

Kapitel 1 – Hardware- und Softwareumgebung

(Engl. Originaltitel: [Chapter 1 - Hardware and Software Environment](#))

Dieser Abschnitt definiert die Hardware- und Softwareanforderungen für die evaluierte Konfiguration.

Allgemeine Hardwarekonfiguration

Festlegen von Bootkennwörtern

Auf vielen Hardwareplattformen kann das System durch das Verwenden eines Bootkennworts geschützt werden. Ein Bootkennwort verhindert, dass nicht autorisiertes Personal ein anderes Betriebssystem als Windows 2000 starten kann, da andernfalls die Systemsicherheit gefährdet werden könnte. Kennwörter beim Start sind eine Funktion der Computerhardware, nicht der Betriebssystemsoftware. Aus diesem Grund hängt das Verfahren zum Festlegen des Kennworts beim Start vom Computertyp ab und wird in der Dokumentation des Herstellers, die mit dem System vertrieben wird, beschrieben.

Einschränken des Startvorgangs

Die meisten PCs unterstützen die Möglichkeit, verschiedene Betriebssysteme zu starten. Selbst wenn Benutzer normalerweise Windows 2000 von Laufwerk C: starten, kann ein anderes Betriebssystem von Wechselmedien oder einem anderen Laufwerk, z. B. einem Diskettenlaufwerk oder CD-ROM-Laufwerk, gestartet werden. Wenn dies geschieht, können möglicherweise alle Sicherheitsvorkehrungen, die zum Sichern des Betriebssystems Windows 2000 vorgesehen wurden, umgangen werden.

Um ein sicheres System zu erhalten, installieren Sie nur eine Version von Windows 2000 auf dem Laufwerk C: und installieren kein weiteres Betriebssystem auf dem Computer. Aktivieren Sie nicht die Multibootfähigkeit des Computers. Die CPU muss ebenfalls physisch geschützt werden, damit sichergestellt ist, dass kein anderes Betriebssystem geladen werden kann. Abhängig von den individuellen Konfigurationsumständen können alle vorhandenen Diskettenlaufwerke entfernt werden. In einigen Computern kann das Einstellen von Schaltern oder Jumpers im BIOS den Systemstart über das Diskettenlaufwerk deaktivieren. Wenn Hardwareeinstellungen zum Deaktivieren des Systemstarts vom Diskettenlaufwerk aus verwendet werden, sollte das Computergehäuse abgeschlossen werden (wenn diese Option für den betreffenden Computer verfügbar ist), oder der Computer kann in einen Schrank eingeschlossen werden, der auf der Vorderseite eine Öffnung für den Zugriff auf das Diskettenlaufwerk aufweist. Wenn sich die CPU in einem abgeschlossenen Bereich befindet, der von der Tastatur und dem Monitor getrennt ist, können keine Laufwerke hinzugefügt oder Hardwareeinstellungen geändert werden, um ein anderes Betriebssystem zu starten.

Aktivieren des hardwareseitigen BIOS-Schutzes

Schützen Sie die BIOS-Konfiguration jedes Windows 2000-Computers mit einem BIOS-Kennwort. Auf vielen Hardwareplattformen kann das BIOS-Kennwort durch Öffnen des Gehäuses und Löschen des BIOS über bestimmte Jumper oder Entfernen der Hauptplattenbatterie deaktiviert werden. Um dies zu verhindern, schützen Sie die Hardware wie weiter oben im Unterabschnitt "Einschränken des Startvorgangs" beschrieben.

Evaluerte Hardwarekonfiguration

Die evaluierte Hardwarekonfiguration umfasst die folgenden Plattformen, die wie gezeigt konfiguriert wurden:

- Dell PE 2500
- Dell PE 6450/550
- Dell PE 2550
- Dell PE 1550
- Dell Optiplex GX400
- Compaq Proliant ML570
- Compaq Professional Workstation AP550
- Compaq Proliant ML330

Evaluerte Softwarekonfiguration

Die evaluierte Konfiguration von Windows 2000 umfasst die Produkte Windows 2000 Professional, Windows 2000 Server und Windows 2000 Advanced Server, die für jede der in der Tabelle unten gezeigte Funktion und gemäß den Installations- und Konfigurationsanweisungen in diesem Dokument konfiguriert wurden. Weitere Informationen hinsichtlich der genauen Sicherheitsanforderungen, die Windows 2000 erfüllt, finden Sie im Windows 2000-Sicherheitsziel (Security Target oder ST).

Produkt	Funktion
Microsoft Windows 2000 Advanced Server	Domänencontroller Domänenmitgliedserver Arbeitsgruppen-Mitgliedserver Eigenständiger Computer
Microsoft Windows 2000 Server	Domänencontroller Domänenmitgliedserver Arbeitsgruppen-Mitgliedserver Eigenständiger Computer
Microsoft Windows 2000 Professional	Domänenmitglied Arbeitsgruppenmitglied Eigenständiger Computer

Das Verständnis des Unterschieds zwischen einer Domänen- und einer Arbeitsgruppenumgebung ist von besonderer Bedeutung. Der Hauptunterschied zwischen einer Domäne und einer Arbeitsgruppe besteht darin, dass Arbeitsgruppenumgebungen dezentralisierte Verwaltung verwenden. Dies bedeutet, dass jeder Computer unabhängig von den anderen Computern verwaltet werden muss. Domänen verwenden zentralisierte Verwaltung, bei der Administratoren ein Domänenkonto erstellen und einem zentralen Benutzer oder einer Benutzergruppe Berechtigungen für alle Ressourcen in der Domäne zuweisen können. Die zentralisierte Verwaltung erfordert weniger Verwaltungszeit und stellt eine sicherere Umgebung zur Verfügung. Im Allgemeinen werden Arbeitsgruppenkonfigurationen in sehr kleinen Umgebungen verwendet, die keine Sicherheitsaspekte berücksichtigen müssen. Größere Umgebungen und Umgebungen, die große Sicherheit für Daten verlangen, sollten eine Domänenkonfiguration verwenden. Grundlegende Definitionen finden Sie im Folgenden.

- **Domäne.** Eine Sammlung von Computern, die eine Verzeichnisdatenbank gemeinsam verwenden, die vom Administrator eines Windows 2000 Server-Netzwerks definiert wird. Eine Domäne besitzt einen

eindeutigen Namen und bietet Zugriff auf die zentralisierten Benutzer- und Gruppenkonten, die vom Domänenadministrator verwaltet werden. Jede Domäne besitzt ihre eigenen Sicherheitsrichtlinien und Sicherheitsbeziehungen mit anderen Domänen und stellt einen eingegrenzten Sicherheitsbereich eines Windows 2000-Computernetzwerks dar.

- **Arbeitsgruppe.** Eine logische Gruppierung vernetzter Computer, die Ressourcen wie z. B. Dateien und Drucker gemeinsam verwenden. Eine Arbeitsgruppe wird manchmal als Peer-to-Peer-Netzwerk bezeichnet, weil alle Computer in der Arbeitsgruppe Ressourcen gleichberechtigt ohne einen dedizierten Server gemeinsam verwenden können. Jeder Windows 2000 Server- und Professional-Computer in einer Arbeitsgruppe verwaltet eine lokale Sicherheitsdatenbank, die eine Liste der Benutzerkonten und Ressourcensicherheitsinformationen enthält, die für diesen Computer spezifisch sind.
- **Domänencontroller.** Derjenige Server in einer Windows 2000 Server-Domäne, der Domänenanmeldungen authentifiziert und die Sicherheitsrichtlinie und die Sicherheitskonten-Masterdatenbank für eine Domäne verwaltet. Domänencontroller verwalten den Benutzerzugriff auf ein Netzwerk, z. B. Anmeldung, Authentifizierung und Zugriff auf das Verzeichnis und freigegebene Ressourcen.
- **Arbeitsgruppenmitglied.** Ein Windows 2000 Server- oder Professional-Computer, der Mitglied einer Windows 2000-Arbeitsgruppe ist, in Form einer logischen Gruppierung vernetzter Computer zum Zweck der gemeinsamen Nutzung von Ressourcen.
- **Domänenmitglied.** Ein Windows 2000 Server- oder Professional-Computer, der Mitglied einer Windows 2000-Domänenumgebung ist.
- **Alleinstehender Computer.** Standarddesktop, z. B. ein Windows 2000 Professional-Computer oder ein Servercomputer, der weder als Domänen- noch als Arbeitsgruppenmitglied mit einem Netzwerk verbunden ist.