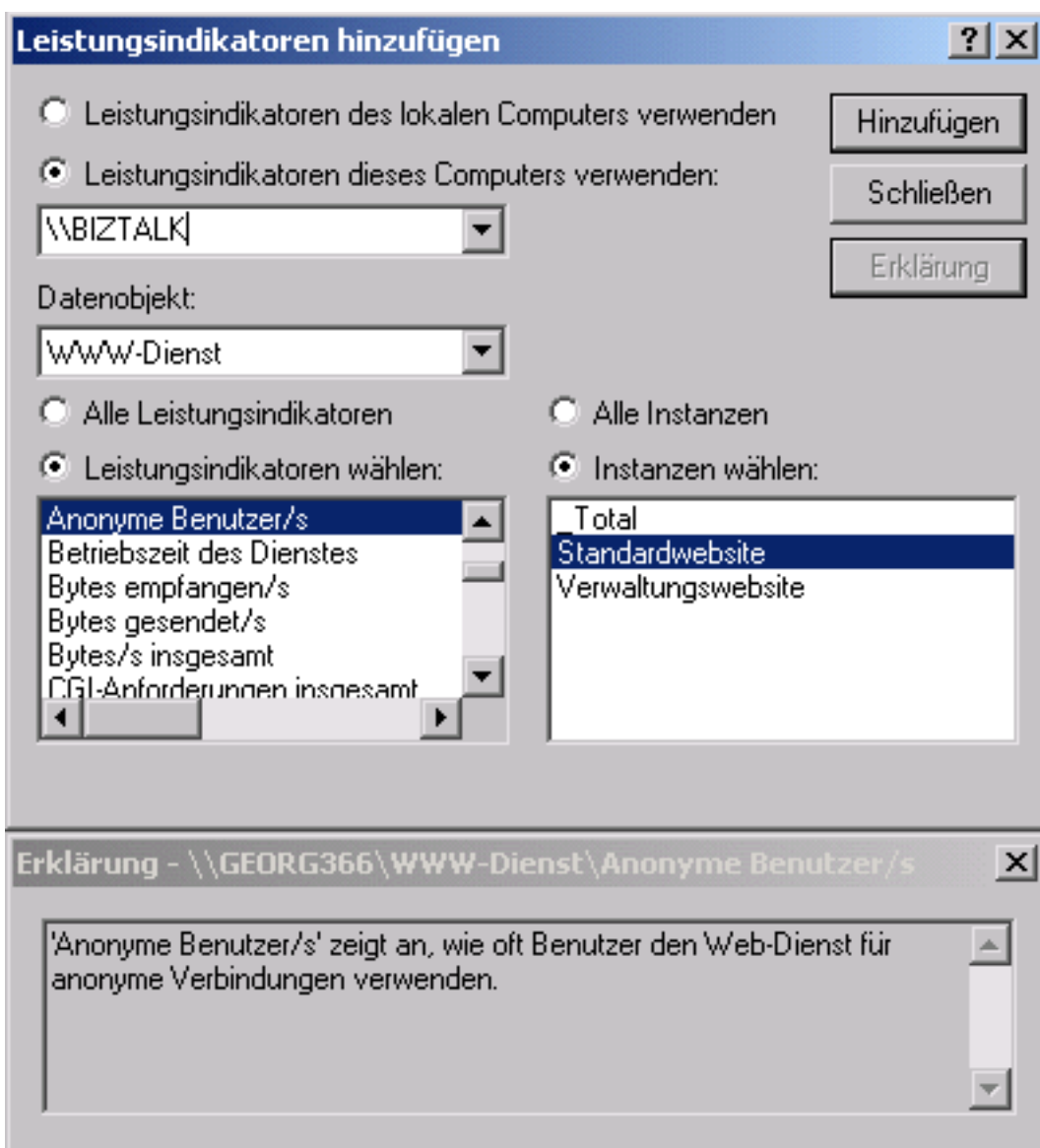


Abbildung 22.30: Auswahl einer speziellen Instanz eines Leistungsindikators in der Leistungsüberwachung

Sehr wahrscheinlich wollen Sie niemals die gesamte Web-Umgebung des IIS überwachen, sondern konzentrieren sich vielmehr auf eine einzige Web-Site auf dem betreffenden Windows 2000 Web-Server. Nachdem Sie den geeigneten Leistungsindikator ausgewählt haben, klicken Sie auf die Schaltfläche **Hinzufügen**, um dem Überwachungsbereich Leistungsindikatoren und Instanzen hinzuzufügen. Nachdem Sie fertig sind, verlassen Sie diesen Bildschirm durch Anklicken der Schaltfläche **Schliessen**.

Damit gelangen Sie zurück zum Bildschirm **Leistung**, sehen aber jetzt alle Leistungsindikatoren und Instanzen, die Sie zuvor hinzugefügt haben, wie in Abbildung 22.31 gezeigt.

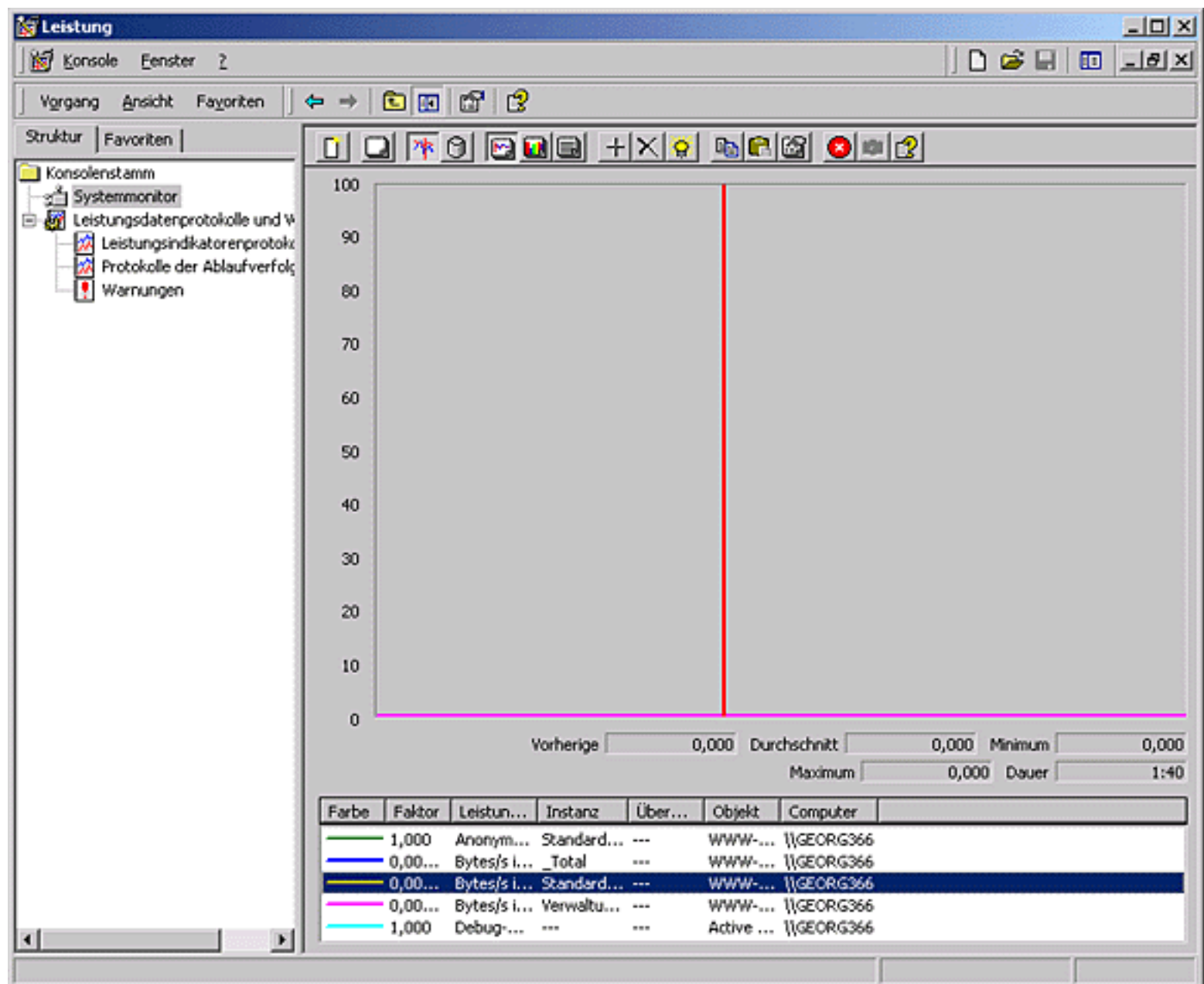


Abbildung 22.31: Ansicht der aktiven Leistungsindikatoren für die Systemüberwachung

22.4.2 Ein Diagramm anlegen

Im letzten Abschnitt haben Sie gelernt, wie man ein Diagramm zur Systemüberwachung anlegt. Darauf wollen wir jetzt aufbauen. Betrachten Sie das in Abbildung 22.32 gezeigte Diagramm.

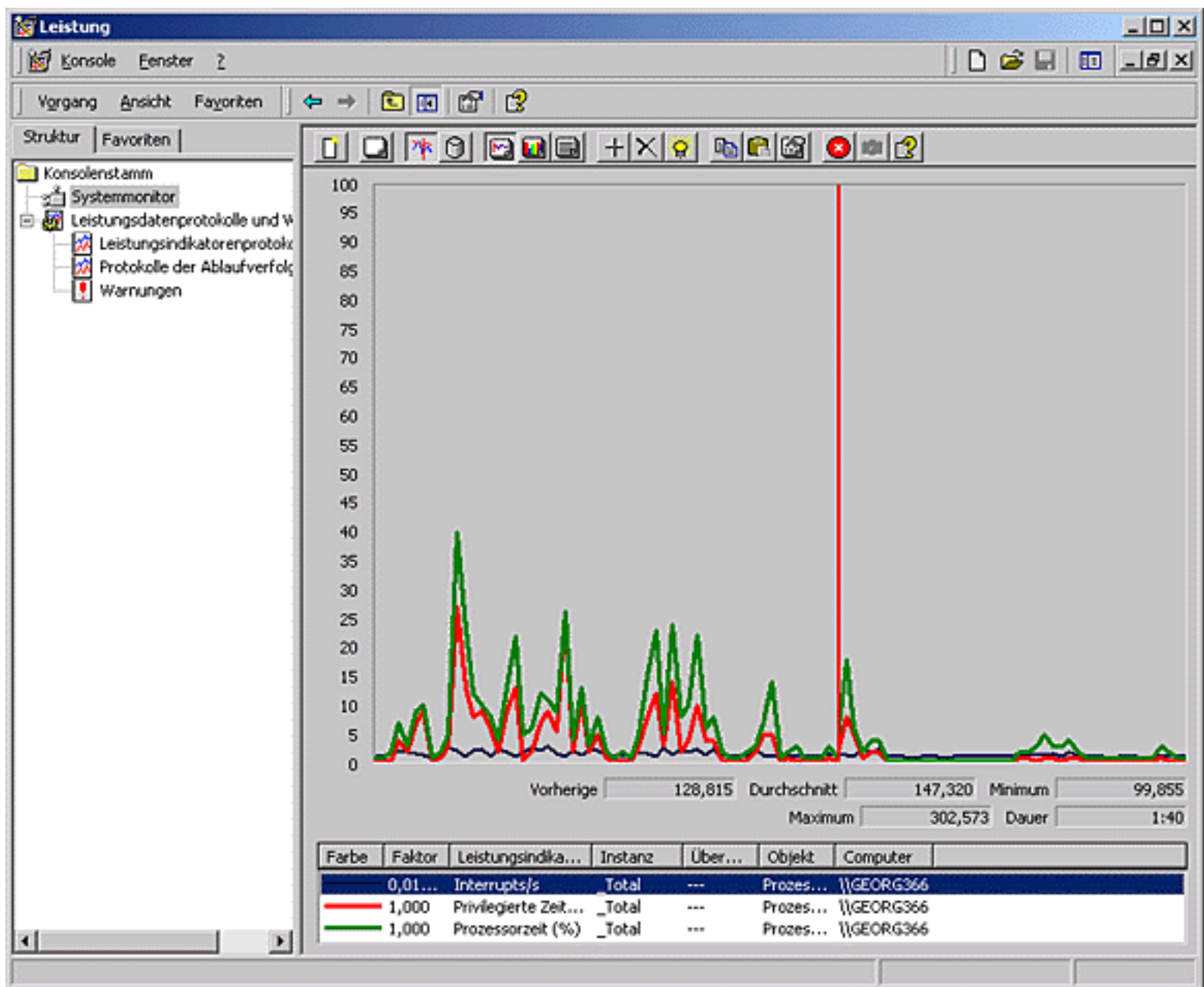


Abbildung 22.32: Interpretation der Daten für einen in der Leistungsüberwachung betrachteten Leistungsindikator

Dieses Diagramm enthält nur ein paar wenige Leistungsindikatoren (*Prozessorzeit (%)*, *Privilegierte Zeit (%)* und *Interrupts/s*) aus einem einzigen Datenobjekt (*Prozessor*) und gleicher Instanzen (*_Total*). Unten im Bildschirm finden Sie eine Auflistung all dieser Informationen. Wenn Sie mehrere Leistungsindikatoren für mehrere Objekte gleichzeitig ausführen, können Sie die angezeigte Information sortieren. Dazu klicken Sie auf die jeweilige Überschrift. Durch Anklicken von **Instanz** werden alle Instanzen in alphabetischer Reihenfolge sortiert. Dasselbe können Sie mit der Überschrift **Objekt** tun; jetzt werden alle Ihre Objekte gruppiert angezeigt. Um die Spalten für die einzelnen Leistungsindikatoren zu verbreitern, verschieben Sie die Linie zwischen den Spaltenüberschriften, so wie beim Verbreitern der Spalten in einer Tabellenkalkulation von Microsoft Excel.



Abbildung 22.33: Einrichtung der allgemeinen Eigenschaften für die Systemüberwachung

Im Eigenschaftenfenster der Systemüberwachung gelangen Sie direkt zur Registerkarte *Allgemein* (das ist der Standard). In diesem Bildschirm stellen Sie den Standardanzeigetyp ein (Grafik, Histogramm oder Bericht), die Anzeigeelemente, die Ebene für die Darstellung der Daten im Bericht und Histogramm sowie das Standardintervall und die Aktualisierungsfrequenz dieses Werkzeugs. Nachdem Sie alle Auswahlen und/oder Änderungen vorgenommen haben, wechseln Sie zur Registerkarte **Quelle**, um den in Abbildung 22.34 gezeigten Bildschirm anzuzeigen.

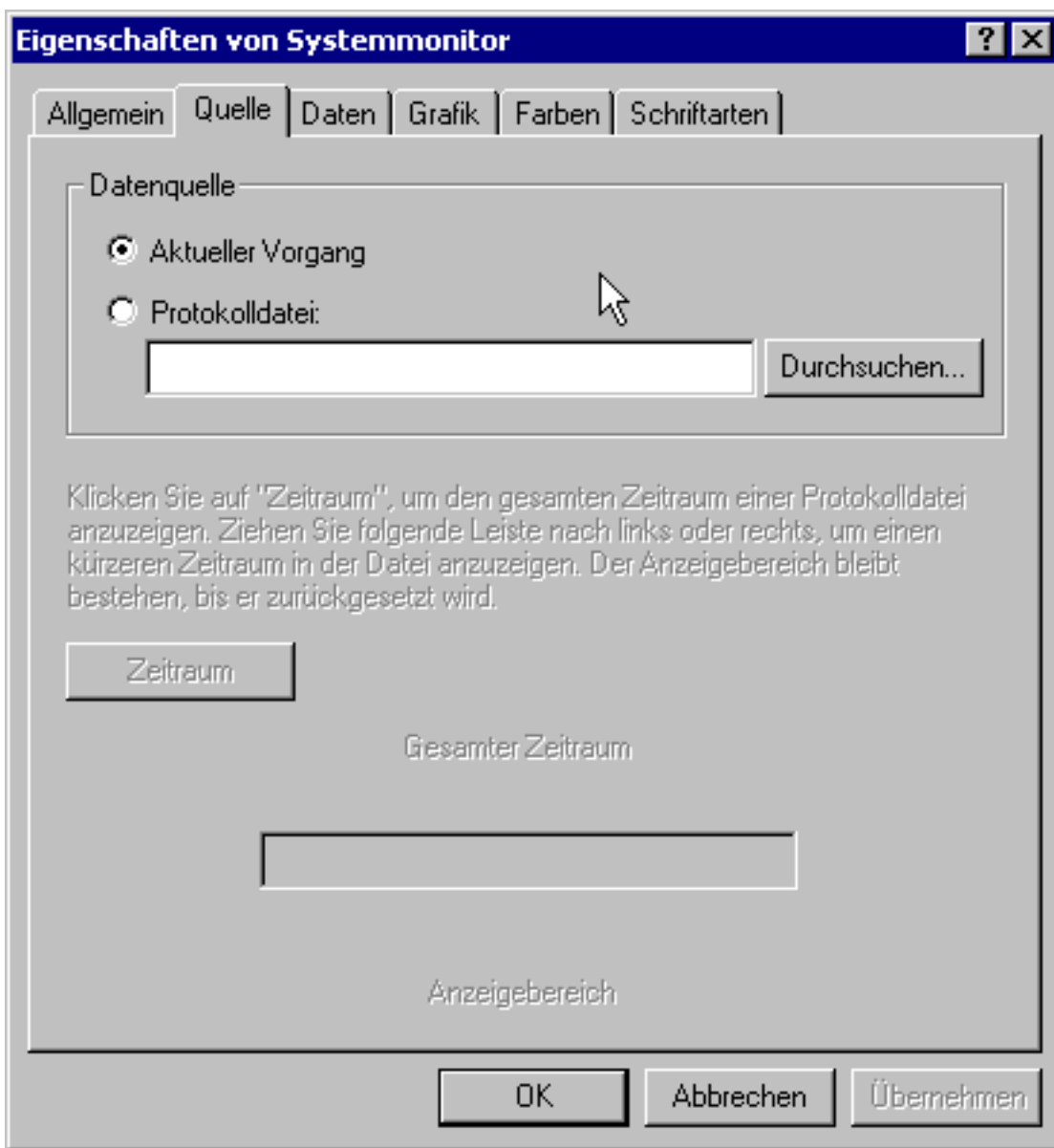


Abbildung 22.34: Auswahl einer Datenquelle für die überwachten Server-Aktivitäten

Auf der Registerkarte **Quelle** legen Sie fest, ob die Daten für Echtzeit-Aktivitäten (*Aktueller Vorgang*) oder für eine zuvor aufgezeichnete Überwachungssitzung (*Protokolldatei*) angezeigt werden sollen. Klicken Sie auf das entsprechende Optionsfeld. Bei der Auswahl einer Protokolldatei haben Sie zusätzlich die Möglichkeit, unten im Dialogfeld einen Zeitraum festzulegen. Nachdem Sie alle Auswahlen und Änderungen vorgenommen haben, wechseln Sie zur Registerkarte **Daten**.

Auf dieser Registerkarte verschaffen Sie sich einen schnellen Überblick, welche Leistungsindikatoren für Ihren Windows-2000-Server aktiv sind. Hier können Sie außerdem beliebige weitere Leistungsindikatoren hinzufügen oder das Erscheinungsbild der aktiven Leistungsindikatoren ändern. Um einen Leistungsindikator zu entfernen, markieren Sie ihn zunächst durch Anklicken. Klicken Sie dann auf die Schaltfläche **Entfernen**, um ihn zu löschen. Nachdem Sie Ihre Auswahl getroffen haben, aktivieren Sie die in Abbildung 22.35 gezeigte Registerkarte **Grafik**.

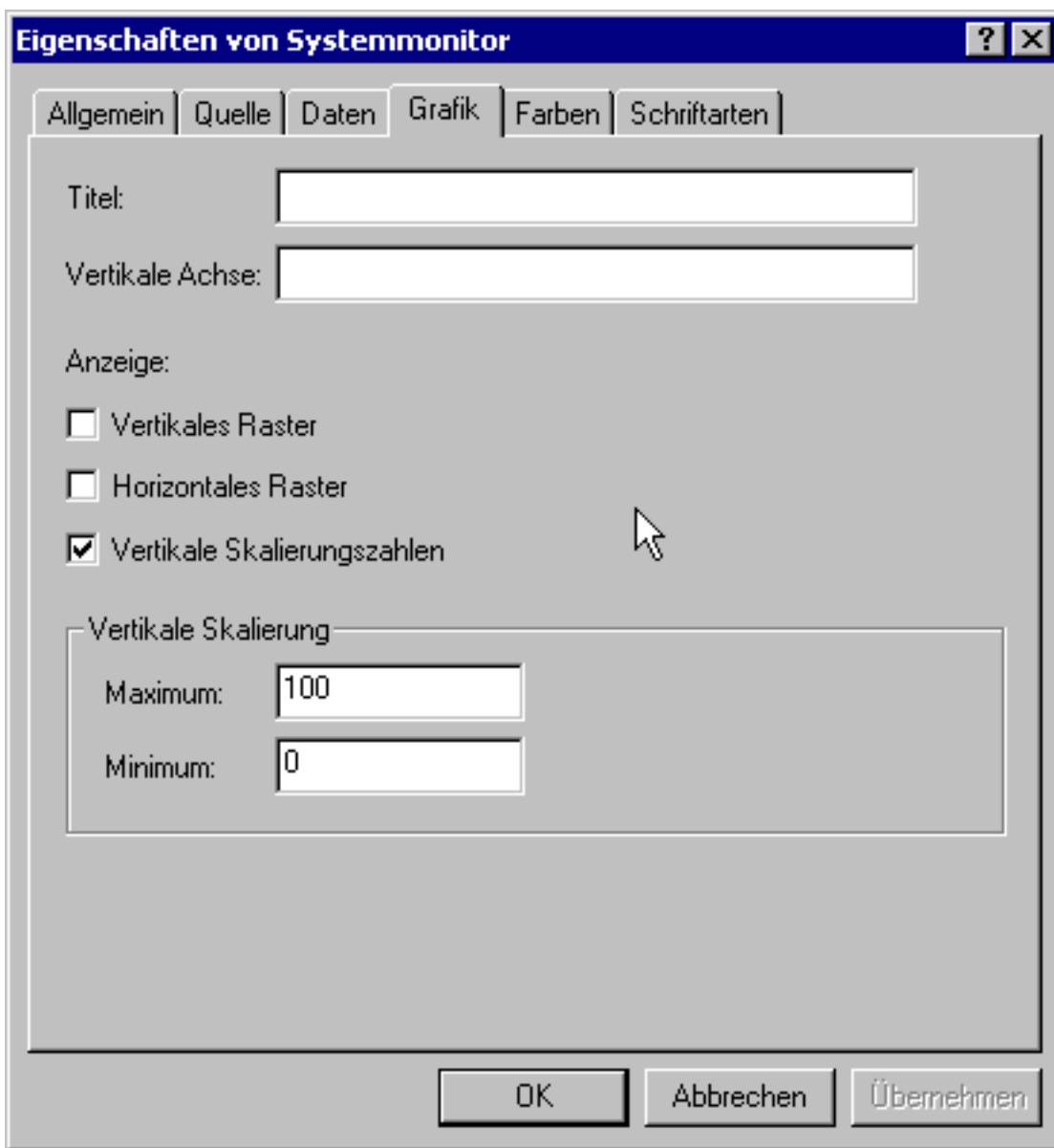


Abbildung 22.35: Einrichtung der Formatattribute für die Grafik

Auf der Registerkarte **Grafik** legen Sie die Standardeinstellungen für die Diagrammansicht Ihrer Überwachungsinformationen fest. Hier können Sie einen Titel einfügen, die Achsenwerte ändern oder die vertikale Skalierung ändern. Nachdem Sie alle Auswahlen und Änderungen vorgenommen haben, wechseln Sie zur Registerkarte **Farben**.

Diese Registerkarte ist die einfachste in diesem Werkzeug. Hier legen Sie die Farbschemata fest, die für die visuelle Darstellung der Überwachungsdaten benutzt werden sollen. Verwenden Sie die Dropdown-Listenfelder, um den betreffenden Bereich auszuwählen. Klicken Sie auf die gewünschte Farbe. Nachdem Sie Ihre Auswahl getroffen haben, wechseln Sie zur Registerkarte **Schriftarten**.

Auch diese Registerkarte ist sehr einfach gehalten. Hier ändern Sie die Schriftart für die Anzeige sowie deren Eigenschaften. Dabei gehen Sie wie in den meisten anderen Windows-basierten Anwendungen vor. Es gibt drei Dropdown-Listenfelder, in denen Sie die Schriftart, den Schriftstil und die Größe auswählen. Im Beispielfeld sehen Sie, wie die ausgewählte Schriftart aussieht. Dadurch erkennen Sie sofort, welche Auswirkung Ihre Auswahl auf eine bestimmte Schriftart hat. Nachdem Sie Ihre Auswahl getroffen haben, klicken Sie auf die Schaltfläche **OK**, um alle Änderungen zu speichern. Sie gelangen

zurück zum Hauptbildschirm der Systemüberwachung.

Hier wollen Sie die Anzeige bestimmter Leistungsindikatoreninformationen deutlicher machen. Dazu klicken Sie diesen Leistungsindikator unten in der Legende an und dann auf die Schaltfläche **Markierung** (das ist die Schaltfläche mit der Glühbirne). Sie sehen den in Abbildung 22.36 gezeigten Bildschirm.

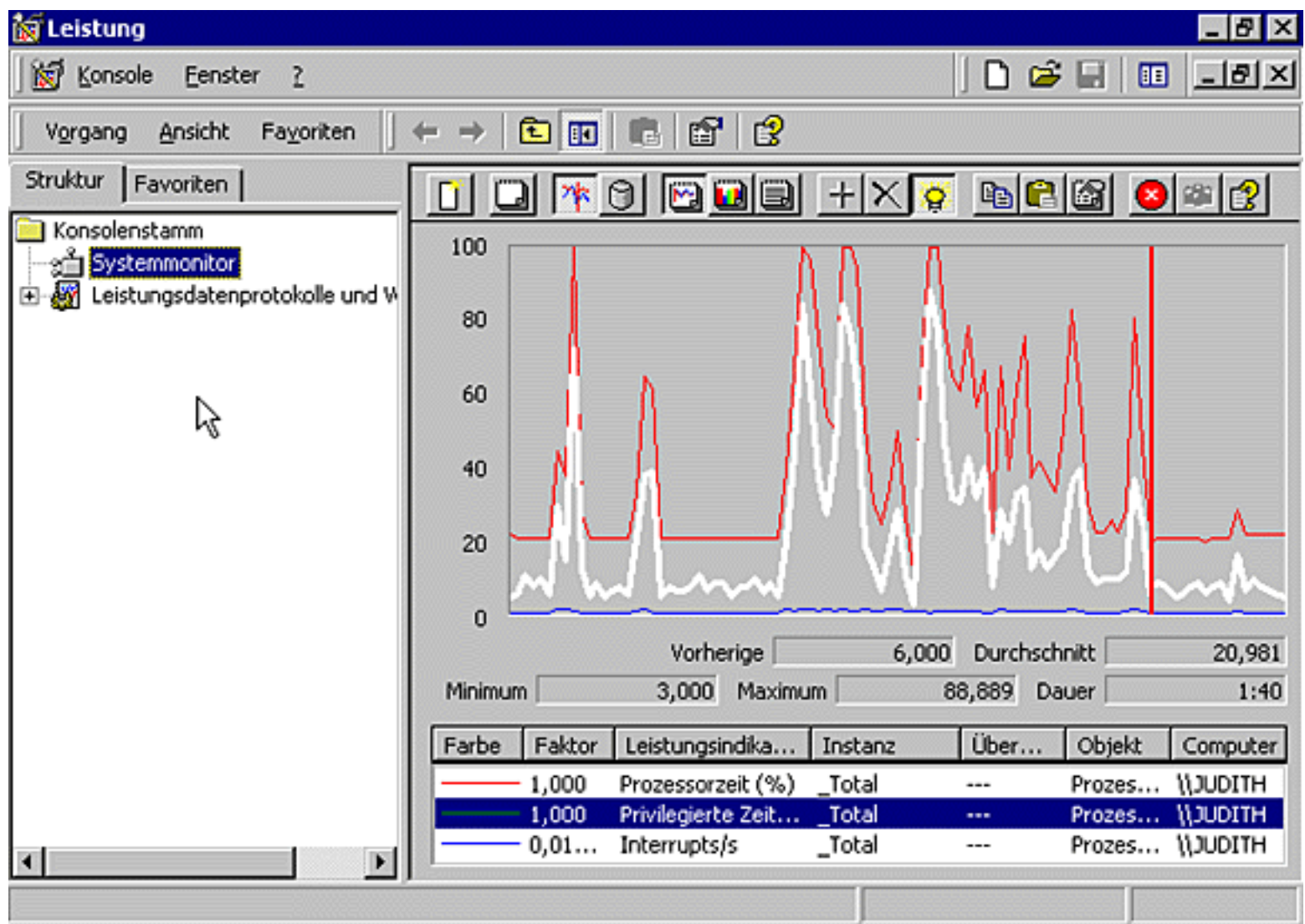


Abbildung 22.36: Markieren der Werte für einen bestimmten Leistungsindikator im Diagramm, um eine übersichtlichere Darstellung zu erzielen

Wie Sie sehen, können Sie mit Hilfe der Schaltfläche **Markierung** die Diagrammwerte für den betreffenden Leistungsindikator schnell und einfach ablesen. Nachdem Sie wissen, wie man ein Diagramm für die Systemüberwachung anlegt und den Systemmonitor manipuliert, wollen wir uns nun mit der Interpretation von Diagrammen beschäftigen.

22.4.3 Diagramme interpretieren

Die Interpretation der Daten in einem Diagramm oder Histogramm des Windows 2000 Server-Systemmonitors ist nicht ganz einfach. Sie wissen jetzt, wie man Diagramme für die Systemüberwachung anlegt. Eine weitere schnelle Methode, Echtzeit-Datenaktivität anzuzeigen, bietet

das Format *Histogramm*, das eigentlich nichts weiter ist als ein einfaches Balkendiagramm. Wenn Sie ein Diagramm im Histogrammformat anzeigen wollen, gehen Sie einfach zurück in den Systemmonitor (falls Sie diesen geschlossen haben) und klicken Sie auf die Schaltfläche **Histogramm anzeigen** (sie zeigt ein Symbol für ein Balkendiagramm). Damit werden die Daten aus dem Diagramm im Systemmonitor als Histogramm angezeigt, wie in Abbildung 22.37 gezeigt.

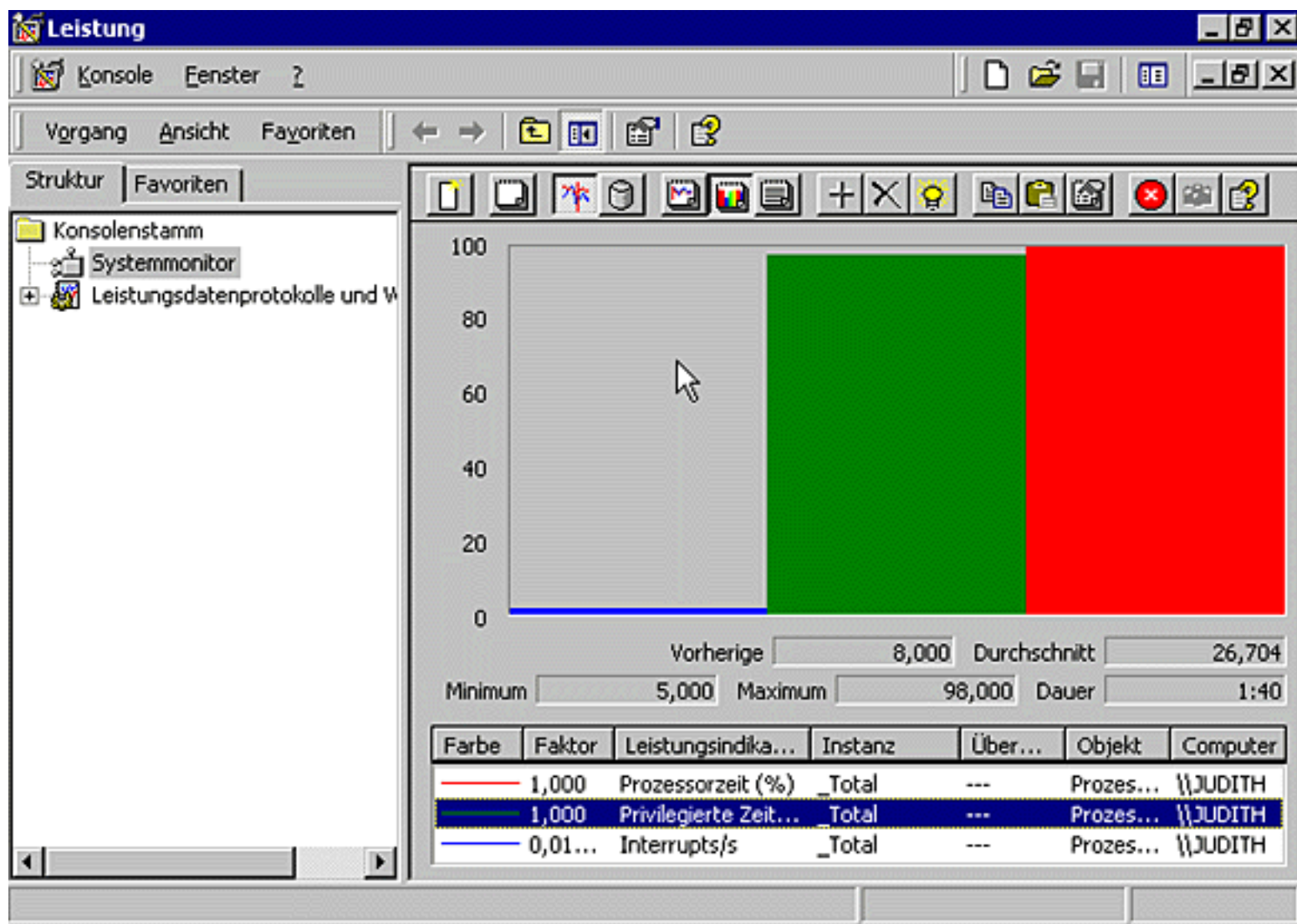


Abbildung 22.37: Anzeige eines Diagramms aus dem Systemmonitor in Histogrammform

Das Histogrammformat bietet zwar dem menschlichen Auge eine einfachere Orientierung, aber es hilft Ihnen kaum bei der Analyse bereits gesammelter Daten. Als Anfänger wollen Sie vielleicht eine Ausgangswertanalyse für Ihre Windows-2000-Server-Maschine ausführen. Dies beinhaltet Informationen wie beispielsweise, ob ein Prozess versucht hat, das Computersystem zu überlasten, indem er übermäßig viele Anforderungen an Speicher, CPU oder Festplattenlaufwerk gestellt hat. Nachdem Sie ungefähr wissen, was für Ihren Computer »normal« ist, können Sie die Überwachung des Computersystems beginnen, um Abweichungen gegenüber diesen Werten auf dem Serversystem zu ermitteln.

Darüber hinaus sollten Sie sich mit den Überwachungsstandards für Ihr Unternehmen beschäftigen. Die folgende Liste beschreibt Aspekte, die in vielen Unternehmen überwacht werden (Format: *Objekt{Leistungsindikator}. Beschreibung*). Hier wird auch erklärt, was diese Überwachung für die Windows 2000-Server Ihres Unternehmens bedeuten könnte:

- *Speicher {Seiten/s}*. Wenn dieser Leistungsindikator ständig höher als erwartet ist, verfügt Ihr System nicht über genügend Arbeitsspeicher (mit anderen Worten, Sie müssen mehr Speicher in Ihren Windows-2000-Server-Rechner einbauen).
- *Logische Festplatte {Durchschnittliche Länge der Festplattenwarteschlange}*. Dieser Leistungsindikator hilft Ihnen, die Aktivität auf den Festplattendatenträgern Ihres Servers zu beurteilen. Zeigt der Leistungsindikator über längere Zeit hohe Werte an (was »längere Zeit« bedeutet, ist von Ihren Vergleichswerten abhängig), dann besteht sehr wahrscheinlich ein Engpass in Hinblick auf Ihre Festplatten.
- *Server {Übertragene Bytes/s}*. In einem Ethernet-Netzwerk sollte dieser Leistungsindikator nicht höher als 0,83 Mbps werden, während in einem Token-Ring-Netzwerk der Wert 0,5 Mbps (auf einem 4-Mbps-Ring) oder 2 Mbps (auf einem 16-Mbps-Ring) nicht überschreiten sollte.
- *Speicher {Verfügbare MB}*. Dieser Wert sollte immer größer als 16 Mbyte sein; andernfalls steht vermutlich zu wenig Arbeitsspeicher zur Verfügung.
- *Speicher {Bestätigte Bytes}*. Dieser Wert sollte immer kleiner als der auf diesem Windows-2000-Server-Rechner Arbeitsspeicher sein. Übersteigt dieser Leistungsindikator den Betrag des physischen RAM, müssen Sie mehr Speicher im Server installieren.
- *Speicher {Seiten/s}*. Dieser Wert sollte für Pentium-Server immer kleiner als 20 sein. Übersteigt er 20, haben Sie ein Seitenrahmen-Speicherproblem (d.h. einen Speicherengpass, der einen RAM-Engpass verursachen kann).
- *Speicher {Nicht-Auslagerungsdateiseiten/Bytes}*. Wächst dieser Wert ständig an, weist eine der Anwendungen auf der Windows-2000-Server-Maschine ein Speicherleck auf. Sie finden die betreffende Anwendung, indem Sie schrittweise alle Anwendungen zuschalten.
- *Prozessor {%Prozessorzeit}*. Dieser Wert sollte kleiner als 90 Prozent sein; andernfalls sollten Sie die Leistung Ihres Prozessors aktualisieren (fügen Sie aber keine weiteren Prozessoren in ein System ein, wo es bereits zwei Prozessoren gibt - diese Möglichkeit ist noch nicht ganz ausgereift).
- *Prozessor {Interrupts/s}*. Hier sollten Sie sowohl den Gesamtwert als auch die einzelnen Prozessoren betrachten. Wenn Ihr System die Interrupts nicht schnell genug verarbeitet (in der Regel ist das eine Zahl kleiner 3.500 für einen einzelnen Prozessor), haben Sie wahrscheinlich einen CPU-Engpass. Exzessive Interruptzugriffe werden in der Regel durch ein Hardware-Problem verursacht, beispielsweise eine defekte Karte, oder durch ein Software-Problem, beispielsweise die Nutzung eines nicht standardisierten Software-Treibers.
- *Prozess {Arbeitsseiten}*. Dieser Leistungsindikator teilt Ihnen mit, welche Anwendung den meisten Speicher auf Ihrem Server belegt. Wird der gesamte Speicher von einer einzigen Anwendung verbraucht, die nicht das Betriebssystem ist, haben Sie ein Problem.
- *Prozess {Auslagerungsdatei Bytes}*. Mit der Instanzeinstellung *_Total* überwachen Sie mit Hilfe dieses Leistungsindikators die vollständige Größe der für Ihre Windows-2000-Server-Maschine erforderlichen Auslagerungsdatei. Anhand dieser Größe legen Sie fest, wo die Auslagerungsdatei abgelegt und welche Größe sie erhalten soll.

Die hier aufgelisteten Leistungsindikatoren beschreiben nur einen Bruchteil dessen, was mit den Werkzeugen zur System- und Netzwerküberwachung in Windows-2000-Server möglich ist. Ihre Systemadministratoren müssen sich selbst diverse Fragen stellen, unter anderem: Sollen wir alle diese

Leistungsindikatoren benutzen, und falls nicht, welche? Sollen wir mehr benutzen? Was erwarten wir von der Leistungsüberwachung in Windows-2000-Server? Nachdem Ihr Unternehmen Antworten auf diese Fragen gefunden hat, sind Sie gerüstet für die korrekte Analyse der aufgezeichneten Daten.

22.4.4 Berichte und Protokolle

Ein letzter Aspekt, den Sie bei der Nutzung des Werkzeugs *Systemleistung* in Windows-2000-Server betrachten sollten, sind die Optionen für Berichte und Protokolle. Dazu betrachten wir noch einmal den Hauptbildschirm des Dienstprogramms *Leistung* (siehe Abbildung 22.38).

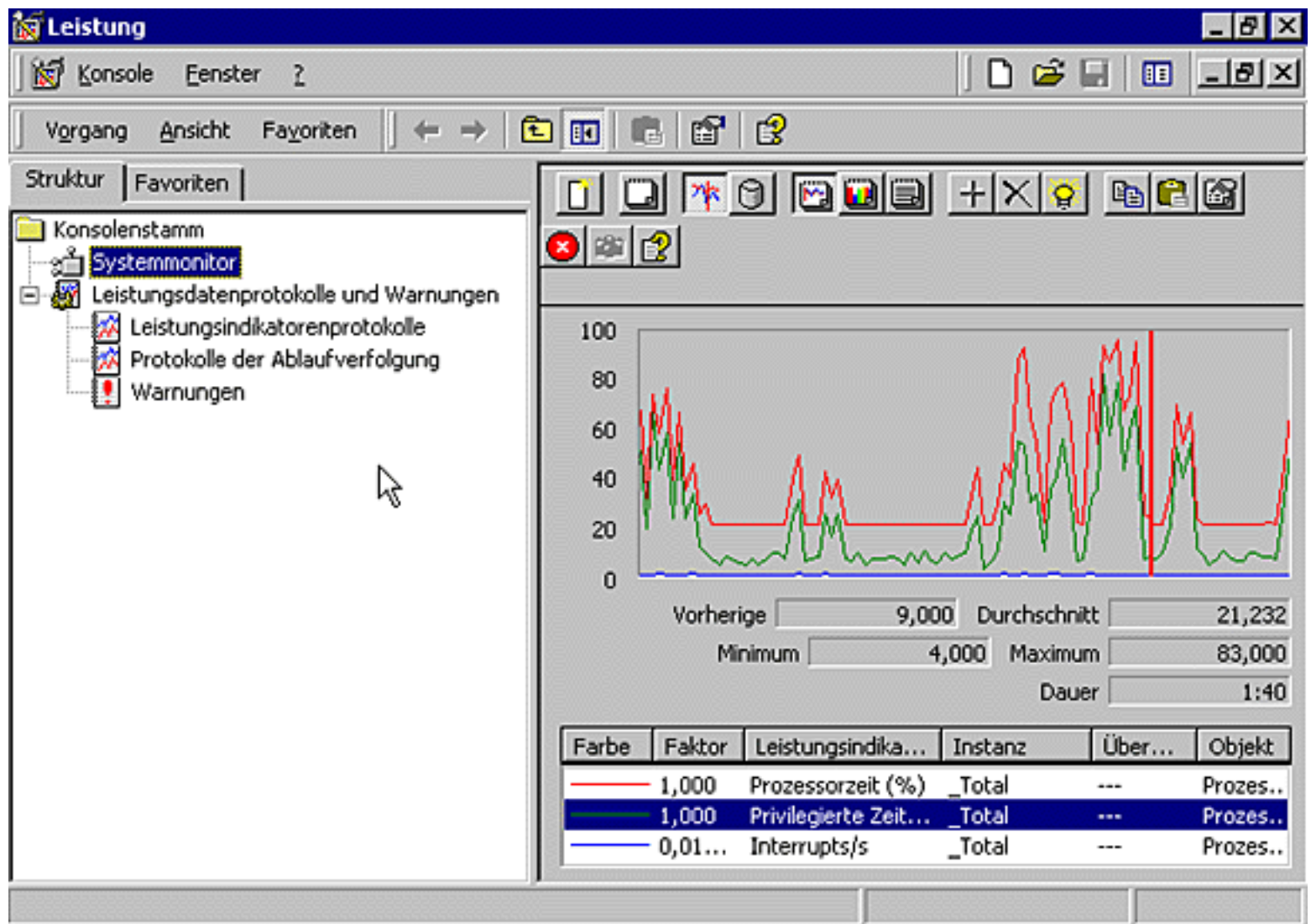


Abbildung 22.38: Ansicht verschiedener aktiver Leistungsindikatoren

Auf der linken Seite des Bildschirms sehen Sie in der Menüstruktur das Symbol für **Leistungsdatenprotokolle und Warnungen** unmittelbar unterhalb des Symbols für den Systemmonitor. Hier werden Sie sehr viel Zeit verbringen. Zuvor klicken Sie jedoch auf die Schaltfläche **Bericht anzeigen** oben im rechten Bereich (die Schaltfläche mit dem Notizblock). Sie sehen den in Abbildung 22.39 gezeigten Bildschirm.

Die Berichtsansicht ist eine der interessantesten Ansichten. Hier sehen Sie schnell alle Werte für alle im Systemmonitor aktivierten Leistungsindikatoren. Dabei werden Gruppierungen nach dem Servernamen

und dann nach den jeweiligen Objekten vorgenommen. Dadurch ist es ganz einfach, den Status Ihrer Server und der dafür überwachten Objekte zu erkennen.

Jetzt betrachten wir die Leistungsprotokolle und Warnungen, indem wir im linken Feld auf das zugehörige Symbol klicken.

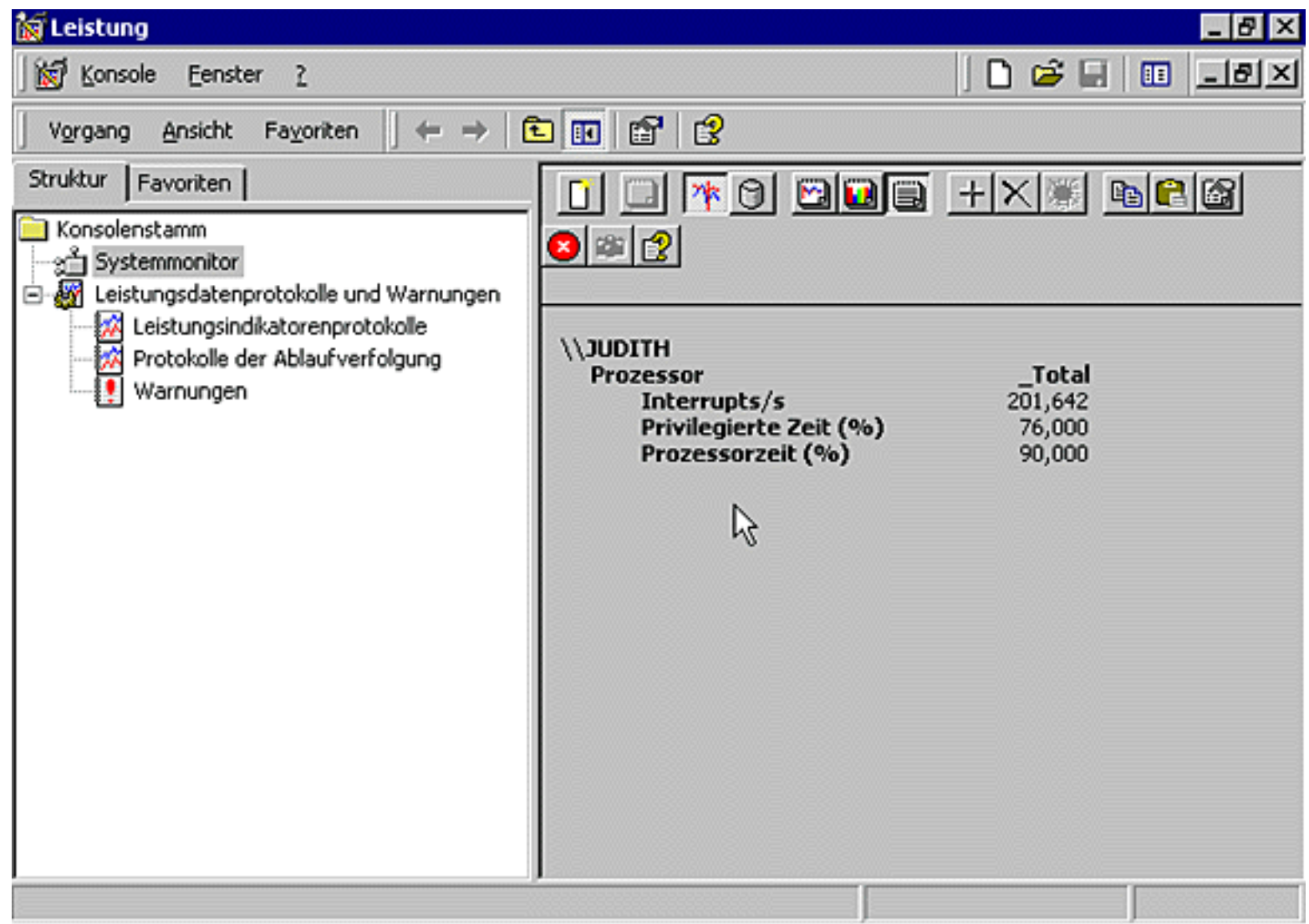


Abbildung 22.39: Berichtsansicht in der Leistungsüberwachung

Nachdem Sie auf dieses Symbol geklickt haben, ändert sich der Inhalt des rechten Bereichs. Jetzt werden die Namen und Beschreibungen der drei Komponenten angezeigt, die momentan im Abschnitt **Leistungsdatenprotokolle und Warnungen** von Windows-2000-Server enthalten sind:

- **Leistungsindikatorenprotokolle.** Diese Funktion konfiguriert Leistungsprotokolle für Leistungsdaten.
- **Protokolle für die Ablaufverfolgung.** In diesem Bereich werden Ablaufverfolgungsprotokolle konfiguriert.
- **Warnungen.** In diesem Bereich werden verschiedene Warnungen der Leistungsüberwachung konfiguriert.

Klicken Sie auf das Symbol **Leistungsindikatorenprotokolle** unterhalb des Icons **Leistungsdatenprotokolle und Warnungen**. Im rechten Feld erscheint ein Beispiel für ein

Leistungsindikatorprotokoll.

Das Leistungsindikatorprotokoll **Systemübersicht** ist eine Beispieldatei, mit der Sie ein bisschen experimentieren können. Auf diese Weise verstehen neue Systemadministratoren schneller, welche Möglichkeiten Windows-2000-Server hier bietet. Klicken Sie das Leistungsindikatorprotokoll **Systemübersicht** mit der rechten Maustaste an, um ein Kontextmenü zu öffnen. Wählen Sie den Menüeintrag **Eigenschaften** aus, um den in Abbildung 22.40 gezeigten Bildschirm aufzurufen.

Das Dialogfeld **Eigenschaften von Systemübersicht** erscheint. Sie befinden sich auf der Registerkarte **Allgemein**. Betrachten Sie den Inhalt dieses Bildschirms, beachten Sie jedoch, dass für eine eigene Version einige dieser Einstellungen geändert werden müssen. Nachdem Sie fertig sind, wechseln Sie zur Registerkarte **Protokolldateien**, die Sie in Abbildung 22.41 sehen.

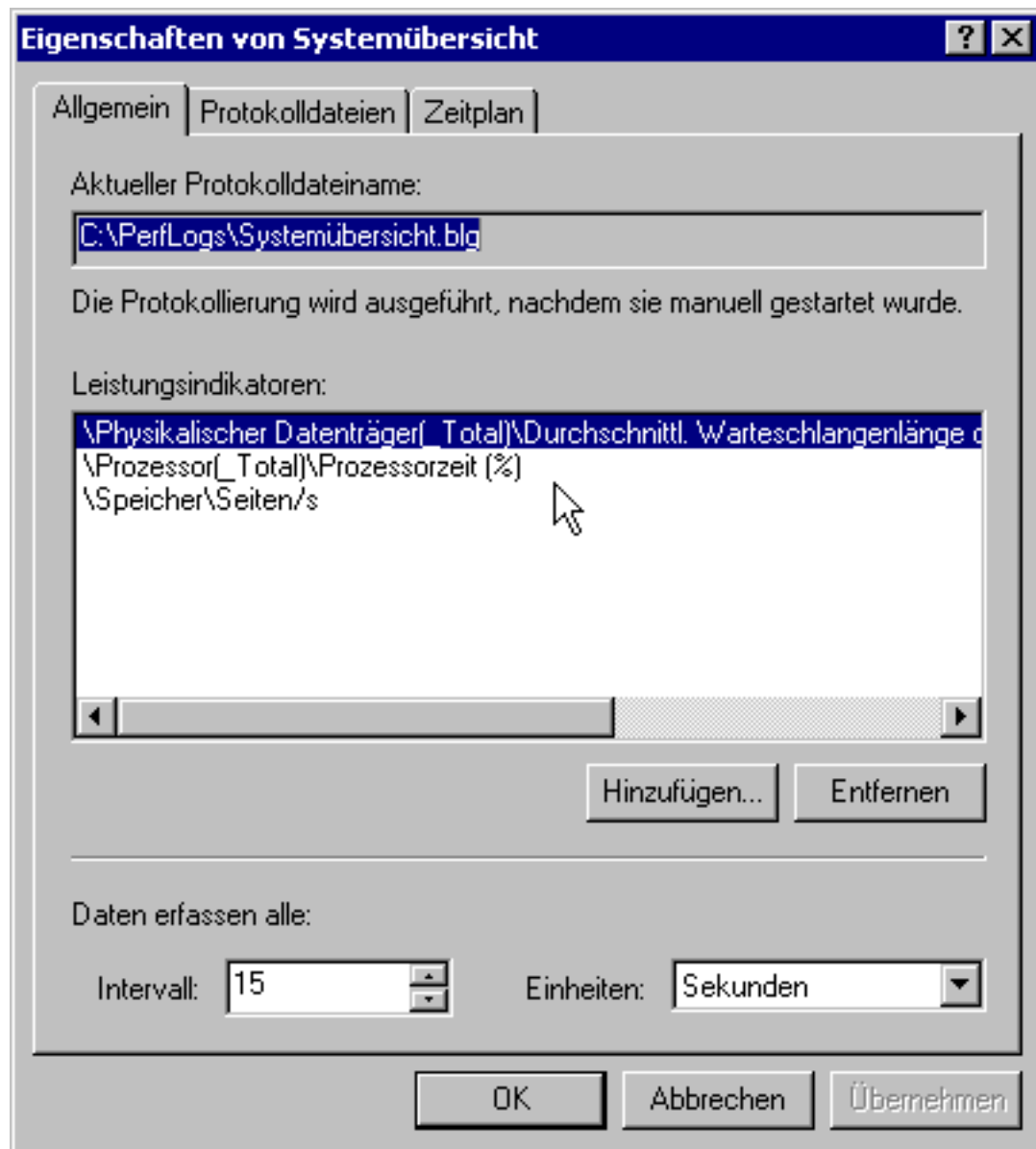


Abbildung 22.40: Anzeige der allgemeinen Eigenschaften für die Leistungsindikatoren in der Protokolldatei

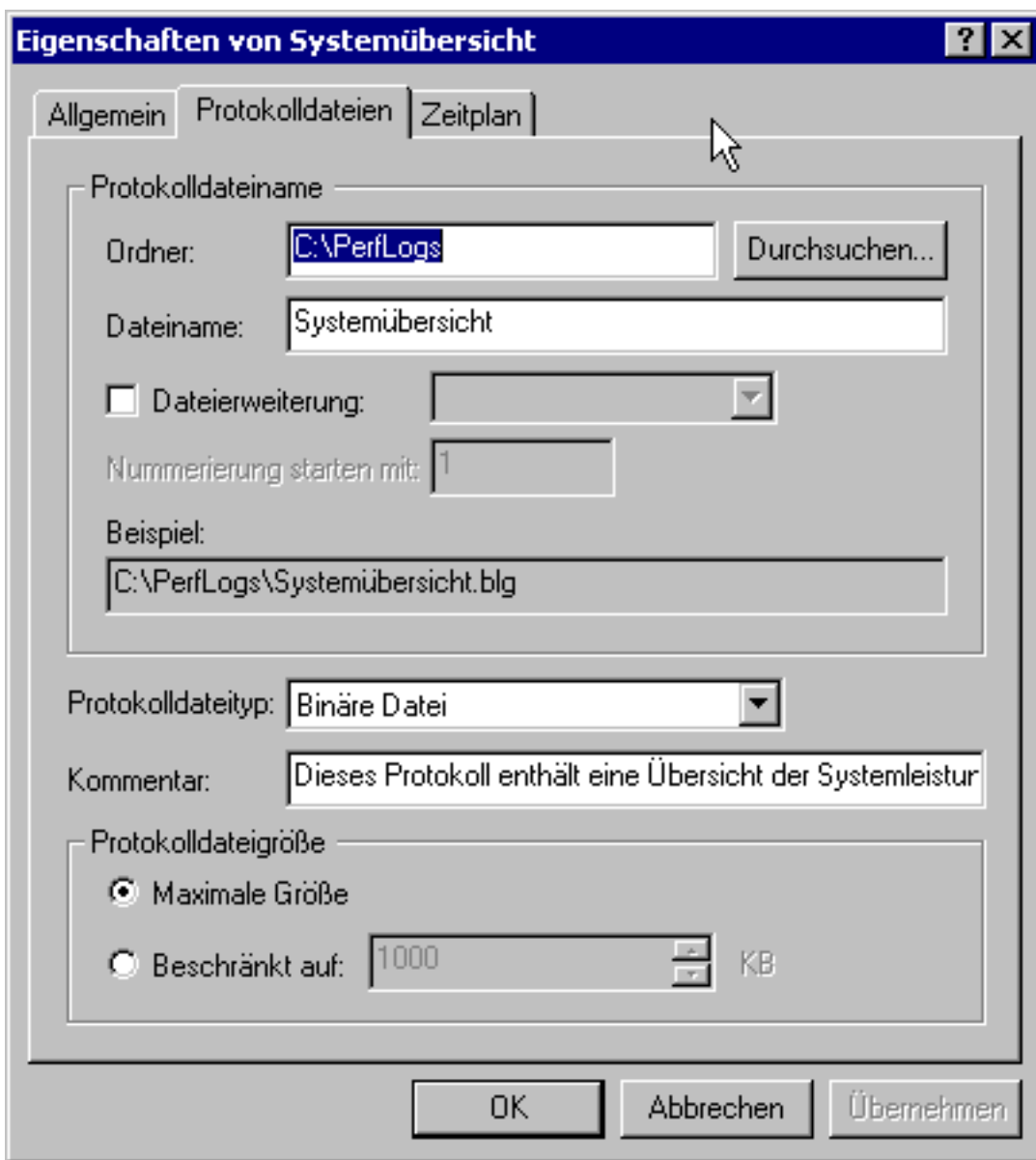


Abbildung 22.41: Konfiguration des Namens, der Position, der Größe und des Typs einer Protokolldatei

Wie die Registerkarte **Allgemein** enthält auch die Registerkarte *Protokolldateien* einige selbst erklärende Einträge. Eine der wichtigsten Funktionen auf diesem Bildschirm ist, die Gesamtgröße der Protokolldateien zu beschränken (die andernfalls eine Größe annehmen, die den verfügbaren Speicher auf der Festplatte Ihrer Windows-2000-Server-Maschine überschreitet). Wechseln Sie jetzt zur Registerkarte **Zeitplan**, wie in Abbildung 22.42 gezeigt.

Auf dieser Registerkarte geben Sie die Uhrzeit, das Datum und die Häufigkeit der betreffenden Aufgabe an. Mit der Schaltfläche **OK** gelangen Sie zum Eigenschaftenfenster für die Systemübersicht zurück. Falls Sie Änderungen an der Beispieldatei vorgenommen haben, erscheint eine Fehlermeldung, in der Sie aufgefordert werden, keine Änderungen vorzunehmen.

Klicken Sie auf die Schaltfläche **OK**, um das Meldungsfeld mit der Fehleranzeige zu schließen, und dann auf die Schaltfläche **Abbrechen**, um das Dialogfeld **Eigenschaften von Systemübersicht** korrekt zu verlassen. (Sie klicken auf **Abbrechen**, weil Sie keine Änderungen speichern wollen.) Um einen eigenen Leistungsindikator hinzuzufügen, klicken Sie mit der rechten Maustaste auf das Symbol

Leistungsindikatorprotokolle im linken Bereich des Fensters. Ein Kontextmenü mit einigen wenigen sinnvollen Optionen erscheint:

- Neue Protokolleinstellungen
- Neue Protokolleinstellungen von
- Ansicht
- Neues Fenster
- Neue Taskpadansicht
- Aktualisieren
- Liste exportieren
- Hilfedatei anzeigen

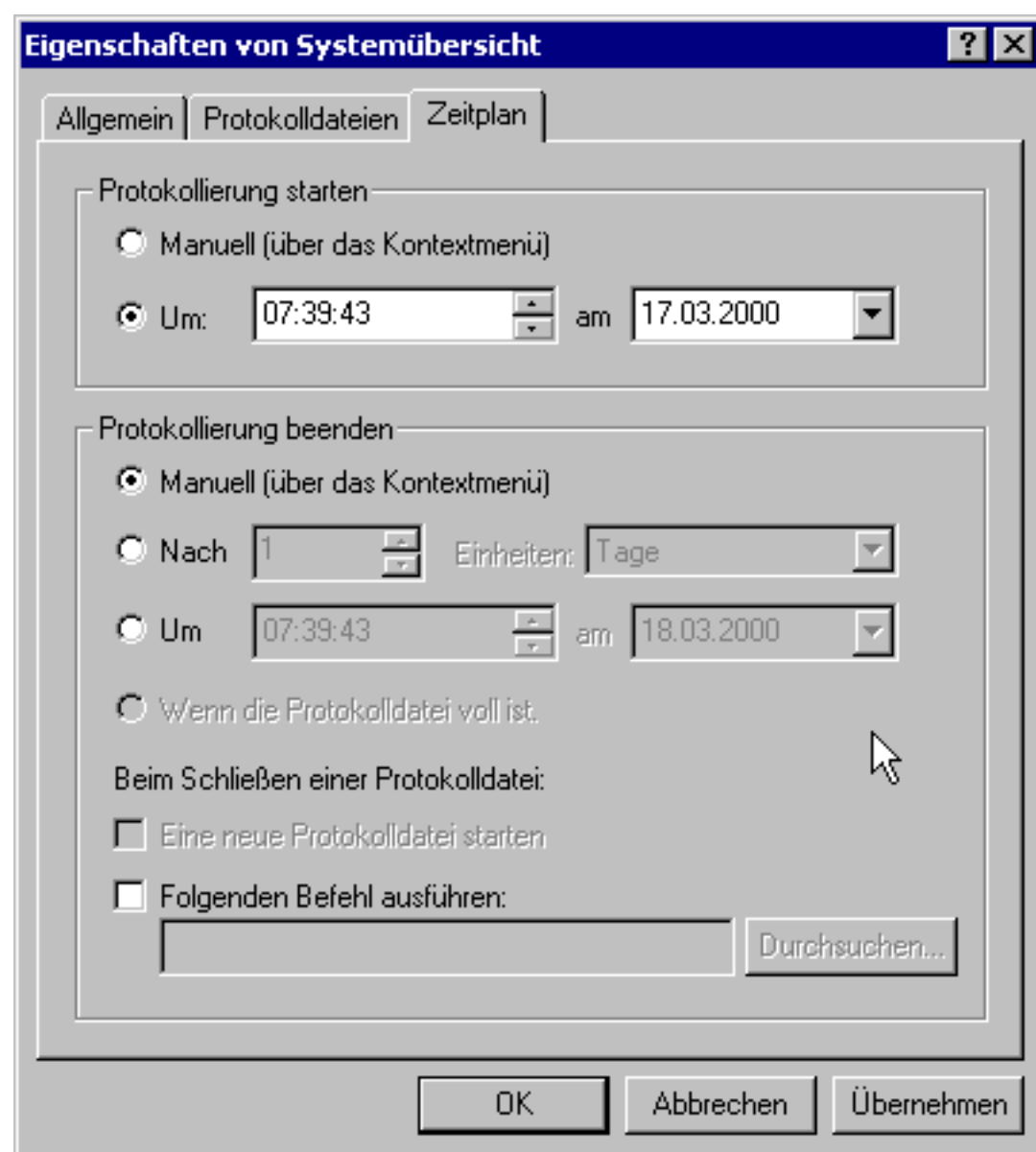


Abbildung 22.42: Konfigurieren von Zeitplanoptionen für das Starten und das Beenden eines Protokolls

In diesem Menü wählen Sie den Eintrag **Neue Protokolleinstellungen** aus. Das Dialogfeld **Neue Protokolleinstellungen** wird geöffnet. Hier geben Sie den Namen Ihrer neuen Protokolldatei an.

Nachdem Sie den gewünschten Namen eingegeben haben, klicken Sie auf die Schaltfläche **OK**. Sie gelangen zu dem in Abbildung 22.43 gezeigten Dialogfeld.

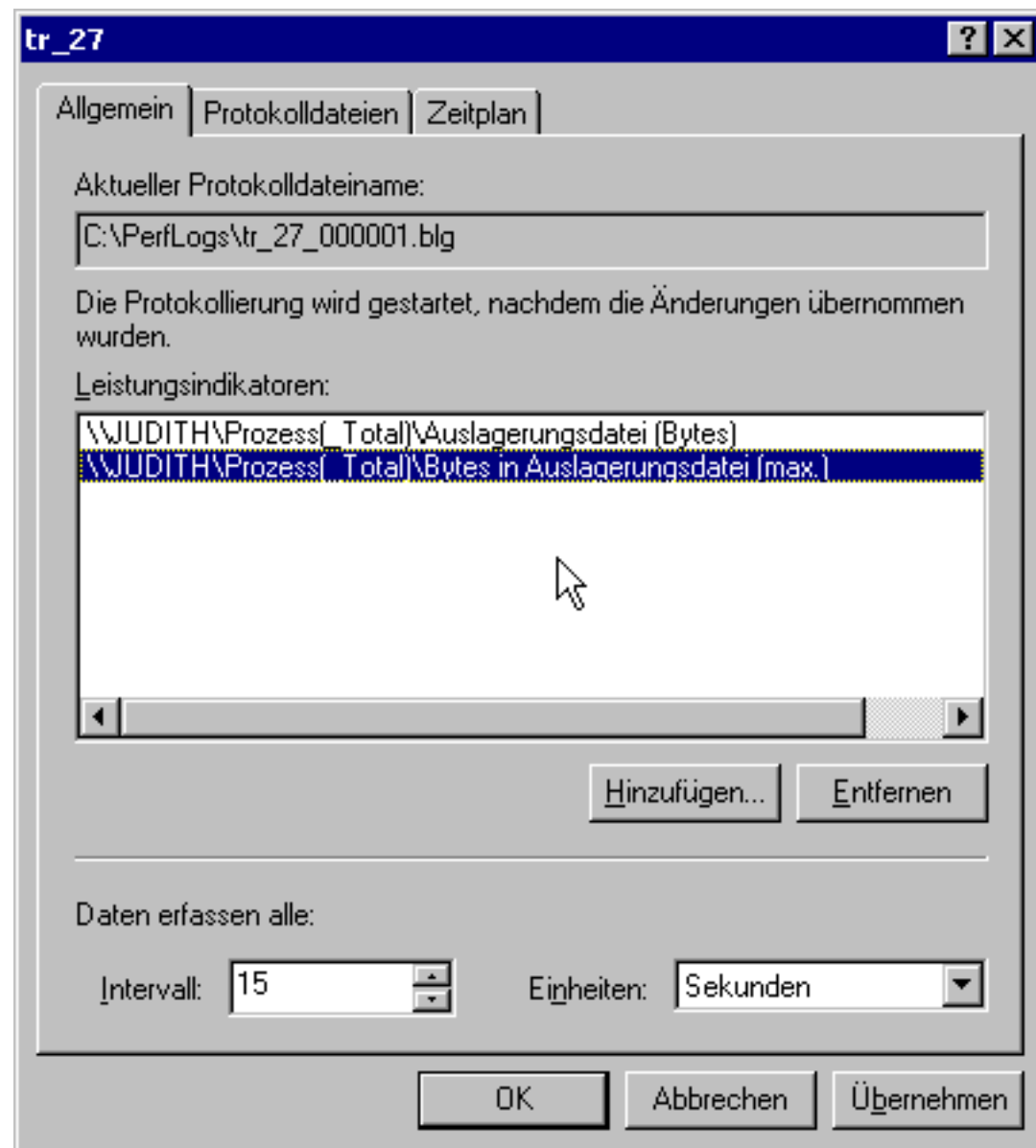


Abbildung 22.43: Anzeige der allgemeinen Optionen für ein Leistungsindikatorprotokoll

Auf der Registerkarte **Allgemein** fügen Sie mindestens einen Leistungsindikator in den Abschnitt **Leistungsindikatoren** ein. Darüber hinaus können Sie gegebenenfalls das Aktualisierungsintervall ändern. Nachdem Sie Ihre Änderungen vorgenommen haben, wechseln Sie zur Registerkarte **Protokolldateien**.

Nehmen Sie Ihre Dateinameneinträge sowie die Konfiguration für Dateityp und -größe vor. Dieser Bildschirm entspricht exakt jenem, den Sie zuvor für das Standardprotokoll kennen gelernt haben, deshalb sollten Ihnen die hier gebotenen Optionen vertraut sein. Beachten Sie, dass Sie die Protokolldatei an beliebiger Stelle speichern können, auch auf anderen Computern im Netzwerk, wodurch ihre Überwachung etwas einfacher zu handhaben ist. Nachdem Sie Ihre Einträge vorgenommen haben, wechseln Sie zur Registerkarte **Zeitplan**, die Sie in Abbildung 22.44 sehen.

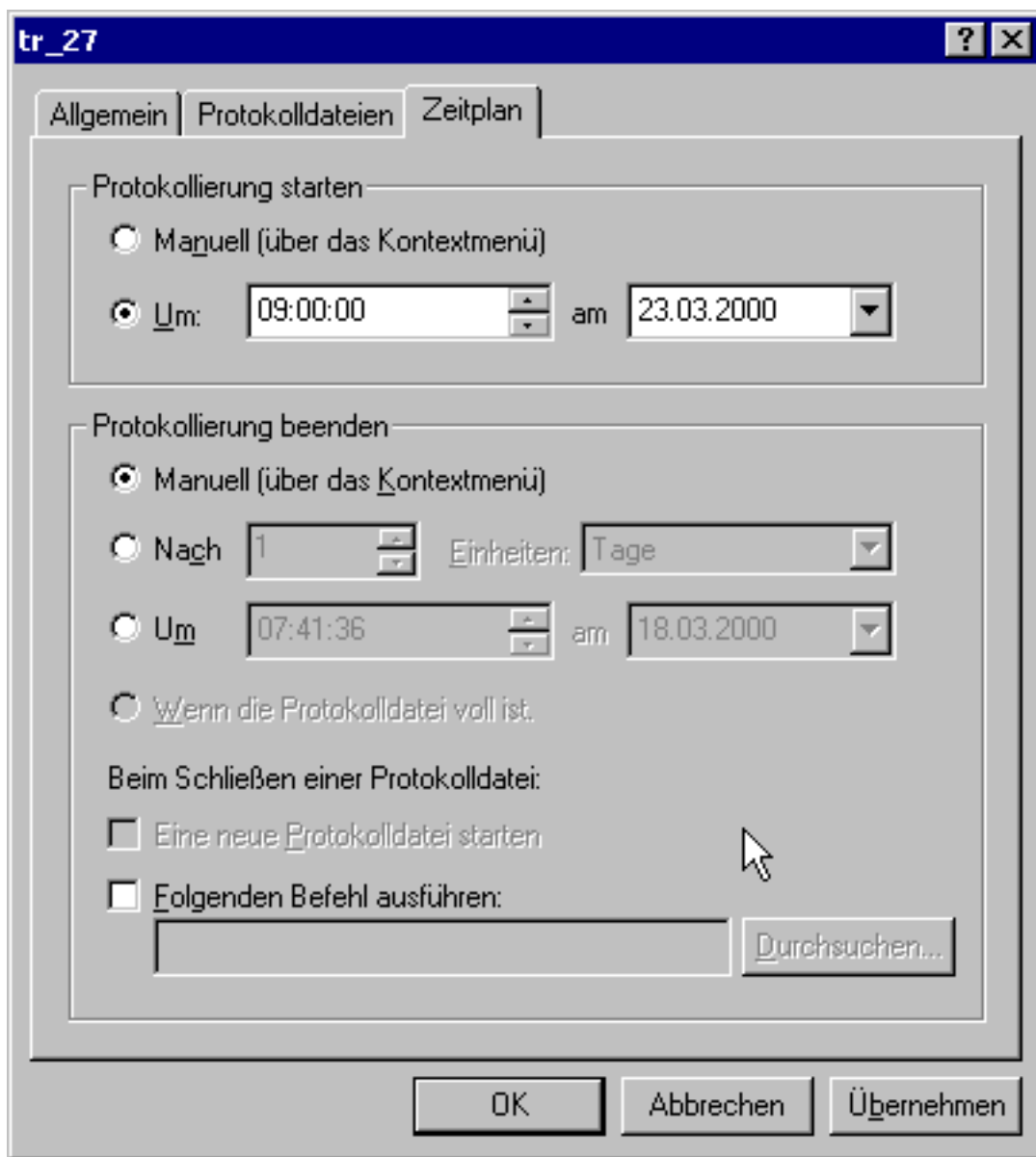


Abbildung 22.44: Einplanen einer Ausführungszeit für Ihr Leistungsindikatorprotokoll

Wie auf der zuvor gezeigten Registerkarte *Zeitplan* legen Sie einfach die Uhrzeit und das Datum fest, wann das Protokoll beginnen und enden soll. Diese Einstellungen setzen voraus, dass Sie das Starten und Beenden manuell nur auf dem lokalen Server vornehmen und nicht über eine Netzwerkfreigabe. Nachdem Sie Ihre Einträge erledigt haben, klicken Sie auf die Schaltfläche **OK**, um auf den Hauptbildschirm der Systemleistung zurückzukehren, wie in Abbildung 22.45 gezeigt.

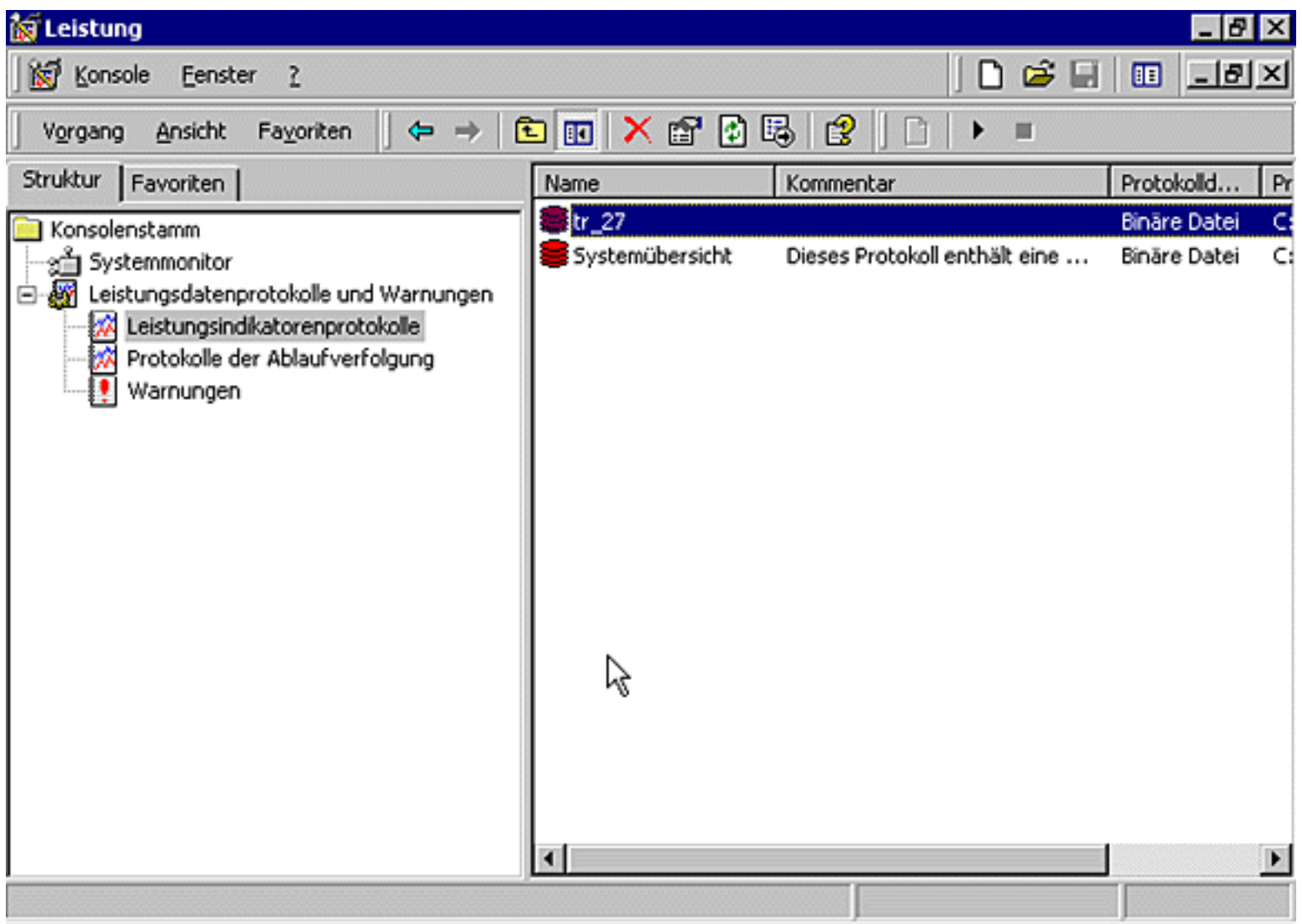


Abbildung 22.45: Anzeige Ihres neu erstellten Überwachungsprotokolls im Hauptbildschirm der Systemleistung

Im Hauptbildschirm sehen Sie, dass Ihr neues Leistungsindikatorprotokoll eingerichtet wurde. Um die Überwachung sofort zu starten, ohne auf die angegebene Startzeit zu warten, klicken Sie mit der rechten Maustaste auf das Protokoll und wählen im Kontextmenü den Eintrag **Starten** aus. Das neue Protokoll wechselt jetzt von der roten in die grüne Anzeige, wobei der Inhalt der Zeile unverändert bleibt (d.h. nur die Farbe des Symbols ändert sich, nichts weiter).

Jetzt wollen wir ein Ablaufverfolgungsprotokoll anlegen. Hier gibt es keine Beispieldatei im Dienstprogramm *Leistung* von Windows-2000-Server, aus dem Sie lernen könnten. Deshalb probieren Sie es jetzt einfach aus. Klicken Sie mit der rechten Maustaste auf das Symbol **Protokolle der Ablaufverfolgung** im linken Bereich des Fensters. Ein Kontextmenü wird angezeigt. Sie kennen es schon, weil es genau dasselbe ist, das bei der Konfiguration Ihres ersten Überwachungsprotokolls angezeigt wurde.

Klicken Sie auf die Menüauswahl **Neue Protokolleinstellungen** oben in diesem Menü. Das Dialogfeld **Neue Protokolleinstellungen** erscheint. Hier geben Sie den Namen Ihrer neuen Protokolldatei an. Klicken Sie auf **OK**. Damit gelangen Sie zum in Abbildung 22.46 gezeigten Dialogfeld.

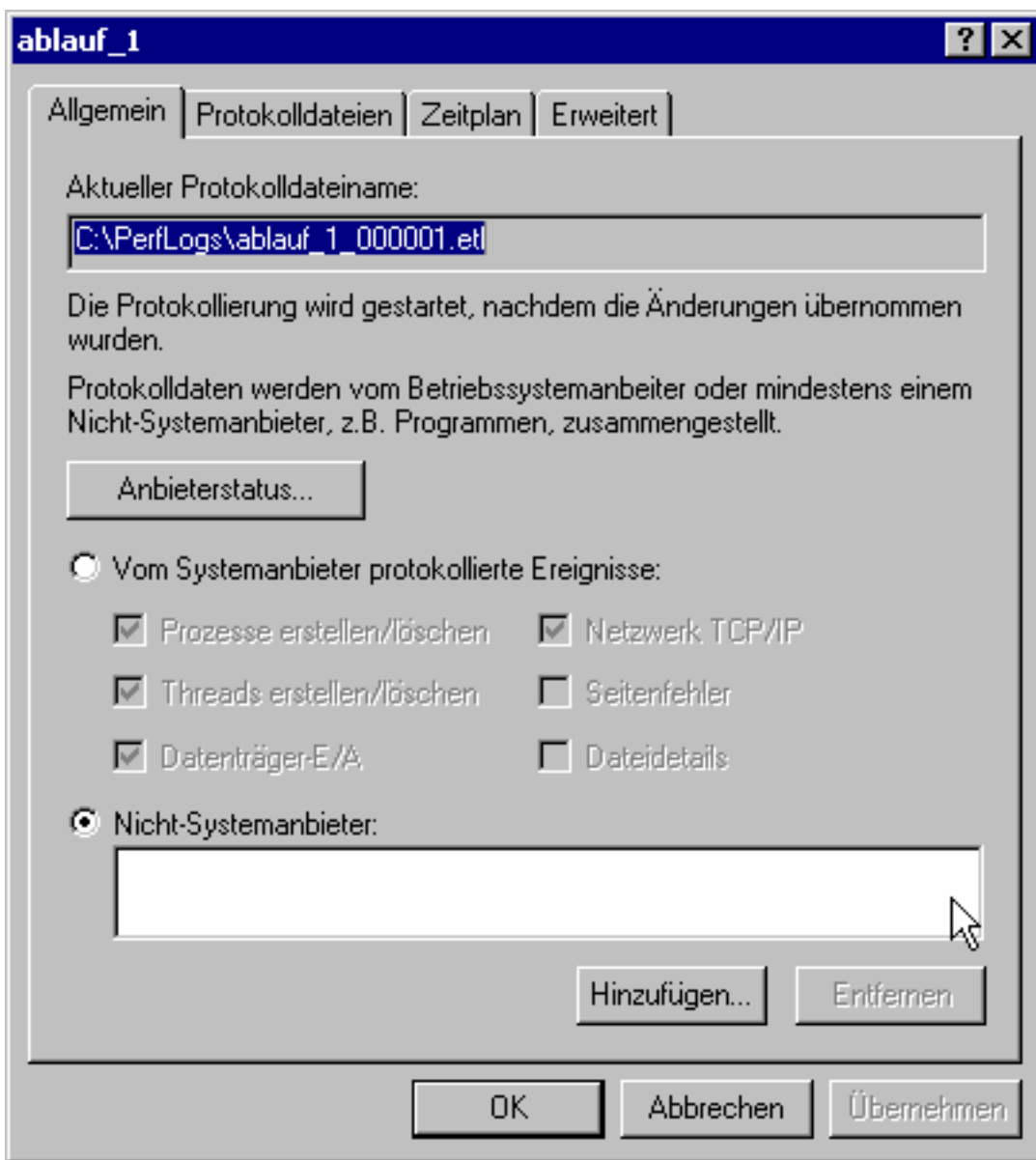


Abbildung 22.46: Anzeige der allgemeinen Eigenschaften für Ihr neues Ablaufverfolgungsprotokoll

Auf der Registerkarte **Allgemein** müssen Sie mindestens den Status des Protokollanbieters angeben. Andernfalls wird beim Wechsel zur Registerkarte **Protokolldateien** sofort ein Dialogfeld mit Fehlermeldung angezeigt, die Ihnen mitteilt, dass Sie mindestens einen allgemeinen Ablaufverfolgungsanbieter oder den Systemanbieter angeben müssen.

Klicken Sie auf die Schaltfläche **Anbieterstatus**, um das in Abbildung 22.47 gezeigte Dialogfeld aufzurufen.



Abbildung 22.47: Anzeige der verfügbaren Anbieter

Wenn Sie in das Kontrollkästchen **Nur aktivierte Anbieter anzeigen** klicken, werden die Einträge wahrscheinlich verschwinden. Lassen Sie daher das Kontrollkästchen besser deaktiviert. Nachdem Sie sich die Optionen für dieses Feld angesehen haben, klicken Sie auf die Schaltfläche **Schliessen**, um das Dialogfeld zu verlassen. Sie gelangen zurück zu dem in Abbildung 22.48 gezeigten Dialogfeld.

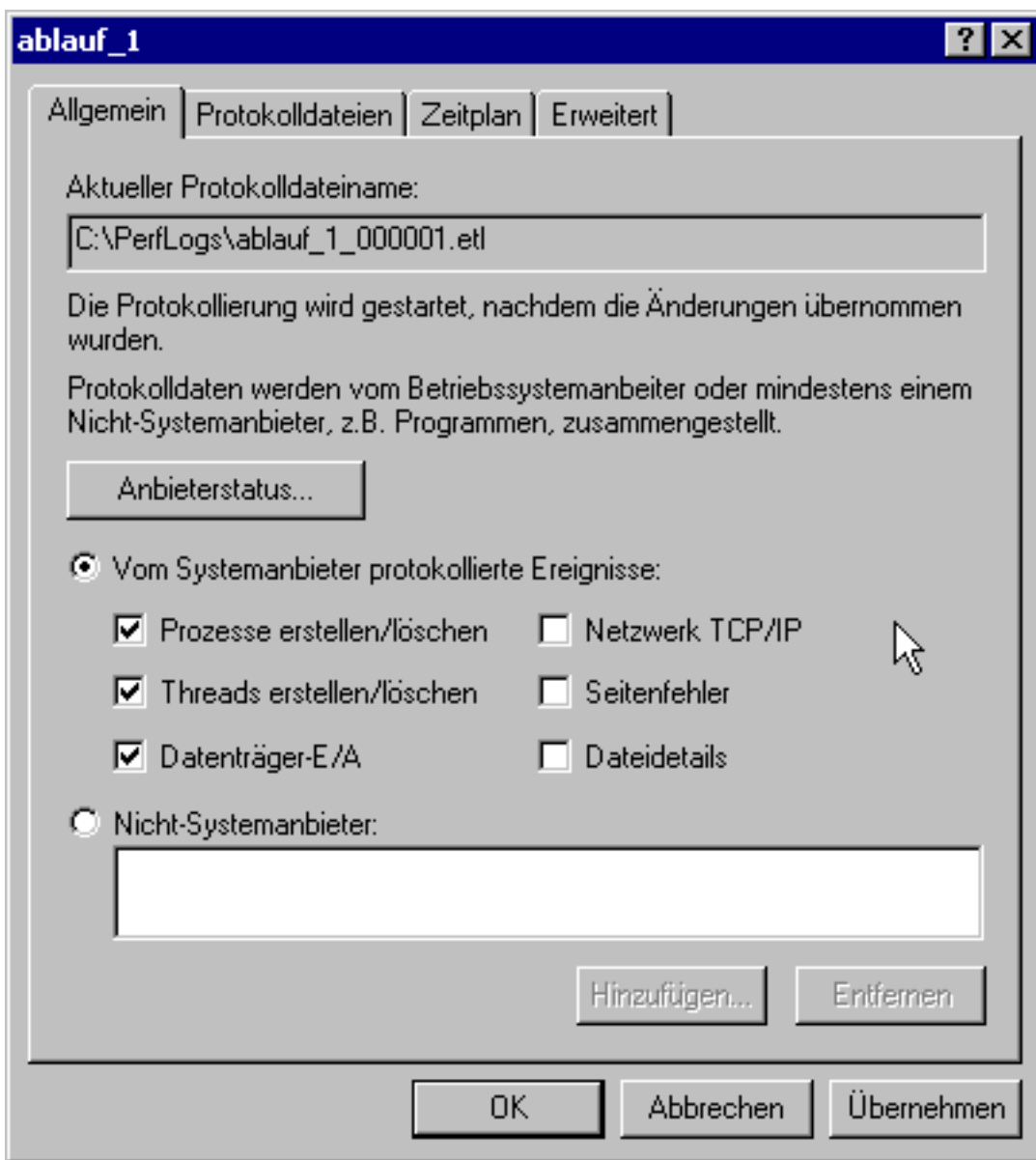


Abbildung 22.48: Der Anbieterbereich in den allgemeinen Eigenschaften

Jetzt klicken Sie auf das Optionsfeld **Vom Systemanbieter protokollierte Ereignisse**, um die entsprechenden Kontrollkästchen zu aktivieren. Diese Optionen können ohne weitere Konsequenzen genutzt werden, mit einer Ausnahme: **Seitenfehler**. Wenn Sie dieses Kontrollkästchen aktivieren, erhalten Sie sofort ein Ablaufverfolgungsprotokoll-Meldungsfeld.

Markieren Sie das Kontrollkästchen in diesem Meldungsfeld nur dann, wenn Sie sicher sind, dass diese Meldung nie mehr erscheinen soll. Andernfalls klicken Sie einfach auf **OK**, um das Meldungsfeld zu verlassen. Nachdem Sie alle Einträge vorgenommen haben, wechseln Sie zur Registerkarte **Protokolldateien**.

Geben Sie hier den Dateinamen und den Dateityp bzw. die Größe an. Diese Registerkarte ist identisch mit derjenigen, die Sie bei der Änderung der Eigenschaften Ihrer Leistungsindikatorenprotokolle kennen gelernt haben. Sie sollten also auch hiermit kein Problem haben. Beachten Sie, dass Sie die Protokolldateien an einer beliebigen Stelle ablegen können, auch auf anderen Computern im Netzwerk, wodurch sich die Überwachung etwas einfacher handhaben lässt. Nachdem Sie Ihre Einträge vorgenommen haben, wechseln Sie zur Registerkarte **Zeitplan**.

Wie auf der Registerkarte **Zeitplan** bei den Leistungsindikatorprotokollen geben Sie hier einfach die Uhrzeit und das Datum an, wann das Protokoll beginnen und enden soll. Diese Einstellungen setzen voraus, dass Sie das Starten und Beenden manuell nur auf dem lokalen Server und nicht über eine Netzwerkfreigabe vornehmen. Nachdem Sie Ihre Einträge vorgenommen haben, wechseln Sie zur in Abbildung 22.49 gezeigten Registerkarte **Erweitert**.

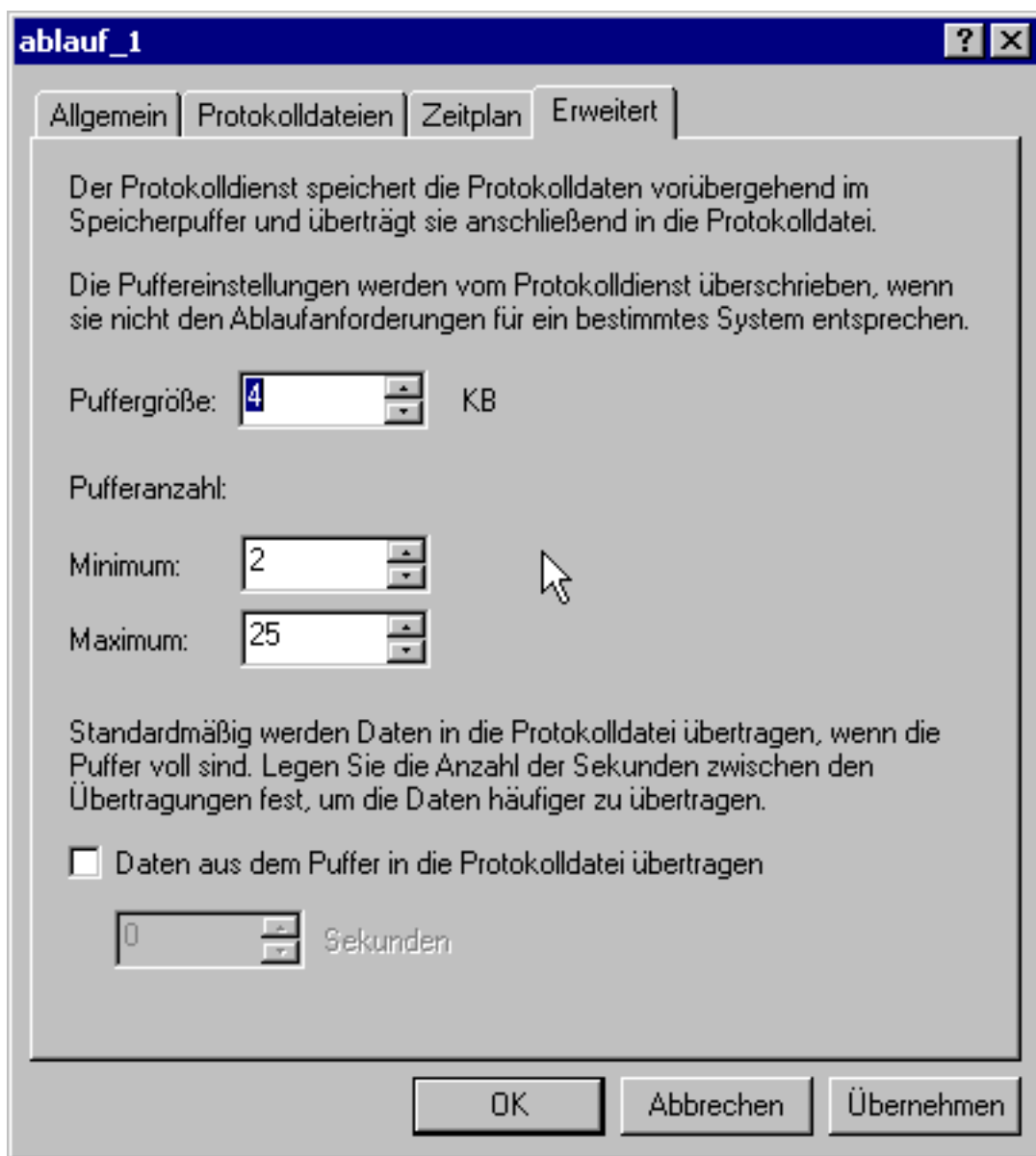


Abbildung 22.49: Erweiterte Konfigurationsoptionen für die Datenaufzeichnung eines Ablaufverfolgungsprotokolls

Auf der Registerkarte **Erweitert** ändern Sie die Speicherpuffer ab, um damit eine optimale Leistung für Ihr Ablaufverfolgungsprotokoll zu erzielen. Nachdem Sie Ihre Änderungen vorgenommen haben, klicken Sie auf die Schaltfläche **OK**, um den Hauptbildschirm für die Systemleistung anzuzeigen, wie in Abbildung 22.50 gezeigt.

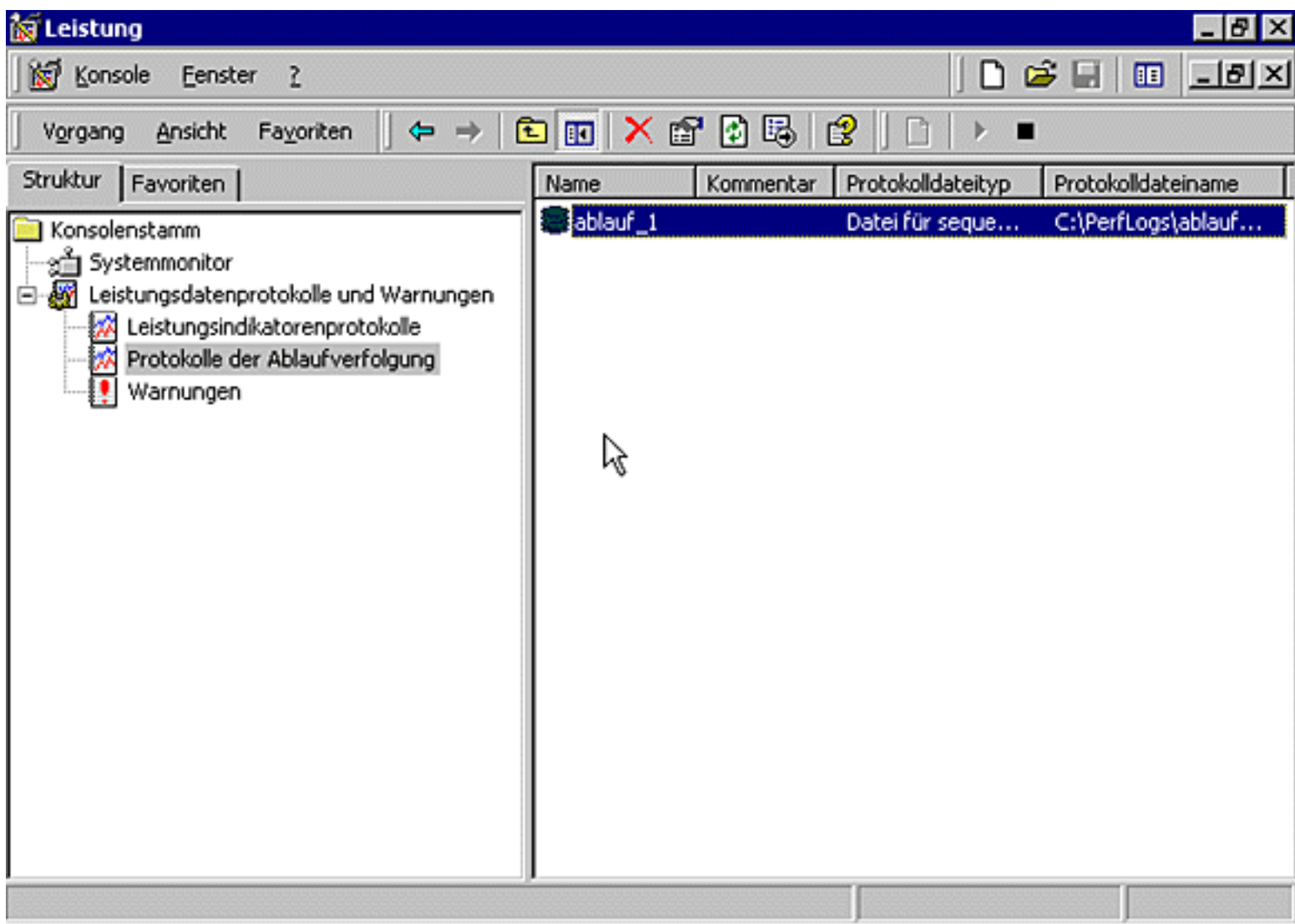


Abbildung 22.50: Anzeige des neu angelegten Ablaufverfolgungsprotokolls im Hauptbildschirm der Leistung

Nachdem Sie zum Hauptbildschirm der Leistung zurückgekehrt sind, sehen Sie, dass ein neues Ablaufverfolgungsprotokoll angelegt wurde. Um die Protokollierung sofort zu starten, ohne auf die festgelegte Startzeit zu warten, klicken Sie mit der rechten Maustaste auf den Protokollnamen und wählen im Kontextmenü die Option **Starten** aus. Das neu angelegte Ablaufverfolgungsprotokoll wechselt die Farbe von Rot nach Grün.

Jetzt legen Sie noch eine Warnung an. Auch dafür gibt es keine Beispieldatei, aus der Sie lernen könnten. Klicken Sie also mit der rechten Maustaste auf das Symbol **Warnungen** im linken Bereich des Bildschirms. Ein Kontextmenü wird geöffnet, ähnlich wie bei der Arbeit mit Leistungs- und Ablaufverfolgungsprotokollen.

Klicken Sie oben in diesem Menü auf den Eintrag **Neue Warnungseinstellungen**. Geben Sie im daraufhin geöffneten Dialogfeld den Namen für Ihre neue Warnungsdatei an und klicken Sie anschließend auf **OK**. Das in Abbildung 22.51 gezeigte Dialogfeld erscheint.

warnungen_123 [?] [X]

Allgemein | Vorgang | Zeitplan

Die Warnungssuche wird gestartet, nachdem die Änderungen übernommen wurden.

Kommentar:

Leistungsindikatoren:

Warnung bei Wert: [] Limit: []

[Hinzufügen...] [Entfernen]

Daten erfassen jeden:

Intervall: [5] Einheiten: [Sekunden]

[OK] [Abbrechen] [Übernehmen]

Abbildung 22.51: Konfiguration der allgemeinen Warnungsoptionen

Auf der Registerkarte **Allgemein** fügen Sie einen Kommentar ein, der die neue Warnung beschreibt. Wählen Sie mindestens einen Leistungsindikator aus. Andernfalls wird eine Fehlermeldung angezeigt, sobald Sie versuchen, zur Registerkarte *Vorgang* zu wechseln. In dieser Fehlermeldung werden Sie darauf hingewiesen, dass Sie mindestens einen zu überwachenden Leistungsindikator einfügen müssen.

Klicken Sie auf **OK**, um auf die Registerkarte **Allgemein** zurückzugelangen und dort einen Leistungsindikator anzulegen. Darüber hinaus müssen Sie eine Begrenzung für die angelegten Warnungen einrichten, die abhängig von den verwendeten Leistungsindikatoren variiert. Nehmen Sie alle Einträge vor, sodass mindestens alle in Abbildung 22.52 gezeigten Variablen abgedeckt sind.

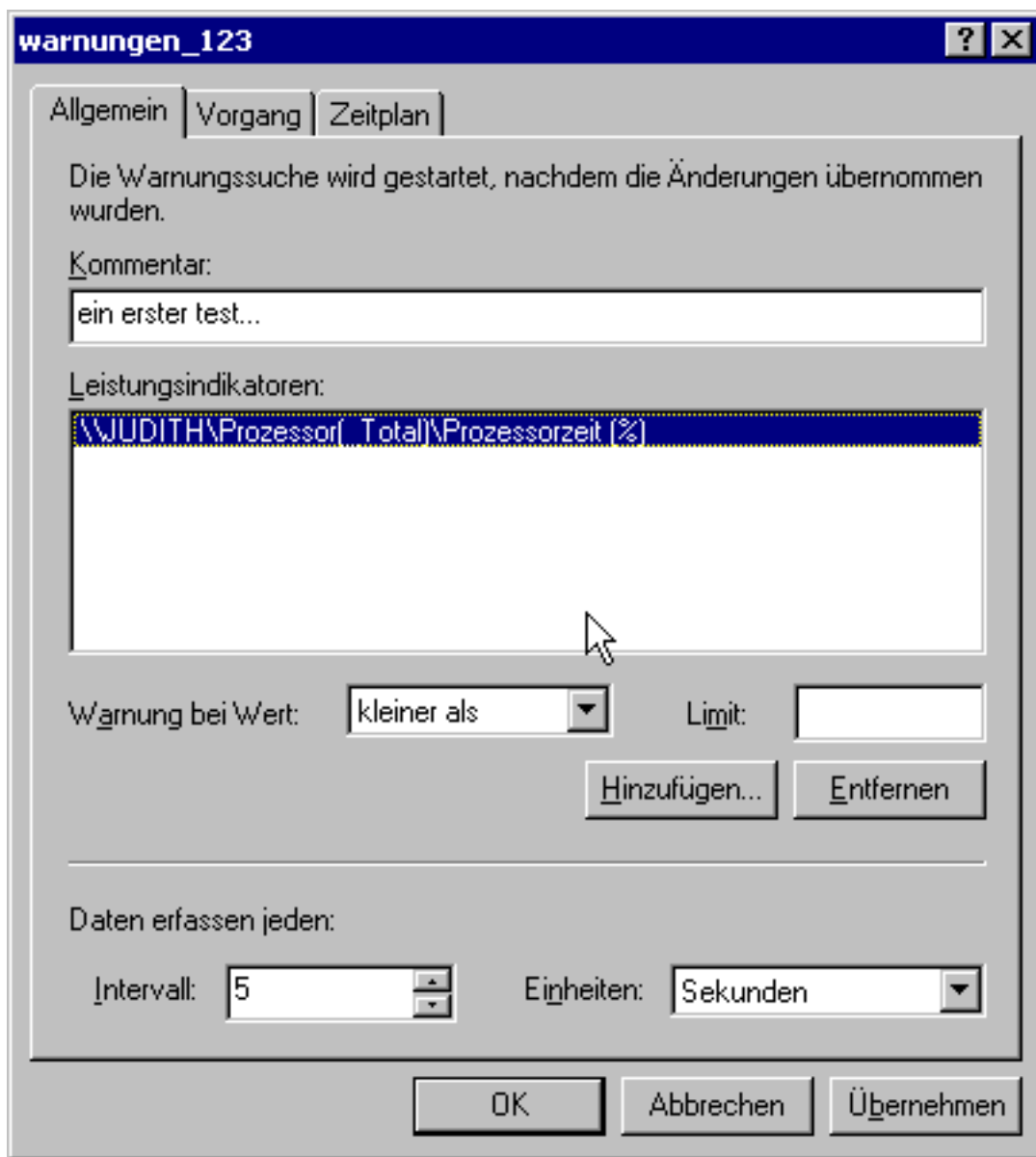


Abbildung 22.52: Überprüfen der Einträge für die Warnungen

Nachdem Sie Ihre Änderungen vervollständigt haben, wechseln Sie zur Registerkarte **Vorgang** (siehe Abbildung 22.53).

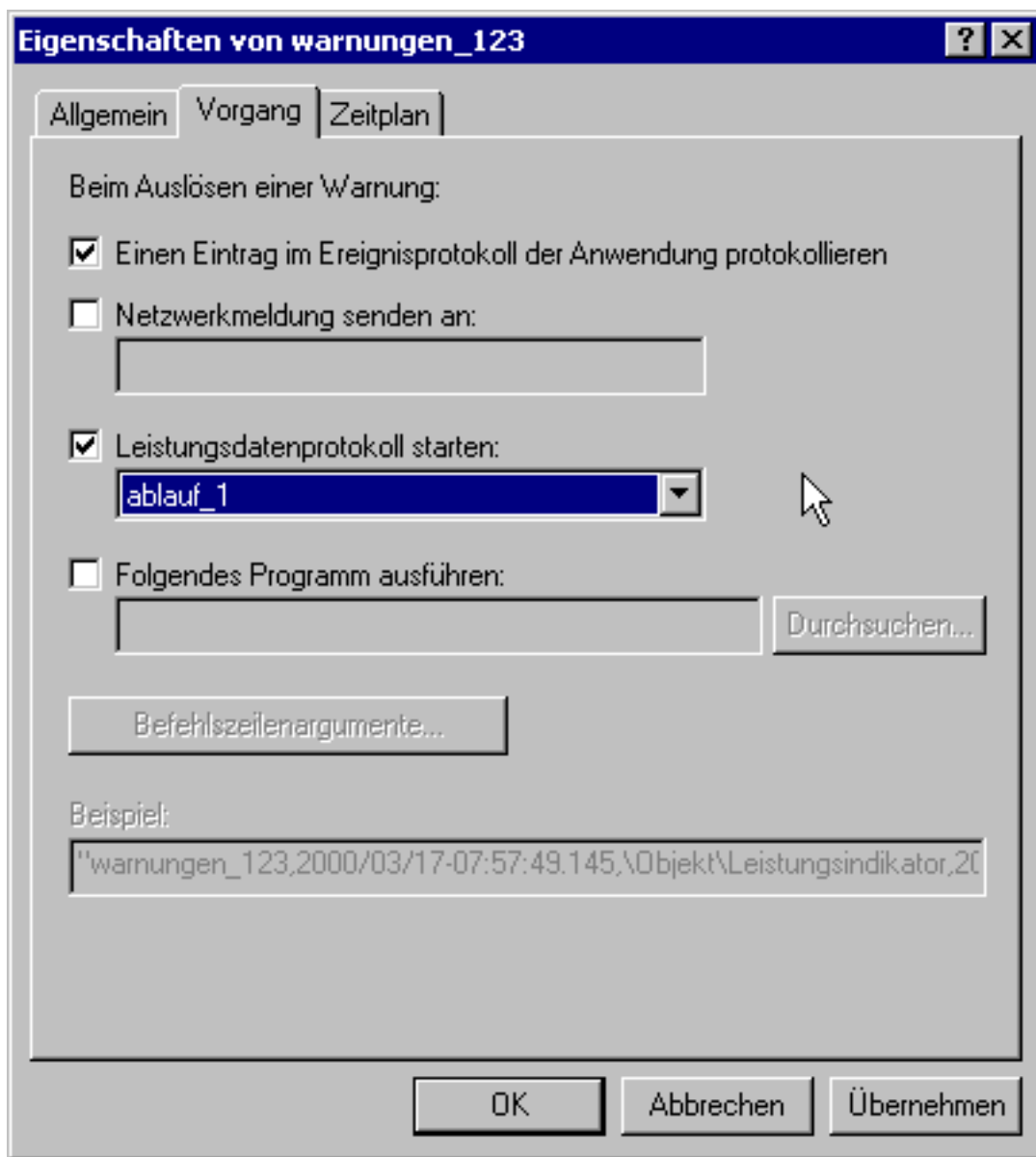


Abbildung 22.53: Einrichtung der Warnungsvorgänge

Auf der Registerkarte *Vorgang* weisen Sie das System an, wie es auf bestimmte Ausfälle reagieren soll. Sie könnten dazu das Dropdown-Listefeld *Leistungsdatenprotokoll starten* nutzen. Dort legen Sie eine bestimmte Protokolldatei für diese Warnung fest. Nachdem Sie Ihre Einträge vorgenommen haben, wechseln Sie zur Registerkarte **Zeitplan** (siehe Abbildung 22.54).

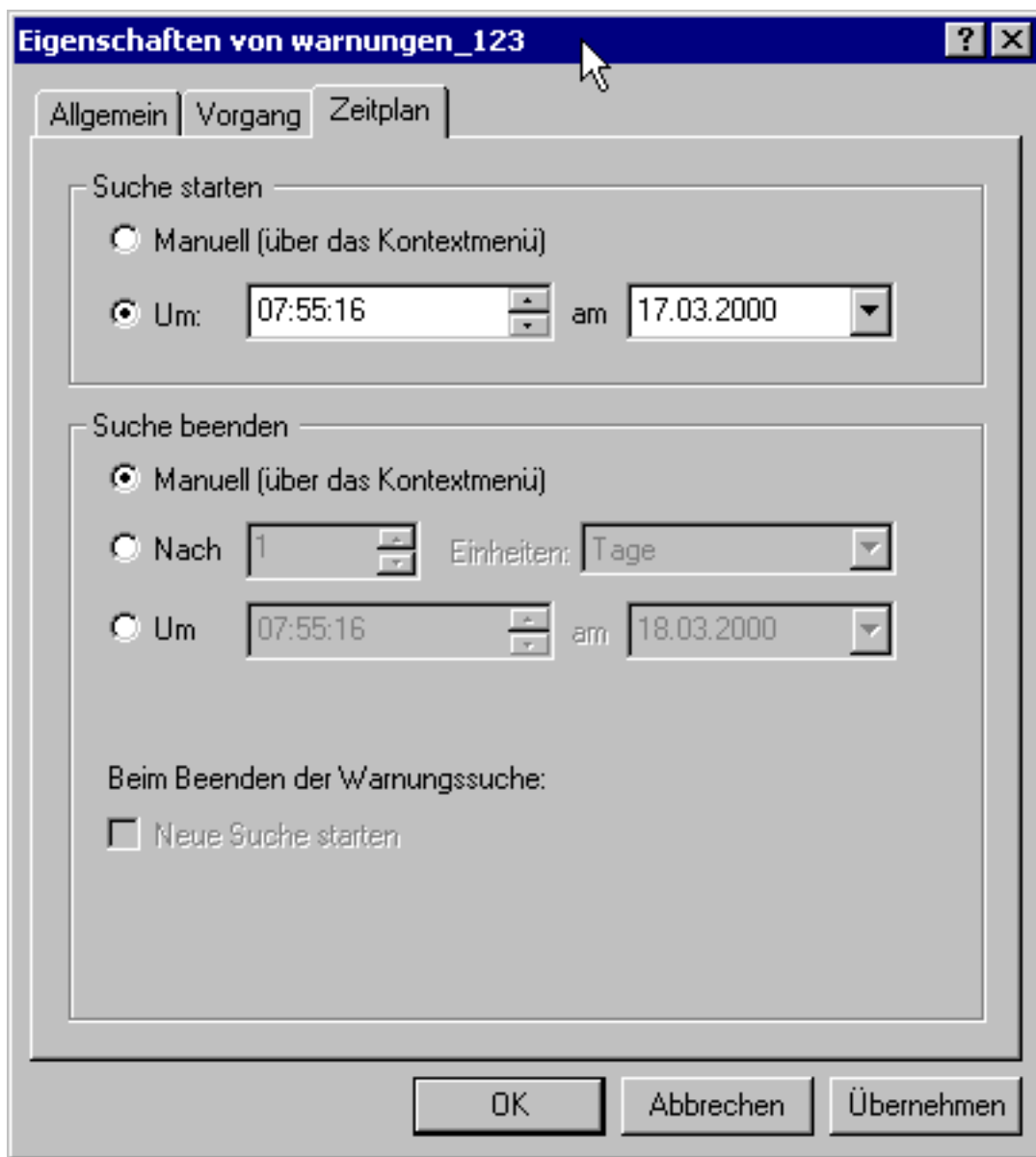


Abbildung 22.54: Zeitplanung der Anfangs- und Endezeiten für die Aufzeichnung Ihrer Warnungen

Wie auf der zuvor gezeigten Registerkarte **Zeitplan** legen Sie die Uhrzeit und das Datum fest, wann das Protokoll gestartet bzw. beendet werden soll. Diese Einstellungen setzen voraus, dass Sie das Starten und das Beenden manuell auf Ihrem lokalen Server und nicht über eine Netzwerkfreigabe ausführen. Nachdem Sie Ihre Einträge vorgenommen haben, klicken Sie auf die Schaltfläche **OK**, um auf den Hauptbildschirm der Systemleistung zurückzukehren (siehe Abbildung 22.55).

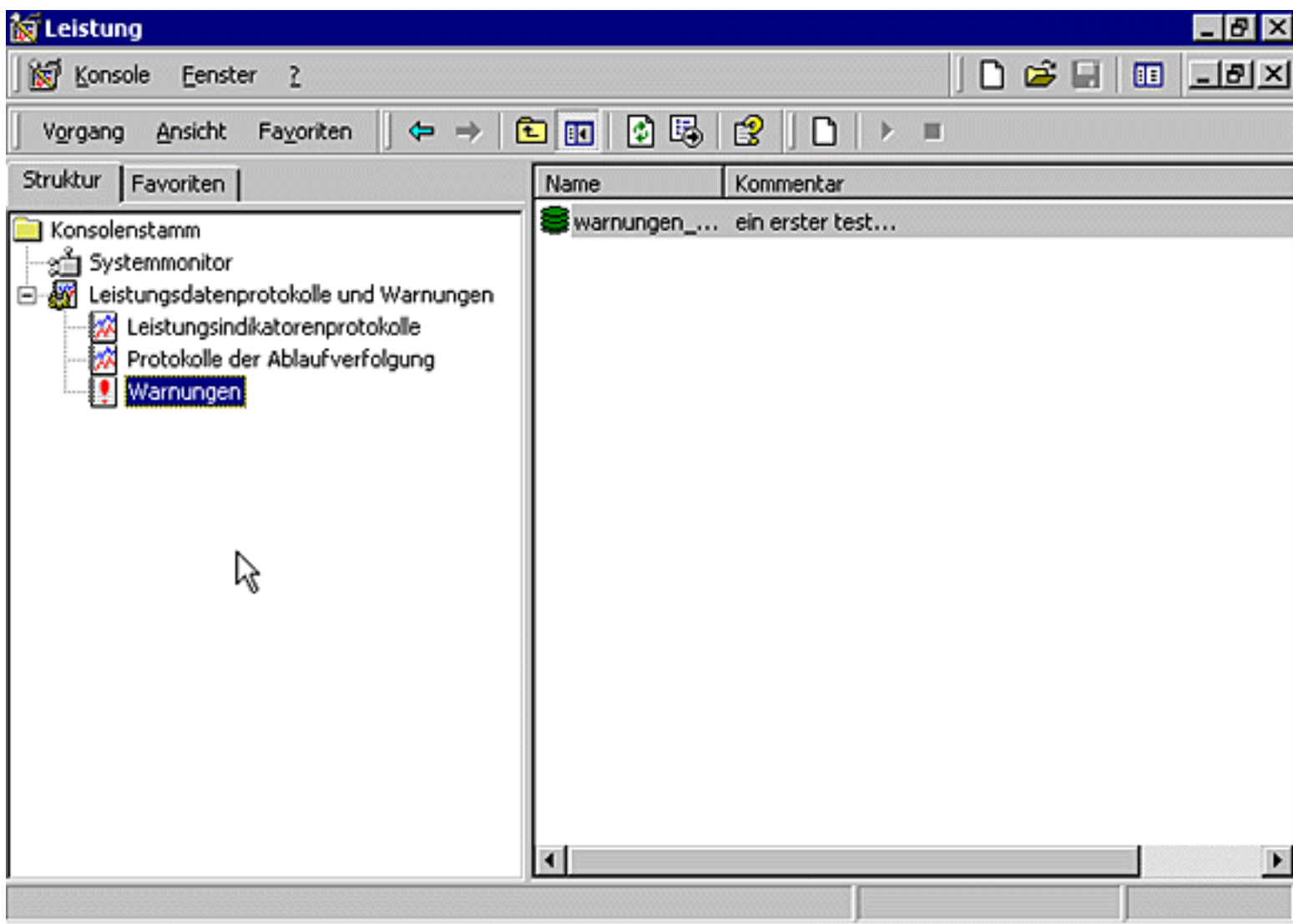


Abbildung 22.55: Anzeige Ihrer neu angelegten Warnungen im Hauptbildschirm der Systemleistung

Nachdem Sie auf dem Hauptbildschirm der Leistung zurück sind, sehen Sie Ihre neue Windows 2000-Warnung. Um die Warnung sofort nutzen zu können, ohne auf die vorgegebene Startzeit zu warten, klicken Sie mit der rechten Maustaste auf die Warnung und wählen im Kontextmenü die Option **Starten**. Das Symbol für die Warnung wechselt die Farbe von Rot nach Grün.

Das ist alles. Auf diese Weise realisieren Sie eine effektive Leistungsüberwachung und Ablaufverfolgung.

Kapitel 23 Dienstprogramme zur Sicherung des Servers

Das Dienstprogramm *Sicherung* im Windows 2000 Server kann eine der wichtigsten neuen Funktionen des neuen Betriebssystems von Microsoft für Sie werden, wenn Sie es ihm erlauben. Zahllose Unternehmen besitzen keine formalen Sicherungsstrategien, ganz zu schweigen von formalen Betriebsstrategien für Abteilungsserver und andere kleinere server-basierte Implementierungen. Viele Unternehmen glauben sogar, dass die Server außerhalb des Rechenzentrums einfach ersetzbar sind und damit nicht in die unternehmensübergreifenden Sicherungs- und Wiederherstellungsdienste einbezogen werden müssen, die die Rechenzentren in der Regel anbieten. Häufig führt dieses Verhalten irgendwann zur Katastrophe, nämlich sobald ein Server im Unternehmen ausfällt und es keine Möglichkeit gibt, die Daten wiederherzustellen.

In früheren Versionen von Windows NT gab es im Betriebssystem eine Funktion zum Sichern und Wiederherstellen. Damit wurde eine grundlegende Methode bereitgestellt, Geschäftsdaten auf einfache Weise zu sichern und wiederherzustellen. Der Begriff »schnell« trifft auf diesen Prozess nicht zu. Aufgrund der enormen Verbesserungen im Technologiebereich der Sicherungsgeräte und durch die Kombination mit einigen Aktualisierungen des Dienstprogramms *Sicherung* wurden diese Unzulänglichkeiten des alten Sicherungsprogramms von Windows NT Server aber häufig erst erkannt, als es zu spät war (während eines mehrtägigen Wiederherstellungsprozesses oder beim Versuch, die Registrierungseinträge eines Servers vollständig wiederherzustellen). In dieser Version von Windows 2000 Server wurden viele Mängel der alten Version behoben und durch die Implementierung einer Wiederherstellungskonsole, eines abgesicherten Modus, eines Reparaturprozesses für den Notfall usw. erweitert.

Windows 2000 stellt sein neues Sicherungswerkzeug in Form von Version 5.0 des Sicherungsprogramms von Microsoft Windows an. Es wurde von Veritas Software Corporation lizenziert und arbeitet ähnlich den älteren Versionen in Windows NT. Sie finden diese Software im Startmenü unter *Programme/Zubehör/Systemprogramme/Sicherung*. Nach dem Aufruf sehen Sie den Startbildschirm des Sicherungsprogramms von Microsoft Windows. Hier können Sie auf die meisten Funktionen und Optionen des Sicherheitsprotokolls zugreifen (natürlich steht auf der grafischen Benutzeroberfläche keine Eingabeaufforderung zur Verfügung). Die korrekte Nutzung des Sicherungsprogramms von Microsoft Windows verringert das Risiko nicht mehr wiederherstellbarer Daten erheblich.

In jedem Unternehmen besteht immer ein gewisses Risiko, Daten zu verlieren, weil nicht immer alles unter Kontrolle sein kann. Beispielsweise können Daten bei Naturkatastrophen (Hochwasser, Taifune, Erdbeben, Vulkanausbrüche, Sturmfluten, Tornados usw.) oder zivilen Katastrophen (Bürgerkriege, Kriege, Atomkriege, Feuer usw.) verloren gehen. Ein Datenverlust kann in einer Windows 2000 Server-Umgebung nie vollständig ausgeschlossen werden, weil es die unterschiedlichsten Ereignisse gibt, gegen die sich auch das mächtigste Unternehmen nicht schützen kann, selbst wenn es noch so gut vorbereitet ist.



Bevor wir genauer auf das Sicherungsprogramm von Microsoft Windows eingehen und Sie Ihre Sicherungslösung implementieren, sollten Sie einige organisatorische Dinge kennen lernen. Unter anderem handelt es sich um Folgendes:

- Planung von Sicherungsstrategien - Diese Planung sollte eine vollständige Strategie nicht nur für die Sicherung und Wiederherstellung der Unternehmensdaten beinhalten, sondern auch Maßnahmen für die Wiederherstellung nach einem Katastrophenfall.
- Rotationsschema für Sicherungsbänder/platten - Sie sollten unbedingt mehrere Sicherheitskopien der Daten anlegen, die für den Betrieb Ihres Unternehmens relevant sind (eine Liste dieser Daten sollte im Rahmen der Sicherungsstrategien angelegt werden). Unter anderem muss dabei berücksichtigt werden, wo diese Datenträger außerhalb des Unternehmens aufbewahrt werden. (Wenn Sie nur in einer kleinen Umgebung arbeiten, könnten beispielsweise einige der Angestellten die Daten eines Tages täglich mit nach Hause nehmen.)
- Sicherheit - Ein Sicherungsband enthält die wichtigsten Ressourcen eines Unternehmens: seine Daten. Achten Sie darauf, dass diese Bänder nicht in die falschen Hände geraten, insbesondere in die Ihrer Konkurrenten. Außerdem sollten Sie diese Datenträger vor Diebstahl oder Beschädigung schützen.
- Sicherungsprotokolle - Sie sollten Ihre Sicherungsaktivitäten unbedingt protokollieren. Andernfalls zerstören Sie bei

der Wiederherstellung von Daten womöglich mehr, als Sie retten können.

- Schulung der Angestellten - Die EDV-Mannschaft Ihres Unternehmens muss in Hinblick auf die Sicherungsprozesse und -prozeduren sowie die Wiederherstellung sinnvoll geschult werden. Ein unzureichend geschulter Systemoperator kann die Datenstruktur Ihres Unternehmens schlimmer beschädigen als die meisten anderen Katastrophen. Wenn der Administrator XYZ beispielsweise eine ältere Version einer eCommerce-Datenbank wiederherstellt und das mehrere Stunden lang nicht bemerkt wird, könnte die Datenbankstruktur in Ihrem Unternehmen ganz schnell hoffnungslos zerstört werden.
- Pflichtenteilung - Wenn nur eine einzige Person in Ihrem Unternehmen (beispielsweise der Systemadministrator) die Befähigung besitzt, Sicherungen und Wiederherstellungen vorzunehmen, dann besteht das Risiko eines einzigen Ausfallpunkts in der Infrastruktur. Wenn Sie mit dieser Person Ärger bekommen oder sie einfach nicht mehr in der Lage ist, ihre Arbeit auszuführen, besteht die Gefahr, dass das System ausfällt und keinerlei Wiederherstellung mehr möglich ist.
- Sicherung von Verzeichnisdiensten - Sie sollten eine vollständige Sicherung des Windows 2000 Server Active Directory von einem Windows 2000-Domänencontroller anlegen. Wird diese Sicherung nicht von einem Domänencontroller aus ausgeführt, gehen die Benutzerkonteninformationen sowie andere persistente Sicherheitsinformationen verloren.
- Vollständige oder partielle Sicherungen - Für eine Systemwiederherstellung ist es immer effizienter, den gesamten Systemdatenträger als Ganzes zu sichern, statt inkrementelle oder differenzielle Sicherungen vorzunehmen. Für den Zeitaufwand gilt natürlich das Gegenteil. Sie sollten ein bisschen experimentieren, um die effektivste Methode für Ihr Unternehmen herauszufinden. Viele Unternehmen stellen fest, dass es ab einer bestimmten Größe nicht mehr sinnvoll ist, täglich vollständige Sicherungen vorzunehmen, deshalb legen sie inkrementelle/differenzielle Sicherungen an. Das hat einen wesentlichen Einfluss auf die Wiederherstellung im Fehlerfall, deshalb sollten Sie diesen Aspekt während der Planungsphase mit größter Sorgfalt berücksichtigen.
- Testen, testen, testen - Sicherungsbänder, die nicht wiederhergestellt werden können, sind für das Unternehmen völlig unbrauchbar. Aus diesem Grund sollten Sie sicherstellen, dass die von Ihnen erstellten Sicherungsbänder zur Wiederherstellung Ihrer Daten genutzt werden können. Die einzige Methode dafür ist, immer wieder eine Wiederherstellung von den Bändern vorzunehmen, um sich davon zu überzeugen, dass es funktioniert.
- Dokumentation - Dieses Thema ist zwar unerfreulich, aber Sie sollten den Sicherungs- und Wiederherstellungsprozess Ihres Unternehmens sorgfältig und gewissenhaft dokumentieren, sodass jeder anhand dieser Beschreibung eine Wiederherstellung der Daten auf dem Server vornehmen kann. Sie sollten natürlich die sensiblen Informationen, wie beispielsweise die IDs und Kennwörter der Sicherungs-Operatoren/Administratoren an sicherer Stelle aufbewahren, sodass niemand unberechtigt auf die Daten des Unternehmens zugreifen kann. Die wichtigste Aufgabe dieser Dokumentation ist es, den Betrieb aufrechtzuerhalten, falls die wichtigsten Angestellten aufgrund irgendeines Umstandes ausfallen.

Nachdem Sie die administrativen und betriebsbedingten Planungsprozesse und Prozeduren kennen gelernt haben, sollten Sie sich auf die eigentliche Sicherung und Wiederherstellung vorbereiten. Dazu stellen Sie zunächst sicher, dass Ihre Sicherungs-/Wiederherstellungs-Operatoren die korrekten Berechtigungen und Rechte für ihre Aufgaben haben, und dass diese Personen die Sicherung von den richtigen Positionen aus ausführen.

23.1 Operatorberechtigungen für das Sicherungsprogramm von Windows 2000 Server

Viele Unternehmen versäumen diesen wichtigen Schritt - die Zuteilung der richtigen Berechtigungen an diejenigen Personen, die für die Sicherungs- und Wiederherstellungsprozeduren der für den Betrieb relevanten Server und der organisatorischen Datenstrukturen zuständig sind. In der Betriebsumgebung von Windows 2000 Server können nur diejenigen Personen Dateien und Ordner auf dem Server sichern, die entweder Systemadministrator sind oder deren Benutzerkonten Mitglieder der Administratoren- oder Sicherungs-Operatoren-Gruppe sind.

Die Berechtigungs- und Sicherheitsebenen für Administratoren sind ganz einfach: Administratoren sind in der IT-Welt allmächtig. Es gibt nichts, was sie nicht erfahren oder beeinflussen könnten (das bedeutet natürlich nicht, dass sie alles erfahren oder beeinflussen wollen). Die Rechte und Berechtigungen der Windows 2000 Server-Gruppe Sicherungs-Operatoren dagegen sind etwas ganz anderes. Beispielsweise kann jemand, der Mitglied dieser Gruppe ist, alle

Dateien oder Ordner auf dem Windows 2000-Server sichern oder wiederherstellen, unabhängig von allen vorherigen Berechtigungen oder Verschlüsselungen, durch die diese Datei oder der Ordner momentan geschützt werden. Sie können jedoch keine bereits bestehenden Berechtigungen ändern.

Ein weiterer, relativ sensibler Aspekt der Gruppe Sicherungs-Operatoren besteht darin, dass sich die Mitglieder dieser Gruppe nicht nur am Windows 2000-Server anmelden, sondern ihn auch nach Belieben herunterfahren können. Das allein kann in einer E-Kommerz-Welt beängstigend sein, in der 99,99 Prozent Präsenz des Servers den Verlust von Millionenverkäufen bedingen, wenn dieses 0,01 Prozent Ausfallzeit auftritt. Aus diesem Grund sollten Sie die Mitgliedschaft bei der Gruppe Sicherungs-Operatoren sehr bewusst handhaben und sie ähnlich beschränken wie die Administratorengruppe.

Noch ein Wort: Um die Systemstatusdaten für einen Windows 2000'-Server zu sichern, müssen Sie den Sicherungsprozess lokal ausführen. Sie können also diese wichtigen Systemdaten nicht remote sichern, beispielsweise über das Unternehmensnetzwerk. Wenn Sie eine vollständige Wiederherstellung eines Windows 2000-Servers vornehmen müssen (beispielsweise nach einem Festplattencrash), brauchen Sie dazu unbedingt die Systemstatusdaten für diesen Server.

Der Windows 2000 Server-Ausdruck Systemstatusdaten wurde von Microsoft als Name für die Gruppe eingeführt, die die Registrierung, die COM+-Klassenregistrierungsdatenbank, die Systembootdateien, die Zertifikatdienstdatenbank (falls der Zertifizierungsserver auf diesem Windows 2000-Server installiert ist), den Active Directory-Verzeichnisdienst und das Verzeichnis SYSVOL enthält (die beiden letzteren finden Sie nur auf Windows 2000-Servern, die als Domänencontroller eingesetzt werden).



23.2 Sicherung von Windows 2000

Bevor Sie die Sicherung beginnen, sollten Sie noch eine Entscheidung in Bezug auf die Sicherung treffen. Sie müssen entscheiden, welche Sicherung Sie vornehmen wollen. Die Sicherung von Microsoft Windows unterstützt fünf verschiedene Sicherungsarten, die hier in alphabetischer Reihenfolge beschrieben werden:

- Differenzielle Sicherung - Dieses Sicherungsschema erlaubt Ihnen, alle Dateien oder Ordner zu sichern, die seit der letzten inkrementellen oder normalen Sicherungssitzung angelegt oder verändert wurden. Viele Unternehmen verwenden in ihrer Sicherungsstrategie eine Kombination aus differenzieller, inkrementeller und täglicher oder normaler Sicherung. Das ist eine gebräuchliche Sicherungsmethode, weil der Zeitaufwand für die Wiederherstellung viel geringer ist als für die Kombination aus normaler und inkrementeller Sicherung, weil dabei weniger Bänder oder Platten benötigt werden. Das Sicherungsschema normal/differenziell dagegen bedeutet einen höheren Zeitaufwand als ein normaler/inkrementeller Sicherungsprozess.
- Inkrementelle Sicherung - Dieser Sicherungstyp scheint attraktiv, weil er den Zeitaufwand für die Sicherung wesentlich verkürzt, aber beachten Sie, dass Sie normale Sicherungsbänder und alle inkrementellen Sicherungsbänder brauchen, wenn Sie Ihr System korrekt wiederherstellen wollen. Inkrementelle Sicherungen markieren Ihre Dateien, dass diese gesichert wurden.
- Kopie-Sicherung - Das ist praktisch, wenn Sie bestimmte Dateien vom Windows 2000-Server auf ein Sicherungsgerät (Band, Platte usw.) kopieren wollen, ohne das Archivattribut für diese Dateien zu löschen.
- Normale Sicherung - Dieser Sicherungsprozess markiert alle Dateien und Ordner mit einem speziellen Attribut als gesichert, woran die anderen Sicherungsarten erkennen, dass diese Datei oder der Ordner bereits gesichert wurden.
- Tägliche Sicherung - Wird verwendet, wenn Sie alle Dateien sichern wollen, die seit der letzten Sicherung irgendwie verändert wurden (geändert, ergänzt usw.). Auch hierbei werden die Dateien nicht als gesichert markiert, was insbesondere für diese nächtlichen Sicherungssitzungen praktisch ist.

Sie finden die Sicherung und Wiederherstellung in Windows im Startmenü unter *Programme/Zubehör/Systemprogramme/Sicherung*.

Wenn Sie Ihren Mauszeiger auf eine Menüoption von Windows 2000 Server platzieren, sehen Sie einen ToolTip zu dieser Option. Beispielsweise sehen Sie auch eine kurze Beschreibung der Option **Sicherung** (der Text im Feld ist »Archiviert Daten, um vor Datenverlust zu schützen«).



Bewegen Sie sich mit Hilfe der oben beschriebenen Menüeinträge zum Sicherungswerkzeug von Windows 2000 Server. Den Eröffnungsbildschirm sehen Sie in Abbildung 23.1.

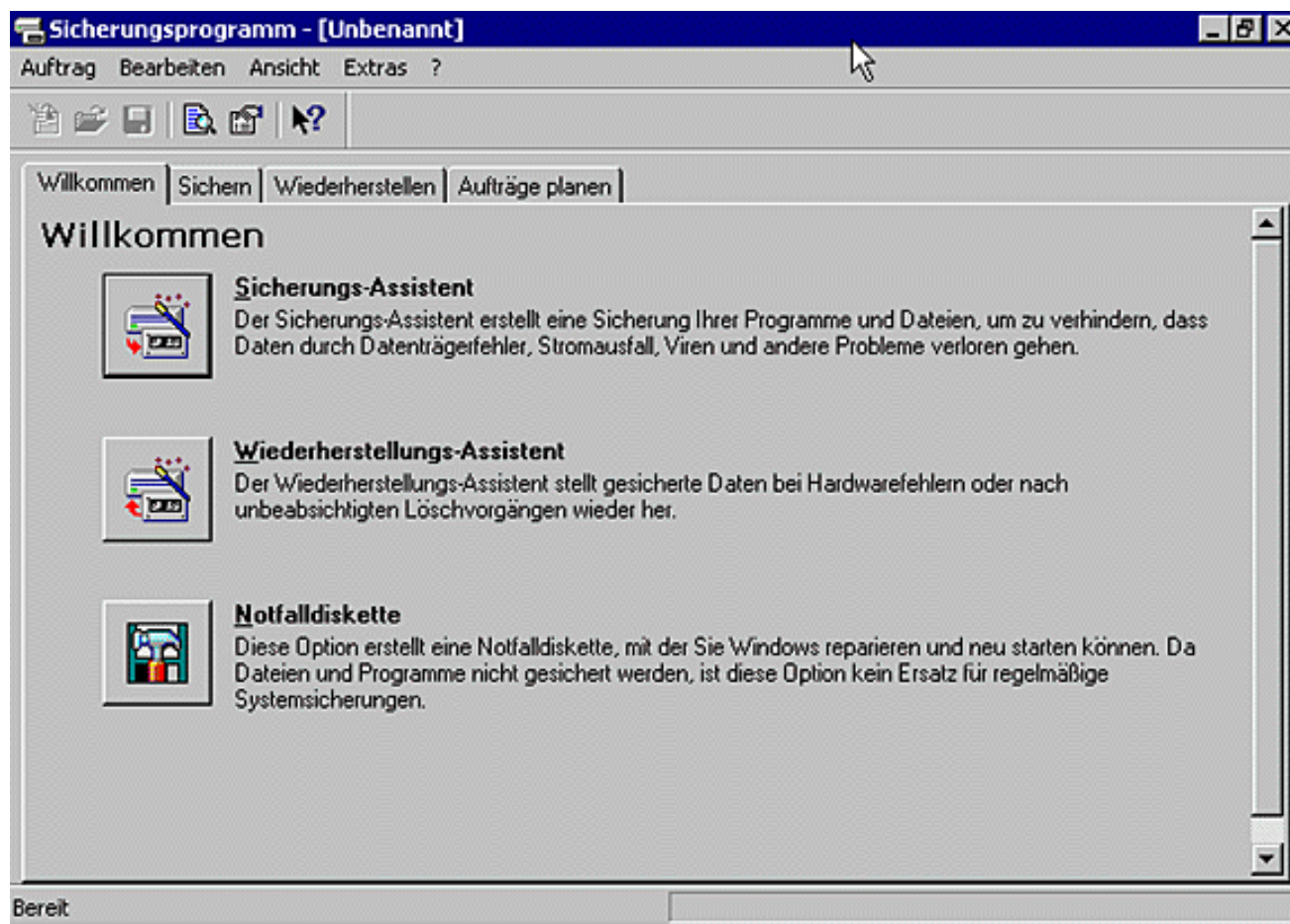


Abbildung 23.1: Hauptfenster von Windows 2000 Sicherung

Als Erstes sollten Sie die Variablen definieren, die genau angeben, wie die Sicherung und die Wiederherstellung für Ihr System ausgeführt werden sollen. Dazu wechseln Sie zum Dialogfeld **Optionen**, in dem Sie alle Attribute für die Sicherung und Wiederherstellung festlegen können. Wählen Sie dazu den Menübefehl **Extras/Optionen**, um das in Abbildung 23.2 gezeigte Dialogfeld aufzurufen.

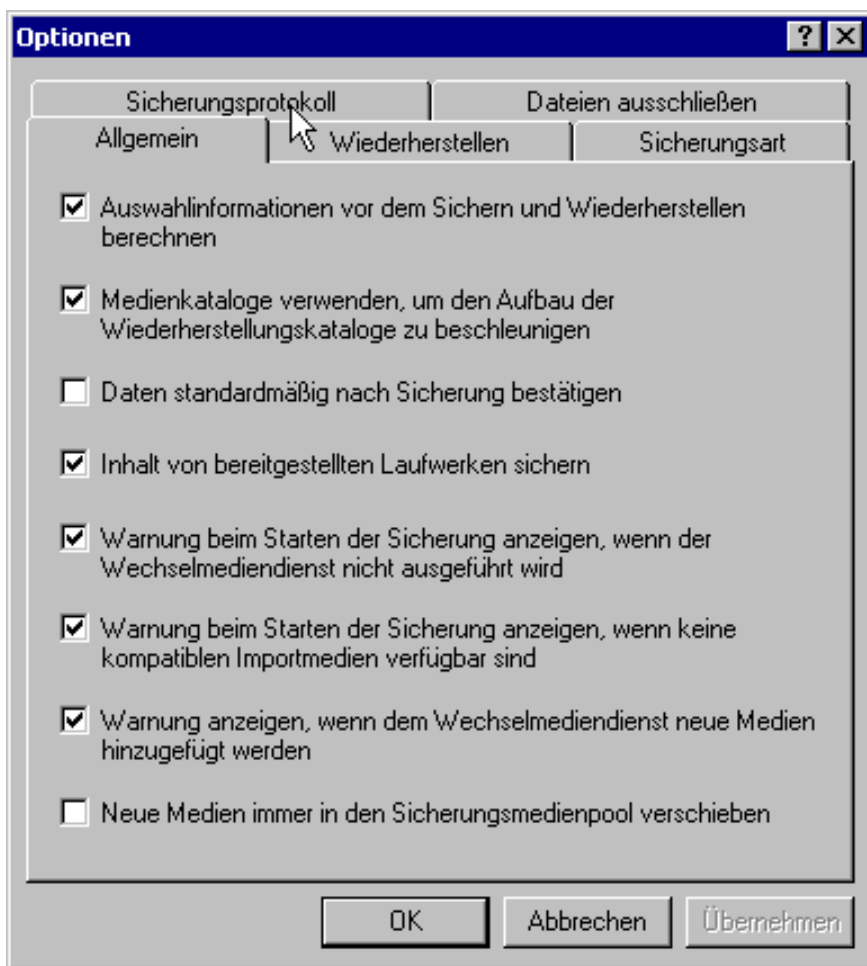


Abbildung 23.2: Einrichtung der Sicherungsoptionen

Beim ersten Zugriff auf das Dialogfeld **Optionen** sehen Sie die Vorgaben auf der Registerkarte **Allgemein**. Das bedeutet nicht, dass diese Optionen für Ihr Unternehmen perfekt sind, sie stellen nur eine Auswahl der besten Werte dar. Zwei Optionen werden nicht automatisch gesetzt, die Datenbestätigung und das Importieren neuer Datenträger. Sie sollten vor allem auf die Datenbestätigung achten. Diese Option verlangsamt die Datensicherung jedoch ganz wesentlich und sollte nur dann aktiviert werden, wenn Sie sehr viel Zeit für eine geplante vollständige Sicherung haben.

Alle diese Optionen sind selbsterklärend. Wenn Sie Fragen haben, sollten Sie das Hilfesystem nutzen. Dazu klicken Sie auf die betreffende Option und drücken dann die (F1)-Taste. Ein ToolTip-Feld mit einer kurzen Beschreibung wird angezeigt. Wenn Sie beispielsweise die zweite Option von oben auswählen (**Medienkataloge verwenden, um ...**) und die (F1)-Taste drücken, sehen Sie einen ToolTip. Er teilt Ihnen mit, dass diese Option einen Katalog auf Ihrem Sicherungsdatenträger anlegt, der Ihnen die Möglichkeit gibt, ein defektes System schneller wiederherzustellen, als wenn kein Katalog verwendet wird. Außerdem informiert Sie dieser Tipp darüber, dass das erste Anlegen des Katalogs mehrere Stunden dauern kann, wenn der Sicherungsdatenträger sehr groß ist. Nachdem Sie den ToolTip gelesen haben, klicken Sie irgendwo auf den Bildschirm oder führen mit Ihrer Maus eine andere Funktion aus, sodass der Tipp automatisch verschwindet.

Nachdem Sie alle Optionen auf der Registerkarte **Allgemein** gesetzt haben, wechseln Sie zur Registerkarte **Wiederherstellen** (siehe Abbildung 23.3).

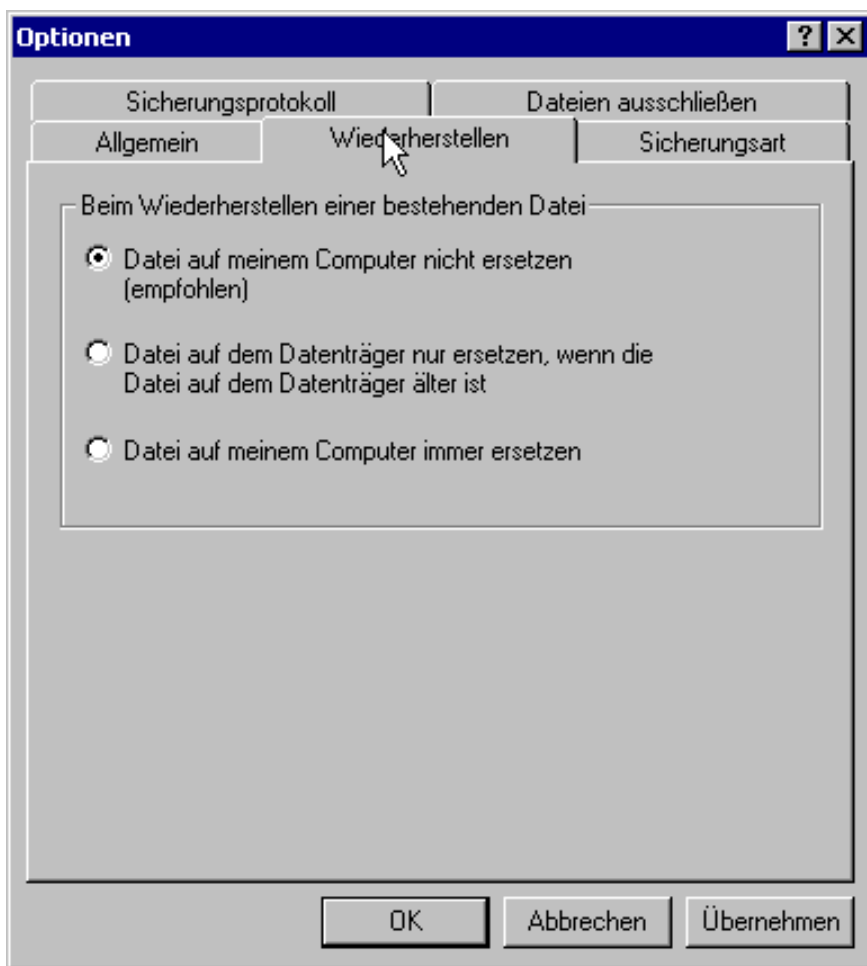


Abbildung 23.3: Optionen für die Wiederherstellung

Das Sicherungssystem von Windows ersetzt standardmäßig keine bereits existierenden Dateien auf Ihrem Computer, was die empfohlene Einstellung ist.

Falls die Datei auf Ihrem Computer bereits installiert ist, ist diejenige auf dem Sicherungsdатenträger vielleicht eine ältere Version derselben Datei. In der Regel wollen Sie diese Datei also nicht ersetzen. Der Autor bevorzugt die Verwendung des mittleren Optionsfeldes: **Datei auf dem Datenträger nur ersetzen, wenn die Datei auf dem Datenträger älter ist**. Für die meisten Unternehmen ist dies die sinnvollste Option. Die letzte Option, **Daten auf meinem Computer immer ersetzen**, ist nur für Lehranstalten sinnvoll. Viele Schulen haben Computerräume, die immer wieder auf eine Standardkonfiguration zurückgesetzt werden sollen, und der Administrator stellt diese Konfiguration in der Regel von einem Sicherungsdатenträger wieder her.

Um die Standardwiederherstellungsmethode für Ihr Unternehmen einzurichten, klicken Sie auf das entsprechende Optionsfeld. Anschließend wechseln Sie zur Registerkarte **Sicherungsart**.

Hier wählen Sie die Standardsicherungsart aus, die bereits früher in diesem Kapitel erklärt wurde. Hier noch einmal die fünf Auswahlmöglichkeiten:

- Kopieren
- Täglich
- Differenziell
- Inkrementell
- Normal

Windows 2000 Server bietet standardmäßig die normale Sicherung an, aber viele Unternehmen verwenden auch die tägliche Sicherung als Standard. Wählen Sie die für Ihr Unternehmen sinnvollste Sicherungsart, indem Sie einmal in das Dropdown-Listenfeld klicken und dann die betreffende Auswahl vornehmen. Damit wird die Sicherungsart oben in das Listenfeld geschrieben und damit zur Standardsicherungsart. Nachdem Sie Ihre Auswahl getroffen haben, wechseln Sie zur

Registerkarte **Sicherungsprotokoll** (siehe Abbildung 23.4).

Hier legen Sie die Sicherungsvorgänge für Ihre Sicherungsaufträge fest. Der schlechteste Fall für die meisten Unternehmen ist die Standardeinstellung **Zusammenfassung**. Bei dieser Einstellung wird eine Art Ereignisprotokoll für Ihre Sicherung angefertigt. Das bedeutet, Sie erhalten nicht eine Liste der gesicherten Dateien und Ordner, sondern für jedes Sicherungsereignis eine Zeile, beispielsweise für das Starten des Auftrags, für das Beenden des Auftrags, für das Laden des Bandes, für das Entladen des Bandes usw. Wenn Sie die Zeit und den Platz für eine detaillierte Protokollierung haben, sollten Sie sie in jedem Fall durchführen. Eine detaillierte Liste bietet Ihnen die Möglichkeit zu kontrollieren, welche Dateien und Ordner gesichert und welche Sicherungsereignisoptionen dafür verwendet wurden. Die letzte Auswahl **Keine** bedeutet, dass Ihre Sicherung nicht protokolliert wird. Nachdem Sie Ihre Auswahl getroffen haben, wechseln Sie zur Registerkarte **Dateien ausschließen** (siehe Abbildung 23.5).



Abbildung 23.4: Auswahl der Protokollierungsebene



Abbildung 23.5: Festlegen der Dateien, die bei der Sicherung auszuschließen sind

Auf der Registerkarte **Dateien ausschließen** kann der Sicherungs-Operator festlegen, dass bestimmte Dateitypen bei der Sicherung des Windows 2000-Servers nicht berücksichtigt werden sollen. Beispielsweise wollen Sie sehr wahrscheinlich nicht die Datei mit den Aufzeichnungen über den Energiesparmodus oder die Auslagerungsdatei von Windows 2000 sichern, weil das zwei sehr große Dateien sind, deren Wiederherstellung nichts mit der korrekten Arbeitsweise Ihres Computers zu tun hat (Windows 2000 Server legt diese Dateien automatisch wieder an, es gibt also keinen Grund, sie zu sichern). Im oberen Fenster dieses Bildschirms sehen Sie alle Dateien und Dateitypen, die für alle Benutzer dieses Windows 2000 Server-Computers ausgeschlossen sind. Im unteren Fenster werden die Dateien angezeigt, die für den Administrator-Benutzer auf diesem Windows 2000 Server-Computer ausgeschlossen werden.

Klicken Sie einmal auf die Schaltfläche **Hinzufügen**, um einer Ausschlussliste eine neue Datei hinzuzufügen (beide Schaltflächen verhalten sich identisch). Sie können die Dateien entweder ihrem Typ (beispielsweise Dateitypen, die in Windows 2000 Server bereits registriert wurden) oder ihrer Datei- oder Ordnerstufe (d.h. einzelne Dateien oder alles innerhalb eines einzelnen Ordners oder einer Ordnerstruktur) nach ausschließen. Nachdem Sie Ihre Auswahl vorgenommen haben, klicken Sie einmal auf die Schaltfläche **OK**, um alle Einstellungen zu bestätigen und das **Optionen**-Dialogfeld zu verlassen.

Nachdem die Sicherungsoptionen für Windows 2000 Server konfiguriert wurden, können Sie nun eine Sicherung durchführen. Dazu klicken Sie auf die Schaltfläche **Sicherungs-Assistent** im Startbildschirm des Sicherungsprogramms. Beachten Sie, dass Sie automatisch zur zweiten Registerkarte dieses Bildschirms (**Sichern**) gelangen, auch wenn diese nach dem Aufruf des Sicherungs-Assistenten zunächst verborgen ist (siehe Abbildung 23.6).

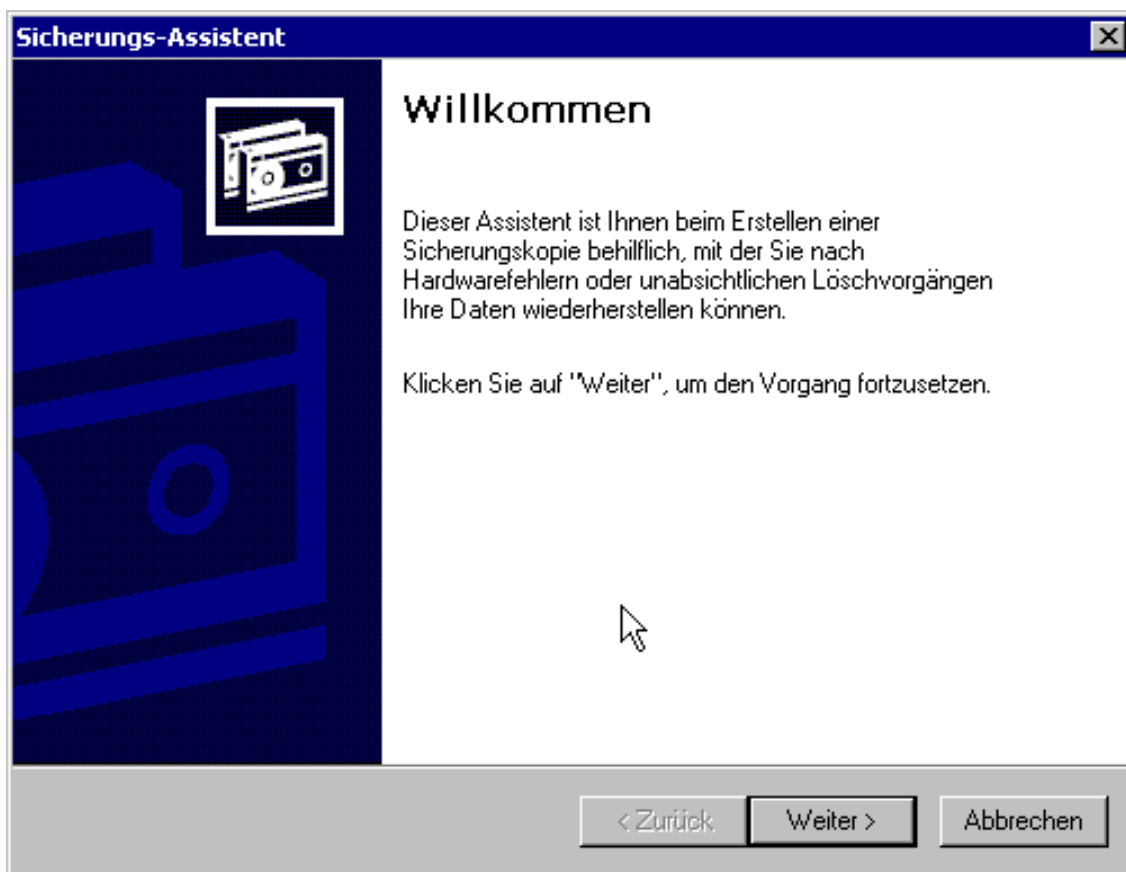


Abbildung 23.6: Starten des Sicherungs-Assistenten

Der erste Bildschirm des Sicherungs-Assistenten von Windows 2000 Server dient nur zu Ihrer Information. Hier können Sie die Sicherung abbrechen, falls Sie sie versehentlich gestartet haben. Vorausgesetzt, Sie wollen die Sicherung wirklich ausführen, klicken Sie auf die Schaltfläche **Weiter**. Der Assistent erlaubt die Auswahl, was gesichert werden soll (Abbildung 23.7).

Es gibt drei Arten von Sicherungen, die Sie über das Sicherungsprogramm von Windows 2000 durchführen können:

- Alle Daten auf dem Computer sichern.
- Ausgewählte Dateien, Laufwerke oder Netzwerkdaten sichern.
- Nur die Systemstatusdaten sichern.



Abbildung 23.7: Hier legen Sie fest, was gesichert werden soll

Die beiden ersten Optionen sind selbsterklärend. Entweder Sie sichern alles, was sich auf Ihrem Windows 2000-Server befindet, oder nur bestimmte Daten auf Ihrem Sicherungsdatenträger. Das dritte Optionsfeld, mit dem die Systemstatusdaten gesichert werden, ist etwas komplizierter. Wie Sie in diesem Kapitel bereits erfahren haben, sind Systemstatusdaten spezielle Systemdateien, die Sie sichern müssen, um Ihren Windows 2000-Server insgesamt wiederherstellen zu können, inklusive der Benutzer- und Systemkonten, unter Bewahrung der Integrität der Systembootinformation und den Zertifikatdiensten (falls diese auf dem Server installiert wurden). Die folgende Liste enthält alle Elemente, aus denen sich die Systemstatusdaten zusammensetzen:

- Windows 2000 Server-Registrierungsdatenbank
- COM+-Klassenregistrierungsdatenbank
- Systemstartdateien
- Zertifikatdienstdatenbank
- Active Directory-Verzeichnisdienst
- SYSVOL-Verzeichnis

Beachten Sie, dass es die Zertifikatdienstdatenbank nur auf Windows 2000-Servern gibt, auf denen der Zertifikat-Server installiert ist. Darüber hinaus gibt es den Active Directory-Verzeichnisdienst und das SYSVOL-Verzeichnis nur auf Windows 2000-Servern, die als Domänencontroller verwendet werden (Mitgliedsserver und Standalone-Server haben keine Systemstatusdatendateien). Nachdem Sie entschieden haben, was gesichert werden soll, klicken Sie einmal auf das betreffende Optionsfeld. Im Sicherungs-Assistenten klicken Sie auf die Schaltfläche **Weiter**. Der in Abbildung 23.8 gezeigte Bildschirm wird geöffnet.

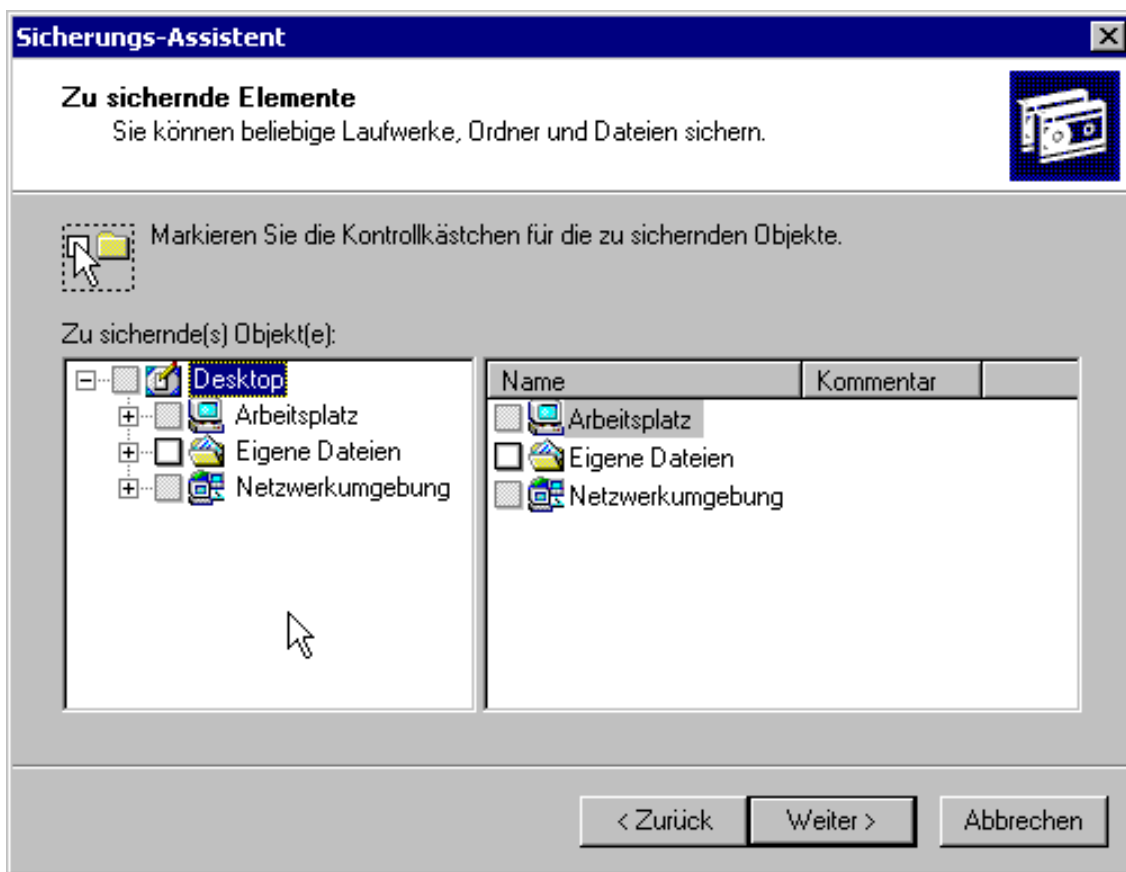


Abbildung 23.8: Hier markieren Sie, was gesichert werden soll

Markieren Sie auf diesem Bildschirm alle Kontrollkästchen neben den Optionen, die gesichert werden sollen. Hier können Sie beliebige Kombinationen aus Dateien, Ordnern und ganzen Laufwerken (auch Netzwerklaufwerken) zur Sicherung auswählen. Nachdem Sie alle Auswahlen vorgenommen haben, klicken Sie auf **Weiter**, um den in Abbildung 23.9 gezeigten Bildschirm aufzurufen.



Abbildung 23.9: Auswahl eines Sicherungsdatenträgers

Auf diesem Bildschirm wählen Sie aus, wohin die Sicherung kopiert werden soll. Wenn Sie kein Sicherungsgerät haben (beispielsweise ein Bandlaufwerk oder ein Festplattenlaufwerk), das an Ihren Windows 2000-Server angeschlossen ist, wird nur die Auswahlmöglichkeit **Datei** angezeigt. Sie sehen sie im oberen Dropdown-Listefeld **Sicherungsmedientyp**). Wenn Sie an Ihren Windows 2000-Server ein Sicherungsgerät angeschlossen haben, können Sie dieses als Ziel für Ihre Sicherung auswählen. Beachten Sie, dass bei diesem Sicherungsprozess über das Netzwerk die Systemstatusdaten nicht gesichert werden können. Im unteren Feld wählen Sie das Ziel für Ihren Sicherungsdatenträger aus (beispielsweise ein anderes Laufwerk, wenn Dateien gesichert werden, oder ein Bandlaufwerk, falls Ihnen ein solches zur Verfügung steht). Nachdem Sie alle Einträge vorgenommen haben, klicken Sie auf die Schaltfläche **Weiter**. Sie gelangen zum letzten Bildschirm des Sicherungs-Assistenten, den Sie in Abbildung 23.10 sehen.



Abbildung 23.10: Bestätigen der Sicherungseinstellungen

Mit diesem Bildschirm will Microsoft ein bisschen freundlich zu Ihnen sein: Hier können Sie alle vorgenommenen Einstellungen noch einmal kontrollieren. Nachdem Sie fertig sind, klicken Sie auf die Schaltfläche **Fertig stellen**, um den Sicherungs-Assistenten zu schließen und die eigentliche Sicherung Ihrer Dateien zu starten. Vorher jedoch können Sie Ihre Sicherungsoptionen noch einmal überprüfen, indem Sie auf die Schaltfläche **Erweitert** klicken. Sie sehen den in Abbildung 23.11 gezeigten Bildschirm.

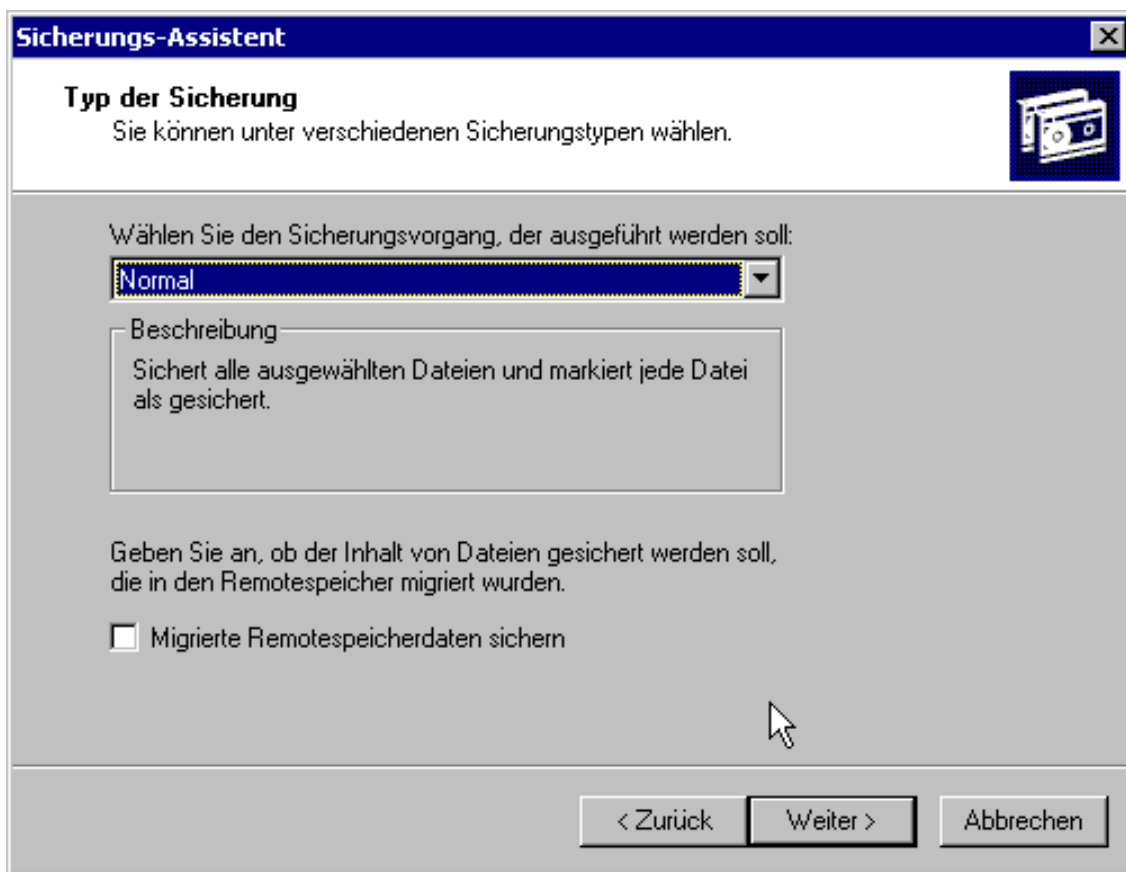


Abbildung 23.11: Die erste erweiterte Option: Auswahl einer Sicherungsart

Im Bildschirm für den Sicherungstyp haben Sie zwei Möglichkeiten: Änderung des Sicherungstyps und Angabe darüber, ob die Dateien gesichert werden sollen, die auf einem Remotespeicher ausgelagert wurden. Ändern Sie die Sicherungsart gegebenenfalls mit Hilfe des Dropdown-Listenfeldes. Falls Sie bei der Sicherung auch Dateien berücksichtigen wollen, die auf einem Remotespeicher ausgelagert wurden, klicken Sie in das untere Kontrollkästchen, **Migrierte Remotespeicherdaten sichern**. Nachdem Sie Ihre Auswahl getroffen haben, klicken Sie auf die Schaltfläche **Weiter**. Der in Abbildung 23.12 gezeigte Bildschirm wird aufgerufen.

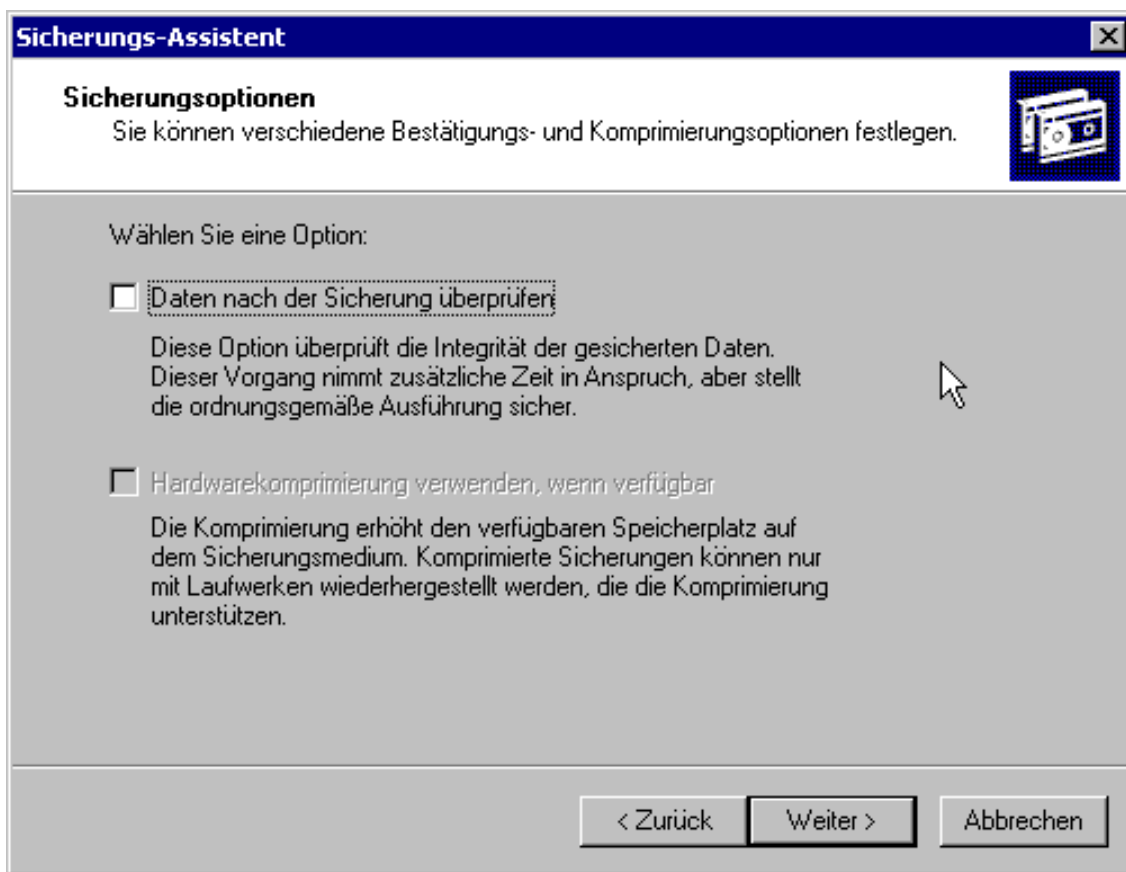


Abbildung 23.12: Einstellung der Optionen für Überprüfung und Komprimierung

In Windows 2000 Server gibt es ein neues Werkzeug zur Datenverwaltung, das erlaubt, weniger häufig genutzte Dateien automatisch an eine sekundäre Speicherposition auszulagern. Nachdem das primäre Festplattenspeichersystem eine bestimmte Größe erreicht hat, wird der Cache der Daten, die an die Remote-Position verschoben wurden, vom primären System für Speicherzwecke verwendet. Diese Remote-Speicherposition kann nur auf einem Windows 2000 NTFS-Datenträger angelegt werden und wird mit Hilfe austauschbarer Speichermedien realisiert, beispielsweise Bänder oder Platten.



Im Bildschirm **Sicherungsoptionen** haben Sie die Möglichkeit, den Sicherungsprozess zu überprüfen und die Hardwarekomprimierung für das Sicherungsgerät zu aktivieren. Nehmen Sie Ihre Auswahlen vor, indem Sie die entsprechenden Kontrollkästchen aktivieren. Klicken Sie auf die Schaltfläche **Weiter**, um zum Bildschirm für die Datenträgeroptionen zu gelangen.

Hier haben Sie wiederum zwei Auswahlmöglichkeiten: Sie können die bereits auf dem Sicherungsdatenträger befindlichen Daten überschreiben oder ergänzen. Wenn Sie den bereits existierenden Inhalt überschreiben, können Sie auch die untere Option auswählen, die verhindert, dass diese Sicherungsdatei versehentlich von einem anderen als dem Eigentümer des Sicherungsbands oder dem Systemadministrator gelöscht wird. Nachdem Sie Ihre Auswahl getroffen haben, klicken Sie auf **Weiter**. Der in Abbildung 23.13 gezeigte Bildschirm wird geöffnet.

Abbildung 23.13: Die Bezeichnung für die Sicherung festlegen

Im Bildschirm für die Sicherungsbezeichnung wählen Sie eine Sicherungs- und eine Datenträgerbeschriftung für Ihren Sicherungsauftrag aus. Windows 2000 Server erzwingt zwar keine Logik für die Einrichtung der Bezeichnungen, aber Sie sollten dennoch beschreibende Texte wählen und außerdem die Uhrzeit und das Datum der Sicherung mit angeben. Nachdem Sie Ihre Einträge vorgenommen haben, klicken Sie auf die Schaltfläche **Weiter**. Sie gelangen zu dem in Abbildung 23.14 gezeigten Bildschirm.

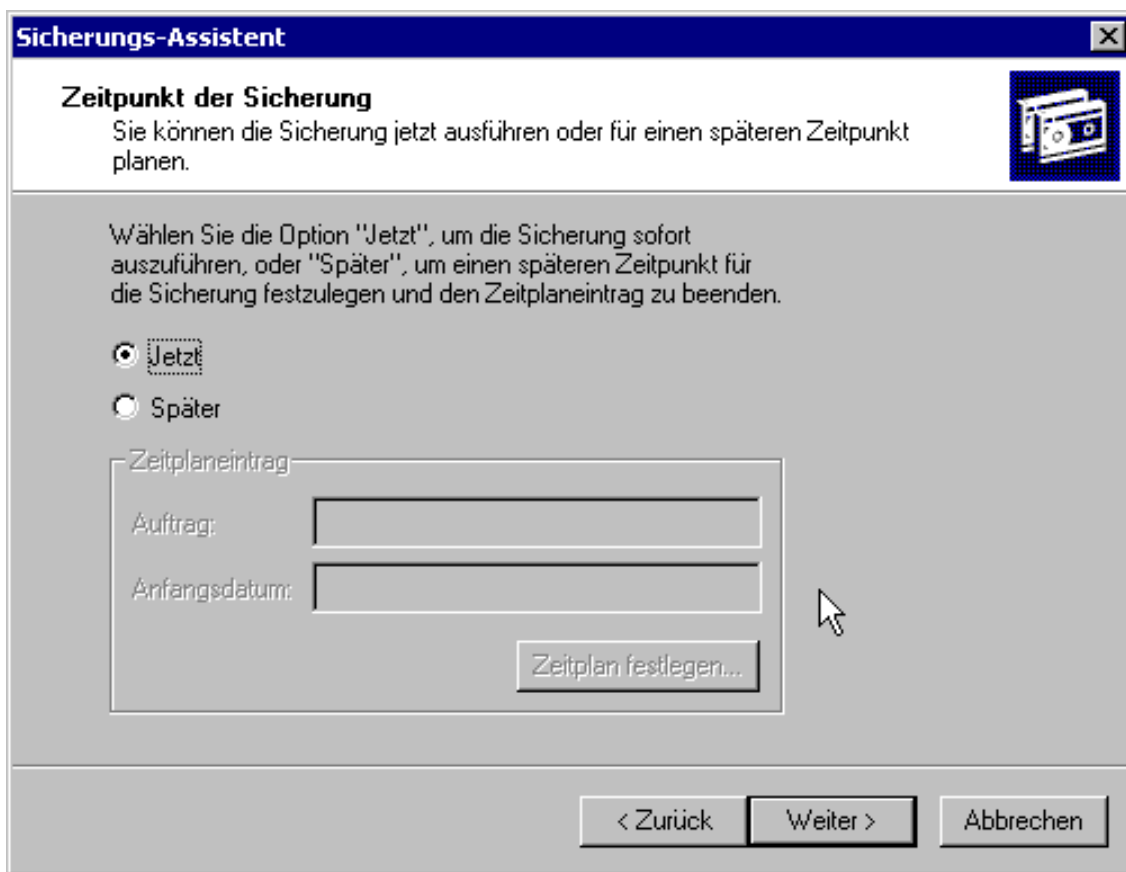


Abbildung 23.14: Hier legen Sie fest, wann die Sicherung ausgeführt werden soll

Jetzt legen Sie fest, wann die Sicherung beginnen soll: sofort oder zu einem späteren Zeitpunkt. Klicken Sie auf das entsprechende Optionsfeld. Beim Anklicken des Optionsfeldes **Später** wird der Bildschirmabschnitt für den Zeitplan aktiviert, wo Sie die gewünschten Zeiten eintragen.

Andernfalls klicken Sie auf die Schaltfläche **Weiter**. Falls Sie auf das Optionsfeld **Später** geklickt haben, wird das in Abbildung 23.15 gezeigte Popup-Fenster **Konteninformation festlegen** angezeigt.



Abbildung 23.15: Eingabe der Konteninformation

In diesem Popup-Fenster geben Sie den Kontennamen und das Kennwort für das Administrator- oder Sicherungs-Operator-Konto ein, das für diesen Sicherungsauftrag genutzt werden soll. Sie müssen hier eine Konteninformation für eine Sicherheitsebene eingeben, die mindestens der einem Systemadministrator gleich ist, oder ein Konto, das Mitglied der Sicherungs-Operatoren-Gruppe von Windows 2000 ist. Andernfalls wird der Sicherungsauftrag sehr wahrscheinlich nicht korrekt ausgeführt. Beachten Sie, dass dem eigentlichen Kontennamen der Domänenname für das betreffende Konto vorausgeht. Nachdem Sie den Eintrag vorgenommen haben, klicken Sie auf **Weiter**.

Sie gelangen damit zu einem Bildschirm, der Ihnen vermutlich bekannt vorkommt. Sie haben ihn gerade erst gesehen, allerdings mit einem Unterschied: Jetzt können Sie einen Eintrag für den Zeitplan vornehmen. Geben Sie einen

beschreibenden Namen in das Feld **Auftrag** ein und klicken Sie auf die Schaltfläche **Zeitplan festlegen**, um den in Abbildung 23.16 gezeigten Bildschirm aufzurufen.

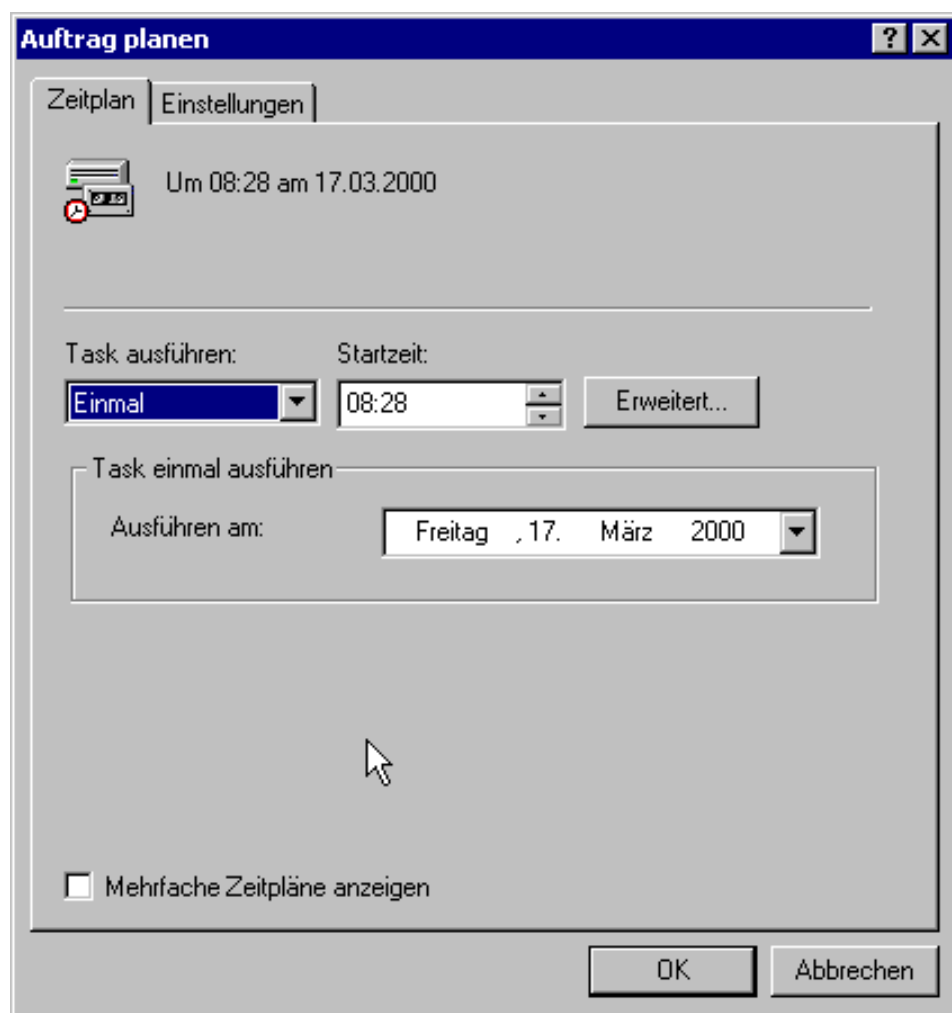


Abbildung 23.16: Einplanung des Sicherungsauftrags

Das Dialogfeld für die Einplanung des Sicherungsauftrags wird geöffnet. Hier legen Sie exakt fest, wann die Sicherung beginnen soll. Die Optionen in diesem Dialogfeld sind selbsterklärend. Es gibt zahlreiche Möglichkeiten, die Startzeit für Ihren Sicherungsauftrag festzulegen. Im Dropdown-Listenfeld **Task ausführen** wählen Sie aus, wann die Sicherung ausgeführt werden soll:

- Täglich
- Wöchentlich
- Monatlich
- Einmal
- Beim Systemstart
- Bei der Anmeldung
- Im Leerlauf

Abhängig von dem ausgewählten Zeitplan fordert Sie der Sicherungs-Assistent zur Eingabe bestimmter Informationen auf (beispielsweise kann keine Monatsangabe vorgenommen werden, wenn Sie tägliche Sicherungen ausgewählt haben). Um die erweiterten Einplanungstechniken zu nutzen, klicken Sie auf die Schaltfläche **Erweitert**. Der in Abbildung 23.17 gezeigte Bildschirm wird aufgerufen.

Abbildung 23.17: Auswahl der erweiterten Optionen für die Einplanung von Sicherungsaufträgen

Eine der praktischsten Funktionen im Dialogfeld *Erweiterte Zeitplanoptionen* besteht darin, einen täglichen Sicherungsauftrag abzubrechen, wenn er beispielsweise zu lange dauert. Dazu aktivieren Sie das Kontrollkästchen **Wiederholungsintervall**. Mit dem Optionsfeld *Bis* geben Sie die Dauer für die Sicherung an (klicken Sie auf **Task beenden**, falls er noch ausgeführt wird, um die Funktion zu aktivieren). Nachdem Sie alle Auswahlen vorgenommen haben, klicken Sie auf die Schaltfläche **OK**, um zum Dialogfeld zur Einplanung des Sicherungsauftrags zu gelangen. Es gibt noch eine praktische Funktion in diesem Dialogfeld, nämlich die Möglichkeit, verschiedene Zeitpläne für denselben Sicherungsauftrag zu benutzen. Um auf diese Funktion zuzugreifen, klicken Sie unten im Bildschirm auf das Kontrollkästchen **Mehrfache Zeitpläne anzeigen**. Oben im Bildschirm wird automatisch eine neue Funktion zur Verfügung gestellt.

Das Symbol für die Einplanungszeit des Sicherungsauftrags wird durch ein Dropdown-Listenfeld ersetzt, in dem Sie eine Sicherungszeit aus einer Liste mehrerer Zeiten auswählen. Um Elemente aus dieser Liste zu löschen, klicken Sie sie an und klicken dann auf die Schaltfläche **Entfernen**. Um der Liste einen neuen Zeitplan hinzuzufügen, klicken Sie auf die Schaltfläche **Neu**. Alle Einträge in der Liste sind nummeriert links im Listenfeld zu sehen.

Nachdem Sie alle Auswahlen vorgenommen haben, sollten Sie die anderen verfügbaren Einplanungsfunktionen ansehen. Dazu wechseln Sie zur Registerkarte **Einstellungen** (siehe Abbildung 23.18).

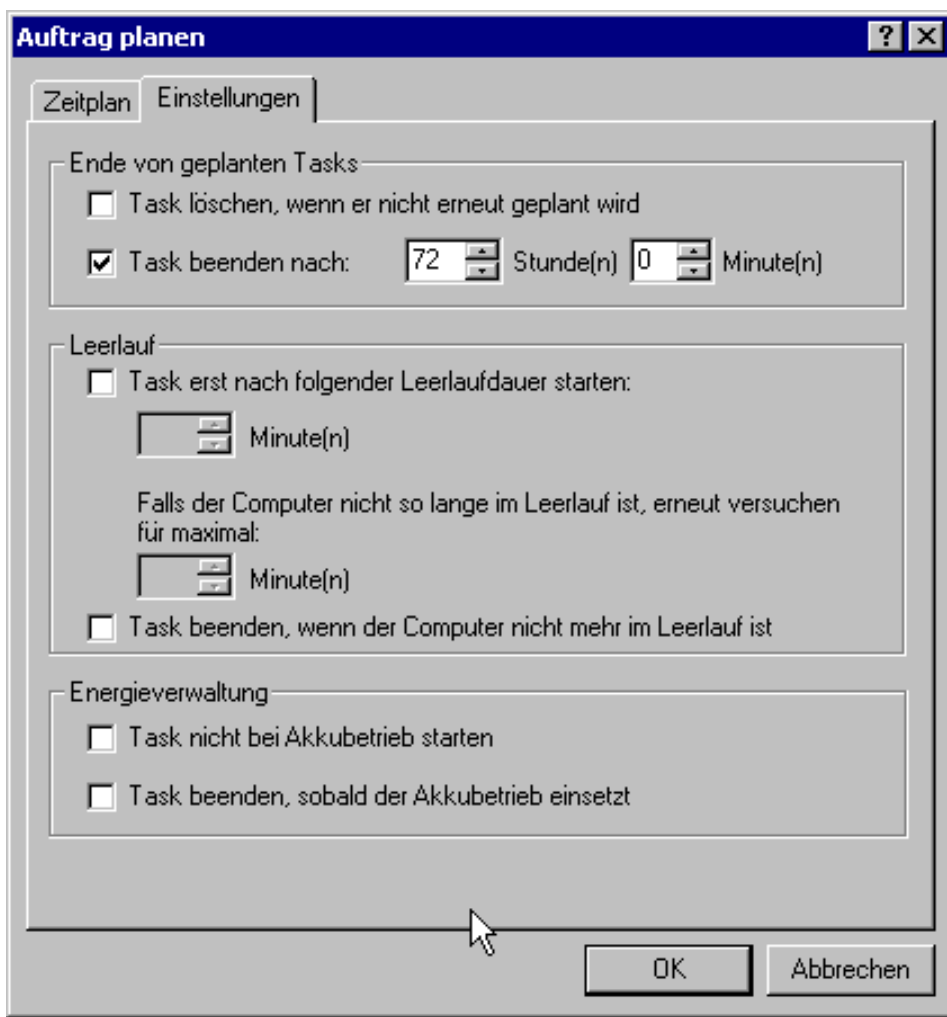


Abbildung 23.18: Bestätigung der Einstellungen für den Sicherungsauftrag

Auf der Registerkarte **Einstellungen** können Sie angeben, wie lange ein Sicherungsauftrag maximal dauern darf, sodass die Sicherung nicht die täglichen Aufgaben in Ihrem Unternehmen überlagert. Eine weitere praktische Funktion ist die Energieverwaltung, die Ihnen ermöglicht, einen Sicherungsauftrag zu beenden, wenn Ihr Computer (beispielsweise ein Notebook-PC oder ein Server, dessen Stromversorgung unterbrochen wurde und nun über eine USV versorgt wird) nur noch über Batterien mit Strom versorgt wird. Nachdem Sie alle Auswahlen vorgenommen haben, klicken Sie auf die Schaltfläche **OK**. Sie sehen den letzten Bildschirm des Sicherungs-Assistenten (Abbildung 23.19).

Hier werden alle Funktionen und Optionen noch einmal angezeigt, die Sie für die Sicherung ausgewählt haben. Nachdem Sie sich davon überzeugt haben, dass alle Einstellungen korrekt sind, klicken Sie auf die Schaltfläche **Fertig stellen**. Der Bildschirm mit dem Assistenten wird geschlossen und die Sicherung wird ausgeführt.



Abbildung 23.19: Überprüfen der im Sicherungs-Assistenten vorgenommenen Einstellungen

Nachdem der Sicherungsprozess begonnen hat, sehen Sie die Registerkarte *Sichern* des Bildschirms **Sicherungsprogramm - [Unbenannt]** (es wird kein Name angegeben, weil Sie diesen Sicherungsauftrag noch nicht gespeichert haben - was wir gleich nachholen werden). Vor diesem Bildschirm sehen Sie das kleinere Statusfenster mit der Auswahlinformation (siehe Abbildung 23.20).

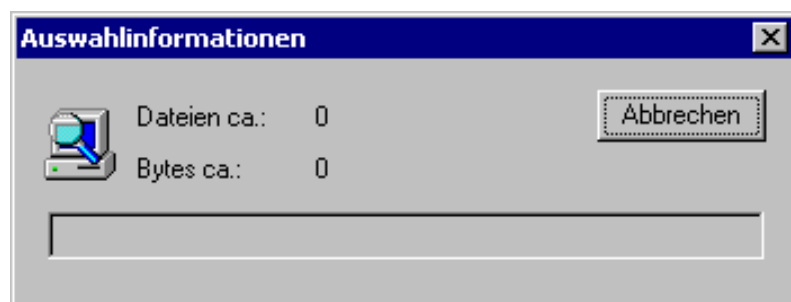
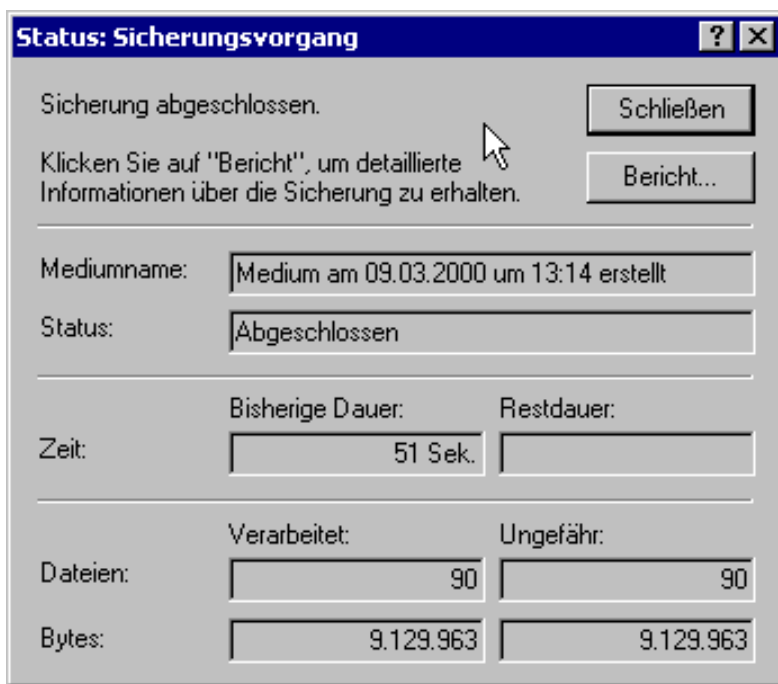


Abbildung 23.20: Anzeige des Statusfensters für einen aktiven Sicherungsauftrag

Das Statusfenster **Auswahlinformationen** gibt Ihnen einen Überblick über die Dateien und Bytes, die während der Einrichtung eines Sicherungsauftrags berücksichtigt werden. Falls Sie den Sicherungsprozess irgendwann unterbrechen wollen, klicken Sie in diesem Statusfenster auf die Schaltfläche **Abbrechen**. Nachdem der Sicherungsauftrag wirklich begonnen hat, sehen Sie das Dialogfeld **Sicherungsvorgang**.

Hier werden dem Sicherungs-Operator Informationen über den Fortschritt der Sicherung bereitgestellt. Aber auch hier haben Sie die Möglichkeit, die Sicherung abzubrechen, indem Sie auf die Schaltfläche **Abbrechen** klicken.

Sehr praktisch sind vor allem die vier Felder unten auf diesem Bildschirm: sie zeigen die verarbeiteten und geschätzten Datenmengen mit Byte- und Dateizähler für den Sicherungsauftrag. Wenn Sie beispielsweise 243 Mbyte Dateien sichern müssen, bisher aber etwa 1,8 Mbyte gesichert sind, ist der Sicherungsauftrag noch lange nicht abgeschlossen. Nachdem der Sicherungsauftrag abgeschlossen ist, gelangen sie automatisch zum Dialogfeld zur Ergebnisanzeige des Sicherungsvorgangs, das Sie in Abbildung 23.21 sehen.



Status: Sicherungsvorgang [?] [X]

Sicherung abgeschlossen.

Klicken Sie auf "Bericht", um detaillierte Informationen über die Sicherung zu erhalten.

[Schließen] [Bericht...]

Mediumname:

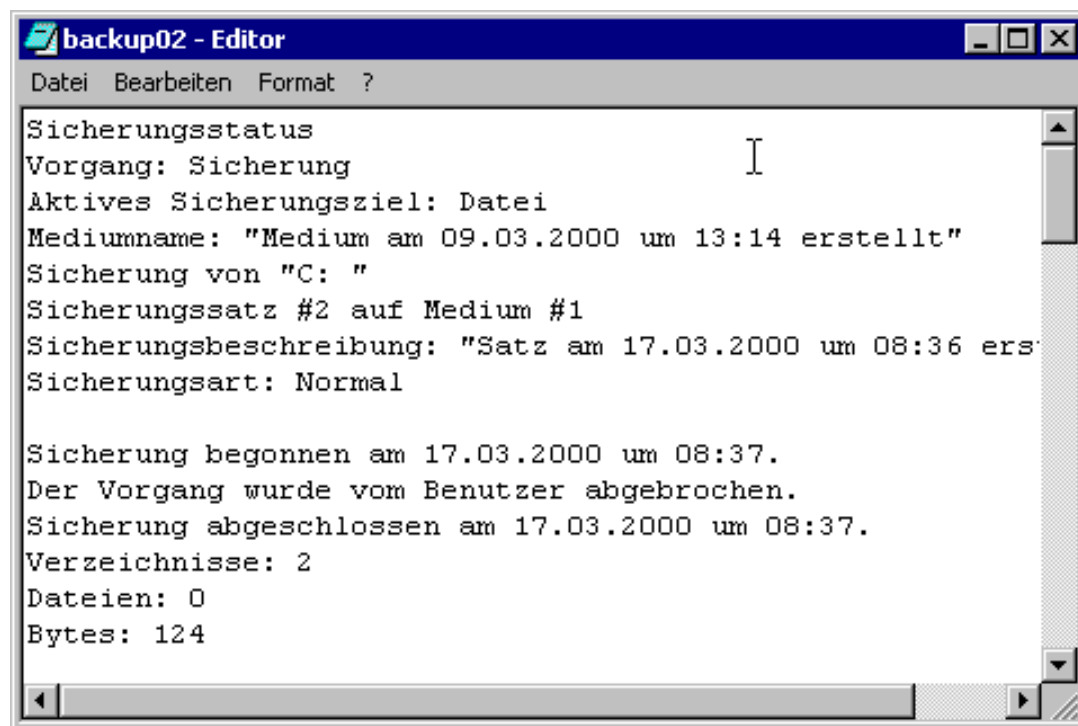
Status:

	Bisherige Dauer:	Restdauer:
Zeit:	51 Sek.	

	Verarbeitet:	Ungefähr:
Dateien:	90	90
Bytes:	9.129.963	9.129.963

Abbildung 23.21: Der Ergebnisbildschirm für den Sicherungsvorgang

Die Informationen in diesem Dialogfeld können nicht geändert werden, aber Sie sollten sie genau lesen, weil Sie daran schnell erkennen, ob ein Sicherungsauftrag erfolgreich war (die Zahlen unten im Bildschirm müssen übereinstimmen: **Verarbeitet** und **Ungefähr**). Eine detailliertere Anzeige dieser Informationen erhalten Sie über die Schaltfläche **Bericht**. Ein für den Windows-Editor formatierter Bericht wird angezeigt (siehe Abbildung 23.22).



```

backup02 - Editor
Datei Bearbeiten Format ?

Sicherungsstatus
Vorgang: Sicherung
Aktives Sicherungsziel: Datei
Mediumname: "Medium am 09.03.2000 um 13:14 erstellt"
Sicherung von "C: "
Sicherungssatz #2 auf Medium #1
Sicherungsbeschreibung: "Satz am 17.03.2000 um 08:36 ers
Sicherungsart: Normal

Sicherung begonnen am 17.03.2000 um 08:37.
Der Vorgang wurde vom Benutzer abgebrochen.
Sicherung abgeschlossen am 17.03.2000 um 08:37.
Verzeichnisse: 2
Dateien: 0
Bytes: 124
  
```

Abbildung 23.22: Anzeige eines Berichts über die Sicherungsergebnisse

Diese Berichte im ASCII-Format können in einem Ordner abgelegt werden. Damit ist es möglich, die Berichte später noch einmal auszuwerten um sicherzustellen, dass die verschiedenen Sicherungsaufträge erfolgreich ausgeführt wurden.

Nachdem Sie sich ausreichend über den Inhalt des Berichts informiert haben, speichern oder schließen Sie ihn. Sie gelangen zurück zum Bildschirm **Sicherungsvorgang**. Hier klicken Sie auf die Schaltfläche **Schliessen** und gelangen so zurück zum allgemeinen Sicherungs-Bildschirm, den Sie in Abbildung 23.23 sehen.

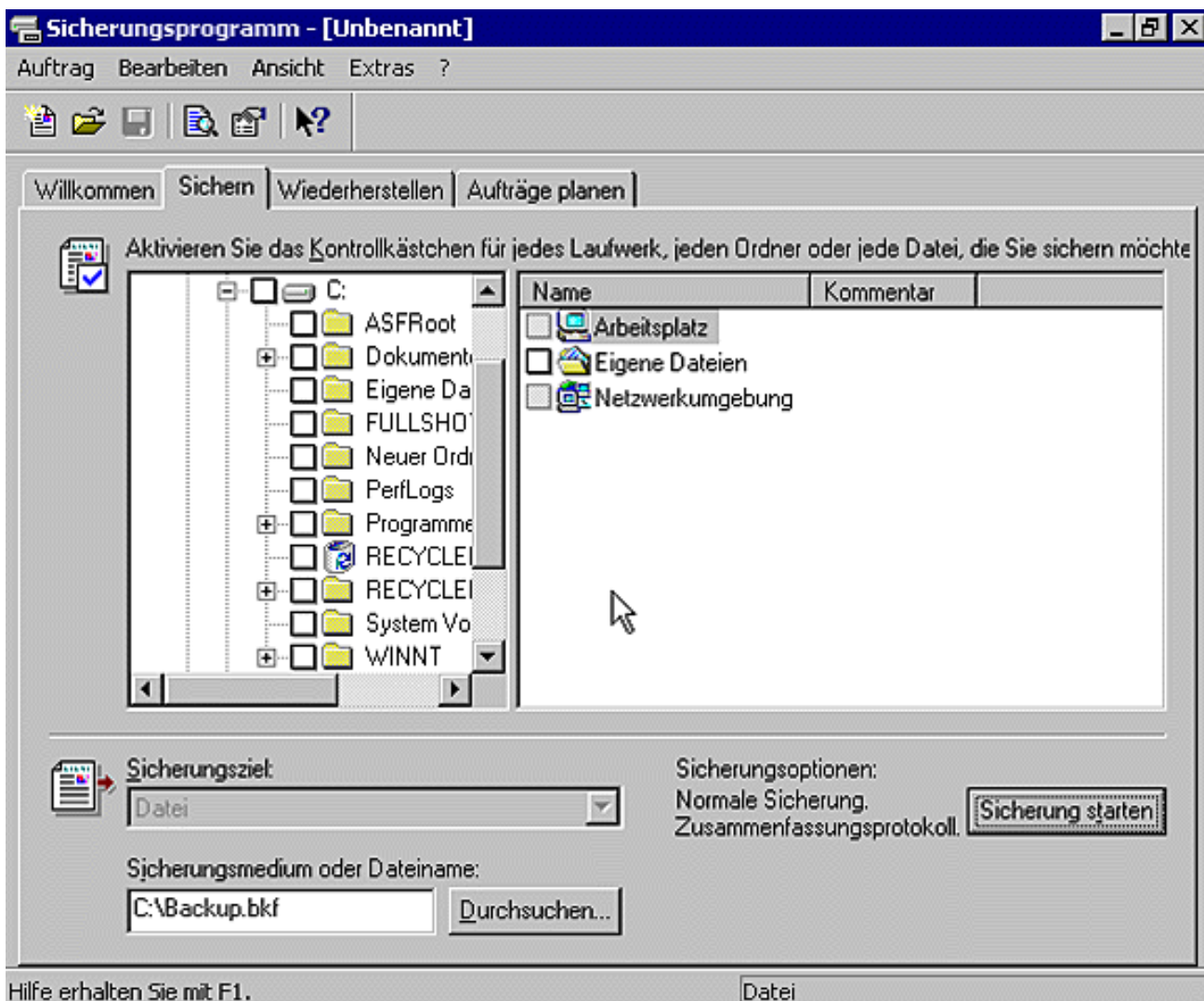


Abbildung 23.23: Der Hauptbildschirm für die Sicherung

Wie Sie sehen, ist der Sicherungsauftrag damit abgeschlossen. Sie können ihn mit denselben Einstellungen erneut starten, indem Sie rechts unten im Bildschirm auf die Schaltfläche **Sicherung starten** klicken (es ist aber eher unwahrscheinlich, dass Sie das jetzt sofort wollen). Um die Einstellungen für diesen Sicherungsauftrag zu speichern, wählen Sie im Menü **Auftrag** den Eintrag **Auswahl speichern** oder **Auswahl speichern unter** (wenn Sie diesen Sicherungsauftrag noch nie gespeichert haben, sollten Sie die Option **Auswahl speichern** verwenden.) Klicken Sie im Menü **Auftrag** auf **Beenden**, um das Sicherungsprogramm zu beenden.

23.2.1 Beaufsichtigte Operationen

Eine »beaufsichtigte« Sicherungsoperation ist nichts anderes als eine Sicherung, bei der der Sicherungs-Operator den gesamten Prozess interaktiv steuert. Ein eingeplanter Sicherungsauftrag, der automatisch ausgeführt wird, ist nicht unbedingt ein beaufsichtigter Sicherungsauftrag. Ein Beispiel dafür wäre, wenn Sie die Sicherungs- und Wiederherstellungswerkzeuge von Windows nutzen, um einen Sicherungsauftrag direkt auszuführen. Für kleinere bis mittlere Unternehmen ist eine beaufsichtigte Sicherung normal. Die Vorgehensweise wurde bereits beschrieben. Für größere Unternehmen mit mehreren Standorten werden in der Regel automatisch eingeplante oder unbeaufsichtigte Sicherungen ausgeführt. Dazu nutzen Sie einfach die Information aus dem nächsten Abschnitt.

23.2.2 Unbeaufsichtigte Operationen

Unbeaufsichtigte Sicherungsoperationen sind nichts anderes als Sicherungsaufträge, die für Zeiten eingeplant wurden, wo kein Sicherungs-Operator anwesend ist, der das Sicherungswerkzeug von Windows 2000 Server interaktiv bedienen könnte. Für die Konfiguration dieser Operation starten Sie zunächst das Sicherungsprogramm von Windows 2000 Server. Klicken

Sie im Startmenü der Reihe nach auf **Programme/Zubehör/Systemprogramme/Sicherung**. Aktivieren Sie nach dem Programmstart die Registerkarte **Aufträge planen** (Abbildung 23.24).

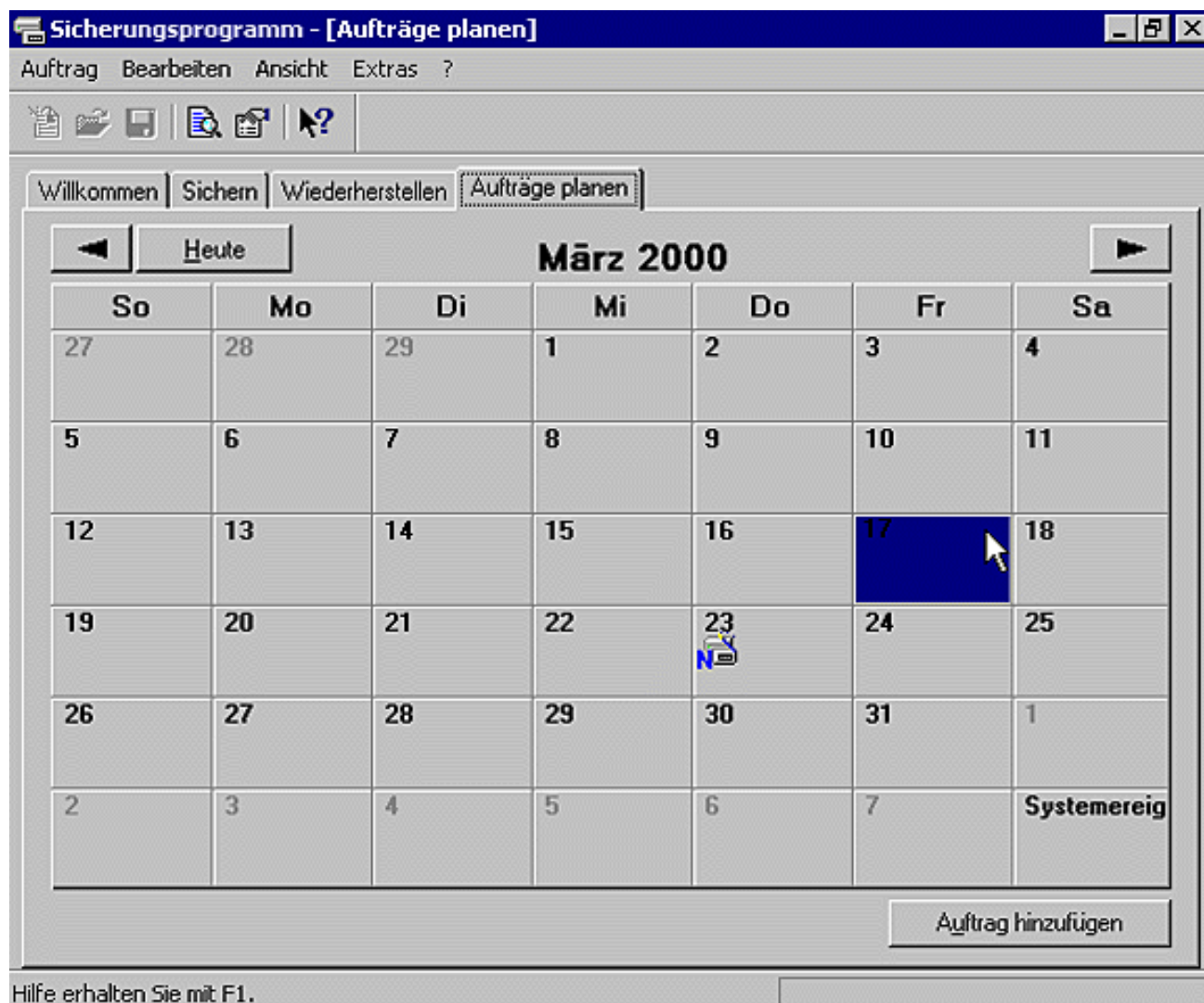


Abbildung 23.24: Der Kalender für die Einplanung von Sicherungsaufträgen

Um einen Sicherungsauftrag einzuplanen, doppelklicken Sie auf das gewünschte Datum für die Ausführung (oder für den Beginn, wenn dieser Auftrag wiederholt werden soll). Falls Sie beispielsweise einen speziellen Sicherungsauftrag am Neujahrsabend 2001 ausführen wollen, doppelklicken Sie auf dieses Datum. Damit wird der Sicherungs-Assistent von Windows 2000 gestartet (der Assistent wurde bereits früher in diesem Kapitel erklärt).

Mit Hilfe dieses Assistenten wählen Sie alle Dateien und Ordner aus, die gesichert werden sollen, die Sicherungsmethode, den Datenträgertyp sowie alle anderen Einstellungen und die Optionen für die Einplanung des Sicherungsauftrags. Nachdem Sie den Assistenten abgeschlossen haben, sehen Sie ein kleines Symbol für das Sicherungsprogramm im Datumsfeld, das Sie zuvor im Kalender ausgewählt haben. Mehr ist nicht erforderlich, um einen Sicherungsauftrag einzuplanen. Sie sollten jedoch einige Dinge beachten, wenn Sie Sicherungsaufträge einplanen:

- Sicherungen können auf FAT16-, FAT32-, NTFS 4.0- (Windows NT) und NTFS 5.0- (Windows 2000) Datenträgern ausgeführt werden. Wenn Sie einen NTFS 5.0-Datenträger sichern, sollten Sie versuchen, ihn auf einem Windows 2000 Server-Datenträger wiederherzustellen, sodass Dateiberechtigungen, Verschlüsselungseinstellungen, Plattenkontingentinformationen und Ähnliches nicht versehentlich verloren gehen (diese Funktionen sind neu im Betriebssystem Windows 2000).
- Der Sicherungsauftrag muss von einem Konto ausgeführt werden, das Administratorberechtigung besitzt oder Mitglied der Gruppe Sicherungs-Operatoren von Windows 2000 Server ist. Hat der Auftrag nicht die korrekten Berechtigungen, schlägt er irgendwann während der Ausführung fehl.
- Sie sollten darauf achten, dass im Sicherungsgerät der richtige Datenträger für die Ausführung Ihres

Sicherungsauftrags eingelegt ist. Windows 2000 Server ist nicht »intelligent« genug, um automatisch ein Bandlaufwerk zu laden, seien Sie also nicht überrascht.

- Der Taskplaner von Windows 2000 Server muss aktiv sein, damit Sie einen Sicherungsauftrag einplanen können. Diesen Dienst starten Sie entweder in der Computerverwaltung von Windows 2000 Server oder Sie geben an der Eingabeaufforderung von Windows 2000 den Befehl `net start schedule` ein.
- Systemstatusdaten können nur von einem lokalen Computer aus gesichert werden; es ist nicht möglich, diese Daten über das Netzwerk zu sichern.
- Weil die Mitglieder der Gruppe Sicherungs-Operatoren sowie die Systemadministratoren in der Lage sind, Dateien und Ordner zu sichern und wiederherzustellen, die mit der EFS-Funktion von Windows 2000 verschlüsselt wurden, sollten Sie die Aktivitäten der Mitglieder dieser beiden Gruppen genau überwachen (keine Sorge, EFS-Dateien und -Ordner werden beim Sichern oder Wiederherstellen nicht entschlüsselt).
- Wenn Sie für Ihre Sicherung Wechseldatenträger verwenden, sollten Sie alle Dateien im Ordner `\NtmsData` sowie im Ordner `\RemoteStorage` sichern (diese beiden Ordner sind im Ordner `%systemroot%\System32` von Windows 2000 Server enthalten). Damit stellen Sie sicher, dass die auf Wechseldatenträgern oder Remotespeicher gesicherten Informationen wiederhergestellt werden können.

23.2.3 Sicherung von der Eingabeaufforderung aus

Windows 2000 Server erlaubt auch, Sicherungen von der Eingabeaufforderung aus auszuführen, aber das ist nicht besonders sinnvoll (insbesondere, wo Microsoft jetzt durch den Deal mit Veritas Software Corporation eine wunderbare grafische Benutzeroberfläche geschaffen hat). Falls Sie Ihre Sicherung dennoch von der Eingabeaufforderung aus ausführen wollen, gehen Sie wie im Folgenden beschrieben vor.

Als Erstes öffnen Sie die Eingabeaufforderung von Windows 2000 Server. Wählen Sie im Startmenü den Eintrag **Ausführen**, geben Sie den Befehl `Cmd` in das Feld **Ausführen** ein und drücken Sie die (Enter)-Taste oder klicken Sie auf die Schaltfläche **OK**. Damit öffnen Sie ein Eingabeaufforderungsfenster in Windows 2000 Server.

Nachdem das Fenster geöffnet ist, starten Sie die Sicherung mit **NTBackup** (interessanter Name, wo das Betriebssystem doch heute Windows 2000 heißt). Beachten Sie, dass für die Sicherung von der Eingabeaufforderung aus dieselben Regeln gelten wie für die Sicherung auf der grafischen Benutzeroberfläche (IDs, Berechtigungen, lokale im Gegensatz zu Netzwerksicherungen usw.), dass die Dateien aber nicht von der Eingabeaufforderung aus wiederhergestellt werden können. Dazu brauchen Sie die grafische Benutzeroberfläche von Windows 2000 Server.

Der Befehl **NTBackup** verfügt über 18 Befehlszeilenschalter (mit entsprechenden Parametern). Eine detaillierte Beschreibung erhalten Sie durch Eingabe von `Ntbackup /?`. Damit greifen Sie auf die GUI-Version des Sicherungsprogramms von Windows 2000 Server zu, das wiederum das Hilfesystem der Sicherung startet und Sie direkt zum korrekten Hilfebildschirm weiterleitet.

Für den Sicherungsprozess verwenden Sie die folgende vollständige Befehlssyntax:

```
ntbackup backup [systemstate] "bks_dateiname" /J {"auftragsname"} [/P {"poolname"}]
[/G {"guid-name"}] [/T {"bandname"}]
[/N {"medium-name"}] [/F {"dateiname"}] [/D {"satzbeschreibung"}]
[/DS {"servername"}] [/IS {"servername"}] [/A] [/V:{yes|no}]
[/R:{yes|no}] [/L:{f|s|n}] [/M {"sicherungsart"}]
[/RS:{yes|no}] [/HC:{on|off}] [/UM]
```

Und nun stellen Sie sich vor, Sie müssen diesen Befehl jedes Mal eingeben, wenn Sie eine Sicherung ausführen wollen! Viele Systemadministratoren führen diese Form der Sicherung mittels einer Batchdatei oder einer Skriptdatei aus, die Schreibarbeit ist also nicht mehr ganz so schlimm, nachdem die Batchdatei oder das Skript erst einmal konfiguriert sind. Beispielsweise könnten Sie einen Sicherungsauftrag von der Eingabeaufforderung aus ausführen, der wie folgt aussieht:

```
ntbackup backup systemstate \\Socrates\d$ /J "Backup Job 1"
```



```
/P "BackupPool" /D "Sicherung über die Eingabeaufforderung"  
/V:yes /R:yes /M daily
```

Dieser Sicherungsauftrag sichert die Systemstatusdaten vom D:-Laufwerk des Servers SOCRATES mit dem Sicherungsnamen BACKUP JOB 1. Der Sicherungsdatenträger ist ein Band aus dem Pool BACKUPPOOL und hat den Bandnamen SICHERUNG ÜBER DIE EINGABEAUFFORDERUNG. Der Sicherungsauftrag wird nach Abschluss überprüft und der Zugriff auf das Band bleibt den Systemadministratoren oder dem Eigentümer des Sicherungsauftrags vorbehalten. Die Sicherung erfolgt täglich.

Beachten Sie, dass Sie nicht immer sämtliche Parameter angeben müssen, und Sie müssen auch keine besondere Reihenfolge einhalten. (Wenn Sie sich jedoch nicht an ein bestimmtes Muster gewöhnen, kann es schwierig sein, Ihre Batch-/Skriptdateien später zu lesen oder zu debuggen.) Statt des UNC-Namens für den Pfad, wobei es sich wahrscheinlich um ein Netzwerklaufwerk handelt, hätte auch der Laufwerksbuchstabe angegeben werden können (falls es sich um ein lokales Laufwerk handelt). Ich persönlich glaube, es ist einfacher und effizienter, auf der grafischen Benutzeroberfläche für das Dienstprogramm Sicherung von Windows 2000 Server zu bleiben - aber das ist Geschmackssache.

23.3 Wiederherstellen einer Sicherung

Irgendwann wird es in jedem Unternehmen nötig, eines der Archive von Sicherungsdatenträgern wiederherzustellen. In der Regel dient das Testzwecken (um sicherzustellen, dass alles funktioniert), aber es gibt auch unglückliche Konstellationen, wo der Ausfall eines der Systeme im Unternehmen eine Wiederherstellung erforderlich macht. In jedem Fall sollte regelmäßig überprüft werden, ob eine Wiederherstellung möglich ist.

Für die Wiederherstellung verwenden Sie das Sicherungsprogramm von Windows 2000 Server. Klicken Sie dazu im Startmenü der Reihe nach auf die Einträge **Programme/Zubehör/Systemwerkprogramme/Sicherung**. Aktivieren Sie im Hauptfenster des Sicherungsprogramms die Registerkarte **Wiederherstellen** (siehe Abbildung 23.25).

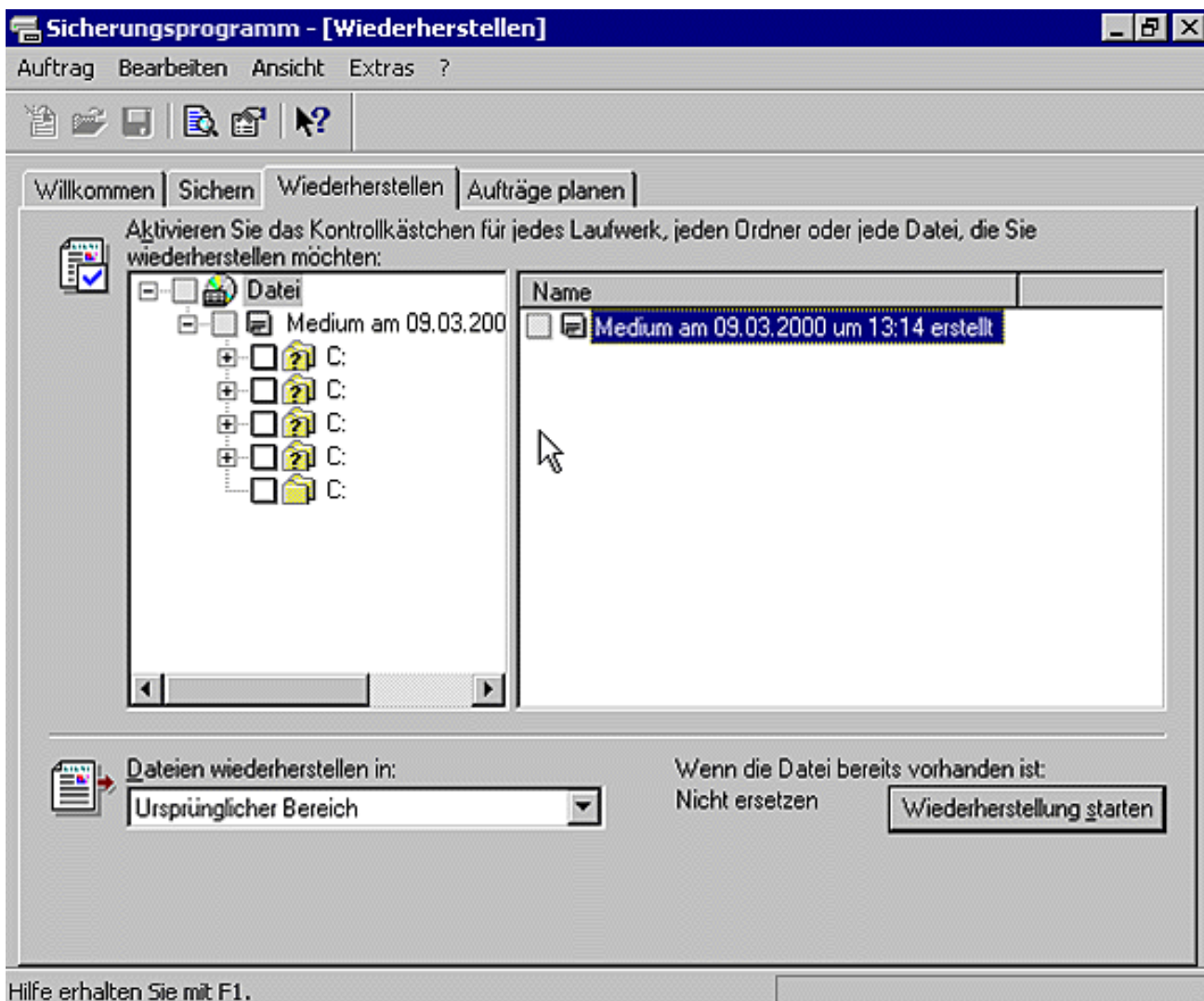


Abbildung 23.25: Der Hauptbildschirm für die Wiederherstellung

Im Sicherungsprogramm sollten Sie vor der eigentlichen Wiederherstellung Folgendes überprüfen:

- Melden Sie sich als Administrator oder als Mitglied der Gruppe Sicherungs-Operatoren bei Windows 2000 Server an.
- Stellen Sie sicher, dass der Sicherungsdatenträger korrekt in das Laufwerk eingelegt ist, von dem aus die Wiederherstellung ausgeführt wird (d.h. legen Sie das Sicherungsband ein).
- Überprüfen Sie Ihre Netzwerkverbindungen, falls die Wiederherstellung über das Netzwerk ausgeführt wird.
- Stellen Sie sicher, dass der Remotespeicher zur Verfügung steht, falls die Wiederherstellung über einen Medienpool erfolgt.
- Falls Systemstatusdaten wiederhergestellt werden sollen, muss Windows 2000 im abgesicherten Modus gestartet werden.
- Nehmen Sie die Wiederherstellung mit Hilfe des GUI-basierten Dienstprogramms Sicherung von Windows 2000 manuell oder automatisch (über den Assistenten) vor.

Um die Wiederherstellung mit Hilfe des Assistenten vorzunehmen, wählen Sie einfach im Menü **Extras** den Befehl **Wiederherstellungs-Assistent**. Der Assistent führt Sie automatisch durch mehrere GUI-basierte Bildschirme und nimmt zusammen mit Ihnen die Wiederherstellung vor. Diese Funktion ist zwar sehr schön angelegt, aber wir werden hier nicht genauer darauf eingehen, weil sie selbsterklärend ist (außerdem werden alle Optionen in diesen Bildschirmen auch im manuellen Wiederherstellungsprozess benutzt, der noch erklärt wird).

Um eine manuelle Wiederherstellung Ihrer gesicherten Daten vorzunehmen, brauchen Sie Zugriff auf das Sicherungsprogramm von Windows 2000 Server, ähnlich wie für den Aufruf des Assistenten. Sie gelangen zum selben Bildschirm, den Sie schon in Abbildung 23.25 gesehen haben. Als Erstes legen Sie fest, wo die wiederhergestellten Dateien abgelegt werden sollen. Es gibt mehrere Auswahlmöglichkeiten:

- Ursprünglicher Bereich
- Alternativer Bereich
- Einzelner Ordner

Die Bedeutung dieser Auswahlmöglichkeiten sollte klar sein, aber Sie sollten sich genau überlegen, wie Sie vorgehen, weil es beispielsweise nicht möglich ist, Systemstatusdaten in einem alternativen Bereich wiederherzustellen. Nehmen Sie eine Wiederherstellung an einer alternativen Position vor, produzieren Sie damit womöglich mehrere Versionen derselben Datei auf dem Windows 2000-Server (das kann für die Endbenutzer sehr verwirrend sein, überdenken Sie also den Wiederherstellungsprozess sorgfältig). Wenn Sie im Dropdown-Listefeld **Dateien wiederherstellen in** die Option **Alternativer Bereich** auswählen, müssen Sie den vollständigen Pfad zu diesem Bereich angeben. Dazu klicken Sie auf die Schaltfläche **Durchsuchen** unten im Bildschirm. Das Dialogfeld zur Auswahl des Wiederherstellungspfades wird angezeigt (siehe Abbildung 23.26).

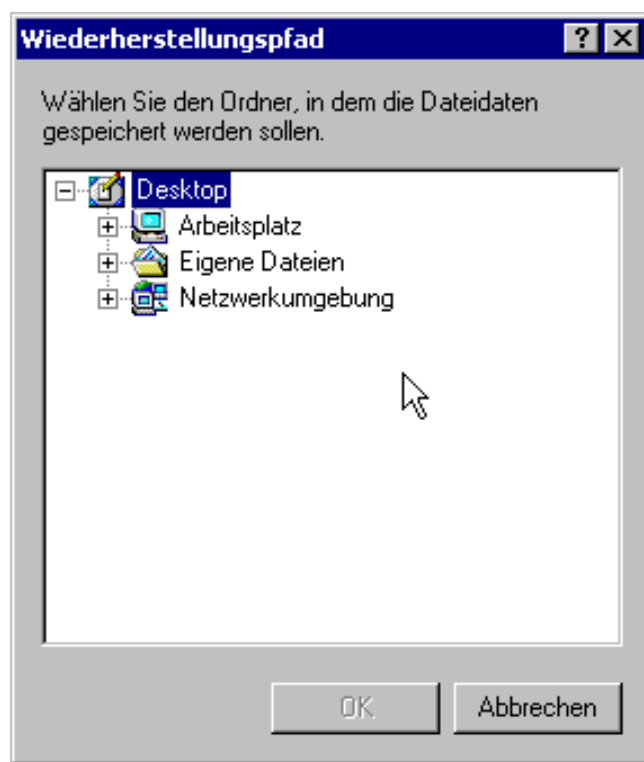


Abbildung 23.26: Auswahl eines Wiederherstellungspfades

Im Dialogfeld **Wiederstellungspfad** suchen Sie auf Ihrem Server nach der Position, an der die gesicherten Dateien wiederhergestellt werden sollen. Klicken Sie die Position zur Auswahl an und bestätigen Ihre Auswahl mit **OK**. Damit gelangen Sie zurück zum Hauptbildschirm für die Wiederherstellung.

Dort sollten Sie die primären Optionen bestätigen, die für die Wiederherstellung genutzt werden sollen. Rufen Sie den Menübefehl **Extras/Optionen** auf, um das Dialogfeld **Optionen** zu öffnen (siehe Abbildung 23.27).

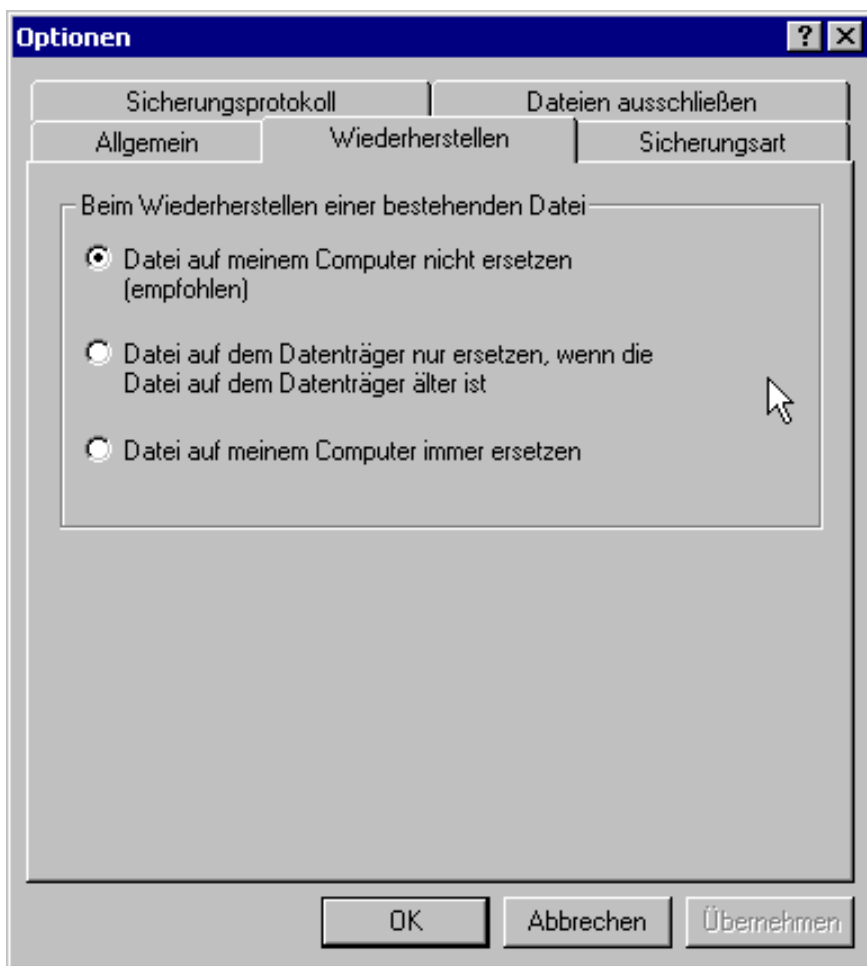


Abbildung 23.27: Einstellung der Wiederherstellungsoptionen

Im Dialogfeld **Optionen** können Sie festlegen, wie reagiert werden soll, wenn die wiederherzustellende Datei auf Ihrem System bereits vorhanden ist. Die Standardeinstellung (die auch von Microsoft empfohlen wird) ist, die bereits existierende Datei nicht zu ersetzen. Die in den meisten Unternehmen am seltensten genutzte Option ist die letzte in der Liste (die bereits existierende Datei immer zu ersetzen). Klicken Sie auf das Optionsfeld für die gewünschte Einstellung und anschließend auf **OK**, um Ihre Auswahl zu bestätigen und das Dialogfeld **Optionen** zu verlassen.

Klicken Sie jetzt auf die Schaltfläche **Wiederherstellung starten**. Wenn Ihre Sicherungsdatei Systemstatusdaten enthält, wird ein Popup-Fenster mit einem Warnhinweis angezeigt, dass nicht alle Systemstatusdaten wiederhergestellt werden können, falls ein alternativer Bereich für die Wiederherstellung gewählt wurde.

Sind in der Sicherungsdatei keine Systemstatusdaten enthalten, wird der Prozess mit einem Hinweisfeld für die Bestätigung der Wiederherstellung fortgesetzt (Abbildung 23.28).

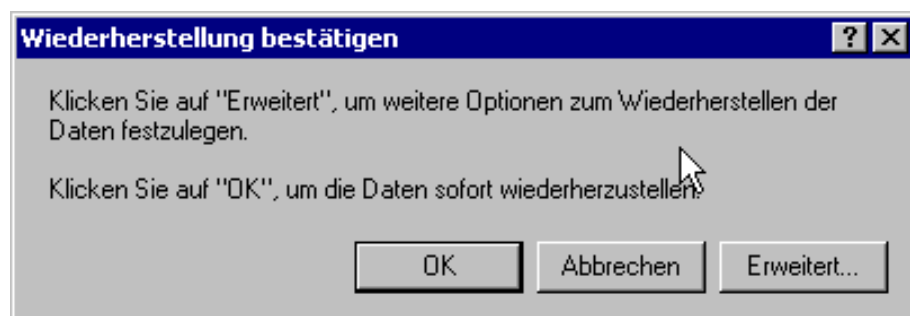


Abbildung 23.28: Bestätigung einer Wiederherstellung

Wenn Sie glauben, dass alle Ihre Optionen korrekt gesetzt wurden, sowohl die primären, die Sie gerade eingerichtet haben, als auch die erweiterten, klicken Sie auf die Schaltfläche **OK**. Die Wiederherstellung der Dateien und Ordner beginnt. Wenn Sie die Wiederherstellung abbrechen wollen, klicken Sie auf die Schaltfläche **Abbrechen**. Damit gelangen Sie zum

Hauptfenster für die Wiederherstellung zurück. Falls Sie die Wiederherstellung fortsetzen wollen, aber nicht sicher sind, dass die erweiterten Optionen korrekt konfiguriert sind, klicken Sie auf die Schaltfläche **Erweitert**. Der in Abbildung 23.29 gezeigte Bildschirm wird angezeigt.

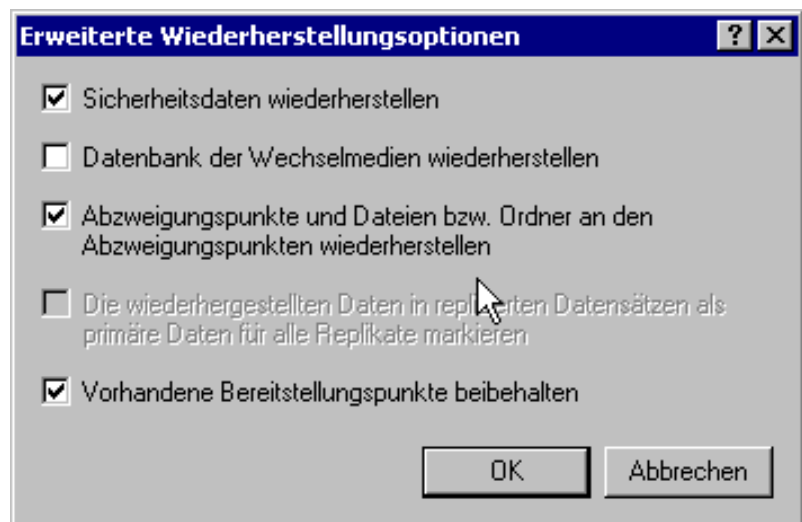


Abbildung 23.29: Die erweiterten Optionen für die Wiederherstellung

Die fünf Optionen auf diesem Bildschirm sind für die Wiederherstellung sehr wichtig. Von den hier vorgenommenen Einstellungen ist es abhängig, ob die Daten Ihres Unternehmens korrekt wiederhergestellt oder möglicherweise sogar beschädigt werden. Es handelt sich um folgende Optionen:

- **Sicherheitsdaten wiederherstellen** - Diese Option richtet die genaue Sicherheitskonfiguration für alle wiederherzustellenden Dateien und Ordner wieder ein. Leider steht diese Option nur für Daten zur Verfügung, die von einem Windows 2000 NTFS 5.0-Datenträger gesichert wurden (FAT16-, FAT32- und NTFS 4.0-Datenträger können nicht verwendet werden), und die auch nur auf einem NTFS 5.0-Datenträger wiederhergestellt werden.
- **Datenbank der Wechselmedien wiederherstellen** - Diese Option bezieht sich nur auf Wiederherstellungen, die von Wechselmedien aus ausgeführt werden sollen. Beachten Sie jedoch, dass die Wiederherstellung dieser Datenbank eine bereits existierende Wechselmediendatenbank überschreibt.
- **Abzweigungspunkte und Dateien bzw. Ordner an den Abzweigungspunkten wiederherstellen** - Diese Option ist selbsterklärend. Im Wesentlichen bewirkt sie, dass alle Daten an ihren ursprünglichen Abzweigungspunkten wiederhergestellt werden. Wählen Sie diese Option aus, wenn Sie Abzweigungspunkte verwenden, die gesichert wurden, weil die Daten, auf die diese Abzweigungspunkte verweisen, andernfalls nicht zur Verfügung stehen.
- **Die wiederhergestellten Daten in replizierten Datensätzen als primäre Daten für alle Replikate markieren** - Diese Option stellt sicher, dass alle FRS-Daten (File Replication Service) automatisch auf andere Windows 2000-Replikationsserver in den Netzwerken des Unternehmens repliziert werden. Falls Sie diese Option nicht setzen, verlieren Sie möglicherweise alle Ihre wiederhergestellten Daten, weil die anderen FRS-Server die wiederhergestellten Daten als älter (und damit nicht mehr benötigt) als ihre eigenen Daten »betrachten«.
- **Vorhandene Bereitstellungspunkte beibehalten** - Mit dieser Option stellen Sie sicher, dass Sie nicht versehentlich existierende Bereitstellungspunkte löschen, die bei der Installation eines neuen Laufwerks (als Ersatz für ein ausgefallenes Laufwerk) angelegt wurden. Wenn Sie vorhaben, ein zuvor neu formatiertes Laufwerk wiederherzustellen, sollten Sie diese Option nicht verwenden, weil Sie möglicherweise alle alten Bereitstellungspunkte Ihres ursprünglichen Datenträgers wiederherstellen wollen.

Klicken Sie auf die Kontrollkästchen neben diesen Optionen, um sie für Ihre Wiederherstellung auszuwählen. Klicken Sie auf die **OK**-Schaltfläche, um die Wiederherstellung fortzusetzen. Ein Dialogfeld für die Eingabe des Sicherungsdateinamen wird geöffnet. Suchen Sie mit Hilfe der Schaltfläche **Durchsuchen** auf Ihrem Computer oder in Ihrem Netzwerk die Sicherungsdatei, die wiederhergestellt werden soll. Klicken Sie auf diese Datei und Sie gelangen zurück zu diesem Bildschirm. Klicken Sie auf **OK**, um die Wiederherstellung fortzusetzen. Wenn Sie versuchen, Ihre Daten in einem alternativen Bereich oder die Systemstatusdaten über ein Netzwerklaufwerk wiederherzustellen, erscheint ein Popup-Fenster mit einer Warnung. Sie können die Warnung ignorieren und die Wiederherstellung fortsetzen, indem Sie auf die Schaltfläche **OK** klicken. Sie können die Wiederherstellung aber auch jederzeit abbrechen, indem Sie auf die Schaltfläche **Abbrechen**

klicken.

Nehmen Sie die für Sie geeigneten Einstellungen vor. Angenommen, Sie haben auf die Schaltfläche **OK** geklickt. Dann gelangen Sie zu dem in Abbildung 23.30 gezeigten Dialogfeld mit Hinweisen zum Status der Wiederherstellung.

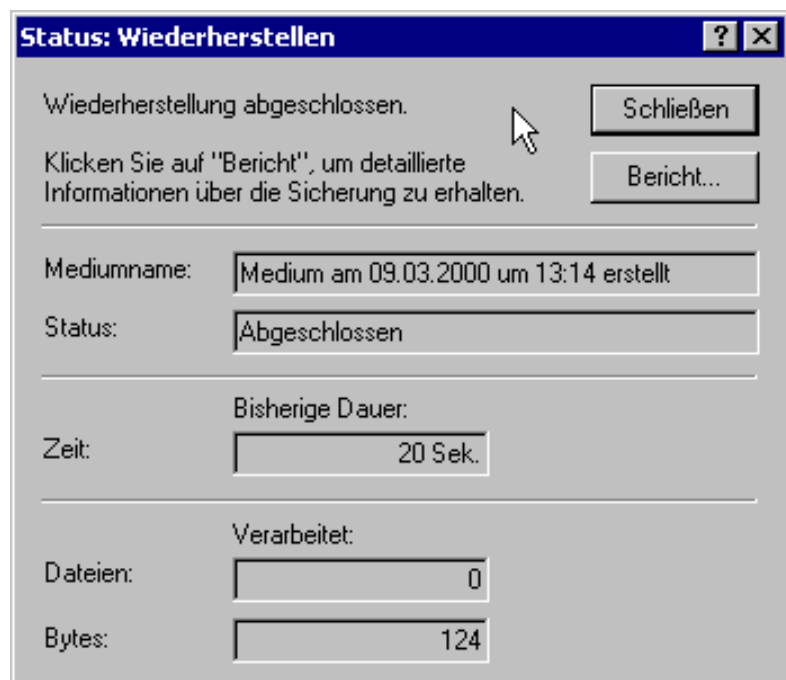


Abbildung 23.30: Fortschrittsanzeige für die Wiederherstellung

Das Dialogfeld mit der Statusanzeige der Wiederherstellung gibt Ihnen einen Überblick zum Fortschritt der Wiederherstellung und erlaubt Ihnen, zu jedem beliebigen Zeitpunkt mit der Schaltfläche **Abbrechen** die Wiederherstellung zu beenden. Nachdem die Wiederherstellung abgeschlossen ist, sehen Sie einen leicht veränderten Bildschirm für die Anzeige des Wiederherstellungsfortschritts (Abbildung 23.31).

Wie im Bildschirm für die Anzeige des Sicherungsfortschritts wird auch hier eine kurze Erklärung des Wiederherstellungsprozesses angezeigt. Weitere Informationen darüber, was bei der Wiederherstellung passiert ist, erhalten Sie durch Anklicken der Schaltfläche **Bericht**.

Nachdem der Windows-Editor mit den Informationen zur Wiederherstellung geöffnet ist, können Sie diese ASCII-Textdatei an eine Position kopieren, von wo aus sie später noch einmal eingesehen werden kann, falls Einzelheiten des Wiederherstellungsprozesses überprüft werden sollen. Nachdem Sie den Bericht eingesehen und geprüft haben, schließen Sie den Editor, um wieder zur Fortschrittsanzeige zu gelangen. Hier klicken Sie auf die Schaltfläche **Schliessen**, um den Bildschirm zu verlassen. Die erfolgreiche Wiederherstellung Ihrer Dateien und Ordner können Sie überprüfen, indem Sie den Windows-Explorer aufrufen, um die wiederhergestellten Dateien durchzusehen.

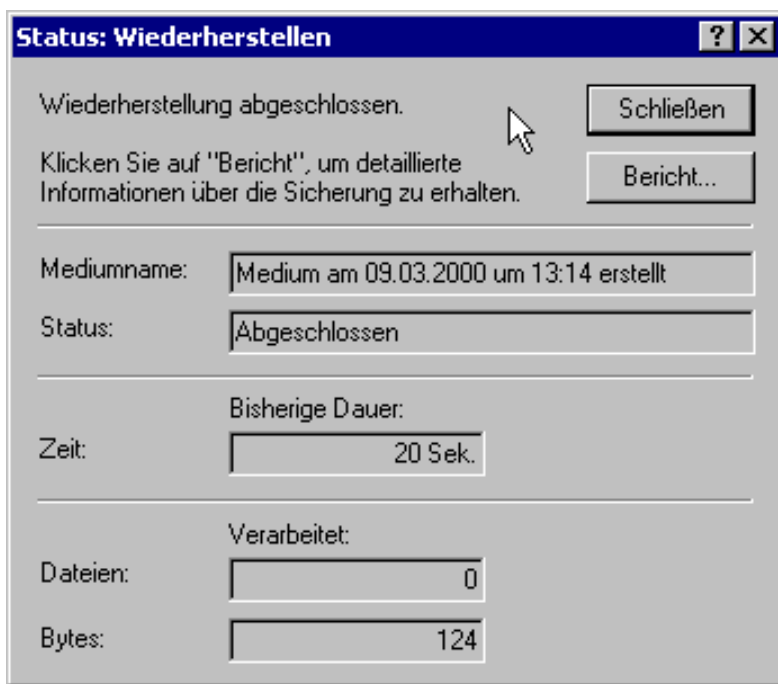


Abbildung 23.31: Anzeige eines abgeschlossenen Wiederherstellungs-prozesses

Öffnen Sie einige der wiederhergestellten Dateien und Ordner um sicherzustellen, dass die Daten korrekt rekonstruiert wurden und ihre Integrität bewahrt wurde (Sie brauchen dazu möglicherweise eine Anwendung, die die Gültigkeit der wiederhergestellten Daten überprüft). Um den Wiederherstellungsprozess abzuschließen, beenden Sie einfach das Sicherungsprogramm von Windows 2000.

23.3.1 Maßgebende Wiederherstellung

Bei der Wiederherstellung betriebskritischer Systemstatusdaten, an der mehrere Domänencontroller in Ihrem Windows 2000 Server-Netzwerk beteiligt sind, sollten Sie eine so genannte *maßgebende Wiederherstellung* ausführen. Wenn Sie versuchen, verteilte Dienste wie etwa Active Directory, das SYSVOL-Verzeichnis oder die Windows 2000 Server-Registrierung wiederherzustellen, müssen Sie eine maßgebende Wiederherstellung ausführen, vor dem Neustarten des Servers, aber nach der Wiederherstellung der eigentlichen Dateien.

Falls Sie keine maßgebende Wiederherstellung ausführen, werden die von Ihnen wiederhergestellten Daten auf anderen Windows 2000-Domänencontroller als »ältere« Daten in Ihrer Windows 2000-Umgebung betrachtet. Bei einer normalen Datenwiederherstellung rekonstruieren Sie Ihre Active Directory-Objekte mit ihrer ursprünglichen Nummerierung. Das bedeutet, die Objektnummern sind auf alle Fälle niedriger als die von Objekten desselben Namens, die es im replizierten Modus irgendwo im Windows 2000-Netzwerk gibt. Diese neu wiederhergestellten Objekte werden dann irgendwann durch ältere Objekte ersetzt, was die gesamte Active Directory-Struktur Ihres Unternehmens zerstört. Um das zu verhindern, führen Sie im Betriebssystem Windows 2000 Server die maßgebende Wiederherstellung aus.

Für eine maßgebende Wiederherstellung nehmen Sie zuerst eine normale Wiederherstellung der Systemstatusdaten vor. Anschließend starten Sie Ihren Windows 2000-Server nicht neu. Stattdessen öffnen Sie die Eingabeaufforderung und führen das Dienstprogramm *NtdsUtil* aus. Sie finden es im Ordner `%systemroot%\system32` (möglicherweise müssen Sie es von der Installations-CD-ROM von Windows 2000 laden, falls es noch nicht auf Ihrem Windows 2000-Server vorhanden ist). Es hat den vollständigen Namen *NtdsUtil.exe* (aktuell in der Version 2.0 vorliegend). Das Dienstprogramm *NtdsUtil* markiert automatisch die wiederherzustellenden Active Directory-Objekte zur maßgebenden Wiederherstellung. Das bedeutet, Windows 2000 aktualisiert die laufende Nummer für jedes Objekt, das für die maßgebende Wiederherstellung vorgesehen ist. Das wiederum bedeutet, dass die fortlaufende Nummer, die diesen Active Directory-Objekten zugewiesen wird, höher als die Nummern aller replizierten Versionen dieser Objekte ist und damit verhindert wird, dass die neu wiederhergestellten Systemstatusdatendateien überschrieben werden.

Zur Ausführung dieses Dienstprogramms gehen Sie zur Eingabeaufforderung und geben den Befehl *NtdsUtil* ein. Das Programm wird sofort ausgeführt und gibt in der Eingabeaufforderung den Prompt *NtdsUtil: aus* (Sie haben Recht, dieses Werkzeug ist tatsächlich etwas seltsam). Hier geben Sie den vollen Namen *Authoritative Restore* ein und drücken die

(Enter)-Taste. Jetzt starten Sie Ihren Windows 2000-Server neu, sodass die maßgebende Wiederherstellung mit dem Neustart Ihres Windows 2000-Servers abgeschlossen wird.

23.3.2 Wiederherstellung verschlüsselter Dateien

Die Wiederherstellung von mit EFS (Encrypting File Service) verschlüsselten Dateien und Ordnern ist ganz einfach, vorausgesetzt, Sie versuchen nicht, diese auf einem anderen Computer auszuführen (auf dem sie nicht erzeugt und verschlüsselt wurden). Eines aber müssen Sie unbedingt beachten: Wenn Sie ein servergespeichertes Benutzerprofil verwenden, mit dem Sie sich auf einem Computer anmelden können, der nicht unter Windows 2000 läuft, und dort die verschlüsselten Dateien wiederherstellen wollen, funktioniert die Wiederherstellung genauso, als wären Sie lokal am Original-Computer angemeldet.

Aus diesem Grund wollen wir hier annehmen, dass Sie auf einem anderen Computer ohne servergespeichertem Benutzerprofil arbeiten. Als Erstes exportieren Sie Ihr Verschlüsselungszertifikat und den privaten Schlüssel vom ursprünglichen Windows 2000-Server-Computer. Dazu öffnen Sie eine MMC-Konsole mit Zertifikaten, klicken im Detailbereich auf das zu exportierende Zertifikat und wählen anschließend im Menü **Vorgang** den Befehl **Alle Aufgaben/Exportieren**. Geben Sie an, dass die .PFX-Datei auf einer Diskette angelegt werden soll. (Weitere Informationen über das Exportieren von Verschlüsselungsdaten und privaten Schlüsseln auf externe Geräte finden Sie im Abschnitt über die Sicherheit in diesem Buch.)

Nachdem Ihnen die Diskette mit der .PFX-Datei vorliegt, bringen Sie diese zu dem neuen Computer. Dort legen Sie die Diskette in das Laufwerk ein und führen im Menü **Vorgang** den Befehl **Alle Aufgaben/Importieren** aus, sodass Sie diese .PFX-Datei in den lokalen persönlichen Speicher importieren können.

Anschließend können Sie die verschlüsselten Dateien auf dem neuen Computer wiederherstellen und nach Bedarf darauf zugreifen. Falls Sie anders vorgehen, können Sie nicht mehr auf die auf dem alten Windows 2000-Server-Computer verschlüsselten Dateien und Ordner zugreifen. Beachten Sie, dass Sie für die Wiederherstellung eine geeignete Maschine benutzen müssen, falls die Sicherungsdateien auf einem Windows 2000-Server mit 128-Bit-Verschlüsselung angelegt wurden. Es ist nicht möglich, Dateien und Ordner, die auf einem mit 128 Bit verschlüsselnden PC erstellt wurden, auf einem Computer mit nur 56 Bit Verschlüsselungsumfang wiederherzustellen.

23.4 Unterstützte Sicherungsgeräte

Das Betriebssystem Windows 2000 Server unterstützt zahlreiche Band- und Platten-Sicherungsgeräte. Am besten stellen Sie sicher, dass das von Ihnen verwendete Gerät unterstützt wird, indem Sie die Hardwarekompatibilitätsliste (HCL) von Windows 2000 konsultieren, die aus verschiedenen Quellen zur Verfügung steht.

- **Im Internet** - <http://www.microsoft.com/windows2000>
- **Microsoft TechNet** - Das einfachere Support-Abo von Microsoft, das eine elektronische Version der Hardwarekompatibilitätsliste für alle 32-Bit-Betriebssysteme beinhaltet.
- **MSDN (Microsoft Developer's Network)** - Ein weiterer Abo-Dienst von Microsoft, der eine elektronische Version der Hardwarekompatibilitätsliste für alle 32-Bit-Betriebssysteme beinhaltet.

Windows 2000 Server unterstützt sehr viel mehr Geräte als das ältere Windows NT (wo keine SCSI-Bandlaufwerke unterstützt wurden, was unter Windows 2000 Server nun sehr wohl der Fall ist). Am besten ziehen Sie die neueste Version der Hardwarekompatibilitätsliste zu Rate, bevor Sie ein neues Bandlaufwerk oder andere Sicherungssysteme für Ihren Windows 2000-Server kaufen.

23.5 Wiederherstellungskonsole

Ein weiterer Aspekt dieser neuen Technologie, den Sie unbedingt kennen sollten, ist die so genannte Wiederherstellungskonsole von Windows 2000. Dieses Befehlszeilenwerkzeug ermöglicht Ihnen, eine spezielle Konsole für das Starten und Beenden von Serverdiensten, die Formatierung von Festplatten usw. zu nutzen. Die Windows 2000-Wiederherstellungskonsole wird von der Installations-CD für Windows 2000 Server gestartet, sodass tiefer gehende Wiederherstellungstechniken für einen ausgefallenen Windows 2000-Server eingesetzt werden können. Beachten Sie, dass

diese neue Technologie sehr leistungsfähig ist und eine fehlerhafte Bedienung Ihren Windows 2000 Server-Computer zerstören kann. Erlauben Sie also nur wirklich erfahrenen Windows 2000-Systemadministratoren die Arbeit mit diesem Werkzeug.

Es gibt zwei Möglichkeiten, um die Wiederherstellungskonsole aufzurufen: von den Setup-Disketten für Windows 2000 bzw. der CD-ROM oder von einer installierten Version der Windows 2000-Wiederherstellungskonsole (die Sie auf den Produktionsservern in Ihrem Unternehmen nicht unbedingt bereitstellen sollten). Um die Wiederherstellungskonsole zu starten, wechseln Sie zur Setup-CD-ROM von Windows 2000 und führen den Befehl `\i386\winnt32.exe /CmdCons` aus.

Die Wiederherstellungskonsole wird gestartet. Folgen Sie den Anweisungen. Unter anderem gibt es die Möglichkeit, die Konsole permanent auf Ihrem Computersystem zu speichern. Beachten Sie, dass Sie als Systemadministrator oder als Mitglied der Administratorengruppe von Windows 2000 Server angemeldet sein müssen, um die Wiederherstellungskonsole ausführen zu können.

23.6 Notfalldisketten

Die Notfalldiskette von Windows 2000 Server macht dasselbe wie die Windows 98-Notfalldiskette. Im Wesentlichen dient sie dazu, Probleme mit Ihren Basisdateien für Windows 2000 Server, der Startumgebung (insbesondere praktisch bei Dual- oder Multi-Boot-Konfigurationen) und Ihrem Partitionsbootsektor zu korrigieren. Es ist ganz einfach, diese Diskette anzulegen. Rufen Sie einfach das Sicherungsprogramm von Windows 2000 auf und legen Sie die Notfalldiskette an.

Rufen Sie das Sicherungsprogramm von Windows 2000 Server auf. Klicken Sie dazu im Startmenü auf **Programme/Zubehör/Systemprogramme/Sicherung**.

Klicken Sie auf die Schaltfläche **Notfalldiskette** (unten im Startbildschirm), um das Dialogfeld **Notfalldiskette** zu öffnen (Abbildung 23.32).

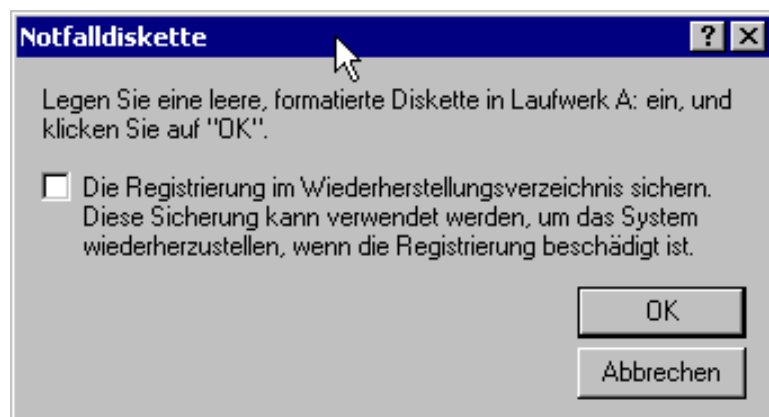


Abbildung 23.32: Anlegen einer Notfalldiskette

Für das Anlegen der Notfalldiskette brauchen Sie zwei Dinge: ein Diskettenlaufwerk (HD-DD, 1,44 MB) und eine leere, formatierte Diskette für dieses Laufwerk. Legen Sie die leere Diskette in das Laufwerk, stellen Sie sicher, dass dieses korrekt an den Windows 2000-Server angeschlossen ist (insbesondere gilt das für Laptops) und klicken Sie auf die Schaltfläche **OK**, um die Notfalldiskette anzulegen. Nachdem der Prozess abgeschlossen ist, nehmen Sie die Diskette aus dem Laufwerk und bewahren sie an einem sicheren, trockenen Ort auf. Schließen Sie das Sicherungsprogramm von Windows 2000 Server. Fertig.

23.7 Sicherungswerkzeuge von Drittanbietern

Es gibt zahlreiche Sicherungswerkzeuge von Drittanbietern, die unter Windows NT ausgezeichnet funktioniert haben und es wohl auch unter Windows 2000 tun. Unter anderem finden Sie hier die Sicherungswerkzeuge von Veritas Software Corporation oder die BackupExec-Software von Seagate, die mit allen Versionen von Windows 2000 kompatibel sind. Stellen Sie jedoch sicher, dass Sie die neueste Version Ihres Sicherungswerkzeugs verwenden, falls das Sicherungsprogramm von Windows 2000 Server für Ihre Einsatzzwecke nicht ausreicht.

Kapitel 24 Wiederherstellung nach Systemausfällen

Wenn Sie dieses Kapitel lesen, nachdem eine Katastrophe aufgetreten ist, lesen Sie es zum falschen Zeitpunkt. Sie sollten sich auf eine systematische Wiederherstellung vorbereiten, falls eine Katastrophe passiert ist. Das Problem bei den meisten Katastrophen ist, dass man nicht darauf vorbereitet ist. Und genau das sollte Ihnen helfen - Vorbereitung. Sie sollten sich nicht erst um eine Wiederherstellung kümmern, nachdem eine Festplatte ausgefallen ist, sondern von dem Moment an, wo sie installiert wird.

Es gibt die unterschiedlichsten Katastrophen. Es kann sein, dass nur ein Festplattenlaufwerk oder ein Server rekonstruiert werden muss, bei Naturkatastrophen können aber auch ganze Büros oder Gebäude zerstört werden. Wir können hier nicht über alle möglichen Szenarios sprechen, aber wir können Ihnen die Werkzeuge zeigen, die Sie für die Katastrophenplanung brauchen. Aber eine Planung ist immer vonnöten. Versuchen Sie nicht erst dann eine Wiederherstellung der Daten von Band vorzunehmen, nachdem ein Server in Ihrem Unternehmen ausgefallen ist.

24.1 Machen Sie einen Plan und halten Sie sich daran

Als Erstes brauchen Sie etwas, was es in den meisten Unternehmen nicht gibt - einen Plan. Und dieser Plan soll nicht nur in den Köpfen der Beteiligten herumgeistern, sondern schriftlich festgehalten werden - ein Plan für jede Art Katastrophe, Festplattenausfall, Serverausfall oder Feuer. Mit Hilfe von Plänen für die Wiederherstellung legen Sie allgemeine Strategien für verschiedene Ausfallkategorien fest - aber ein Plan muss sein.

Beim Einrichten eines Wiederherstellungsplans müssen Sie zunächst definieren, was *Wiederherstellung* für Ihr Unternehmen bedeutet. Für einige Unternehmen reicht es aus, alle Daten und Ressourcen innerhalb von 24 oder 48 Stunden wieder zur Verfügung zu haben. In anderen werden nur die Kundendaten sofort wieder gebraucht. In der Finanzwelt können Minuten Millionenverluste bedeuten. Letztlich muss jedes Unternehmen selbst wissen, welche Strategie die sinnvollste ist.

Ein sinnvoller Plan sollte die folgenden Punkte umfassen:

- *Eine Liste der Angestellten.* Hier werden die Angestellten aufgeführt, die für die verschiedenen Punkte des Plans verantwortlich sind (Sicherungsdatenträger, Hardwaresysteme, Herstellerinformation) sowie die zu benachrichtigenden Hersteller.
- *Physischer Plan.* Ein Übersichtsplan der Hardware und des Standorts.
- *Dokumentation.* Eine Liste der Hardware, Telefonnummern von Angestellten, chronologische Aufzeichnung der Ereignisse und Treffpunkte.

Sie brauchen auf alle Fälle einen Plan und müssen ihn befolgen. Gibt es zwar einen Plan, wird dieser aber nicht befolgt, kann das Ganze eher schaden als nutzen. Die Leute verlassen sich auf ein System, nachdem es einmal funktioniert, und machen sich keine eigenen Gedanken, wenn es einen Plan gibt, von dem sie annehmen, er würde auch sie berücksichtigen.

24.1.1 Dokumentation und Ereignisse

Bei der Formulierung eines Plans zur Wiederherstellung im Katastrophenfall sollten Sie so viele Leute wie möglich einbeziehen, um die richtigen Entscheidungen zu treffen. Sie sollten nicht erst bei einem Meeting nach der Katastrophe feststellen, dass Sie die falschen oder nicht genügend Daten haben. Am besten befragen Sie einen Verantwortlichen für jede Gruppe, die mit den betreffenden Servern arbeiten.

Die Dokumentation muss die folgenden Dinge beinhalten:

- Hardwarelisten
 - Computersysteme, die für die Wiederherstellung erforderlich sind.
 - Bandlaufwerke und Software für die Wiederherstellung von Sicherungsdatenträgern.
 - Telefonleitungen und gemietete Leitungen, die für die Neueinrichtung von WAN-Verbindungen erforderlich sind.
 - Allgemeine Büroausstattung (Papier, Stifte, Ordner usw.)



Ihr ISP kann Ihnen helfen, Ihre Internet-Präsenz wieder einzurichten, indem er Ihrem Unternehmen die ISP-Site zur Verfügung stellt. Treffen Sie die Abkommen im Voraus.

- Angestellten-Telefonlisten
 - Private Telefonnummern aller Angestellten, die von der Katastrophe betroffen sind.
 - Wenn möglich, sollten Sie diese Telefonlisten außerhalb des Unternehmens aufbewahren. Auf diese Weise stehen sie auch zur Verfügung, wenn die Katastrophe größere Ausmaße hat.
- Unterstützung von Herstellern
 - Auflistung aller Garantien und Verträge mit den Herstellern.
 - Wichtige Techniker und Support-Personal.
 - Verkäufer, die Ihnen helfen, die erforderliche Ausrüstung zu beschaffen.
- Chronologische Auflistung der Ereignisse
 - Ereignislisten für alle Szenarien, unter anderem Festplattenausfall, Datenzerstörung, Naturkatastrophe (Standortverlust), Stromausfall usw.
 - Wann die Ereignisse stattfinden müssen.
 - Die Ereignisse, die andere Ereignisse auslösen.
- Treffpunkte
 - Einfache Treffpunkte zur Besprechung der Maßnahmen (Filialbüros, Restaurants, Hotels usw.).
 - Mögliche Büros im Unternehmen, die Angestellte oder Hardware im Falle einer größeren Katastrophe aufnehmen können.

24.1.2 Katastrophenbeauftragte

Es ist keine einfache Aufgabe, diese Gruppen zu planen. Man will schließlich nicht, dass die Beteiligten schreiend davonlaufen, wenn sie glauben, der Himmel fiele ihnen auf den Kopf. Panik kann diese Meetings sehr schnell sprengen und wenn sie ausbricht, kann das Ganze noch schneller ausarten. Die Gruppen brauchen eigene Kontrollen, eigene Hardware und eigene Pläne.

Bei der Rekrutierung eines Vertreters aus der Führungsebene sollten Sie darauf hinweisen, dass dieser Computerkenntnisse benötigt. Er muss die Konzepte von Festplattenspeicher, RAM und Sicherung verstehen und den Unterschied zwischen einem Server und einer Workstation kennen. Er muss kein Ingenieur sein, aber zumindest über grundlegende Kenntnisse verfügen. Wenn Sie diesen Gruppenmitgliedern mitteilen, dass die Daten auf der ausfallträchtigsten Komponente des Servers gespeichert werden, sollte niemand aus allen Wolken fallen.

Die Gruppe sollte nicht nur aus Mitgliedern des Rechenzentrums bestehen. Man braucht Vertreter aus dem gesamten Unternehmen. Die Katastrophe betrifft die ganze Firma und die Pläne für die Wiederherstellung müssen sich ebenfalls auf die ganze Firma erstrecken. Damit vermeiden Sie Anfeindungen und Missverständnisse. Wenn der Vertreter der Buchhalter beim Meeting sagt, dass man 24 Stunden Ausfallzeit kompensieren kann, wird es sehr viel einfacher anzukündigen, dass die neue Festplatte für den Buchhaltungsserver morgen früh eintreffen wird.

Die verschiedenen Aufgaben sollen an die Verantwortlichen verteilt werden. Damit überblickt jeder aus der Gruppe, wofür er zuständig ist. Jedem Mitglied sollte eine bestimmte Aufgabe übertragen werden.

24.1.3 Physische Betrachtungen

Man will ja den Teufel nicht an die Wand malen, aber das Firmengebäude könnte zerstört werden, sodass es nicht mehr zur Verfügung steht, und das Unternehmen deshalb schnell einen Ausweichstandort benötigt. Für viele Unternehmen würde durch den Geschäftsaufall die Existenz auf dem Spiel stehen.

Planung alternativer Standorte

Am besten ist es natürlich, wenn das Unternehmen in Filialbüros ausgelagert werden kann. Damit können bereits existierende Telefonleitungen, Unternehmensunterlagen und das dort vorhandene System genutzt werden - mehr oder weniger. Es könnte jedoch auch erforderlich sein, das Unternehmen in einem Hotel oder in einem fremden Gebäude unterzubringen. Ein Mitglied Ihrer Gruppe sollte für die nötigen Kontakte verantwortlich sein.

Hier einige Dinge, die Sie bei der Auswahl eines alternativen Standorts berücksichtigen sollen:

- Besteht eine ausreichende Stromversorgung?
- Kann die Netzwerk-WAN-Verbindung aufrechterhalten werden?
- Wie viele Telefonleitungen gibt es und sind sie ausreichend?
- Gibt es Möbel?
- Gibt es eine ausreichende Infrastruktur?

24.2 Wiederherstellung der Daten

Die Sicherung eines Servers und die Software, die dafür erforderlich ist, war Thema von Kapitel 23. Die dafür erforderliche Planung wird hier beschrieben.

Viele Administratoren verstehen unter der Serversicherung eine Methode, Daten nach dem Ausfall eines gesamten Laufwerks wiederherzustellen. Nutzen Sie sie aber vielmehr als Möglichkeit, beliebige Daten jederzeit wiederherzustellen. Die Sicherungsmedien können für unterschiedliche Formen der Datenwiederherstellung genutzt werden:

- Wiederherstellung nach Ausfall einer Festplatte
- Wiederherstellung nach Verlust einzelner Dateien
- Rücksetzen von Dateien auf einen früheren Inhalt
- Aufzeichnungen für chronologische oder Überwachungsaufgaben

Der Ausfall der gesamten Festplatte ist wohl der seltenste Fall bei der Wiederherstellung. Viel häufiger entstehen kleinere Katastrophen durch Fehler der Benutzer. Und diese Katastrophen können noch schlimmer sein als ein Hardwareausfall. Benutzerfehler werden oft tagelang, wochenlang und sogar monatelang nicht erkannt. Die Wiederherstellung der Daten von gestern ist also nicht ausreichend.

Beachten Sie außerdem, dass Sicherungsbänder ebenso defekt werden können wie Disketten, Videobänder oder Kassetten. Es handelt sich dabei um magnetische Datenträger, die nur eine gewisse Zeit lang genutzt werden können. Aus diesem Grund sollten Sie immer wieder testen, ob die Sicherung wiederhergestellt werden kann. Nichts ist perfekt und sogar ein gutes System wird älter.

Netzwerktechniker sind immer wieder erstaunt, wenn ihnen mitgeteilt wird, dass die ausgeführte Wiederherstellung die erste ist, die jemals durchgeführt wurde. Trauen Sie niemandem. Auch nicht Ihrem Sicherungssystem. Testen Sie Ihre Sicherungen und stellen Sie das System auch einmal selbst wieder her.

24.2.1 Sicherungsoperationen

Aufgrund dieser Probleme sollten Sie die verschiedenen Sicherungsarten kennen und wissen, welche Sicherungspläne eingerichtet werden können. Hier einige Faustregeln, die für jede Datenwiederherstellung berücksichtigt werden sollten:

- Automatisieren Sie den Sicherungsprozess so weit wie möglich. Menschen vergessen Dinge. Egal wie gut die Vorsätze sind - sie vergessen die Dinge zu den unpassendsten Gelegenheiten (Beispiele dafür folgen in den anderen Regeln).
- Vermeiden Sie Fehlermöglichkeiten, indem Sie möglichst wenig Variablen zulassen. Jede neue Komponente kann einen Ausfall verursachen (Menschen zählen als Doppelfehler).
- Versuchen Sie immer, die Sicherung auf einem einzigen Datenträger unterzubringen. Auf diese Weise ist der Eingriff durch den Menschen so gering wie möglich zu halten. Wird ein Band gewechselt, muss das Sicherungsprogramm kurzzeitig darauf warten und möglicherweise werden einige Dateien schon wieder genutzt, wenn die Sicherung fortgesetzt wird. Automatische Bandwechsler können Bänder wechseln und sind der manuellen Bedienung vorzuziehen. Jedes zusätzliche Band stellt einen möglichen Fehlerfall dar.

- Sichern Sie zu Zeiten geringer Auslastung. Damit gewährleisten Sie eine optimale Leistung Ihres Servers und Netzwerks. Auf Servern sind zu Spitzenzeiten des Tages Dateien geöffnet, die nicht gesichert werden, weil sie geöffnet sind. Es könnte sogar erforderlich sein, dass sich die Benutzer vor der Sicherung abmelden. Es gibt jedoch Dienstprogramme, mit denen auch geöffnete Dateien gesichert werden können. Ein Server, auf dem eine Sicherung ausgeführt wird, bedient jedoch seine Clients nicht so effizient wie gewöhnlich.

Während der Spitzenzeiten wird das Netzwerk schwer belastet, wenn der Sicherungsserver Daten von anderen Servern abrufen. Die Sicherung eines Servers verursacht einen konstanten Datenfluss im Netzwerk, im Gegensatz zu den gelegentlichen Abfragen der Benutzer. Einige Systeme beinhalten aus diesem Grund ein SAN (Server Area Network = Serverbereichsnetzwerk), das für die Sicherung des Servers verwendet wird.

Viele Sicherungsprogramme beinhalten Dienstprogramme, für die der Server mehr Ressourcen für die Weitergabe von Dateien für die Sicherung bereitstellen muss. Damit wird die den Benutzern gebotene Leistung noch weiter reduziert.



Ein SAN (Server Area Network = Serverbereichsnetzwerk) ist ein Netzwerk, das insbesondere für die Serverkommunikation entwickelt wurde. Dabei kann es sich um einfache Ethernet-Segmente handeln, die bestimmten Servern zugeordnet sind, oder um riesige eigenständige Systeme.

Bei Ausführung einer Sicherung kann das Archivattribut der Datei geändert werden, um sie als gesichert zu kennzeichnen. Wird in die Datei geschrieben, wird das Attribut wieder zurückgesetzt. Auf diese Weise kann die Sicherung unterscheiden, welche Dateien sich geändert haben, falls eine komplexere Sicherungsmethode angewendet wird. Es gibt drei Sicherungsmethoden, die für die Sicherung von Servern angewendet werden können. Die Auswahl, die Sie hier treffen, wirkt sich auf die Sicherungsgeschwindigkeit, die Wiederherstellungsgeschwindigkeit und die Anzahl der verwendeten Sicherungsmedien aus. Hier die drei Arten:

- **Vollständige Sicherung.** Eine Sicherung aller Daten auf einer bestimmten Ressource (Laufwerk oder Freigabe). Wird für das Laufwerk C: eine vollständige Sicherung vorgenommen, werden alle Dateien von diesem Server auf das Band gesichert, unabhängig davon, wann die letzte Sicherung stattgefunden hat und ob seitdem Änderungen vorgenommen wurden. Im Allgemeinen wird bei einer vollständigen Sicherung das Archivattribut geändert und zeigt damit an, dass die Dateien gesichert wurden.

Einige Vorteile dieser Sicherungsart:

- Alle Daten befinden sich in einem Sicherungssatz.
- Die Datei kann ganz einfach wiederhergestellt werden.
- Es sind weniger Eingriffe durch das Bedienpersonal erforderlich.

Einige Nachteile dieser Sicherungsart:

- Es werden mehrere Speichermedien benötigt (Bänder, optische Datenträger, Platten).
- Die Sicherung dauert länger.
- **Inkrementelle Sicherung.** Dateien werden abhängig vom Status des Archivattributs gesichert. Alle Dateien, die sich seit der letzten Sicherung geändert haben, werden gesichert. Das Archivattribut wird immer gesetzt, um anzuzeigen, dass die Datei gesichert wurde.

Einige Vorteile dieser Sicherungsart:

- Es werden weniger Datenträger für die Sicherung benötigt.
- Die Sicherung erfolgt schneller.
- Die Wiederherstellung einzelner Dateien ist schneller, weil weniger Bänder durchsucht werden müssen, um eine Datei zu finden.

Einige Nachteile dieser Sicherungsart:

- Für die Wiederherstellung müssen Sie wissen, auf welchem Band die Daten enthalten sind.
- Eine vollständige Wiederherstellung dauert länger, weil dafür die letzte vollständige Sicherung sowie alle inkrementellen Sicherungen benötigt werden.
- Differenzielle Sicherung. Dateien werden abhängig davon gesichert, wann sie seit der letzten »vollständigen« Sicherung gesichert wurden (vollständig ist der Unterschied zwischen inkrementell und differenziell). Wird beispielsweise am Freitag eine vollständige Sicherung ausgeführt und am Montag ändert sich eine Datei, wird diese Datei täglich und inklusive in der letzten vollständigen Sicherung gesichert. Damit ist eine schnellere Wiederherstellung gewährleistet. Weil der aktuelle Status der Datei jetzt auf einem von zwei Bändern aufgezeichnet ist, müssen Sie nicht mehr zahllose inkrementelle Bänder durchsuchen.

Einige Vorteile dieser Sicherungsart:

- Die vollständige Sicherung ist schneller als die inkrementelle Sicherung.
- Es werden weniger Bänder benötigt als bei einer weiteren vollständigen Sicherung.
- Die Sicherung dauert nicht so lange wie eine vollständige Sicherung.

Einige Nachteile dieser Sicherungsart:

- Für die Wiederherstellung von Daten muss man wissen, welches Band die Daten enthält.
- Die vollständige Wiederherstellung dauert länger, weil die letzte vollständige Sicherung sowie ein differenzielles Band benötigt werden.

24.2.2 Zeitabhängige Sicherungspläne

Ein Sicherungsplan bedeutet, dass Sie eine Methode haben, Daten zu sichern und zu speichern, die eine einfache Wiederherstellung über einen ausreichend langen Zeitraum erlauben. Dieser Zeitraum ist variabel. Einige Unternehmen können sich leisten, Daten von einer ganzen Woche zu verlieren, während andere nicht einmal die der letzten 24 Stunden verschmerzen können. Wieder andere Unternehmen müssen Datensätze von den letzten sieben Jahren aufbewahren.

Wie bereits erwähnt, sollte die Sicherung nicht als Maßnahme der Fehlertoleranz verstanden werden. Es ist eine Methode, Daten wiederherzustellen, die geändert wurden. Beispielsweise könnte bei dieser Änderung das Buchhaltungshauptbuch geschlossen worden sein, das jetzt neu geöffnet werden muss, oder eine Festplatte ist ausgefallen. Die Daten müssen in jedem Fall nach einem konsequenten Plan gesichert und wiederhergestellt werden.

GFS (Grandfather/Father/Son, Großvater/Vater/Sohn)

Das GFS-Konzept für die Sicherungsrotation soll die Möglichkeit bieten, Daten von bis zu fünf Tagen wiederherstellen, von bis zu vier Wochen und von beliebig vielen Monaten. Die Namensgebung dieser

Methode basiert auf der Beziehung, die die Bänder im Gesamtsicherungssatz zueinander haben.

Das Rotationsschema verwendet tägliche Bänder (Montag, Dienstag, Mittwoch, Donnerstag), wöchentliche Bänder (Freitag 1, Freitag 2, Freitag 3, Freitag 4, Freitag 5) und ein Band für jeden neuen Monat (siehe Tabelle 24.1). Hier das Schema:

- Sohn. An jedem Wochentag (Montag, Dienstag, Mittwoch und Donnerstag) wird eine vollständige Sicherung auf dem zugehörigen Band ausgeführt.
- Vater. Freitags wird das Band für den jeweiligen Freitag des Monats (Freitag 1, Freitag 2, Freitag 3, Freitag 4, Freitag 5) für eine weitere vollständige Sicherung benutzt.
- Großvater. Am letzten Tag des Monats wird das Band für den jeweiligen Tag entfernt, markiert und als Monatsband aufbewahrt. Dem Sicherungssatz wird ein neues Band für diesen Tag hinzugefügt.

Die Bänder für die Freitage und die Monate sollten irgendwo außerhalb der Firma aufbewahrt werden um zu vermeiden, dass im Katastrophenfall mit einer etwaigen Zerstörung des Servers auch die Daten zerstört werden. Dieses Schema wird in den unterschiedlichsten Variationen eingesetzt.

Wochentag (1. Monat)	Band
Montag	Montag
Dienstag	Dienstag
Mittwoch	Mittwoch
Donnerstag	Donnerstag
Freitag	Freitag 1
Montag	Montag
Dienstag	Dienstag
Mittwoch	Mittwoch
Donnerstag	Donnerstag
Freitag	Freitag 2
Montag	Montag
Dienstag	Dienstag
Mittwoch	Mittwoch
Donnerstag	Donnerstag
Freitag	Freitag 3
Montag	Montag
Dienstag	Dienstag
Mittwoch	Mittwoch

Donnerstag	Donnerstag
Freitag	Freitag 4

Tabelle 24.1: Bandrotationsschema für vier Wochen

Eine Variation wäre, ein einziges Band für die Sicherung von Montag bis Donnerstag (tägliches Band) zu verwenden und diese Sicherung differenziell vorzunehmen. Damit spart man Datenträger, verursacht aber auch eine Lücke für die wöchentliche Wiederherstellung, falls die Wiederherstellung von diesem einen täglichen Band fehlschlägt, sodass das Unternehmen die Daten von einer ganzen Woche rekonstruieren müsste.

Falls die vollständige Sicherung mehr als ein Band umfasst, könnten für die Bänder von Montag bis Donnerstag inkrementelle oder differenzielle Sicherungen ausgeführt werden. Damit behält man die Stabilität durch Nutzung mehrerer Bänder bei, spart aber durch die inkrementellen oder differenziellen Sicherungen Datenträger.

Die Türme von Hanoi

Das Schema der Türme von Hanoi ist etwas komplexer, um die Wiederherstellung älterer Daten innerhalb einer Rotation zu ermöglichen und eine gewisse Sicherheit zu bieten. Die Vorgehensweise ist sehr kompliziert. Dabei werden weniger Bänder verwendet, aber die Daten können ebenfalls für einen längeren Zeitraum rückwirkend wiederhergestellt werden.

Das Rotationsschema folgt einem Muster, in dem Bänder mit den Bezeichnungen A bis E verwendet werden:

- Band A wird als Erstes verwendet und dann für jede zweitnächste Sicherung, d.h. an den Tagen 1, 3, 5, 7, 9 usw. (also an den Tagen mit den ungeraden Nummern).
- Band B wird als Zweites verwendet und dann für jede viertnächste Sicherung, d.h. an den Tagen 2, 6, 10, 14, 18 usw.
- Band C wird am vierten Tage verwendet und dann für jede achtnächste Sicherung, d.h. an den Tagen 4, 12, 20, 28, 36 usw.
- Band D wird am achten Tag verwendet und dann für jede sechzehnnächste Sicherung, d.h. an den Tagen 8, 24, 40, 56, 72 usw.
- Band E wird am sechzehnten Tag verwendet und dann für jede sechzehnnächste Sicherung, d.h. an den Tagen 16, 32, 48, 64, 80 usw.

Sie sollten sich den Algorithmus auf Papier aufzeichnen. Er ist interessant, weil keine Wiederholung auftritt (siehe Tabelle 24.2). Dabei wird eine bestimmte Anzahl von Bändern für die Rotation innerhalb unterschiedlicher Zeitabstände genutzt. Die A-Bänder beispielsweise enthalten immer relativ aktuelle Daten. Die Bänder D und E dagegen enthalten ältere Daten.

Wochentag (1. Monat)	Band
Montag	A
Dienstag	B

Mittwoch	A
Donnerstag	C
Freitag	A
Montag	B
Dienstag	A
Mittwoch	D
Donnerstag	A
Freitag	B
Montag	A
Dienstag	C
Mittwoch	A
Donnerstag	B
Freitag	A
Montag	E

Tabelle 24.2: Bandrotation für 16 Tage



Der französische Mathematiker Edouard Lucas hat 1983 die Türme von Hanoi als Puzzle für Studenten geschaffen. Die Studenten erhielten Stapel mit acht Scheiben aufsteigender Größe, von unten nach oben geordnet, und drei Stangen. Die Scheiben wurden auf eine der Stangen gesteckt. Bei dem Puzzle musste der gesamte »Turm« von einer Stange auf eine andere gesteckt werden. Dabei durfte bei jedem Zug nur eine Scheibe bewegt werden und es durfte nie eine größere Scheibe auf einer kleineren Scheibe zu liegen kommen.

Dieses System verwendet unterschiedliche Bandnummern, die vom Administrator gewählt werden. Wenn er beispielsweise vier B-Bänder verwendet, werden diese (B1, B2, B3, B4) ähnlich verwendet wie die Freitagsbänder des GFS-Plans. Durch die seltsamen Kombinationen der Bandnutzung ist es relativ kompliziert, diese Rotation einzusetzen. Darüber hinaus braucht die Rotation 16 Tage, bevor die Bänder wiederverwendet werden, und eine Wiederherstellung über 24 Tage hinaus ist nicht möglich, ohne ein Band zu archivieren.

Viele Unternehmen verwenden dieses Schema und ersetzen Bänder aus Archivierungszwecken. Sie sollten sich dann aber fragen, warum Sie nicht einfach den GFS-Ansatz verwenden, in dem die Archivierung Teil des Schemas ist.

Einige Vorteile dieser Methode:

- Es sind weniger Bänder für einen langen Zeitraum erforderlich. Eine Rotation umfasst 16 Tage.
- Weil das System so kompliziert ist, ist es weniger gefährdet gegenüber Missbrauch.

Einige Nachteile dieser Methode:

- Die Wiederherstellung kann sehr frustrierend sein. Man muss das Rotationsschema dafür wirklich verstehen.
- Weil das System so kompliziert ist, wird es nicht ohne Bedenken genutzt.
- Es ist schwierig zu erklären und zu implementieren. Wird der Zyklus unterbrochen, ist die Wiederherstellung unter Umständen nicht mehr möglich.

24.3 Maßnahmen gegen Hardwareausfall

Die beweglichen Teile einer Maschine sind am ausfallträchtigsten. In einem PC ist die Festplatte das einzige Teil, das sich ständig bewegt. Festplatten drehen sich wie eine Schallplatte auf einem Plattenspieler, vom Anschalten bis zum Abschalten. Einige Festplatten werden aus Energieersparnisgründen angehalten, aber auf einem Server sollte das nicht der Fall sein.

Die Festplatte enthält alle im PC gespeicherten Daten. Falls der gesamte PC ausfällt und die Festplatte gerettet werden kann, können die Daten ganz einfach wiederhergestellt werden. Damit wird die Festplatte zum wichtigsten Teil im Server. Sie muss bei jedem Plan zur Wiederherstellung der Hardware berücksichtigt werden. Es gibt zwei wichtige Hardwareimplementierungen, die heute in den Servern eingesetzt werden, um den Inhalt der Festplatte bei Ausfall der Hardware zu retten.

Die gebräuchlichste ist Hardware-RAID (Redundant Array of Inexpensive Disks). Damit kann das Betriebssystem weiterarbeiten, falls eine oder mehrere Festplatten ausfallen, ohne dass das Betriebssystem den Fehler erkennen muss.

Eine Lösung, die immer gebräuchlicher und immer einfacher wird, ist das so genannte *Server-Clustering*. Dabei werden zwei Server an ein Festplattensystem angeschlossen und im Fehlerfall oder durch Eingreifen des Administrators kann zwischen den beiden Servern gewechselt werden. Heute werden diese Systeme hauptsächlich zur Realisierung von Fehlertoleranz eingesetzt, aber irgendwann wird ihre Nutzung weit darüber hinaus gehen.

24.3.1 Hardware-RAID

RAID wurde bereits in Kapitel 4 als Teil des Betriebssystems Windows 2000 Server beschrieben. Diese Form des RAID wird auch als Software-RAID bezeichnet, weil Verwaltung und Steuerung der Platten über das Betriebssystem erfolgen. Beim Hardware-RAID steuert der Festplattencontroller das RAID-System.

Der Vorteil dabei ist, dass das Betriebssystem keinen Aufwand für diesen Prozess hat, weder zeitlich noch ressourcenbedingt. Bei Hardwarelösungen enthält der Controller den Prozessor und das RAM, um die Umschaltung und die Fehlertoleranz zu verwalten. Auf diese Weise wird das System schneller.

Die Verwaltung der Kommunikation mit dem Controller wird vom Betriebssystem verwaltet, dient jedoch nur Warnungen. Dienstprogramme für diese Warnungen erlauben dem Betriebssystem, den Administrator im Fehlerfall zu benachrichtigen.

24.3.2 Geclusterte Server

Das Clustering von Systemen hat in der Computerwelt unterschiedliche Bedeutungen. Für das Betriebssystem bedeutet es, dass zwei Server an ein einziges Festplattensystem angeschlossen werden und dass die Steuerung im Fehlerfall oder durch Eingreifen des Administrators zwischen den beiden umgeschaltet werden kann.

Die Hardware in diesen Konfigurationen ist häufig eine proprietäre Kombination der folgenden Elemente (siehe Abbildung 24.1):

- Ein Festplattencontroller (SCSI oder Fibre) in jedem Server, der den Anschluss an das gemeinsame Festplattensystem erlaubt.
- Ein Festplattensystem mit den folgenden Elementen:
 - einem internen Festplattencontroller
 - Festplatten
 - einem Schrank

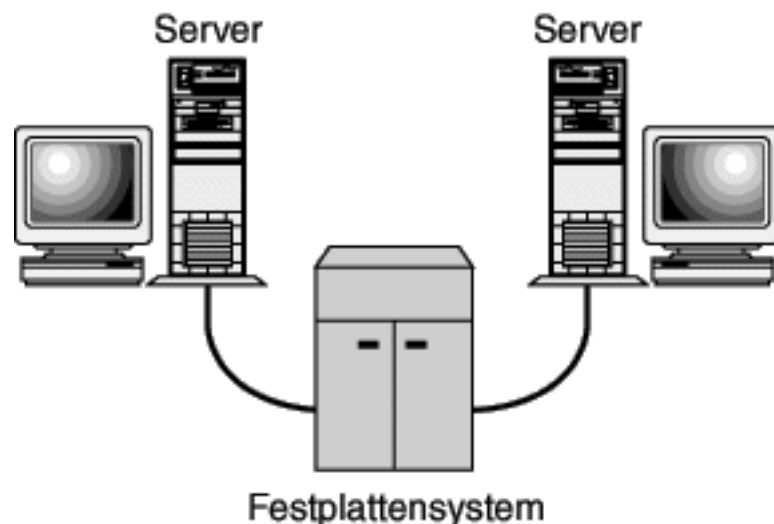


Abbildung 24.1: Windows-Server-Clustering

Die Verbindung zwischen den beiden Servern und dem Festplattensystem erfolgt abhängig von der Implementierung über SCSI oder Fibre Channel. Shared SCSI ist die ältere der beiden Lösungen und durch die physischen Grenzen der SCSI-Kabel und SCSI-Technologie eingeschränkter. Fibre Channel ist eine neuere Technologie und bietet die Vorteile, die Glasfaserkabel in Hinblick auf die Entfernung der Komponenten unterstützen. Darüber hinaus können mehrere Server und andere Peripherieverbindungen (auch Festplattenlaufwerke) an einem Zentralrechner angeschlossen werden.



Fibre Channel ist eine Technologie, die zur Verbindung von Massenspeicher mit mehreren Computern entwickelt wurde. Mittlerweile erlaubt sie auch den Anschluss anderer Peripheriegeräte.

Das Windows-Clustering in dieser Umgebung wird manchmal auch als *Shared Nothing* bezeichnet, weil die Systeme keinen gleichzeitigen gemeinsamen Zugriff auf den Speicher haben (siehe Abbildung 24.2). Jedes Gerät wird immer von einem einzigen Server angesprochen. Enthält ein Laufwerkssystem beispielsweise zwei logische Laufwerke, können die folgenden Kombinationen genutzt werden:

- Server 1 steuert die Laufwerke A und B.
- Server 2 steuert die Laufwerke A und B.
- Server 1 steuert Laufwerk A, Server 2 steuert Laufwerk B.
- Server 1 steuert Laufwerk B, Server 2 steuert Laufwerk A.

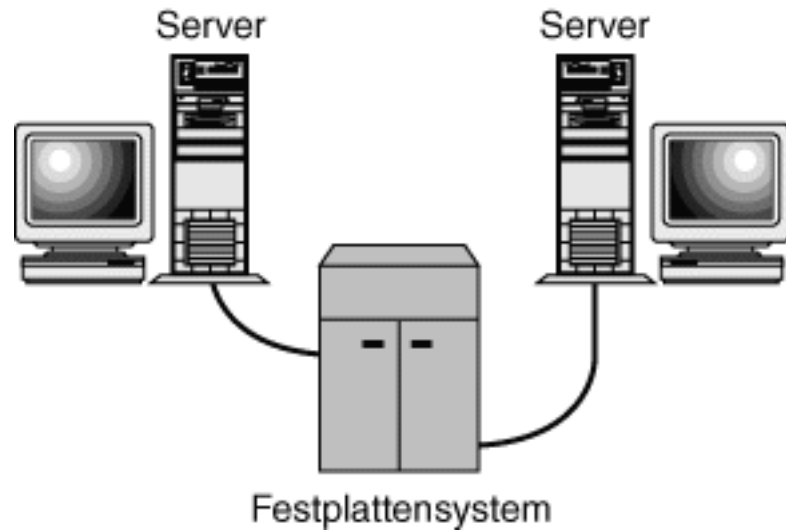


Abbildung 24.2: Ein Beispiel für Shared Nothing

Es gibt keinen Zeitpunkt, zu dem Server 1 und Server 2 gleichzeitig Laufwerk A steuern. Und sie können auch nicht gleichzeitig Laufwerk B steuern. Für beide sind nur die oben aufgelisteten Kombinationen möglich, es gibt keine gemeinsame Kontrolle.

Nachdem der gemeinsame Speicher eingerichtet ist, kann das Cluster angelegt werden. Für den Benutzer erscheinen die beiden Server unter demselben Namen. Das Cluster präsentiert sich unter diesem Namen, als handelte es sich um einen separaten »logischen« Server. Wie sich separate Festplatten als einziges logisches Laufwerk präsentieren können, können auch die beiden Server und ihre gemeinsamen Freigaben als ein logischer Server dargestellt werden.

In Abbildung 24.3 werden die Server 1 und 2 unter dem Namen »Cluster_1« geführt.

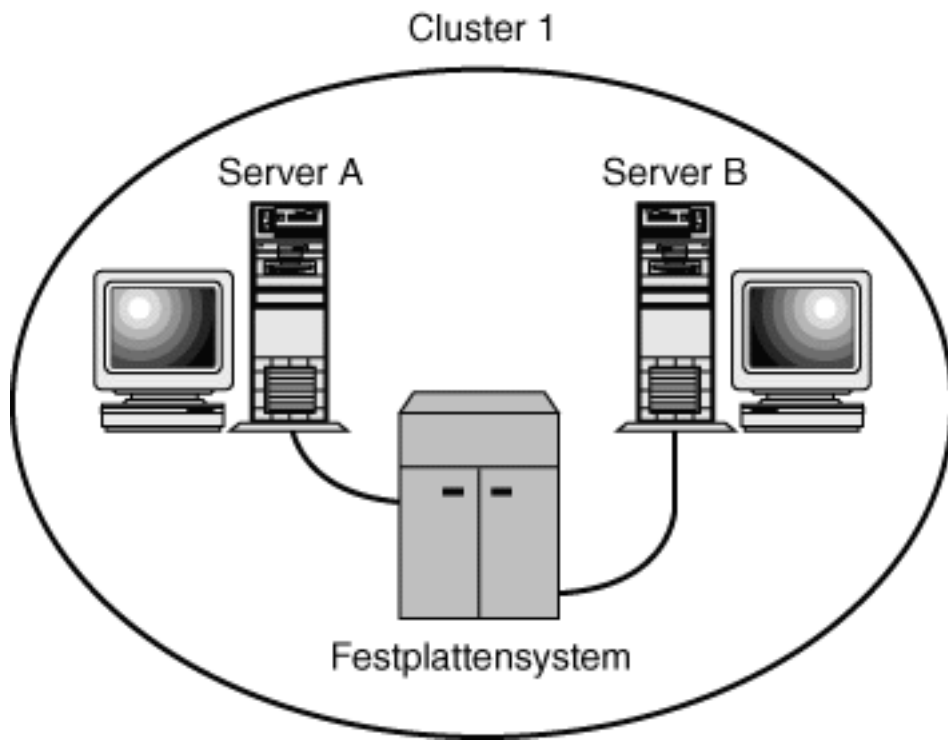


Abbildung 24.3: Die Cluster-Darstellung

Die Server teilen sich ihren aktuellen Status mit, indem sie sich über eine Netzwerkverbindung gegenseitig ein »Puls«- oder »Herzschlag«-Signal zusenden. Wenn ein Server im Cluster ausfällt (Software oder Hardware), wodurch der Prozessor angehalten wird, stoppt auch der Puls. Sieht ein Server seinen Partner im Cluster eine gewisse Zeit lang nicht mehr, übernimmt er die Aufgaben des Partners im Festplattensystem.

Weil alle Cluster-Ressourcen unter einem einzigen logischen Servernamen angezeigt werden, bemerken die Benutzer nichts von diesem Wechsel, außer vielleicht eine kleine Verzögerung. Das Clustering kann sich auf Druckerfreigaben und Festplattenfreigaben erstrecken und beim Umschalten sollte keine Unterbrechung auftreten.

Weil die Ressourcen sich auf den Laufwerken befinden, die der Cluster-Partner jetzt bedient, arbeitet der logische Server weiter.

Wie bereits erwähnt, können auch Festplatten ausfallen. Aus diesem Grund ist es sinnvoll, diese gemeinsamen Festplatten auch mit irgendeiner Form von Hardware-RAID auszustatten. Es ist nämlich nicht zweckmäßig, viel Geld für die Verfügbarkeit der Server auszugeben, um dann nach dem Ausfall einer Festplatte feststellen zu müssen, dass die Ressource nicht mehr zur Verfügung steht.

Das Clustering kann hier nicht im Detail besprochen werden, weil es Teil der Advanced Server-Version von Windows 2000 ist. Dennoch ist die Technologie wichtig und Sie sollten sie kennen.

Bald schon wird es möglich sein, mehrere Server in einer Art »Freibereichs«-Clustering an mehrere Festplattensysteme anzuschließen. Leider aber ist dies unter Windows 2000 Server heute noch nicht möglich. Es steht in Systemen wie beispielsweise Himalaya Non-Stop Systems von Compaq (Tandem) zur Verfügung. Mit Windows 2000 DataCenter ist dieser Prozess jedoch durchaus in greifbare Nähe gerückt.

© Copyright [Markt+Technik Verlag](#), ein Imprint der Pearson Education Deutschland GmbH
Elektronische Fassung des Titels: Windows 2000 Server Kompendium, ISBN: 3-8272-5611-9 Kapitel:
Wiederherstellung nach Systemausfällen

Anhang

Teil VII

A. Problemlösungen/Fehlerliste

B. Inhalt der CD-ROM zum Buch

© Copyright [Markt+Technik Verlag](#), ein Imprint der Pearson Education Deutschland GmbH
Elektronische Fassung des Titels: Windows 2000 Server Kompendium, ISBN: 3-8272-5611-9 Kapitel:
VII

Anhang A Problemlösungen/Fehlerliste

Es sieht zwar so aus, als wäre Windows 2000 stabiler als frühere Windows-Versionen, aber in jedem Betriebssystem können Fehler auftreten.

A.1 Service Packs

Jedes bessere Betriebssystem bietet kurz nach der Veröffentlichung einer neuen Version eine Art Patch oder Bug Fix. Ein Patch ist einfach eine Überarbeitung der Software zur Behebung eines erkannten Problems. Dabei kann das gesamte Teilsystem neu geschrieben sein, aber auch einfach nur eine Link-Datei.

Microsoft ist dafür bekannt, dass es immer sehr schnell Patches für seine Betriebssysteme bereitstellt, nachdem eine neue Version veröffentlicht wurde. Diese Patches heißen *Service Packs*. Für Windows NT 4.0 beispielsweise gibt es Service Pack 5.

Natürlich gibt es für Windows 2000 zum Zeitpunkt der Drucklegung dieses Buchs noch kein Service Pack. Sehen Sie einfach in gewissen Zeitabständen auf der Website von Microsoft unter <http://www.microsoft.com/windows/server/> nach.

A.2 STOP-Fehler

STOP-Fehler werden häufig auch als »Blue Screen of Death« bezeichnet, die bekannten blauen Bildschirme. Tritt ein solcher Fehler auf, wird der Server vollständig angehalten, daher auch der Name *STOP-Fehler*. STOP-Fehler können jederzeit auftreten, aber am häufigsten findet man sie nach der Installation neuer Software oder bei der eigentlichen Installation von Windows 2000.

Was Sie bei der Anzeige von STOP-Bildschirmen im Kernelmodus tun können

Die folgende Liste von Microsoft beschreibt die häufigsten STOP-Fehler von Windows 2000. Damit verschaffen Sie sich einen allgemeinen Überblick, was Sie erwartet und wie Sie mit diesen Fehlern umgehen.

1. Ermitteln Sie die folgende Information aus dem System:

- Die oberen vier Zeilen des STOP-Bildschirms. Im Allgemeinen sieht die dort bereitgestellte Information wie folgt aus:

```
STOP 0x0000000A(0x0000000B, 0x00000002, 0x00000000,  
0xFE34C882  
IRQL_NOT_LESS_OR_EQUAL  
ADDRESS 0xFE34C882 has base at 0xFE000000: NTOSKRNL.EXE
```

- Vollständige Hardwareinformation, unter anderem:
- Systeminformation (BIOS, CMOS-Einstellung usw.)
- Alle installierten Controller/Karten und deren BIOS-Version.
- Die Version des installierten Windows und der Service Packs, SSDs, Hotfixes und Treiber von Drittanbietern.

TIPP :-)
Der Begriff SSD wird von vielen Herstellern für die Software Support Disk verwendet, die zusammen mit der Hardware bereitgestellt wird. Diese Disketten enthalten häufig Treiber, Dienstprogramme und Erweiterungen des Betriebssystems.

- Wann der STOP-Bildschirm erscheint und wie häufig er erscheint. Sie sollten möglichst die Antworten auf die folgenden Fragen bereitstellen:
- Was hat sich seit dem letzten erfolgreichen Starten des Servers geändert?
- Erscheint der STOP-Bildschirm immer, wenn Sie eine bestimmte Operation ausführen?
- Wenn er scheinbar zufällig erscheint, wie oft passiert das?

2. Stellen Sie fest, ob das Problem bekannt ist und ein Hotfix oder eine Lösung dafür bereitstehen.

TIPP :-)
Ein Hotfix ist eine kleinere Änderung, die von Microsoft zwischen der Veröffentlichung von Service Packs bereitgestellt wird. Hat ein Kunde ein spezielles Problem, erhält er häufig Hilfe in Form eines Hotfix.

Im nächsten Schritt sollten Sie die Microsoft Knowledge Base sowie andere Ressourcen durchsuchen um festzustellen, ob es für Ihr Problem bereits eine Lösung gibt. Suchen Sie in der Microsoft Knowledge Base nach den folgenden Schlüsselwörtern:

- Suchen Sie nach dem Wort »STOP«, nach dem STOP-Code und den in den ersten vier Zeilen des STOP-Bildschirms als eine Zeichenkette angegebenen Programmmodulen. In unserem Beispiel würden Sie nach den Schlüsselwörtern STOP 0x0000000A NTOSKRNL.EXE suchen.
- Falls diese Suche kein Ergebnis bringt, suchen Sie einfach nach dem STOP-Code um festzustellen, ob es bereits Informationen zur allgemeinen Fehlersuche gibt. Bei einigen STOP-Fehlern erhalten Sie damit jedoch eine sehr umfangreiche Liste.

In diesen Suchergebnissen suchen Sie nach Beschreibungen, die die Symptome des Problems so genau wie möglich beschreiben, und wenden Sie die empfohlenen Hotfixes und Lösungen an.

3. Stellen Sie fest, ob das Problem durch die Hardware verursacht wird.

Ein STOP-Bildschirm kann durch Hardwarefehler verursacht werden, durch ein veraltetes BIOS oder andere Probleme in der Hardwarekonfiguration, selbst wenn das System und alle seine Komponenten auf der Hardwarekompatibilitätsliste (HCL) aufgeführt sind. Die folgenden Hinweise deuten auf ein Hardwareproblem hin:

- Das System hat bisher problemlos gearbeitet und fällt plötzlich aus, nachdem eine bestimmte Operation ausgeführt wird. Ein Beispiel dafür wäre etwa eine tägliche Sicherung, die bisher funktioniert hat, jetzt aber mit einem Kernel-STOP beendet wird. In diesem Fall sind die beteiligten Hardwaresysteme zu untersuchen und für Testzwecke durch neue Systeme zu ersetzen.
- Neue Hardware wurde installiert und der STOP-Bildschirm erscheint während des Systemneustarts oder bei der Benutzung der neuen Hardware. Das weist darauf hin, dass die neue Hardware die Fehlerursache ist, auch wenn sie in der Hardwarekompatibilitätsliste aufgeführt ist. Untersuchen Sie, ob es an der Hardware liegen kann, ob dafür alte BIOSe ausgetauscht werden

müssen, ob Einstellungskonflikte vorliegen (IRQ, E/A-Adresse usw.) oder ob eine fehlerhafte Konfiguration vorliegt. Möglicherweise können Sie das Problem auch durch einen neuen Treiber aus der Welt schaffen.

- Achten Sie auf STOP-Fehler, die nicht jedes Mal auftreten, wenn eine bestimmte Operation ausgeführt wird (beispielsweise beim Systemstart, beim Kopieren von Dateien oder bei Sicherungen), sondern nur sporadisch. Ein Softwareproblem würde den Fehler konsequent jedes Mal aufwerfen, während Hardwareprobleme ein sporadisches Auftreten verursachen können. Nicht immer muss ein Hardwareproblem die Ursache sein, aber es ist wahrscheinlich und Sie sollten auf die Fehlersuche gehen, beispielsweise eine Überprüfung, ob das BIOS veraltet ist oder ein Problem verursacht oder ob Interrupt oder E/A-Konflikte bestehen. Tauschen Sie alle Komponenten aus, die mit dem Problem zu tun haben könnten.

Auch wenn Sie keinen der hier aufgeführten Hinweise feststellen können, sollten Sie sicherstellen, dass das Problem nichts mit der Hardware zu tun hat. Gehen Sie dazu wie folgt vor:

- Überprüfen Sie die BIOS-Versionen für die Hauptplatine sowie für den SCSI-Controller und andere Controller.
- Suchen Sie nach IRQ-, E/A-Adressen- oder DMA-Konflikten.
- Überprüfen Sie die korrekte Konfiguration der Hardware, insbesondere für SCSI-Laufwerke.

4. Fehlersuche für bekannte STOP-Codes.

Möglicherweise finden Sie keinen Artikel mit einer exakten Lösung; es gibt jedoch mehrere STOP-Fehler, die ähnliche Ursachen haben. Hier einige Beispiele:

```
STOP 0x0000000A  IRQL_NOT_LESS_OR_EQUAL
STOP 0x0000001E  KMODE_EXCEPTION_NOT_HANDLED
STOP 0x00000024  NTFS_FILE_SYSTEM
STOP 0x0000002E  DATA_BUS_ERROR
STOP 0x0000003E  MULTIPROCESSOR_CONFIGURATION_NOT_SUPPORTED
STOP 0x00000058  FTDISK_INTERNAL_ERROR
STOP 0x00000077  KERNEL_STACK_INPAGE_ERROR
STOP 0x00000079  MISMATCHED_HAL
STOP 0x0000007A  KERNEL_DATA_INPAGE_ERROR
STOP 0x0000007B  INACCESSIBLE_BOOT_DEVICE
STOP 0x0000007F  UNEXPECTED_KERNEL_MODE_TRAP
STOP 0x0000008B  MBR_CHECKSUM_MISMATCH
STOP 0xC0000218  STATUS_CANNOT_LOAD_REGISTRY_FILE
STOP 0xC000021A  STATUS_SYSTEM_PROCESS_TERMINATED
STOP 0xC0000221  STATUS_IMAGE_CHECKSUM_MISMATCH
```

Eine detaillierte Beschreibung dieser Fehler und mögliche Lösungen finden Sie im nächsten Abschnitt dieses Anhangs.

5. Stellen Sie fest, ob das Problem durch Hardware verursacht wird, die nicht in der Hardwarekompatibilitätsliste aufgeführt ist.

Falls das System nicht auf der Hardwarekompatibilitätsliste enthalten ist oder eine solche Komponente

enthält, beispielsweise Festplattencontroller, Netzwerkkarte oder Grafikkarte, bietet Microsoft möglicherweise keine Unterstützung bei der Lösung dieses Problems.

Lösungen für STOP-Fehler

In diesem Abschnitt werden die in Schritt 4 aufgelisteten STOP-Fehler aus dem vorigen Abschnitt beschrieben und Lösungsvorschläge angeboten.

STOP 0x0000000A IRQL_NOT_LESS_OR_EQUAL

Eine der häufigsten Kernel-STOP-Meldungen, STOP 0x0000000A, weist darauf hin, dass ein Prozess im Kernelmodus versucht hat, auf eine Speicheradresse zuzugreifen, für die er keine Berechtigung hat. Häufig ist dafür ein fehlerhafter Zeiger verantwortlich, der wiederum durch einen Softwarefehler, einen Speicherdefekt oder falsche Ergebnisse von Hardwareabfragen entsteht.

Im Allgemeinen gibt es nur eine Möglichkeit, die Ursache eines STOP 0xA festzustellen, nämlich den Debugger; der STOP-Bildschirm weist jedoch häufig auf die Ursache des Fehlers hin. Weitere Informationen über die Interpretation des STOP-Bildschirms und die Ursachensuche für STOP 0xA finden Sie im folgenden Artikel der Microsoft Knowledge Base:

- Q130802: General Information on STOP 0x0000000A

Sie können auch in der Microsoft Knowledge Base nach dem STOP-Code suchen; vielleicht finden Sie einen Hotfix oder eine Lösung, falls es sich um ein bekanntes Problem handelt. Die Microsoft Knowledge Base ist ein sehr praktisches Werkzeug bei der Fehlersuche. Sie finden sie unter <http://support.microsoft.com/search>.

STOP 0x0000001E KMODE_EXCEPTION_NOT_HANDLED

Der STOP-Fehler 0x000000001E ist möglicherweise der zweithäufigste STOP-Fehler unter Windows 2000. Diese Meldung weist darauf hin, dass der Kernel einen Fehler erkannt hat und dass Windows deshalb nicht fortgesetzt werden konnte. Die Probleme, wodurch diese STOP-Meldung verursacht wird, sind ähnlich denen für den Fehler STOP 0x0000000A, unter anderem also fehlerhafte Zeiger, ungültige Adressen und andere Arten von Zugriffsverletzungen.

Die oberen vier Zeilen der Meldung STOP 0x1E erscheinen normalerweise wie folgt:

```
STOP: 0x0000001E (0xAAAAAAAA, 0BBBBBBBB, 0CCCCCCCC, 0DDDDDDDD)
KMODE_EXCEPTION_NOT_HANDLED AAAAAAAA from BBBBBBBB (CCCCCCCC, DDDDDDDD)
Address BBBBBBBB has base at XXXXXXXX - MODULE1.SYS
Address CCCCCCCC has base at YYYYYYYY - MODULE2.SYS
```

In der oberen Zeile haben die vier hexadezimalen Parameter hinter dem STOP-Code die folgende Bedeutung:

- 0xAAAAAAAA ist der Code, der die Ausnahme beschreibt, die nicht verarbeitet wurde.
- 0BBBBBBBB ist die Adresse, an der die Ausnahme aufgetreten ist.

- 0xC0000000 ist der erste Parameter der Ausnahmen; manchmal auch eine weitere Adresse im Code.
- 0xD0000000 ist der zweite Parameter für die Ausnahme, was in der Bedeutung variieren kann.

Interpretation der Parameter

Der erste Parameter ist ein Windows 2000-Fehlercode; diese Codes sind in der Datei *Ntstatus.h* definiert, die Sie auch im SDK (Software Developer Kit) finden. Dieser Parameter gibt den Fehlertyp an. Der zweite Parameter ist ebenfalls wichtig, weil er Ihnen mitteilt, in welchem Codemodul der Fehler aufgetreten ist. Das weist häufig auf einen fehlerhaften Treiber oder ein defektes Hardwaregerät hin, was im Allgemeinen in der dritten Zeile des STOP-Bildschirms beschrieben ist. Die beiden letzten Parameter variieren je nach aufgetretener Ausnahme. Im Allgemeinen finden Sie eine Beschreibung der Parameter unter dem Namen des Fehlercodes in *Ntstatus.h*. Falls es für diesen Fehlercode keine Parameter gibt, sind die beiden letzten Hexadezimalzahlen gleich 0x00000000.



Ein SDK wird vom Hersteller eines Betriebssystems oder einer Anwendung veröffentlicht. Häufig wird er von Softwareentwicklern verwendet, um konform zu den Standards eines Betriebssystems oder einer Anwendung zu arbeiten. Diese Kits werden normalerweise als Pakete verkauft, aber Microsoft veröffentlicht Teile dieser Werkzeuge unter [http:// www.microsoft.com/technet/support/drivers.htm](http://www.microsoft.com/technet/support/drivers.htm).

Betrachten Sie beispielsweise die folgende STOP-Fehlermeldung:

```
STOP: 0x0000001E (0xC0000005, 0xFCA733B9, 0x00000000, 0x00000000)
KMODE_EXCEPTION_NOT_HANDLED 0xC0000005 from 0xFCA733B9 (0x0, 0x0)
Address FCA733B9 has base at FCA70000 - SRV.SYS
```

Hier sehen Sie, dass in Modul *Srv.sys* eine Zugriffsverletzung (0xC0000005) stattgefunden hat, der Kernelmodus-Serverdienst. Dieser Fehlercode beinhaltet keine Parameter.

Fehlersuche für diesen STOP-Fehler

Überprüfen Sie bei der Fehlersuche für diesen STOP-Fehler Folgendes:

- Suchen Sie in der Microsoft Knowledge Base nach dem STOP-Code, dem Fehlercode und dem Modul, in dem die Verletzung auftrat. Möglicherweise ist das Problem bekannt und es gibt eine Lösung. Suchen Sie beispielsweise in der Microsoft Knowledge Base nach den Schlüsselwörtern »STOP« und »Services für Macintosh«. Damit finden Sie den folgenden Artikel:

Q135667: STOP 1E When Using File Manager and Services for Macintosh (SFM)

- Suchen Sie in *Ntstatus.h* nach dem Fehlercode und in der Microsoft Knowledge Base nach dem Fehlertext (beispielsweise »access violation«) und zusätzlich nach dem Modul, in dem der Fehler aufgetreten ist.
- Falls es sich bei dem betreffenden Modul um einen Treiber eines Drittanbieters handelt, bitten Sie dort um Unterstützung.

Falls Ihre Suche in der Knowledge Base nichts ergibt oder wenn der STOP-Bildschirm nicht auf einen Treiber eines Drittanbieters oder ein Hardwaregerät hinweist, brauchen Sie ein Debugging um festzustellen, ob das Problem von der Hardware oder von der Software verursacht wird.

STOP 0x00000024 NTFS_FILE_SYSTEM

Der STOP-Code 0x00000024 lässt sich insbesondere Fehlerbedingungen und Traps im Windows 2000-Dateisystemtreiber (NTFS) zuordnen. Ein STOP-Fehler im NTFS wird in der Regel nicht durch Hardwareprobleme verursacht, obwohl dies durchaus möglich ist.

STOP 0x0000002E DATA_BUS_ERROR

Der STOP-Fehler 0x0000002E weist darauf hin, dass ein Paritätsfehler im Systemspeicher erkannt wurde. Dieser STOP-Fehler wird fast immer durch ein Hardwareproblem verursacht, beispielsweise ein Konfigurationsproblem, fehlerhafte oder inkompatible Hardware. Eine Ausnahme besteht darin, wenn ein Gerätetreiber versucht hat, auf eine Adresse im Bereich 0x8XXXXXXX zuzugreifen, die es nicht gibt (d.h. es gibt keine physische Adresszuordnung).

Die Parameter des STOP-Fehlers 0x2E sehen wie folgt aus:

STOP: 0x0000002E (0xAAAAAAAA, 0BBBBBBBB, 0xCCCCCCCC, 0xDDDDDDDD)

Diese Parameter haben die folgende Bedeutung:

- 0xAAAAAAAA ist die virtuelle Adresse, die den Fehler verursacht hat.
- 0BBBBBBBB ist die physische Adresse, die den Fehler verursacht hat.
- 0xCCCCCCCC ist das Prozessorstatusregister.
- 0xDDDDDDDD ist das fehlerhafte Anweisungsregister.

Fehlersuche für diesen STOP-Fehler

Die häufigste Ursache für diesen STOP-Fehler ist ein Hardwareproblem. Ohne Debugging werden Sie jedoch kaum herausfinden, ob die Ursache in der Hardware begründet, oder ob der Treiber fehlerhaft ist. Die folgenden Hinweise könnten Ihnen helfen:

- Lief das System längere Zeit und der STOP-Fehler trat plötzlich auf, ist sehr wahrscheinlich eine defekte Hardware die Fehlerursache.
- Tritt der STOP-Fehler nach der Installation eines neuen oder aktualisierten Gerätetreibers auf, sollten Sie den Treiber untersuchen und entfernen oder ersetzen. Tritt der STOP-Fehler während des Bootens auf, müssen Sie möglicherweise eine separate Kopie von Windows 2000 installieren, um den Gerätetreiber umbenennen oder ersetzen zu können.
- Wurde neue Hardware eingebaut, ist vermutlich die Hardware die Ursache und sollte entfernt werden um zu prüfen, ob der Fehler anschließend weiterhin auftritt.
- Tritt das Problem auch bei einem neu installierten System auf, sollten Sie die folgenden Dinge überprüfen, ob sie vielleicht aktualisiert werden sollten:

- Firmware auf RISC-Systemen
- BIOS-Revisionen auf der Hauptplatine
- BIOS-Revisionen auf dem SCSI-Controller oder auf Netzwerkkarten

STOP 0x0000003E MULTIPROCESSOR_CONFIGURATION_NOT_SUPPORTED

Der STOP-Fehler 0x0000003E weist darauf hin, dass die Prozessoren auf einem System mit mehreren Prozessoren asymmetrisch zueinander sind. Um symmetrisch zu sein, müssen alle Prozessoren denselben Typ und dieselbe Version haben. Beispielsweise würde dieser Fehler auftreten, wenn Sie versuchen, einen Pentiumprozessor mit einem 80486-Prozessor zu kombinieren. *Auf x86-Systemen sollten alle Prozessoren Fließkommafunktion aufweisen oder keiner.*

Darüber hinaus unterstützt Windows NT 3.5 und höher keine 386-Multiprozessor-Computer mehr. Dieser STOP-Fehler weist nicht auf eine fehlende Übereinstimmung zwischen HAL (Hardware Abstraction Layer = Hardwareabstraktionsschicht) und Kernel hin; dadurch würde der STOP-Fehler STOP 0x00000079 erzeugt.

Dieser STOP-Fehler wird immer durch Hardwareinkompatibilitäten oder Fehlkonfigurationen erzeugt und sollte entsprechend behandelt werden.

STOP 0x00000058 FTDISK_INTERNAL_ERROR

Der STOP-Fehler 0x00000058 tritt auf, wenn Ihre Boot- oder Systempartition gespiegelt wird und das Bild auf dem Spiegelungslaufwerk aktueller ist als das Bild auf dem primären Laufwerk.

Diese Situation kann auftreten, wenn Sie von der gespiegelten Partition gebootet haben, während die primäre Partition nicht lief und nachträglich zugeschaltet wurde. Weitere Informationen über diesen Fehler finden Sie im folgenden Artikel in der Microsoft Knowledge Base:

Q128630: How to Recover From a STOP 0x00000058
FTDISK_INTERNAL_ERROR

STOP 0x00000079 MISMATCHED_HAL

Dies ist eine seltene STOP-Fehlermeldung; der STOP-Fehler 0x00000079 hat eine sehr spezielle Ursache. Er weist darauf hin, dass Sie eine Einprozessor-HAL (Hardware Abstraction Layer) mit dem Multiprozessorkernel benutzen oder umgekehrt. Er kann auch darauf hinweisen, dass eine der beiden Dateien nicht mehr aktuell ist (wenn beispielsweise die HAL für Windows NT 3.5 ausgelegt ist, der Kernel aber aus Windows NT 3.51 stammt). In jedem Fall müssen Sie feststellen, welche HAL und welcher Kernel (*Ntoskrnl.exe* oder *Ntkrnlmp.exe*) verwendet werden sollen, und die fehlerhafte Datei durch eine korrekte ersetzen.

Die Kerneldatei ist für Einprozessorsysteme immer *Ntoskrnl.exe*, für Mehrprozessorsysteme *Ntkrnlmp.exe*. Beachten Sie, dass diese Dateinamen mit der Datei auf dem Installationsdatenträger übereinstimmen. Nachdem Windows installiert wurde, wird die Datei in *Ntoskrnl.exe* umbenannt,

unabhängig davon, welche installiert wurde.

Auch die HAL-Datei wird immer in *Hal.dll* umbenannt, nachdem die Installation abgeschlossen ist. Auf dem Installationsdatenträger sind aber mehrere mögliche HALs vorhanden. Die Standard-HAL für Einprozessor-x86-Systeme ist *Hal.dll*, die Standard-HAL für Mehrprozessor-x86-Systeme ist *Halmps.dll*.

STOP 0x00000077 und 0x0000007A KERNEL_STACK_INPAGE_ERROR

Die STOP-Fehler 0x77 und 0x7A weisen darauf hin, dass Windows versucht hat, eine Seite mit Kerneldaten aus der Auslagerungsdatei zu lesen und dies nicht möglich war. Beide Fehler werden häufig durch Hardwareprobleme verursacht, in einigen seltenen Ausnahmefällen können sie jedoch auch durch Softwarefehler verursacht werden. Weitere Informationen zur Fehlersuche für 0x77 oder 0x7A finden Sie im folgenden Artikel der Microsoft Knowledge Base:

Q130801: Common Causes of STOP Messages 0x00000077 and 0x0000007A

STOP 0x0000007B INACCESSIBLE_BOOT_DEVICE

Ein weiterer sehr häufiger STOP-Fehler, 0x0000007B, weist darauf hin, dass Windows beim Booten aus irgendeinem Grund nicht auf das Bootlaufwerk zugreifen konnte. Dieser STOP-Fehler tritt immer auf, wenn das System gebootet wird, und kann nicht debugged werden, weil es in der Regel auftritt, bevor das System den Debugger laden kann.

Fehlersuche für diesen STOP-Fehler

Der STOP-Fehler 0x7B kann fast immer gelöst werden, ohne den technischen Support von Microsoft anzurufen, indem die folgenden Ursachen überprüft werden:

- Master Boot Record- (MBR) und Bootsekturviren. Selbst auf einer NTFS-Partition kann es sein, dass ein MBR- oder Bootsektor-Virus auftritt, wenn das System von einer infizierten Diskette gebootet wurde. Ein MBR- oder Bootsektor-Virus verursacht häufig einen STOP-Fehler 0x7B. Um eine Prüfung auf Viren auszuführen, booten Sie von einer Diskette, die auf Viren untersucht wurde, und führen dann ein aktuelles Antiviren-Dienstprogramm aus. Außerdem kann man booten, indem man eine NTFS-Bootdiskette (auch als FT-Bootdiskette bezeichnet) anlegt, die frei von Viren ist. Damit wird der Bootsektor auf dem Festplattenlaufwerk umgangen und der Virus kann nicht geladen werden. Damit ist Ihr System noch nicht sauber, aber Sie können eines der für Windows entwickelten Antiviren-Programme ausführen.
- Ein falscher Gerätetreiber wurde installiert. Im Allgemeinen beginnt Windows das Booten mit INT 13, um auf das Festplattenlaufwerk zuzugreifen. Beim Laden des Betriebssystems lädt Windows jedoch einen Gerätetreiber für den Laufwerkscontroller. Ist der Gerätetreiber fehlerhaft, veraltet oder auf andere Weise nicht korrekt, entsteht ein STOP-Fehler 0x7B.
- Inkompatible, fehlerhaft konfigurierte oder defekte Hardware. Eine häufige Ursache für den STOP-Fehler 0x7B ist ein Laufwerkscontroller oder Laufwerk, der bzw. das inkompatibel mit Windows ist, fehlerhaft konfiguriert wurde oder andere Probleme aufweist. Überprüfen Sie die folgenden Dinge:

- Überprüfen Sie, ob das Laufwerk oder der Controller in der Hardwarekompatibilitätsliste von Windows aufgeführt ist. Beachten Sie, dass die meisten SCSI- und EIDE-Laufwerke mit Windows kompatibel sind, auch wenn sie nicht in der Hardwarekompatibilitätsliste enthalten sind.
- Überprüfen Sie für einen SCSI-Controller dessen Firmware-Version. Achten Sie darauf, dass der SCSI-Bus korrekt terminiert ist und die Kabel richtig angeschlossen sind. Tauschen Sie die Kabel aus; das ist kein großer Aufwand und könnte die Lösung bedeuten.
- Versuchen Sie, den Laufwerkscontroller, die Verkabelung oder sogar die Laufwerke auszutauschen.

STOP 0x0000007F UNEXPECTED_KERNEL_MODE_TRAP

Der STOP-Fehler 0x0000007F tritt auf Systemen mit Intel x86-basierten Prozessoren auf und weist darauf hin, dass der Prozessor eine unerwartete Fehlerbedingung signalisiert hat. Diese STOP-Meldung weist darauf hin, dass auf Prozessorebene ein Fehler aufgetreten ist. Sie wird fast immer durch Hardwareprobleme verursacht, außer in einigen seltenen Fällen.

STOP 0x0000008B MBR_CHECKSUM_MISMATCH

Der STOP-Fehler 0x0000008B weist darauf hin, dass die Prüfsumme des MBR (Master Boot Record) beim Booten nicht mit der im Loader übergebenen Prüfsumme übereinstimmt. Das deutet fast immer auf einen MBR-Virus hin. Sie sollten ein Antivirenprogramm ausführen, um das System zu bereinigen. Alternativ booten Sie von einer MS-DOS-Diskette und führen FDISK /MBR aus, womit auch der MBR-Virus gelöscht wird.

Durchsuchen Sie die Microsoft Knowledge Base nach dem STOP-Code, in dem die Verletzung aufgetreten ist. Auf diese Weise finden Sie vielleicht einen Hotfix oder eine Lösung, falls es sich um ein bekanntes Problem handelt.

STOP 0xC0000218 STATUS_CANNOT_LOAD_REGISTRY_FILE

Dieser STOP-Fehler zeigt an, dass beim Starten die Registrierungsdatenbank nicht geladen werden konnte. Wahrscheinlich ist die Registrierungsdatei defekt oder fehlt. Verwenden Sie die Notfalldiskette oder installieren Sie sie neu bzw. stellen Sie sie von einer Sicherung wieder her. In der Regel ist das Problem dadurch behoben.

Eine weitere häufige Ursache für diese Fehlermeldung ist eine Beschädigung der Festplatte, in der Regel ein defekter Sektor in einer der Registrierungsdateien. In diesem Fall ist möglicherweise eine Low-Level-Formatierung des Laufwerks erforderlich, gefolgt von einer Neuinstallation und Wiederherstellung von einer Sicherung. Falls Sie vor der Low-Level-Formatierung auf das Laufwerk zugreifen müssen, installieren Sie eine zweite Version von Windows auf einem anderen Laufwerk.

STOP 0xC000021a STATUS_SYSTEM_PROCESS_TERMINATED

Dieser STOP-Fehler weist in der Regel darauf hin, dass Winlogon oder CSRSS (Win32 API-Unterstützung) unerwartet beendet wurden. In der Regel ist der Exitcode dafür C0000005, d.h. eine nicht verarbeitete Ausnahme hat Winlogon oder CSRSS beendet. Sie können nicht sehr viel dagegen tun,

es sei denn, das Problem bleibt hartnäckig bestehen. Weitere Informationen über Exitcodes finden Sie in der Datei *Ntstatus.h*. Weil Windows nicht ohne Winlogon oder CSRSS arbeiten kann, ist dies eine der wenigen Situationen, in der ein Dienst im Benutzermodus das gesamte System zum Absturz bringen kann.

Diese STOP-Fehlermeldung kann nicht debugged werden, weil der eigentliche Fehler in einem Prozess im Benutzermodus aufgetreten ist. Der erste Schritt bei der Fehlersuche für diesen STOP-Fehler ist, Informationen darüber zu sammeln, wo er auftritt, und dann in der Microsoft Knowledge Base nach dem Schlüsselwort 0xC000021A, dem Modul, in dem die Verletzung aufgetreten ist, Winlogon oder CSRSS und dem Exitcode zu suchen.

Falls Sie dadurch keine Lösung finden, muss das System für ein Debugging im Benutzermodus konfiguriert werden, sodass der Benutzermodusprozess debugged werden kann, wenn der eigentliche Fehler auftritt. Tritt die STOP-Fehlermeldung bei jedem Starten auf, müssen Sie das System in einen Startstatus versetzen. Probieren Sie Folgendes:

- Wählen Sie beim Starten die Option Letzte als funktionierend bekannte Konfiguration.
- Führen Sie eine Notfallreparatur für das System aus.
- Falls das Problem auftritt, nachdem ein Treiber installiert, neue Hardware eingebaut oder das System verändert wurde, sollten Sie versuchen, die Änderung rückgängig zu machen.
- Durchsuchen Sie die Microsoft Knowledge Base nach STOP 0xC000021A. Beispielsweise wird dafür der folgende Artikel angezeigt:

Q139274: Updated System Environment Variables Result in STOP 0x0000021a

STOP 0xC0000221 STATUS_IMAGE_CHECKSUM_MISMATCH

Der STOP-Fehler 0xC0000221 weist darauf hin, dass ein Treiber defekt ist oder eine fehlerhafte System-DLL erkannt wurde. Windows versucht, die Integrität von Treibern und wichtigen System-DLLs zu gewährleisten. Wenn diese defekt sind, gibt Windows einen STOP-Fehler mit dem Namen der betreffenden Datei zurück. Damit wird verhindert, dass das System abstürzt, wenn der Defekt später auftritt.

Um das Problem zu beheben, gehen Sie wie folgt vor:

- Führen Sie eine Notfallreparatur aus und wählen Sie die Option *Systemdateien zu reparieren*.
- Führen Sie eine Aktualisierung der existierenden Windows-Kopie durch. Damit werden alle Registrierungseinstellungen und Konfigurationsinformationen beibehalten, aber alle Systemdateien ersetzt.
- Wurde auf dem STOP-Bildschirm eine bestimmte Datei als defekt moniert, versuchen Sie, diese Datei manuell zu ersetzen. Falls Sie eine FAT-Systempartition verwenden, booten Sie von einer MS-DOS-Diskette und ersetzen Sie die Datei manuell. Handelt es sich um eine NTFS-Systempartition, müssen Sie eine neue Kopie von Windows in einem anderen Verzeichnis installieren und die Datei dann manuell ersetzen.

- Falls alles andere scheitert, versuchen Sie es mit einer Neuinstallation und Wiederherstellung von einer Sicherung.
- Durchsuchen Sie die Microsoft Knowledge Base nach STOP 0xC0000221 und allen Schlüsselwörtern, die die Umstände beschreiben, unter denen der STOP-Fehler aufgetreten ist. Es gibt viele Artikel über konkrete Ursachen für diesen STOP-Fehler.

Die Lösung für alle Probleme ist davon abhängig, wie viele Informationen Sie darüber haben. Wenn Sie die Fehler exakt notieren und in der Microsoft Knowledge Base nach Lösungen suchen, werden Sie sehr wahrscheinlich eine Antwort finden. Wenn Sie allerdings nach ganz allgemeinen Antworten suchen, werden Sie schnell frustriert sein.

© Copyright [Markt+Technik Verlag](#), ein Imprint der Pearson Education Deutschland GmbH
Elektronische Fassung des Titels: Windows 2000 Server Kompendium, ISBN: 3-8272-5611-9 Kapitel:
Problemlösungen/Fehlerliste

Anhang B Inhalt der CD-ROM zum Buch

Auf der CD-ROM zum Buch finden Sie eine umfangreiche Sammlung von nützlichen Programmen und Utilities für Windows 2000. Bei der Auswahl der Programme haben wir insbesondere Wert darauf gelegt, Ihnen echte »Software-Perlen« zu bieten, die Sie bei der Administration von Windows 2000 Server und beim Support Ihrer Netzwerkbenutzer unterstützen sollen.

Hinweise zu den enthaltenen Produkten finden Sie im folgenden Abschnitt. Bitte lesen Sie dazu unbedingt den Abschnitt über die »Grundregeln im Umgang mit Free- und Shareware« weiter unten in diesem Anhang.



Bitte haben Sie Verständnis, dass weder Verlag noch die Autoren dieses Buchs oder die jeweiligen Software-Anbieter irgendeine Garantie für das Funktionieren der jeweiligen Programme übernehmen können. Sie sind als kostenlose Zugabe zu verstehen und sollen Ihnen z.B. Umstiegsentscheidungen oder die Prüfung von Einsatzmöglichkeiten erleichtern.

B.1 Grundregeln im Umgang mit Free- und Shareware

Freeware

Sie dürfen diese Programme ohne den Erwerb von Nutzungsrechten zeitlich unbeschränkt nutzen. Bei einigen Versionen bestehen allerdings Einschränkungen bezüglich der Nutzung. Häufig ist die kommerzielle Nutzung oder der Weiterverkauf nicht erlaubt.

Shareware

Sie dürfen diese Programme für eine begrenzte Zeit benutzen. Nach Ablauf der Testzeit müssen Sie die Software beim Autor registrieren lassen. Die Programme sind in der Regel sehr preisgünstig, und Sie sollten die Arbeit der Autoren honorieren, damit diese auch zukünftig in der Lage sind, Spitzenprogramme zu entwickeln und über den Shareware-Weg zu verbreiten. Hinweise zur Registrierung der einzelnen Programme finden Sie in den jeweiligen Registrierungsdateien, die meist Dateinamen wie REGISTER.DOC oder ORDER.DOC tragen.

B.2 Die Programme auf der CD-ROM im Detail

Programmname	Beschreibung	Ordner
Administrator		

Binary Browser	Ein Programm zur Suche, Anzeige und Bearbeitung von Dateien im Hexadezimalformat. Zusätzlich lassen sich Ordner nach bestimmten Strings oder doppelten Dateien suchen. Ein absolutes Muss zur Analyse von Dateiinhalten.	/Programme/Administrator/Binary Browser/
Hyena	Dieses Programm eignet sich zur Administration sowohl großer als auch kleiner auf Windows 2000 basierenden Netzwerke. Hyena vereint die Funktionen der Benutzer- und Serververwaltung, des Ereignisprotokolls und des Windows-Explorers in einem einzigen Programm. Funktionen sind unter anderem: Benutzer, Gruppen und Gruppenmitglieder anlegen, ändern und löschen, neue Netzwerklaufwerke und Druckerverbindungen anlegen, entfernte Rechner herunter fahren und neu starten, Remote-Druckwarteschlangen verwalten und vieles mehr.	/Programme/Administrator/Hyena/
LANGuard	Mit LANGuard können Sie die Internet-Nutzung in Ihrem Netzwerk überwachen und feststellen, ob Ihre User den Internet-Zugang entsprechend den Firmenrichtlinien benutzen. Beispielsweise lassen sich jene Websites anzeigen, die ein Benutzer momentan besucht, oder Sie legen Regeln fest, über die Sie die Zugriffe auf bestimmte Sites blockieren können. Zusätzlich bietet LANGuard Möglichkeiten, um Ihr Netzwerk vor externen Zugriffen über das Internet zu schützen.	/Programme/Administrator/LANGuard/

SystemTools MMC Toolbox	Ein Snap-In für die Microsoft Management Console (MMC) zur zentralen Netzwerk-Administration. Außerdem lässt sich das Snap-In hervorragend als Grundlage für eigene erweiterte Snap-Ins verwenden. Weitere Informationen zu den SystemTools finden Sie auf der Webseite http://www.systemtools.com/mmc .	/Programme/Administrator/SystemTools MMC Toolbox/
UltraAdmin	Ein benutzerfreundliches Werkzeug zur Administration von Domänen, das zusätzlich die Verwaltung von Active Directory-Informationen für Benutzer, Gruppen und Computer sowohl in gemischten als auch nativen Windows-2000-Domänen unterstützt. Weitere Funktionen: Remote-Anzeige von Netzwerkgeräten und installierten Programmen, Umbenennen von Gruppen, Kopieren von Benutzern und Gruppen, Geräteverwaltung und vieles mehr.	/Programme/Administrator/UltraAdmin/
UltraEdit	Ein Text-, HTML- und Hexadezimal-Editor mit Makrounterstützung, Konvertierung von DOS- in Unix-Dateitypen, synchronem vertikalen Scrollen, FTP-Erweiterungen, Unterstützung von CHM-Dateien und vielen Funktionen mehr. Zur Installation von UltraEdit rufen Sie bitte die Datei »Uedit32i.exe« auf. Bei der Datei »Dictam.exe« handelt es sich um ein englischsprachiges Wörterbuch, das von UltraEdit zur Rechtschreibprüfung verwendet werden kann.	/Programme/Administrator/UltraEdit/

WindowFX	Gestalten Sie Ihren Windows-2000-Desktop nach Ihrem Geschmack, zum Beispiel mit animierten Hintergründen, die sich so gut wie nicht auf die CPU-Leistung auswirken, oder durch halbtransparente Fenster.	/Programme/Administrator/WindowFX/
xReminder	Ein Personal Information Manager, mit dem Sie nie mehr etwas vergessen und der sich auf Grund der Fülle von Funktionen insbesondere für Netzwerk-Administratoren eignet.	/Programme/Administrator/xReminder/
X-Setup	Das ultimative Werkzeug zur Optimierung Ihres Windows-2000-Systems. Mit X-Setup lassen sich durch ein paar einfache Mausklicks über 500 verborgene Funktionen ändern. Dies geschieht fast ausschließlich über Plug-Ins und Assistenten. Beispielsweise können Sie als Netzwerk-Administrator Ihre Änderungen über einen »Recorder« aufzeichnen, daraus eine REG-Datei generieren und an beliebig viele Rechner weitergeben, ohne dass auf diesem X-Setup installiert sein muss.	/Programme/Administrator/X-Setup/ /Programme/Administrator/X-Setup/SDK/
	Über das zusätzlich mitgelieferte X-Setup SDK können Sie eigene Assistenten erstellen und diese in X-Setup verwenden. X-Setup ist kompatibel mit Windows 95/98/NT/2000 und Millennium.	
CD-Recording		
CDCheck	Ein Programm zur Überprüfung von CD-ROMs auf Korrektheit der enthaltenen Daten (Binärvergleich).	/Programme/CD-Recording/CDCheck/

CDCopy	Dieses Programm ermöglicht es, Audio-Tracks von CD auf die Festplatte zu kopieren. In der registrierten Version besteht die Möglichkeit, die einzelnen Tracks per Brenner wieder zurückzuschreiben.	/Programme/CD-Recording/CDCopy/
CloneCD	CloneCD erstellt 1:1-Kopien Ihrer CDs im RAW-Modus (Ihr CD-Brenner muss diesen Modus unterstützen). Dadurch lassen sich Kopien von jeder CD anfertigen, gleichgültig ob diese kopiergeschützt ist oder nicht. Mit dieser unregistrierten Version lassen sich bis zu fünf CDs erstellen. Danach ist eine Registrierung erforderlich.	/Programme/CD-Recording/CloneCD/
Feurio!	Ein ausgezeichnetes Programm zum Brennen von Daten und Audio-Tracks.	/Programme/CD-Recording/Feurio/
MCreator	Mit diesem Programm können Besitzer eines CD-Brenners Programmoberflächen erstellen, die beim Einlegen der CD in das CD-ROM-Laufwerk automatisch starten.	/Programme/CD-Recording/MCreator/
NTI Backup	Verwenden Sie Ihren CD-Brenner als Backup-Laufwerk.	/Programme/CD-Recording/NTI Backup/
E-Mail		
AvirMail	Mit AvirMail lassen sich eingehende E-Mails prüfen, ohne diese vorher auf Ihren Rechner laden zu müssen. Obwohl die E-Mails zunächst auf dem Server verbleiben, können Sie jede Mail lesen, ausdrucken, filtern, direkt beantworten oder löschen. Zum Download der von Ihnen akzeptierten E-Mails nutzen Sie den üblicherweise von Ihnen verwendeten Mail-Client (z.B.	/Programme/ E-Mail/AvirMail/

	Outlook).	
AY Mail	Dieses Programm unterstützt den gleichzeitigen Versand von E-Mail-Nachrichten an verschiedene Empfänger, wobei die normalerweise von Ihnen verwendete Internet-Verbindung benutzt wird. Einige der Funktionen: Bei Nutzung eines 28,8K-Modems lässt sich eine Nachricht pro Minute an rund 2.000 Empfänger versenden, jede Nachricht kann zusätzlich mit dem Namen und/oder der Adresse des Empfängers versehen werden, der Versand kann im Nur-Text- oder HTML-Format erfolgen, pro Nachricht lassen sich bis zu 20 Dateien anfügen.	/Programme/ E-Mail/AY Mail/
SpamKiller	Mit diesem Programm lassen sich beliebig viele E-Mail-Konten filtern. Über ein Symbol in der Taskleiste können Sie erkennen, ob eine Spam-Mail oder eine gewöhnliche E-Mail eingegangen ist. Zusätzlich können Sie das Programm so einrichten, dass bei Eingang einer normalen E-Mail automatisch Ihr bevorzugtes E-Mail-Programm gestartet wird.	/Programme/ E-Mail/SpamKiller/
FTP		
FTP Server	Dieser FTP Server ist das ideale Werkzeug sowohl für Anfänger als auch für Fortgeschrittene. Highlights dieses Programms sind die herausragende Geschwindigkeit bei Dateitransfers und die einfache Konfiguration und Verwaltung von Usern.	/Programme/FTP/FTP Server/
HTML		
Arachnophilia	Erstellen Sie mit diesem ausgezeichneten HTML-Editor Ihre eigenen Webseiten.	/Programme/HTML/Arachnophilia/

FAR	Mit FAR können Sie Webseiten in kompilierte HTML-Hilfedateien konvertieren.	/Programme/HTML/FAR/
HotDog Professional	Ein preisgekrönter HTML-Editor, der absolut keine Wünsche mehr offen lässt.	/Programme/HTML/HotDog/
HP-Edit Century	Ein komfortabler HTML-Editor, der sich sowohl für Einsteiger als auch für fortgeschrittene Anwender eignet. Durch die WYSIWYG-Vorschau haben Sie ständig das fertige Layout vor sich. Wahlweise kann aber auch der Quelltext eingeblendet werden. Ein vollwertiger FTP-Client liegt dem Programm bei.	/Programme/HTML/HP-Edit/
Internet Designer Pro	Das optimale Tool zur Homepage-Erstellung, sowohl für Laien ohne HTML-Kenntnisse als auch für Spezialisten. Erstellen Sie innerhalb kürzester Zeit eine perfekte und professionelle Homepage.	/Programme/HTML/Internet Designer Pro/
Tarantula	Ein Web-Editor, mit dem sowohl Anfänger ohne HTML-Kenntnisse als auch Profis innerhalb kürzester Zeit hervorragende Ergebnisse erzielen. Selbst komplizierte Seitenlayouts lassen sich innerhalb weniger Minuten realisieren.	/Programme/HTML/Tarantula/
WebTwin	Konvertiert HTML-Dateien, Websites und Intranets in Windows-Hilfedateien. Diese Demoversion ist auf 30 Tage beschränkt und kann nur bis zu 100 URLs gleichzeitig bearbeiten.	/Programme/HTML/Webtwin/

XMLWriter	Ein mächtiger XML-Editor, mit dem sowohl Webautoren als auch Anwendungsentwickler die XML-Sprache und daraus abgeleitete Technologien wie beispielsweise XSL und XQL nutzen können.	/Programme/HTML/XMLWriter/
Internet		
Blazenet	Dieses Programm optimiert die Art und Weise, wie Ihr Computer Informationen über das Internet verschickt und empfängt. Insbesondere die Übertragungsraten beim Datei-Download können sich durch den Einsatz von Blazenet merklich erhöhen.	/Programme/Internet/Blazenet/
Copernic 2000	Ihr ganz persönlicher Such-Assistent im Internet! Copernic 2000 unterstützt die gleichzeitige Nutzung von bis zu 130 Suchmaschinen und ist spezialisiert auf die Suche nach schwer auffindbaren Websites, E-Mail-Adressen und Newsgroup-Artikeln. Die Recherche lässt sich offline planen. Erst nach dem Festlegen der Suchkriterien wird eine Internet-Verbindung hergestellt.	/Programme/Internet/Copernic 2000/
Download Accelerator	Ein Programm, mit dem sich der Download von Dateien aus dem Internet um bis zu 300% beschleunigen lässt. Download Accelerator unterstützt Multiserver-Verbindungen, nimmt unterbrochene Downloads an der Abbruchstelle wieder auf und bezieht auch eventuell vorhandene Mirror-Sites in den Download mit ein.	/Programme/Internet/Download Accelerator/

Mass Downloader	Dieses Programm ermöglicht es Ihnen, einzelne oder mehrere Dateien bei maximal möglicher Geschwindigkeit aus dem Web oder von FTP-Sites zu laden. Zusätzlich können Sie ZIP-Archive durchsuchen und darin nur jene Dateien auswählen, die tatsächlich übertragen werden sollen. Eine einzigartige und nützliche Funktion, die Sie sonst bei keinem anderen Download-Programm finden.	/Programme/Internet/Mass Downloader/
Net Optimizer	Net Optimizer ermöglicht es Ihnen, auf einfache Weise zahlreiche Windows-2000-Einstellungen so zu ändern, dass die Geschwindigkeit Ihrer Internet-Verbindung spürbar erhöht wird.	/Programme/Internet/Net Optimizer/
NETAttache	Ein Web-Agent der zweiten Generation. Mit diesem Programm lassen sich Webseiten archivieren und automatisch aktualisieren. Außerdem kann man über Filter Websites nach bestimmten Begriffen durchsuchen, wobei automatisch nur jene Seiten geladen werden, deren Informationen für Sie wichtig sind.	/Programme/Internet/NETAttache/
Offline Explorer	Laden Sie bestimmte Web-, FTP- und HTTPS-Sites (bis zu 100 gleichzeitig) auf Ihren Rechner, um die entsprechenden Seiten später offline zu lesen, zu durchsuchen und zu bearbeiten.	/Programme/Internet/Offline Explorer/
Opera	Als klein, aber fein lässt sich dieser Internet-Browser bezeichnen. Insbesondere zeichnen ihn seine Schnelligkeit und seine benutzerfreundliche Oberfläche aus.	/Programme/Internet/Opera/

SpeedNet	Ein Programm, mit dem sich die Download-Geschwindigkeit um bis zu 600% erhöhen lässt. SpeedNet funktioniert mit Windows 95/98/NT und Windows 2000.	/Programme/Internet/SpeedNet/
WebWalks	Ein Internet-Browser, der sich beliebig anpassen lässt und mit dem der Zugriff auf unerwünschte Websites verhindert werden kann. Zusätzlich kann über den Browser festgelegt werden, wie viel Zeit der Benutzer im Internet bleiben darf.	/Programme/Internet/WebWalks/
WebZIP	Laden Sie Webseiten und ganze Websites einschließlich Bildern, Klängen und weiteren Mediadateien auf Ihre Festplatte, um diese später offline durchzusehen. Dieses Programm spart Zeit und damit Online-Gebühren!	/Programme/Internet/WebZIP/
ISDN		
ISDNMonitor	Für alle, die eine ISDN-Karte in ihren PC eingebaut haben und eingehende Anrufe komfortabel verwalten wollen, ist der roSoft ISDN Anruf-Monitor das ideale Werkzeug. Auf Wunsch können entweder alle oder nur bestimmte MSNs überwacht werden. Zu jedem Anruf wird die Nummer des Anrufers (falls übermittelt), die angerufene Nummer (MSN), das Datum, die Uhrzeit und die Rufbehandlung gespeichert.	/Programme/ISDN/ISDNMoni/
ISDN4WIN Message	Versendet Kurznachrichten (SMS) an Mobiltelefone (D1, D2, E-Plus und VIAG Interkom Mobilservice).	/Programme/ISDN/Message/

Teli	Ein CAPI-basierender ISDN-Anrufbeantworter mit computergestützter Telefonie über die Soundkarte (inkl. TAPI-Treiber). Voraussetzungen: ein ISDN-Controller von AVM, Teles oder Creatix sowie Full-Duplex-Treiber für die Soundkarte.	/Programme/ISDN/Teli/
Kommunikation		
32Bit Fax	Übertragen und empfangen Sie Faxesendungen von einem einzelnen Computer oder vom Netzwerk aus. Zum Versand lässt sich jedes beliebige Windows-Programm nutzen, das über Druckfunktionen verfügt. Das Programm kann unter Windows 2000 als Dienst eingerichtet werden und steht somit sämtlichen Benutzern im Netzwerk zur Verfügung.	/Programme/Kommunikation/32Fax/
FaxMail Network	Ein mit allen nur denkbaren Funktionen ausgestattetes Faxprogramm für Windows 2000. Erstellen Sie qualitativ hochwertige Faxesendungen ebenso einfach, wie wenn Sie ein Dokument ausdrucken.	/Programme/Kommunikation/FaxMail Network/
Flash Messaging System	Ein netzwerkbasierendes Kommunikationsprogramm, das sich auf allen Windows-Plattformen einsetzen lässt. Sämtliche PCs in einem Netzwerk können sich per einfachem Mausklick Nachrichten zusenden. Für den Netzwerk-Administrator ist ein Tool enthalten, mit dem sich eine Liste der im Messaging System angemeldeten Benutzer anzeigen und deren Verbindungsstatus feststellen lässt.	/Programme/Kommunikation/Flash Messaging System/
Netzwerk		

Anasil	Ein ausgereiftes Analyseprogramm für Ethernet-Netzwerke. Aufgrund seiner vielfältigen Funktionen ist es das ideale Werkzeug für Netzwerk-Administratoren. Unter anderem lassen sich damit nicht autorisierte Stationen feststellen, die sich mit dem Netzwerk verbunden haben.	/Programme/Netzwerk/Anasil/
Enterprise ipMonitor	Überwacht rund um die Uhr die Qualität und Verfügbarkeit Ihres Netzwerks und alarmiert den Administrator beim Auftreten von Fehlern oder versucht auf Wunsch, abgestürzte Dienste automatisch neu zu starten. ipMonitor ist das ideale Sicherheitstool für eCommerce- und eBusiness-Installationen.	/Programme/Netzwerk/Enterprise ipMonitor/
Net User Info	Dieses Programm trägt detaillierte Informationen (z.B. Alter des Kennworts, Gruppenmitgliedschaft, Home-Directory) über die Benutzer in einer Windows-2000-Domäne zusammen. Die Informationen lassen sich auf Wunsch im CSV- oder HTML-Format speichern.	/Programme/Netzwerk/Net User Info/
PCS DNS Utility Suite	Eine Sammlung wichtiger Tools zur Netzwerkdiagnose. Lassen Sie sich beispielsweise die IP-Adresse oder den Hostnamen eines bestimmten Rechners oder eine Gruppe von Rechnern im Netzwerk anzeigen. Auf lokalen Rechnern lassen sich diverse zusätzliche Informationen (z.B. installierte Adapter, MAC-Adressen oder Winsock-Stackversion) abrufen.	/Programme/Netzwerk/PCS DNS Utility Suite/

WhatsUp	Ein grafisches Tool zur Netzwerküberwachung von Hosts, Servern, Hubs, Druckern, Workstations, Bridges, Routern und vielem mehr. Zusätzlich stehen Werkzeuge zur Lösung von Netzwerkproblemen zur Verfügung (Whois, Traceroute, Ping, Finger und Lookup).	/Programme/Netzwerk/WhatsUp/
Nützliches		
Acrobat Reader 4.05d	Ein Programm zur Anzeige von Online-Dokumenten im PDF-Format.	/Programme/Nützliches/Acrobat Reader 4.05/
VB-Runtime 5/6	Viele Shareware-Programme benötigen zur Ausführung die Visual Basic-Runtime-Module. Hier finden Sie die erforderlichen Installationsdateien für die Versionen 5 und 6.	/Programme/Nützliches/VB-Runtime/Vb5/ /Programme/Nützliches/VB-Runtime/Vb6/
Packer		
Archive Peek	Durchsuchen Sie komprimierte Archive nach bestimmten Dateien. Unterstützt werden dabei folgende Formate: ZIP, RAR, LZH, ARJ, ZOO, PAK, ARC, TAR, SQZ, HYP, WAD, GRP, CAB und ACE. Die Suchergebnisse können im HTML- oder Textformat gespeichert werden.	/Programme/Packer/Archive Peek/
TurboZIP	Ein ZIP-Datei-Manager mit vielen einzigartigen Funktionen. Unterstützt werden alle gängigen Archiv- und E-Mail-Attachment-Formate wie beispielsweise ZIP, selbst entpackende EXE, CAB, ARJ, LHA, GZ, TAZ, TGZ, Z, TAR, UUE, MIME, BHX und HQX. Zusätzlich lassen sich über eine Schnellansicht im Archiv enthaltene Dateien prüfen. Unterstützt werden dabei u.a.	/Programme/Packer/TurboZIP/

	Programme bzw. Dateiformate wie Word, Excel, PowerPoint, AutoCAD (DXF, DWG und DWF), PDF, WordPerfect, WPG, HTML, CorelDRAW, CMX, MPEG, FlashPix und animierte GIFs.	
WinRAR	Ein Archivierungsprogramm für RAR-Dateien. Unterstützt auch Archive anderer Packer und erlaubt die Erstellung selbst extrahierender Dateien.	/Programme/Packer/WinRAR/
WinZip 7.0 SR-1 Deutsch	Der ultimative Packer, den man einfach haben muss.	/Programme/Packer/WinZip 7.0 SR-1 D/
Sicherheit		
WinZip 8.0 Englisch	Selbst der Standard unter den Packprogrammen lässt sich noch verbessern. In dieser Version wurde insbesondere der Dateiversand per E-Mail berücksichtigt.	/Programme/Packer/WinZIP 8.0 E/
AppsTraka	Überwachen und kontrollieren Sie die Aktivitäten von Benutzern am Rechner und stellen Sie beispielsweise fest, welche Programme, Dateien oder Webseiten genutzt wurden. Zusätzlich lässt sich auch die Dauer der jeweiligen Nutzung abrufen.	/Programme/Sicherheit/AppsTraka/
Backup 2001	Ein Programm zum Sichern und Wiederherstellen von Dateien unter Windows 95 (OSR2)/98/NT4/2000. Zum zeitgesteuerten Sichern kann entweder der programmeigene oder der in Windows integrierte Taskplaner benutzt werden.	/Programme/Sicherheit/Backup 2001/
FileBack PC	Ein Backup-Programm mit Komprimierungsunterstützung. Unter anderem ist es möglich, automatisch Sicherungskopien von Dateien zu erstellen, sobald diese gespeichert oder modifiziert werden.	/Programme/Sicherheit/FileBack PC/

NovaBACK	Ein ausgezeichnetes Backup-Programm für Windows NT/2000 Workstation mit Unterstützung einer Vielzahl von IDE-Bandlaufwerken.	/Programme/Sicherheit/NovaBACK/
Password Explorer	Mit diesem Programm lassen sich Passwörter, PIN-Nummern und andere sensible Informationen organisieren und sicher speichern. Es lassen sich verschiedene Passwortlisten (auch für verschiedene Anwender) anlegen. Passwörter können mit bestimmten Programmen oder URLs verknüpft werden. Zusätzlich kann Ihnen das Programm Vorschläge für Passwörter unterbreiten.	/Programme/Sicherheit/Password Explorer/
Password Officer	Sie müssen sich keine langen und schwierigen Passwörter mehr merken. Deren Verwaltung übernimmt Password Officer für Sie. Zusätzlich können Sie das Programm so konfigurieren, dass Passwörter bei Bedarf automatisch in das zugehörige Fenster eingetragen werden.	/Programme/Sicherheit/Password Officer/
Pretty Good Privacy	Der Standard unter den Verschlüsselungsprogrammen!	/Programme/Sicherheit/Pretty Good Privacy/
WinRescue	Statt einer Neuinstallation: Stellen Sie innerhalb weniger Minuten eine defekte Windows-2000-Installation wieder her. WinRescue funktioniert ausschließlich mit Windows 2000!	/Programme/Sicherheit/WinRescue/
Utilities		

AutoDialogs	Dieses Programm ermöglicht es Ihnen, innerhalb von bestimmten Dialogfeldern (z.B. Öffnen, Speichern unter, Durchsuchen) schnell auf häufig benutzte Ordner zuzugreifen. Wählen Sie den gewünschten Ordner einfach mit zwei Mausklicks über ein kleines Menü in der Taskleiste aus oder weisen Sie ihm einen Hotkey zu, um den Pfad direkt in das Dialogfeld zu übernehmen.	/Programme/Utilities/AutoDialogs/
AutoTask	Ein Taskplaner der neuesten Generation, der sich entweder als Service oder als Desktop-Anwendung im Hintergrund ausführen lässt. Pro Task lassen sich mehrere Anweisungen ausführen.	/Programme/Utilities/AutoTask/
CommView	Ein Programm zur Überwachung von Netzwerkaktivitäten, mit dem sich im Netz befindliche Datenpakete abfangen und analysieren lassen.	/Programme/Utilities/CommView/
Connections Watcher	Überwachen Sie sämtliche TCP/IP- und UDP-Verbindungen von und zu einem Rechner. Das Programm zeigt die IP-Adresse sowie die TCP- oder UDP-Ports der jeweils beteiligten Computer (lokal und remote) an.	/Programme/Utilities/Connections Watcher/
Disk Advisor	Erstellt Reports zur Speicherbelegung von Dateien. Die Angaben zu den Dateien beinhalten unter anderem: Große Dateien, Neue Dateien, Alte Dateien, Dateiduplikate, Zuletzt benutzte Dateien, Nutzung pro Anwender und vieles mehr.	/Programme/Utilities/Disk Advisor/

Dr. Hardware	Die Windows-Version des bekannten Analyseprogramms erlaubt Low-Level-Analysen der gesamten PC-Hardware. Neben detaillierten Infos über CPU, Bios, Chipsatz, Festplatten und PCI-Geräte werden zusätzlich Windows-spezifische Analysen durchgeführt.	/Programme/Utilities/DrHardware/
EmptyDrive	Dieses kleine Programm meldet Ihnen, ob sich beim Herunterfahren von Windows eine Diskette, eine CD-ROM oder ein anderes entfernbare Medium im entsprechenden Laufwerk befindet.	/Programme/Utilities/EmptyDrive/
G6 Renamer	Ein nützliches kleines Programm zur »Massen«-Umbenennung von Dateien. Dabei lassen sich Strings einfügen, ersetzen, Dateierweiterungen modifizieren (z.B. .html auf .htm) und vieles mehr.	/Programme/Utilities/G6 Renamer/
HzTool	Mit diesem Tool lassen sich schnell und einfach die Bildwiederholraten für sämtliche Auflösungen ändern. Dabei werden auch solche Einstellungen unterstützt, auf die Sie unter Windows normalerweise keinen Zugriff haben.	/Programme/Utilities/HzTool/
IC3	Ein Drive-Imaging-Programm, mit dem sich schnell 1:1-Kopien von Festplatten in Standalone- und vernetzten PCs erstellen lassen. Wichtig ist dies insbesondere für den schnellen Festplattenaustausch oder für Sicherungszwecke.	/Programme/Utilities/IC3/

Konvertor	Konvertor liest und konvertiert 171 unterschiedliche Dateiformate: 141 Grafikformate (BMP, PCD, K25, PSD, TGA, HP-GL, PDF, GIF, JPEG, VRML und weitere) sowie 30 Audio-, Text- und Videoformate (MP3, WAV, TXT, VOC, MOD, AVI, MPEG und weitere).	/Programme/Utilities/Konvertor/
Macro Express	Erstellen Sie Makros, die sich in jedem beliebigen Windows-Programm oder nur in bestimmten Programmen verwenden lassen. Die Makros können entweder manuell oder mit einem Script-Editor erzeugt werden.	/Programme/Utilities/Macro Express/
NTFS	Ein Treiber, durch den sich von Windows 98 aus auf NTFS-Partitionen von Windows NT und Windows 2000 zugreifen lässt. In der unregistrierten Version ist nur der Lesezugriff möglich, in der registrierten Version auch der Schreibzugriff.	/Programme/Utilities/NTFS/
PC-Config	Ein System-Info-Benchmark-Programm der Spitzenklasse. Mit CD-ROM-Benchmark, erkennt Pipeline-Burst-Cache, EDO-Ram, viele Chipsatzdetails, VESA-Modi, alle Arten von CPUs bis hin zu Pentium III und Athlon sowie vieles mehr.	/Programme/Utilities/PCConfig/
Phoenix Millenium	Ein »Schweizer Messer« mit Funktionen zur Dateiver- und -entschlüsselung, einem Download-Kalkulator, einem Screenshot-Programm, automatischem Speichern von Dateien, automatischem Starten von Anwendungen und vielem mehr.	/Programme/Utilities/Phoenix Millenium/

Sandra	Mit diesem Programm bleibt nicht einmal mehr das kleinste Detail Ihres PC im Verborgenen. Noch weiter kann Ihr Rechner nicht in seine Bestandteile »zerlegt« werden.	/Programme/Utilities/Sandra/
SyncMan	Ein Tool, mit dem sich zwei verschiedene Ordner auf demselben Windows-Laufwerk oder auf unterschiedlichen Laufwerken synchronisieren lassen. SyncMan kann so programmiert werden, dass sich bis zu 25 verschiedene Ordner synchronisieren lassen.	/Programme/Utilities/SyncMan/
Transmac	Dieses Programm führt zwei Betriebssystem-Welten (Macintosh und Windows) zusammen. Mit Transmac lassen sich auf einem Windows-PC Macintosh-Disketten und SCSI-Laufwerke lesen, schreiben und formatieren sowie CD-ROMs lesen.	/Programme/Utilities/Transmac/
TurboBrowser	Der Standard zur Verwaltung und Anzeige von Dateien und Dateiinhalten!	/Programme/Utilities/TurboBrowser/
Tweaki ... for Powerusers	Dieses Programm ermöglicht Ihnen die Manipulation sämtlicher Einstellungen in Bezug auf Grafikkarte und Monitor.	/Programme/Utilities/Tweaki/
WhatCpuIs	Stellen Sie fest, welcher Typ von Mikroprozessor in Ihren Rechner eingebaut ist. Erkennt auch den AMD Athlon und den Intel Pentium III.	/Programme/Utilities/WhatCpuIs/

WinCon	Ein professionelles Werkzeug, um jegliche Art von Veränderungen auf Ihrem Computer festzustellen. WinCon braucht nur einmal die Daten Ihres Laufwerks einzulesen und schon werden alle darauf stattfindenden Änderungen von WinCon festgestellt und protokolliert.	/Programme/Utilities/WinCon/
WinInBlack	Ein revolutionäres und benutzerfreundliches Programm, das Ihr System optimiert und Ihnen die Möglichkeit gibt, das System entsprechend Ihren Bedürfnissen anzupassen. Sie können umfangreiche Windows-, System-, Internet- und Booteinstellungen vornehmen, Ihr System auf Fehler und überflüssige Einstellungen hin analysieren sowie diese löschen. Zudem erhalten Sie einen Überblick über die Systembelastung.	/Programme/Utilities/WinInBlack/
WinRAM Booster	Vergrößert den verfügbaren Hauptspeicher für beliebige Anwendungen, einfach per Mausklick oder automatisch beim Aufruf einer Anwendung. Dabei werden Ihr Systemspeicher und die Windows-Auslagerungsdatei defragmentiert, wodurch zusätzlicher Arbeitsspeicher frei wird.	/Programme/Utilities/WinRAM Booster/