Originaltitel: Chapter 1 – Introduction

1

Einführung

Willkommen zum Handbuch über den sicheren Betrieb von Windows 2000 Servern. Die Welt wächst mehr und mehr zusammen, und die Vision der ständigen Verfügbarkeit von Informationen, überall und auf jedem Gerät, wird zunehmend zur Realität. Unternehmen und deren Kunden werden in einer solchen Umgebung private Daten nur speichern, wenn sie davon ausgehen können, dass die Umgebung sicher ist.

Eine Umfrage zur Computerkriminalität und -sicherheit des Computer Security Institute (CSI) und des Federal Bureau of Investigation (FBI) im Jahr 2001 hat gezeigt, dass 85 % der großen Unternehmen und Regierungsbehörden Sicherheitsverletzungen festgestellt haben. Der durchschnittliche Verlust im Verlauf des Jahres wird für jeden der Befragten auf über 2 Millionen US-Dollar geschätzt. In den letzten Monaten kam es zu einer Serie von Angriffen auf Computerumgebungen. Viele dieser Angriffe erfolgten über das Internet und viele richteten sich gegen Systeme mit dem Betriebssystem Microsoft® Windows®. Dies sind jedoch nur die bekanntesten Sicherheitsprobleme, mit denen sich Organisationen heute beschäftigen müssen. In diesem Handbuch werden verschiedene Sicherheitsrisiken, die in einer bestimmten Umgebung auftreten können, näher beleuchtet. Zusätzlich erhalten Sie Informationen über effektive Schutzmaßnahmen.

Unabhängig von der verwendeten Umgebung sollten Sie das Problem der Sicherheit ernst nehmen. Viele Organisationen machen den Fehler, den Wert ihrer IT-Umgebung (Information Technology) zu unterschätzen. Meistens ist dies darauf zurückzuführen, dass die beträchtlichen indirekten Kosten nicht berücksichtigt werden. Handelt es sich um einen ausreichend schwerwiegenden Angriff, können die indirekten Kosten dem Wert der gesamten Organisation entsprechen. Wenn beispielsweise die Website Ihres Unternehmens infolge eines Angriffs so geändert wird, dass sie fiktive schlechte Nachrichten verkündet, könnte dies zum Einbruch des Aktienkurses Ihres Unternehmens führen. Bei der Auswertung der Kosten für die Sicherheit sollten Sie also die indirekten Kosten, die mit einem Angriff verbunden sind, und die Kosten durch den Verlust von IT-Funktionen berücksichtigen.

Die weltweit sichersten Computersysteme sind diejenigen, die vollständig von Benutzern und anderen Computern isoliert sind. Im Allgemeinen werden jedoch funktionelle Computersysteme benötigt, die mit einem Netzwerk verbunden sind. Häufig sind dies öffentliche Netzwerke. Mithilfe dieses Handbuchs können Sie die Risiken einer Netzwerkumgebung identifizieren, den für Ihre Umgebung geeigneten Sicherheitsgrad bestimmen und die erforderlichen Schritte festlegen, um diesen Sicherheitsgrad zu erreichen. Dieses Handbuch richtet sich zwar vorwiegend an große Unternehmen, große Teile des Handbuchs sind aber auch für Organisationen jeder beliebigen Größe geeignet.

Microsoft Operations Framework (MOF)

Damit der Betrieb in Ihrer Umgebung so effizient wie möglich verläuft, muss er effektiv verwaltet werden. Deshalb hat Microsoft das Microsoft Operations Framework (MOF) entwickelt. Dabei handelt es sich im Wesentlichen um eine Sammlung optimaler Vorgehensweisen, Prinzipien und Modelle, die Sie beim Betrieb der IT-Umgebung Ihres Unternehmens unterstützen. Das Befolgen der MOF-Richtlinien soll Ihnen dabei helfen, die Sicherheit, Zuverlässigkeit, Unterstützungsfähigkeit und Verwaltbarkeit unternehmenswichtiger Produktionssysteme dauerhaft mithilfe von Microsoft-Produkten zu gewährleisten.

Das MOF-Prozessmodell ist in vier integrierte Quadranten unterteilt:

- Ändern
- Betreiben
- Unterstützen
- Optimieren

Gemeinsam bilden die Phasen einen kreisförmigen Lebenszyklus (siehe Abbildung 1.1), der auf sämtliche Szenarien, von einer bestimmten Anwendung bis zu einer vollständigen Betriebsumgebung mit mehreren Rechenzentren, angewendet werden kann. In diesem Fall verwenden Sie MOF im Kontext des Sicherheitsvorgangs.

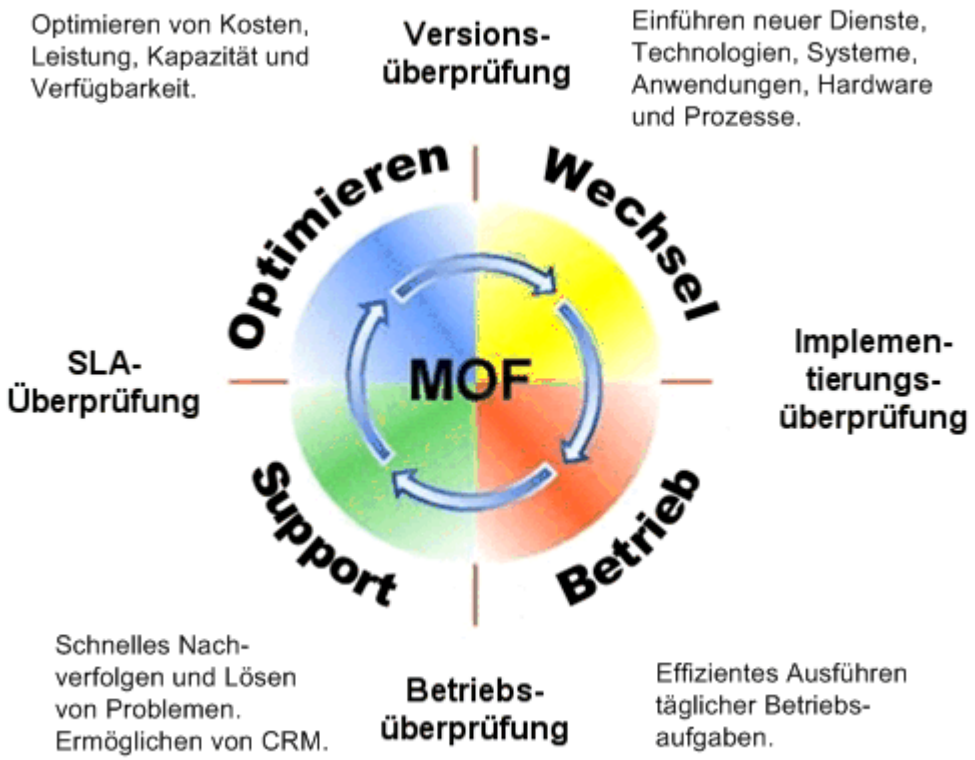


Abbildung 1.1: MOF-Prozessmodell

Das Prozessmodell wird von 20 Service Management-Funktionen (SMF), einem integrierten Teammodell und einem Risikomodell unterstützt. Jeder Quadrant wird durch eine entsprechende Überprüfung des Systembetriebsmanagements (auch Überprüfungsmeilenstein genannt) unterstützt. Dabei werden die SMF des jeweiligen Quadranten in ihrer Effektivität beurteilt.

Sie müssen kein MOF-Experte sein, um dieses Handbuch zu verstehen und anzuwenden, aber umfassende Kenntnisse in Bezug auf MOF-Prinzipien helfen Ihnen beim Verwalten und Aufrechterhalten einer zuverlässigen, verfügbaren und stabilen Betriebsumgebung.

Wenn Sie mehr zu MOF und dazu, wie MOF Ihnen im Unternehmen helfen kann, erfahren möchten, besuchen Sie die Microsoft Operations Framework-Website. Weitere Informationen finden Sie im gleichnamigen Abschnitt am Ende dieses Kapitels.

Get Secure und Stay Secure

Im Oktober 2001 hat Microsoft eine neue Initiative, das Strategic Technology Protection Program (STPP), gestartet. Mit diesem Programm sollen Microsoft-Produkte, -Dienste und -Support mit dem Schwerpunkt Sicherheit integriert werden. Microsoft unterteilt den Prozess zur Beibehaltung einer sicheren Umgebung in zwei zusammenhängende Phasen: "Get Secure" (Sicherheit schaffen) und "Stay Secure" (Sicherheit wahren).

Get Secure

Die erste Phase wird als "Get Secure" bezeichnet. Damit Ihre Organisation den geeigneten Sicherheitsgrad erreicht, folgen Sie den Empfehlungen zu "Get Secure" im englischsprachigen Microsoft Security Toolkit, auf das Sie online zugreifen können. Weitere Informationen finden Sie im gleichnamigen Abschnitt am Ende dieses Kapitels.

Stay Secure

Die zweite Phase wird als "Stay Secure" bezeichnet. Schon das Erstellen einer von Beginn an sicheren Umgebung ist nicht ganz einfach. Wenn die Umgebung jedoch aktiv ist und genutzt wird, ist es ein ganz anderes Problem, die Sicherheit der Umgebung auch dauerhaft zu gewährleisten. Außerdem müssen vorbeugende Maßnahmen zum Schutz vor Risiken ergriffen werden, um auf eintretende Risiken effektiv reagieren zu können.

Umfang dieses Handbuchs

Der Schwerpunkt dieses Handbuchs liegt explizit auf den Vorgängen, die zum Erstellen und Bewahren einer sicheren Umgebung auf Servern unter Windows 2000 erforderlich sind. Es werden bestimmte für Server definierte Rollen betrachtet. Allerdings wird nicht detailliert dargestellt, wie bestimmte Anwendungen sicher ausgeführt werden können.

Beim Implementieren von Sicherheit gibt es mehrere Bereiche, die Sie entwerfen und implementieren müssen. Abbildung 1.2 gibt einen allgemeinen Überblick über diese Bereiche. Die schattierten Bereiche werden in diesem Handbuch behandelt.

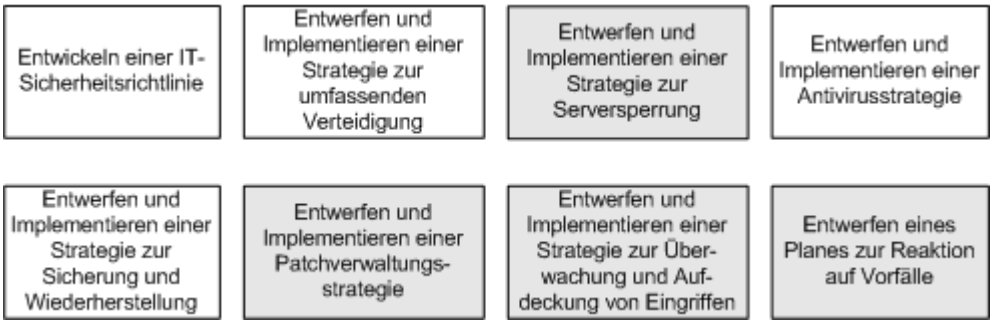


Abbildung 1.2: Sicherheitsbereiche

In der nachfolgenden Abbildung 1.3 werden die Schritte gezeigt, die erforderlich sind, um für einen Server Sicherheit zu schaffen (Get Secure) und um diese Sicherheit zu wahren (Stay Secure). Es wird auch dargestellt, wie die Kapitel dieses Handbuchs Ihnen dabei helfen, diese Ziele zu erreichen.

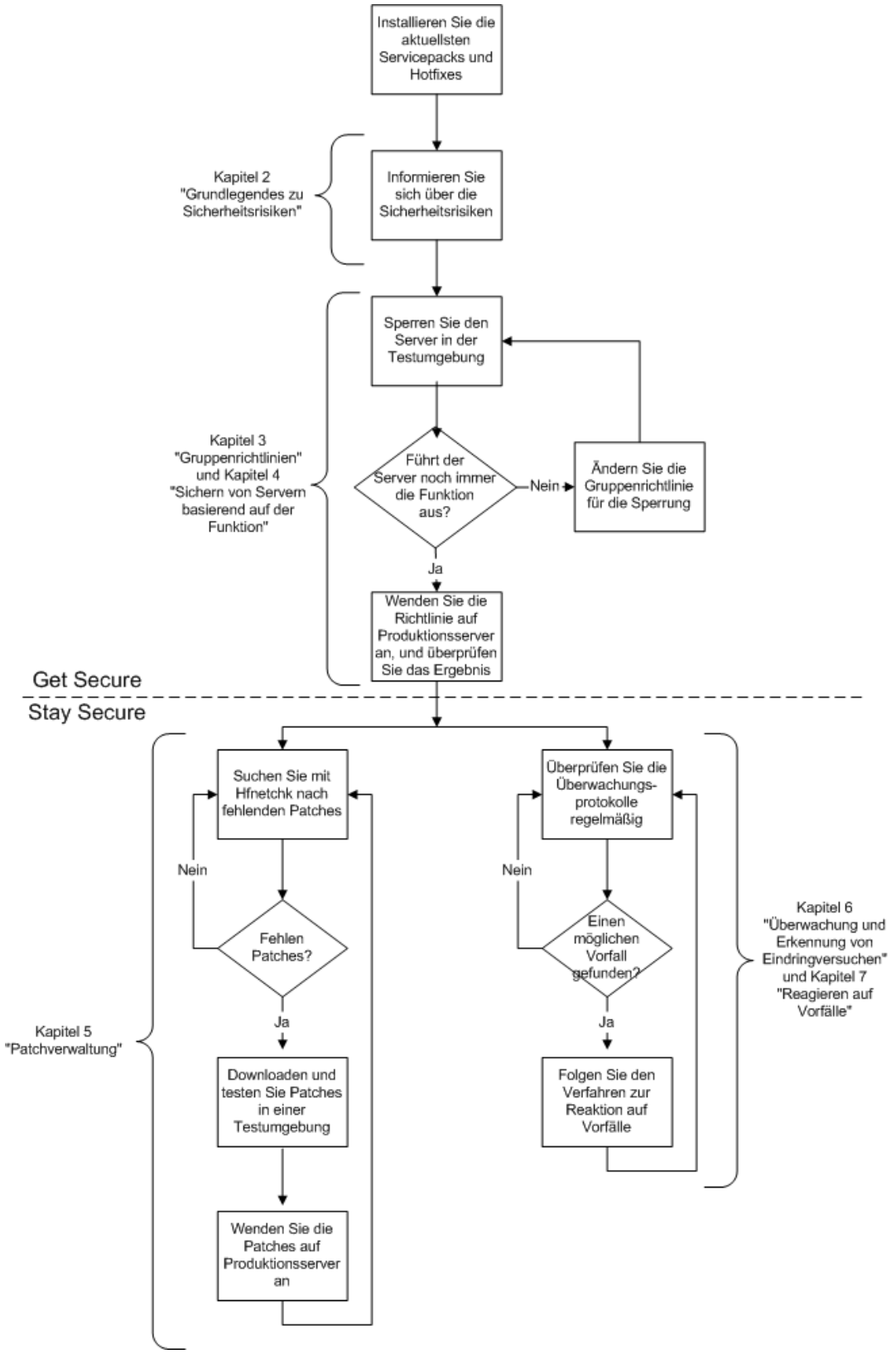


Abbildung 1.3: Flussdiagramm zu Sicherheitsverfahren

Anmerkung: In diesem Diagramm sind nicht alle Aufgaben aufgeführt, die zu den betrieblichen Prozessen zur Wahrung von Sicherheit gehören. Das Ausführen von Antivirensoftware und das Durchführen regelmäßiger Sicherungen werden beispielsweise nicht näher beschrieben. Es werden nur die Aufgaben gezeigt, die in diesem Handbuch ausführlich erläutert werden.

Sie sollten dieses Handbuch als Bestandteil Ihrer gesamten Sicherheitsstrategie verwenden, nicht als ein eigenständiges und vollständiges Handbuch, in dem alle Aspekte zum Erstellen und Verwalten einer sicheren Umgebung behandelt werden.

Zusammenfassung der Kapitel

Das Handbuch besteht aus den im Folgenden genannten Kapiteln. Jedes dieser Kapitel enthält Informationen zu einem Teil des Sicherheitsvorgangs. Sie können die einzelnen Kapitel je nach Bedarf vollständig oder teilweise lesen.

Kapitel 2: Grundlegendes zu Sicherheitsrisiken

Bevor Sie versuchen, eine sichere Umgebung zu schaffen, müssen Sie ein Verständnis für Bedrohungen, Schwachstellen, Ausnutzungsmöglichkeiten und Gegenmaßnahmen im Kontext der IT-Sicherheit entwickelt haben. In diesem Kapitel werden diese Probleme erläutert und die geschäftlichen sowie technischen Entscheidungen untersucht, die Ihnen beim effektiveren Umgang mit Sicherheitsrisiken in Ihrer Umgebung helfen.

Kapitel 3: Verwalten von Sicherheit mit Windows 2000-Gruppenrichtlinien

In Windows 2000 werden zahlreiche Sicherheitseinstellungen mithilfe von Gruppenrichtlinien definiert, die das Verhalten von Objekten auf dem lokalen Computer und im Verzeichnisdienst Active Directory™ steuern sollen. Diese Richtlinien müssen in geeigneter Weise festgelegt worden sein. Außerdem müssen Sie durch Überwachung sicherstellen, dass die Richtlinien nicht ohne entsprechende Berechtigung geändert werden. Dieses Kapitel beschäftigt sich ausführlich mit dem Verwalten von Sicherheit mithilfe von Gruppenrichtlinien.

Kapitel 4: Sichern von Servern basierend auf ihrer Rolle

Für einen Anwendungsserver, einen Dateiserver und einen Webserver sind unterschiedliche Einstellungen erforderlich, um deren Sicherheit zu erhöhen. In diesem Kapitel werden Domänencontroller und eine Reihe unterschiedlicher Mitgliedsserverrollen behandelt. Außerdem werden die Schritte gezeigt, denen Sie folgen sollten, um die höchstmögliche Sicherheit für diese Serverrollen sicherzustellen.

Anmerkung: In diesem Handbuch wird davon ausgegangen, dass Server bestimmte definierte Rollen ausführen. Wenn diese Rollen denen Ihrer Server nicht entsprechen, oder wenn Sie Mehrzweckserver verwenden, sollten Sie die hier definierten Einstellungen als Leitfaden für das Erstellen eigener Sicherheitsvorlagen verwenden, die die erforderliche Funktionalität bieten. Sie sollten dabei jedoch bedenken, dass ein Server mit vielen verschiedenen Funktionen anfälliger für Angriffe ist.

Kapitel 5: Patchverwaltung

Eine der wichtigsten Methoden zum Schutz vor Angriffen ist, die Umgebung mit den notwendigen Sicherheitspatches auf dem neuesten Stand zu halten. Patches können auf Servern und Clients erforderlich sein. In diesem Kapitel wird gezeigt, wie Sie sicherstellen können, rechtzeitig über neue Patches informiert zu werden, und wie diese Patches schnell und zuverlässig in der Organisation implementiert werden können. Außerdem erfahren Sie, wie Sie die Bereitstellung auf allen Computern überwachen können.

Kapitel 6: Überwachung und Erkennung von Eindringversuchen

Nicht alle Angriffe sind offensichtlich. Manchmal sind die weniger offenkundigen Angriffe die gefährlicheren: Sie bleiben unter Umständen unentdeckt, und es ist schwierig zu erkennen, welche Änderungen vorgenommen wurden. In diesem Kapitel wird gezeigt, wie Sie die Umgebung überwachen sollten, so dass Sie mit größter Wahrscheinlichkeit alle Angriffe entdecken. Außerdem werden Systeme zur Erkennung von Eindringversuchen erläutert. Dabei handelt es sich um Software, mit der Verhaltensweisen gefunden werden, die auf Angriffe hindeuten.

Kapitel 7: Vorgehensweise bei Vorfällen

Unabhängig vom Sicherheitsgrad der Umgebung bleibt ein gewisses Angriffsrisiko bestehen. Jede sinnvolle Sicherheitsstrategie muss Informationen dazu umfassen, wie die Organisation auf unterschiedliche Angriffe reagieren soll. In diesem Kapitel werden die besten Methoden für eine Reaktion auf die verschiedenen Angriffsmöglichkeiten behandelt. Außerdem werden die Schritte genannt, denen Sie folgen sollten, um Vorfälle effektiv zu melden. Zu diesem Kapitel gehört eine Fallstudie, in der eine typische Reaktion auf einen Vorfall gezeigt wird.

Zusammenfassung

Das vorliegende Kapitel enthält eine Einführung in das Handbuch sowie eine Zusammenfassung der anderen Kapitel. Außerdem wurde das Strategic Technology Protection Program (STTP) vorgestellt. Da Sie jetzt die Struktur dieses Handbuchs kennen, können Sie nun entscheiden, ob sie es ganz oder nur in ausgewählten Teilen lesen möchten. Sie sollten nicht vergessen, dass für effektive und erfolgreiche Sicherheitsvorkehrungen Anstrengungen in allen Bereichen erforderlich sind, nicht nur Verbesserungen in einem Bereich. Es ist daher empfehlenswert, alle Kapitel des Handbuchs zu lesen.

Weitere Informationen

Weitere Informationen dazu, wie MOF Ihnen in Ihrem Unternehmen helfen kann, finden Sie unter folgender Adresse:

http://www.microsoft.com/germany/ms/technetdatenbank/overview.asp?siteid=495299

Microsoft Security Toolkit (englischsprachig):
http://www.microsoft.com/germany/themen/security/default.htm

Website für das Microsoft Strategic Technology Protection Program:

http://www.microsoft.com/germany/themen/security/default.htm

Informationen zum Microsoft-Sicherheitsbenachrichtigungsdienst (Microsoft Security Notification Service):

http://www.microsoft.com/germany/ms/technetdatenbank/overview.asp?siteid=430926

Originaltitel: Chapter 2 – Understanding Security Risk

2

Grundlegendes zu Sicherheitsrisiken

Mit der Weiterentwicklung von IT-Systemen ergeben sich auch immer mehr Sicherheitsrisiken für diese Systeme. Wenn Sie Ihre Umgebung effektiv vor Angriffen schützen möchten, müssen Sie die Risiken kennen.

Beim Identifizieren von Sicherheitsrisiken sollten Sie zwei wichtige Faktoren berücksichtigen: 1) Welche Arten von Angriffen wahrscheinlich sind, und 2) wo die Angriffe eintreten können. Viele Organisationen vernachlässigen den zweiten Faktor, indem sie davon ausgehen, dass schwerwiegende Angriffe von außerhalb erfolgen (i. d. R. über die Internetverbindung). In einer Umfrage des CSI/FBI zu Computerkriminalität und -sicherheit nannten 31 % der Befragten die internen Systeme als häufigen Angriffspunkt. Viele Unternehmen wissen jedoch wahrscheinlich gar nicht, dass interne Angriffe stattfinden. Der Grund ist oft, dass derartige Angriffe nicht überwacht werden.

In diesem Kapitel werden mögliche Arten von Angriffen untersucht. Es werden auch einige der betrieblichen und technischen Schritte behandelt, die Sie zur Begrenzung der Risiken für Ihre Umgebung ausführen können.

Risikomanagement

Es gibt keine IT-Umgebung, die vollständig gesichert und gleichzeitig nützlich ist. Bei der Untersuchung der Umgebung müssen Sie die Risiken beurteilen, die derzeit für Ihre Umgebung bestehen, bestimmen, welcher Umfang an Risiken akzeptabel ist, und dafür sorgen, dass die Risiken diesen Umfang nicht übersteigen. Risiken können vermindert werden, indem die Sicherheit der Umgebung erhöht wird.

Allgemein gilt, je höher die Sicherheit in einer Organisation, desto aufwändiger ist deren Implementierung und desto wahrscheinlicher ist eine Reduzierung der Funktionalität. Nach dem Beurteilen der potenziellen Risiken müssen Sie möglicherweise die Sicherheit reduzieren, um die Funktionalität zu erhöhen und die Kosten zu senken, wie im nachfolgenden Beispiel beschrieben.

Nehmen Sie z. B. eine Kreditkartenfirma, die die Implementierung eines Systems zum Schutz vor Betrug erwägt. Wenn durch Betrug für die Firma jährlich Kosten in Höhe von 3 Millionen Dollar entstehen, das Implementieren und Verwalten eines Systems zum Schutz vor Betrug jährlich jedoch 5 Millionen Dollar kostet, ergibt sich aus der Installation des Systems kein direkter finanzieller Vorteil. Die indirekten Verluste können aber weit über den 3 Millionen Dollar liegen, da die Unternehmensreputation leidet und Kunden das Vertrauen in die Firma verlieren. Dementsprechend ist die Berechnung deutlich komplexer.

Manchmal bedeutet eine höhere Sicherheit, dass Benutzer mit komplexeren Systemen umgehen müssen. Eine Onlinebank könnte beispielsweise mehrere Authentifizierungsebenen für die Benutzer verwenden, wenn diese auf ihr Konto zugreifen. Wenn die Authentifizierung jedoch zu kompliziert ist, werden einige Kunden das System nicht verwenden. Dadurch werden möglicherweise höhere Kosten verursacht, als durch die Angriffe auf das Computersystem der Bank.

Um die Prinzipien des Risikomanagements zu verstehen, müssen Sie einige wichtige Begriffe kennen, die beim Risikomanagement verwendet werden. Dazu gehören Ressourcen, Bedrohungen, Schwachstellen, Ausnutzungsmöglichkeiten und Gegenmaßnahmen.

Ressourcen

Ressourcen sind alle Bestandteile in der Umgebung, die Sie schützen möchten. Dies können Daten, Anwendungen, Server, Router und sogar Personen sein. Durch die Sicherheit soll verhindert werden, dass die Ressourcen angegriffen werden.

Ein wichtiger Bestandteil des Risikomanagements ist, den Wert der Ressourcen zu ermitteln. Sie würden keine handelsüblichen Türschlösser und Alarmanlagen verwenden, um die Kronjuwelen zu schützen. Entsprechend wird im Allgemeinen durch den Wert der Ressourcen bestimmt, welches Maß an Sicherheit für ihren Schutz erforderlich ist.

Bedrohungen

Eine Bedrohung ist eine Person, die auf Ressourcen zugreifen und Schaden verursachen kann, bzw. ein Ort oder ein Gegenstand, durch den dies geschieht. In der Tabelle sind verschiedene Arten von Bedrohungen und Beispiele dafür aufgeführt.

Tabelle 2.1: Bedrohungen für Computerumgebungen

Art der Bedrohung	Beispiele
Natürlich und physisch	Feuer, Wasser, Wind, Erdbeben Stromausfall
Unbeabsichtigt	Nicht informierte Mitarbeiter Nicht informierte Kunden
Beabsichtigt	Angreifer Terroristen Industriespione Regierung Schädlicher Code

Schwachstellen

Eine Schwachstelle ist ein Punkt, an dem eine Ressource anfällig für einen Angriff ist. Schwachstellen werden häufig in die in der folgenden Tabelle dargestellten Kategorien unterteilt.

Tabelle 2.2: Schwachstellen in Computerumgebungen

Art der Schwachstelle	Beispiele
Physisch	Nicht verschlossene Türen
Natürlich	Beschädigtes System zur Feuerbekämpfung
Hardware und Software	Veraltete Antivirensoftware
Medien	Elektrische Störungen
Kommunikation	Nicht verschlüsselte Protokolle
Menschlich	Unsichere Helpdeskverfahren

Anmerkung: Die aufgeführten Beispiele für Bedrohungen und Schwachstellen treffen möglicherweise nicht auf Ihre Organisation zu, da alle Organisationen unterschiedlich sind.

Ausnutzung

Eine Bedrohung kann eine Ressource gefährden, indem eine Schwachstelle in der Umgebung ausgenutzt wird. Diese Art von Angriff wird als Ausnutzung bezeichnet. Die Ausnutzung einer Schwachstelle kann auf verschiedene Arten erfolgen. Einige der häufigsten sind in der folgenden Tabelle aufgeführt.

Tabelle 2.3: Ausnutzungsmöglichkeiten in Computerumgebungen

Art der Ausnutzung	Beispiele
Ausnutzung technischer Schwachstellen	Brute Force-Angriff Pufferüberlauf Konfigurationsfehler Wiederholungsangriff Sitzungsübernahme (Session Hijacking)
Sammeln von Informationen	Adressidentifikation Betriebssystemidentifikation Scannen von Ports Testen von Anwendungen und Diensten Suchen nach Schwachstellen Analyse von Antworten Auflistungen von Benutzern Untersuchen von Dokumenten Sicherheitslücken beim Funknetzbetreiber Kontakt zu Mitarbeitern
Denial-of-Service	Physische Beschädigung Entfernen von Ressourcen Ändern von Ressourcen Überlastung von Ressourcen

Wenn eine Schwachstelle für einen Angriff auf eine Ressource ausgenutzt wird, kann dies schwerwiegende Folgen haben. In der Tabelle werden einige der Ergebnisse der Ausnutzung von Schwachstellen in der Umgebung und Beispiele dafür aufgeführt.

Tabelle 2.4: Ergebnisse der Ausnutzung von Schwachstellen

Ergebnisse der Ausnutzung von Schwachstellen	Beispiele
Vertrauensverlust	Unberechtigter Zugriff Ausweitung von Berechtigungen Identitätswechsel oder Diebstahl der Kennung
Integritätsverlust	Beschädigung von Daten Falsche Informationen
Verlust der Verfügbarkeit	Denial-of-Service

Beziehungen zwischen Bedrohungen, Schwachstellen und Risiken

Jede in der Organisation erkannte Bedrohung oder Schwachstelle sollte beschrieben und mithilfe eines Standards, z. B. **niedrig**, **mittel**, **hoch**, bewertet werden. Die Bewertungen sind von Organisation zu Organisation und manchmal auch innerhalb einer Organisation unterschiedlich. So ist z. B. die Bedrohung durch ein Erdbeben in Niederlassungen, die sich in der Nähe von Erbebengebieten befinden, deutlich höher als an anderen Orten. In einer Organisation, in der sehr empfindliche und zerbrechliche Elektrogeräte hergestellt werden, stellt die physische Beschädigung der Ausrüstung eine schwerwiegende Schwachstelle dar, während physische Beschädigungen in einem Bauunternehmen eher als geringe Schwachstelle zu bewerten sind.

Anmerkung: Aufgabenhilfe 1: "Tabelle zur Analyse möglicher Bedrohungen und Schwachstellen" kann verwendet werden, um Bedrohungen und deren Auswirkungen auf die Organisation zu bewerten.

Der Umfang an Risiken in der Organisation erhöht sich mit dem Umfang an Bedrohungen und Schwachstellen. Dies ist in der folgenden Abbildung dargestellt.

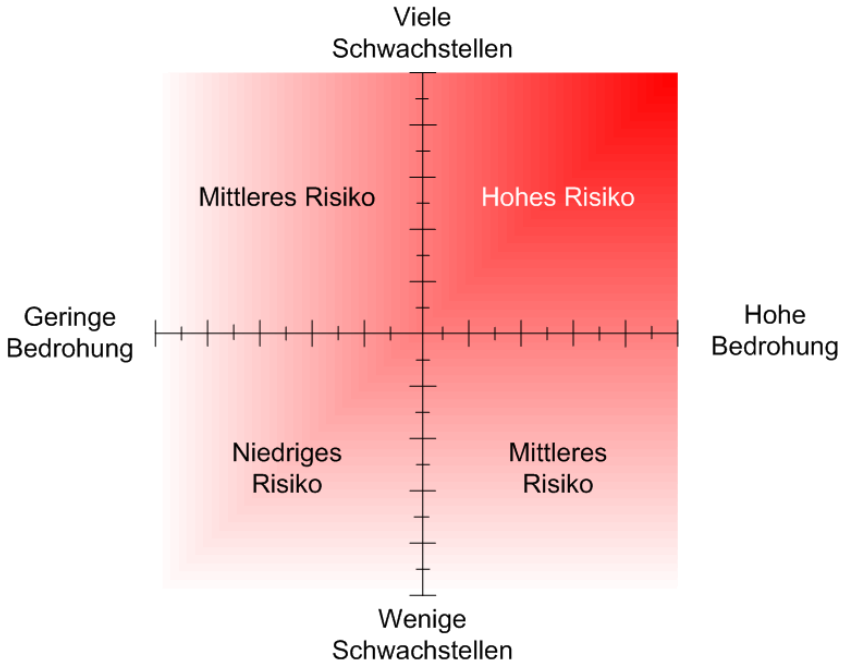


Abbildung 2.1: Risikomatrix

Gegenmaßnahmen

Gegenmaßnahmen werden eingesetzt, um Bedrohungen und Schwachstellen entgegen zu wirken und so die Risiken für die Umgebung zu reduzieren. Beispielsweise kann eine Organisation, die zerbrechliche Elektrogeräte herstellt, aus Sicherheitsgründen physische Gegenmaßnahmen ergreifen, indem z. B. Ausrüstung am Fundament des Gebäudes befestigt wird oder Mechanismen zur Dämpfung eingebaut werden. Durch diese Gegenmaßnahmen wird die Wahrscheinlichkeit verringert, dass die Anlagen durch ein Erdbeben physisch beschädigt werden. Das Restrisiko ist das Risiko, das bestehen bleibt, nachdem alle Gegenmaßnahmen zur Reduzierung der Bedrohungen und Schwachstellen angewendet wurden.

Umfassende Verteidigung

Um das Risiko in Ihrer Umgebung zu reduzieren, sollten Sie eine Strategie der umfassenden Verteidigung verwenden, um die Ressourcen vor externen und internen Bedrohungen zu schützen. Der Begriff *umfassende Verteidigung* (auch als umfassende Sicherheit oder mehrschichtige Sicherheit bezeichnet) wurde von einem militärischen Ausdruck abgeleitet, um die Schichtung der Gegenmaßnahmen zur Gewährleistung der Sicherheit zu beschreiben, durch die eine zusammenhängende Sicherheitsumgebung ohne Einzelpunktversagen gebildet wird. Zu den Sicherheitsschichten, die Ihre Strategie der umfassenden Verteidigung bilden, sollte das Bereitstellen von Schutzmaßnahmen an allen Punkten gehören, angefangen bei externen Routern bis hin zum Standort der Ressourcen.

Durch das Bereitstellen mehrerer Sicherheitsschichten können Sie gewährleisten, dass auch bei der Verletzung einer Sicherheitsschicht die anderen Schichten eine ausreichende Sicherheit zum Schutz der Ressourcen bieten. Beispielsweise sollte die Verletzung des Firewalls einer Organisation Angreifern nicht den uneingeschränkten Zugriff auf die vertraulichsten Daten der Organisation ermöglichen. Idealerweise sollte jede Schicht andere Gegenmaßnahmen bereitstellen, damit eine Methode zur Ausnutzung von Schwachstellen nicht bei allen Schichten verwendet werden kann.

In der folgenden Abbildung ist eine effektive Strategie der umfassenden Verteidigung dargestellt:

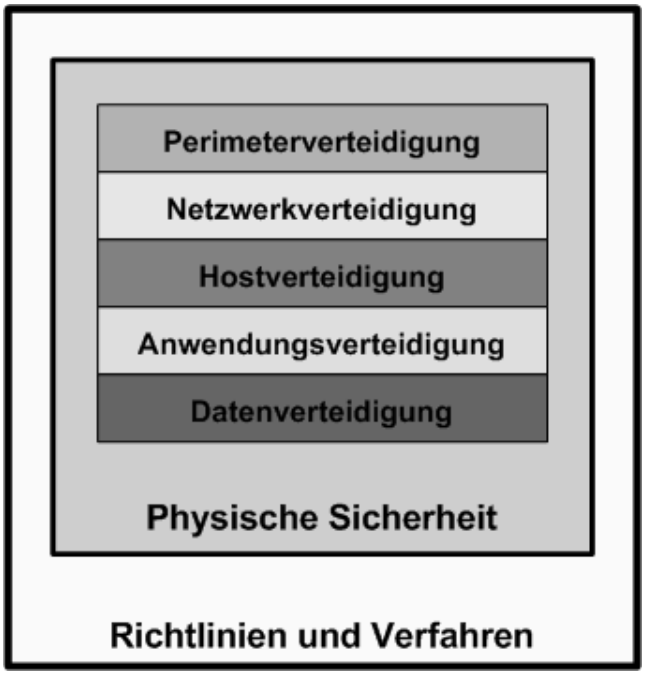


Abbildung 2.2: Strategie der umfassenden Verteidigung

Sie dürfen nicht vergessen, dass zu Ihren Ressourcen nicht nur Daten zählen, sondern alles in der Umgebung, das anfällig für einen Angriff ist. Als Bestandteil der Risikomanagementstrategie sollten Sie die Ressourcen untersuchen, die Sie schützen. Außerdem sollten Sie ermitteln, ob der Schutz für alle Ressourcen ausreicht. Der Grad an Sicherheit, den Sie gewährleisten, hängt natürlich von der Risikobeurteilung und von der Kosten-Nutzen-Analyse für den Einsatz von Gegenmaßnahmen ab. Das Ziel ist jedoch, sicherzustellen, dass ein Angreifer beträchtliche Kenntnisse, Zeit und Ressourcen benötigt, um alle Gegenmaßnahmen zu umgehen und Zugriff auf die Ressourcen zu erhalten.

Anmerkung: Wie Sie die umfassende Verteidigung genau bereitstellen, hängt von den Besonderheiten der Umgebung ab. Sie sollten Ihre Strategie der umfassenden Verteidigung neu beurteilen, wenn sich Ihre Umgebung ändert.

Es ist sinnvoll, die einzelnen Schichten der Strategie der umfassenden Verteidigung genauer zu untersuchen.

Datenverteidigung

In vielen Unternehmen stellen Daten die wertvollste Ressource dar. Wenn die Daten Konkurrenten in die Hände fielen oder beschädigt würden, hätte dies schwerwiegende Folgen für das Unternehmen.

Die lokal auf Clients gespeicherten Daten sind besonders gefährdet. Wenn ein Laptop gestohlen wird, können die Daten gesichert und auf einem anderen Computer wiederhergestellt und gelesen werden, auch wenn sich der Dieb nicht am System anmelden kann.

Es gibt eine Reihe von Möglichkeiten, um Daten zu schützen. Daten können verschlüsselt werden, u. a. mit dem verschlüsselnden Dateisystem (EFS oder Encrypting File Service) oder mit Verschlüsselungslösungen von Drittanbietern, und die freigegebenen Zugriffssteuerungslisten (DACLs oder Discretionary Access Control Lists) für Dateien können geändert werden.

Anwendungsverteidigung

Als weitere Verteidigungsschicht spielt die Anwendungsabsicherung eine wichtige Rolle in jedem Sicherheitsmodell. Viele Anwendungen verwenden das Sicherheitsteilsystem von Windows 2000, um Sicherheit zu gewährleisten. Es liegt jedoch in der Verantwortung des Entwicklers, Sicherheitsvorkehrungen in der Anwendung vorzusehen, die zusätzlichen Schutz für die Bereiche der Architektur bieten, auf welche die Anwendung zugreifen kann. Eine Anwendung muss im Kontext des Systems betrachtet werden. Sie sollten immer die Sicherheit der gesamten Umgebung berücksichtigen, wenn Sie die Anwendungssicherheit prüfen.

Jede Anwendung in Ihrer Organisation sollte in einer Testumgebung sorgfältig auf ausreichende Sicherheit getestet werden, bevor sie in einer Produktionsumgebung eingesetzt wird.

Hostverteidigung

Sie sollten alle Hosts in Ihrer Umgebung prüfen und Richtlinien erstellen, mit denen die Server soweit eingeschränkt werden, dass sie nur noch die ihnen zugewiesenen Aufgaben ausführen können. Auf diese Weise schaffen Sie eine weitere Sicherheitshürde, die ein Angreifer überwinden muss, bevor er Schaden anrichten kann. In Kapitel 4, "Sichern von Servern basierend auf ihrer Rolle", sind Richtlinien aufgeführt, mit denen die Sicherheit für fünf allgemeine Windows 2000-Serverrollen verbessert werden kann.

Dazu können Sie z. B. einzelne Richtlinien erstellen, die auf der Klassifikation und dem Typ der Daten basieren, die auf den Servern gespeichert sind. In der Richtlinie

einer Organisation kann beispielsweise festgelegt sein, dass alle Webserver für die öffentliche Nutzung bestimmt sind und deshalb nur öffentliche Informationen enthalten dürfen. Die Datenbankserver sind dagegen als für das Unternehmen vertraulich klassifiziert, was bedeutet, dass die auf ihnen gespeicherten Informationen unter allen Umständen geschützt werden müssen. Daraus ergeben sich die in der folgenden Tabelle dargestellten Klassifikationen.

Tabelle 2.5: Klassifikation von Servern

Wert	Definition
Öffentliche Nutzung	Die enthaltenen Materialien können uneingeschränkt verbreitet werden. Dazu gehören Marketinginformationen, Vertriebsmaterialien und zur Veröffentlichung freigegebene Informationen. Daten auf öffentlichen Internetservern sollten grundsätzlich für die öffentliche Nutzung bestimmt sein.
Nur interne Nutzung	Die interne Veröffentlichung dieser Informationen ist sicher, eine Weitergabe der Informationen an die Öffentlichkeit könnte der Organisation deutlich schaden. Diese Informationen sollte vom Internet durch mindestens einen Firewall abgeschirmt werden.
Geschäftsgeheimnis	Eine Veröffentlichung dieser Art von Informationen könnte der gesamten Organisation ernsthaften Schaden zufügen. Es handelt sich um besonders vertrauliche Informationen, die nur weitergegeben werden dürfen, wenn dies unbedingt erforderlich ist. Diese Informationen sollten vom Internet durch mindestens zwei Firewalls abgeschirmt werden.

Netzwerkverteidigung

Ihre Organisation kann über eine Reihe von Netzwerken verfügen, und Sie sollten jedes einzelne prüfen, um sicherzustellen, dass alle Netzwerke ausreichend gesichert sind. Ein erfolgreicher Angriff auf einen Router kann dazu führen, dass er ganzen Netzwerksegmenten den Dienst verweigert.

Sie sollten den rechtmäßigen Datenverkehr in den Netzwerken prüfen und die Netzwerke für nicht erforderlichen Datenverkehr sperren. Sie sollten außerdem überlegen, IPSec zum Verschlüsseln der Pakete in internen Netzwerken und SSL für die externe Kommunikation zu verwenden. Darüber hinaus sollten Sie das Netzwerk auf Paketsniffer überprüfen, die nur unter strenger Kontrolle verwendet werden sollten.

Perimeterverteidigung

Der Schutz des Perimeternetzwerks ist der wichtigste Aspekt beim Verhindern externer Angriffe. Wenn das Perimeternetzwerk sicher bleibt, ist das interne Netzwerk vor externen Angriffen geschützt. Ihre Organisation sollte über eine sichere Vorrichtung verfügen, durch die alle Zugriffspunkte auf das Netzwerk geschützt werden. Jede Vorrichtung sollte geprüft und es sollte über die zulässigen Arten von Datenverkehr entschieden werden. Anschließend sollte ein Sicherheitsmodell zum Sperren des Netzwerks für sonstigen Datenverkehr entwickelt werden.

Firewalls sind ein wichtiger Bestandteil der Perimeterverteidigung. Es ist mindestens ein Firewall erforderlich, um sicherzustellen, dass Angriffe von außerhalb minimiert werden. Durch Überwachung und Identifizierung von Eindringversuchen können Sie sicherstellen, dass Sie die Angriffe auch erkennen. Weitere Informationen dazu finden Sie in Kapitel 6, "Überwachung und Erkennung von Eindringversuchen".

Sie dürfen außerdem nicht vergessen, dass bei Netzwerken mit Remotezugriff auch die Laptops von Mitarbeitern und sogar Heim-PCs zum Perimeternetzwerk gehören können. Sie müssen sicherstellen, dass diese Computer Ihren

Sicherheitsanforderungen entsprechen, bevor sie eine Verbindung mit dem Netzwerk herstellen dürfen.

Physische Sicherheit

Eine Umgebung, in der nicht berechtigte Benutzer physisch auf Computer zugreifen können, ist in sich nicht sicher. Ein sehr effektiver Denial-of-Service-Angriff ist, die Stromversorgung des Servers zu unterbrechen oder Datenträger zu entfernen. Datendiebstahl (und Denial-of-Service) kann durch eine Person erfolgen, die einen Server oder einen Laptop stiehlt.

Sie sollten die physische Sicherheit als Basis Ihrer gesamten Sicherheitsstrategie betrachten. Zuerst müssen Sie die Standorte der Server physisch sichern. Dies können Serverräume im Gebäude oder vollständige Rechenzentren sein.

Sie sollten außerdem den Zugang zu den Gebäuden Ihrer Organisation überprüfen. Wenn jemand Zugang zu einem Gebäude hat, hat er auch viele Möglichkeiten für einen Angriff, auch ohne eine Anmeldung am Netzwerk. Dazu gehören z. B. die folgenden Möglichkeiten:

- Denial-of-Service (z. B. Verbinden eines Laptops, bei dem es sich um einen DHCP-Server handelt, mit dem Netzwerk oder Unterbrechen der Stromversorgung eines Servers)
- Datendiebstahl (z. B. Stehlen eines Laptops oder Paketsniffer im internen Netzwerk)
- Ausführen von schädlichem Code (z. B. Starten eines Wurms innerhalb der Organisation)
- Diebstahl wichtiger Sicherheitsinformationen (z. B. Sicherungsbänder, Betriebshandbücher und Netzwerkdiagramme)

Als Teil Ihrer Risikomanagementstrategie sollten Sie ermitteln, welcher Grad an physischer Sicherheit für Ihr System angemessen ist. Zu möglichen Maßnahmen in Bezug auf die physische Sicherheit gehören die folgenden.

- Alle Bereiche des Gebäudes müssen physisch gesichert werden (z. B. mit Schlüsselkarten, biometrischen Geräten und Sicherheitspersonal).
- Besucher müssen ständig in Begleitung sein.
- Besucher müssen alle mitgeführten Computergeräte bei ihrer Ankunft angeben.
- Alle Mitarbeiter müssen ihre eigenen tragbaren Geräte registrieren lassen.
- Alle Laptops und Desktopcomputer müssen an Tischen befestigt werden.
- Alle Datenspeichergeräte müssen registriert werden, bevor sie aus dem Gebäude entfernt werden.
- Server müssen in gesonderten Räumen platziert werden, zu denen nur Administratoren Zutritt haben.
- Redundante Internetverbindungen, Stromversorgung, Feuerbekämpfung usw.
- Schutz vor Naturkatastrophen und Terroranschlägen
- Der Zugang zu Bereichen, an denen ein Denial-of-Service-Angriff möglich wäre, muss gesichert werden (z. B. die Bereiche, an denen die Verkabelung aus dem Hauptgebäude hinausführt).

Richtlinien und Verfahren

Das Ziel fast aller bisher beschriebenen Maßnahmen ist es, unberechtigten Zugriff auf Systeme zu verhindern. Es gibt aber bestimmt Personen in Ihrer Umgebung, für die ein umfassender Zugriff auf Systeme erforderlich ist. Jede Sicherheitsstrategie hat schwerwiegende Mängel, wenn nicht sichergestellt werden kann, dass diese Personen die ihnen gewährten Rechte nicht ausnutzen.

Bevor Sie in Ihrer Organisation neue Mitarbeiter einstellen, sollten Sie sie einer Sicherheitsüberprüfung unterziehen. Die Mitarbeiter, denen in größerem Umfang Zugriff auf die Systeme gewährt wird, müssen Sie genauer überprüfen.

Bei den bereits in Ihrem Unternehmen beschäftigten Mitarbeitern ist es wichtig, dass sie die Sicherheitsrichtlinien und ihre Rechte (vorzugsweise mit Begründung) kennen. Dies ist aus zwei Gründen wichtig. Zum einen ist es möglich, dass Ihre Mitarbeiter möglicherweise Aktionen ausführen, die unbeabsichtigt die Sicherheit der Umgebung gefährden, wenn sie nicht wissen, was verboten ist. Zum anderen kann das Ergreifen von Maßnahmen gegen einen Mitarbeiter erschwert werden, wenn dieser absichtlich Ihre IT-Umgebung angreift und dies in den Unternehmensrichtlinien nicht explizit verboten ist.

In einer Windows 2000-basierten Umgebung können Sie sehr genau steuern, über welche Administratorrechte Benutzer verfügen. Sie sollten sicherstellen, dass Sie den Umfang der Administratorrechte, die den einzelnen IT-Mitarbeitern zur Verfügung stehen, ganz genau definieren. Keiner der Mitarbeiter sollte über weitreichendere Administratorrechte verfügen, als für seine Aufgaben unbedingt erforderlich sind.

Die Information der Benutzer über die Sicherheit kann Folgendes einschließen: einen Orientierungskurs, an den sich regelmäßige Erinnerungen sowie die Bekanntgabe von Aktualisierungen der Sicherheitsverfahren anschließen. Es ist sehr wichtig, dass alle Mitarbeiter erkennen, dass sie zur Wahrung der Sicherheit in der Organisation beitragen.

Anmerkung: Aufgabenhilfe 2: Die "häufigsten Fehler" in Bezug auf die Sicherheit zeigen sich als Liste weit verbreiteter Fehler, die in jeder Organisation auftreten können. Diese "häufigsten Fehler" erhöhen das Risiko für Ihre Organisation in beträchtlichem Umfang. Bei der Definition der Sicherheitsrichtlinien sollten Sie sicherstellen, dass Sie die Wahrscheinlichkeit solcher "häufigsten Fehler" minimieren.

Verbreitete Abwehrmethoden und Vorsorgemaßnahmen

Als Bestandteil Ihrer Strategie der umfassenden Verteidigung müssen Sie die Methoden kennen lernen, die von Angreifern verwendet werden. Außerdem müssen Sie wissen, wie Sie sich gegen die am häufigsten verwendeten Angriffe verteidigen können. In diesem Abschnitt werden verschiedene Arten von Angriffen beschrieben und Schritte zum Schutz der Umgebung vor diesen Angriffen vorgeschlagen.

Anmerkung: Aufgabenhilfe 3: "Angriffe und Gegenmaßnahmen" enthält eine Tabelle verbreiteter Ausnutzungsmöglichkeiten technischer Schwachstellen und entsprechende Gegenmaßnahmen.

Sammeln von Informationen

Angreifer versuchen immer, Informationen über die Umgebung herauszufinden. Manchmal sind diese Informationen selbst nützlich, manchmal sind sie auch ein Mittel, um weitere Informationen und Ressourcen zu erhalten.

Wenn Sie das Sammeln von Informationen verhindern möchten, müssen Sie den unberechtigten Zugriff auf Ihre Ressourcen von außerhalb beschränken. Dazu können Sie die folgenden Methoden verwenden:

Sicherstellen, dass Remotezugriff nur bei bestimmten, identifizierten Geräten im Netzwerk zugelassen wird. Überprüfen aller Durchwahlnummern des Unternehmens auf das Vorhandensein nicht autorisierter Geräte mithilfe eines Modempeilprogramms (Modem-Sweep Utility). Ermitteln von Remotezugriffsgeräten durch Aktivierung der Scanerkennung der Telefonanlage, sofern vorhanden.

Deaktivieren von NetBIOS über TCP/IP, einschließlich der Ports 135, 137, 139 und 445 auf Computern, die eine direkte Verbindung mit dem Internet durch den äußeren Firewall besitzen. Dadurch wird es Außenstehenden erschwert, Verbindungen mit Servern über Standardnetzwerke herzustellen.

Ausschließliches Aktivieren der Ports 80 und 443 sowohl an den mit dem Internet verbundenen Netzwerkadaptern als auch am Firewall für den Datenverkehr zu einer Webfarm. Dadurch werden die meisten portbasierten Erkundungstechniken unterbunden.

Überprüfen der Informationen auf der öffentlichen Website, um Folgendes sicherzustellen:

Die auf der Site verwendeten E-Mail-Adressen gehören nicht zu Administratorkonten.

Die Technologie des Netzwerks wird nicht angegeben.

Nur geeignete allgemeine Geschäftsinformationen wurden dort veröffentlicht, aus denen sich keine Hinweise zu Eigenschaften des Sicherheitssystems entnehmen oder ableiten lassen. Dies gilt auch für Informationen zu aktuellen oder kürzlich geschehenen Ereignissen. Wenn beispielsweise auf der Website bekannt gegeben wird, dass Ihr Unternehmen kürzlich eine andere Firma übernommen hat, könnten Angreifer diese Firma in der Hoffnung ins Visier nehmen, dass das dortige Netzwerk in Eile an das neue Unternehmensnetzwerk angeschlossen wurde und daher weniger sicher ist.

Überprüfen der von Mitarbeitern in Usenet-Newsgroups bereitgestellten Beiträge, um zu untersuchen, welche Art von Informationen sie dort veröffentlichen.

Prüfen der Inhalte im Quellcode der Website, um zu verhindern, dass ein Angreifer durch Auswerten dieses Codes wertvolle Informationen erhält (diese Methode wird auch als "Source Sifting" bezeichnet). Das Sicherheitsteam sollte dabei im Quellcode u. a. auf nicht ordnungsgemäße Kommentare, eingebettete Kennwörter und versteckte Tags achten.

Überprüfen der Informationen, die der allgemeinen Öffentlichkeit zu IP-Adressen und Domänennamenregistrierungen zur Verfügung gestellt werden.

Sicherstellen, dass ein Angreifer den DNS-Server nicht nach dem Referenznetzwerk abfragen oder ihn zum Durchführen einer vollständigen Zonenübertragung veranlassen kann. Durch das Abrufen aller Einträge im DNS-Server kann ein Angreifer sich einen guten Überblick darüber verschaffen, welche Computer am leichtesten angreifbar sind. Um die DNS-Abfrage zu verhindern, können Sie mithilfe der Option **Benachrichtigen** Rechte für den Windows 2000-DNS-Server zuweisen und Zonenübertragungen auf autorisierte Server beschränken. Ein anderer Ansatz besteht darin, einen DNS-Server mit Nur-Lesen-Berechtigung zu implementieren und Richtlinien und Verfahren zu seiner Aktualisierung bereitzustellen.

Berücksichtigen der wichtigen Überlegungen zur Gestaltung von Richtlinien im *Site Security Handbook* (RFC 2196). Ein Unternehmen, das Geschäfte mit der Öffentlichkeit tätigt, muss bestimmte Informationen veröffentlichen. Dabei ist es wichtig, nur die erforderlichen Informationen bereitzustellen, und nicht solche, die missbräuchlich verwendet werden können.

Bestimmen, welche Arten von Informationen sich Personen verschaffen können, die das Netzwerk mit Dienstprogrammen wie z. B. Traceroute untersuchen. Diese Dienstprogramme, die den TTL-Parameter (Time-To-Live oder Gültigkeitsdauer) nutzen, werden verwendet, um der Route eines IP-Pakets von einem Host zum nächsten zu folgen; anhand der Ergebnisse erstellen sie dann ein Abbild des Netzwerks.

Anmerkung: RFC 2196 ist über die Website **Request for Comments** verfügbar, die im Abschnitt "Weitere Informationen" am Ende dieses Kapitels aufgeführt ist.

Einschränken von Scans zur Beschaffung wertvoller Informationen

Sowohl TCP (Transmission Control Protocol) als auch UDP (User Datagram Protocol) verwenden Scans für die Kommunikation. Mithilfe von Portscannern können Angreifer die Server in Ihrer Umgebung ausmachen, die empfangsbereit sind, und diese Informationen dann zum Aufdecken von Schwachstellen verwenden.

Es gibt eine Reihe von Scans, die für Angreifer von Nutzen sind. Sie können dazu verwendet werden, Informationen von zu überwachenden Ports, vorhandenen Protokollen oder sogar zum Betriebssystem des Host (einschließlich der Versionsnummer) zu erhalten. Durch das Identifizieren der Ports, Protokolle und des Betriebssystems eines Hosts können Schwachstellen aufgedeckt werden, die ohne das Scannen nicht aufgedeckt worden wären.

In der Tabelle sind einige wichtige Scanmethoden sowie deren Funktionsweise und Nutzen aufgeführt:

Tabelle 2.6: Scanmethoden und deren Nutzen

Scanmethode	Funktionsweise	Nutzen
ICMP-Echo oder -Ping (Internet Control Message Protocol)	Sendet ICMP-Port 0-Pakete an das empfangende System. Wenn das System Antworten auf ICMP-Echos zulässt, sendet es eine ICMP-Antwort an das scannende System und zeigt damit, dass es aktiv ist und den Netzwerkverkehr überwacht.	Ein Pingscan wird verwendet, um die überwachenden Hosts im Netzwerk zu identifizieren. Er identifiziert nur die überwachenden ICMP-Ports und -Protokolle. Viele Sicherheitsfiltervorrichtungen sperren ICMP-Echoanforderungen und verhindern so Pings über das Perimeternetzwerk.

Scanmethode	Funktionsweise	Nutzen
TCP Connect oder Three-Way Handshake	Verwendet das standardmäßige Three-Way Handshake-Verfahren, um eine Verbindung mit einem überwachenden TCP-Port zu überprüfen.	Sehr nützlich, wenn Sie TCP-filternde Sicherheits-vorrichtungen wie Firewalls oder einen Router mit Paketfilterung umgehen möchten.
TCP Spoofed Connection Request (SYN)	Verwendet die ersten beiden Schritte des Three-Way-Handshake-Verfahrens. Das scannende System sendet als letzten Schritt ein Paket mit dem Flag RST (Reset) statt einer Statusbestätigung (ACK), so dass keine vollständige Verbindung hergestellt wird.	Die Wahrscheinlichkeit einer Entdeckung oder Filterung durch Sicherheitsvorrichtungen ist gering, da keine Verbindung hergestellt wird. Etwas langsamer als ein TCP Connect-Scan.
TCP Finish (FIN)	Alle Flags außer dem Flag FIN werden deaktiviert. Wenn Pakete dieses Typs von überwachenden Ports empfangen werden, wird normalerweise keine Antwort gesendet. Ein nicht überwachender Port sendet normalerweise ein RST-Paket. Ports, die nicht antworten, sind überwachende Ports.	Kann Systeme oder Sicherheitsvorrichtungen umgehen, die auf reine SYN-Pakete scannen, wie beim TCP SYN-Scan. Die Ergebnisse von Windows-basierten Systemen sind möglicherweise nicht genau, daher ist es schwieriger, offene Ports in solchen Systemen zu ermitteln.
Fragmentiertes Paket	TCP-Pakete werden in Fragmente zerlegt, die am Ziel wieder zusammengesetzt werden. Dabei wird eine der oben aufgeführten Scantechniken verwendet.	Bei einigen Sicherheitsvorrichtungen, einschließlich der Systeme zur Erkennung von Eindringversuchen, kann es schwierig sein, diese Paketströme wieder zusammenzusetzen. Manchmal können Filtervorrichtungen umgangen oder deren Absturz verursacht werden. Kann zu einer erheblichen Arbeitslast für diese Vorrichtungen führen.
Ident-Abruf	Eine Ident-Anforderung wird gesendet, nachdem eine TCP-Verbindung (Three-Way Handshake) hergestellt wurde, um zu ermitteln, welches Konto dem überwachenden Port zugeordnet ist.	Mit diesem Scantyp werden keine überwachenden Ports identifiziert, sondern Konten und die dazugehörigen Dienste. Microsoft-Betriebssysteme stellen diese Informationen nicht zur Verfügung.

Scanmethode	Funktionsweise	Nutzen
FTP-Proxyscan (File Transfer Protocol)	Zum ursprünglichen RFC für FTP gehörte ein Proxydienst, mit dem Benutzer eine Verbindung zu einem FTP-Server herstellen und bei diesem FTP-Server eine Dateiübertragung zu einem anderen System anfordern konnten. Ein FTP-Proxyscan nutzt diese Schwachstellen bei Verbindungsanforderungen mit anderen Systemen über Proxyports.	Kann beim Scannen von Systemen, die durch einen Firewall geschützt sind, nützlich sein. Die Entdeckung eines Systems, bei dem dies möglich ist, stellt selbst eine Schwachstelle dar, da der Datenverkehr an Standorte weitergeleitet wird, die laut Sicherheitsrichtlinie oder Sicherheitsvorrichtung nicht zulässig sind.
UDP	UDP ist ein verbindungsloses Protokoll, d. h., das sendende System erwartet keine Antwort vom Zielsystem. Ein System, das einen UDP-Scan durchführt, erhält nur Antworten von nicht überwachenden Ports.	Aufgrund der fehlenden Verbindungen werden UDP-Ports von Sicherheits-vorrichtungen häufig nicht oder nur beschränkt gefiltert. Häufig sind UDP-Dienste, wie DNS und SNMP (Simple Network Management Protocol), nicht sicher implementiert und können Sicherheits-perimeternetzwerke durchlaufen. Bei langsamen Verbindungen oder Verbindungen mit hohen Paketverlusten werden fälschlicherweise alle Ports als offen angezeigt.
Erkennung des Betriebssystems	Die Erkennung des Betriebssystems kann auf verschiedene Arten erfolgen. Häufig ist es aber am genauesten, die TCP-Antworten des Geräts mit einer Liste bekannter Systemtypen zu vergleichen. Zu den Komponenten, die zur Ermittlung von Hostinformationen verwendet werden, zählen TTL, TCP-Sequenznummern, Fragmentierung, FIN- und ACK-Antworten, Antworten mit nicht definierten Flags, Fenstergrößen, ICMP-Antworten und mehrere TCP-Optionen.	Häufig können mit einem Scan zur Erkennung des Betriebssystems viele Filtervorrichtungen umgangen werden. Eine Ausnahme bilden dabei Proxyfirewalls, da eigentlich der Firewall die Antworten sendet. Es kann mehr als ein Betriebssystemtyp zurückgegeben werden, und die Ergebnisse können ungenau sein. Firewalls oder Router verhindern häufig ICMP-basierte Scans zur Erkennung des Betriebssystems.

Da Angreifer diese Scanmethoden einsetzen, sollten Sie die Schwachstellen kennen, die damit aufgedeckt werden könnten. Daher ist es nützlich, in Ihrer Umgebung streng kontrolliertes Scannen zu unterstützen.

Um das Netzwerk vor dem Scannen zu schützen, sollten Sie zumindest Folgendes durchführen:

- Identifizieren der erforderlichen Ports; alle Mitglieder der Sicherheitskommission sollten das Öffnen weiterer Ports vorher besprechen.
- Implementieren eines Systems zur Erkennung von Eindringversuchen für das Netzwerk.
- Beenden aller nicht erforderlichen Dienste in dem System. Informationen zu den Diensten, die für die fünf Windows 2000-Serverrollen beendet werden, finden Sie in Kapitel 4, "Sichern von Servern basierend auf ihrer Rolle".
- Anwenden aller aktuellen Systempatches. Informationen dazu, wie Sie im Hinblick auf Systempatches auf dem aktuellen Stand bleiben, finden Sie in Kapitel 5, "Patchverwaltung".

Ausnutzung technischer Schwachstellen

Angreifer werden versuchen, technische Schwachstellen in Ihrer Umgebung auszunutzen, um Zugriff auf die Systeme zu erhalten und ihre Berechtigungen auszuweiten. Dazu können eine Reihe von Methoden verwendet werden. In diesem Abschnitt werden einige der wichtigsten Methoden aufgeführt und wie Sie sich davor schützen können.

Sitzungsübernahme

Tools zur Sitzungsübernahme (Session Hijacking) ermöglichen einem Angreifer, eine laufende Sitzung zu unterbrechen, zu beenden oder unbemerkt zu übernehmen. Angriffe dieser Art richten sich vornehmlich gegen sitzungsbasierte Anwendungen. Viele Tools zur Sitzungsübernahme können mehrere Sitzungen zugleich beobachten. Die beste Lösung zum Schutz der Architektur vor Sitzungsübernahmen ist Verschlüsselung.

Vorkehrungen gegen DNS Poisoning

DNS-Server sind ein wichtiger Bestandteil aller Windows 2000-basierten Netzwerke. Die DNS-Server werden von allen Netzwerkclients nach Servern abgefragt, mit denen sie kommunizieren müssen. Für Angriffe auf DNS-Server kann ein Angreifer DNS Poisoning verwenden. Beispielsweise kann ein Angreifer mithilfe verschiedener Techniken die Cachedatei des DNS-Servers mit falschen Daten überschreiben. Wenn ein Benutzer dann den DNS-Produktionsserver abfragen will, wird er zu einem gefälschten DNS-Server weitergeleitet, den der Angreifer kontrolliert und zur Schädigung des Systems verwenden kann. Zur Abwehr von Angriffen gegen den DNS-Server können folgende Verfahren verwendet werden:

- Verwenden anderer DNS-Server zur Auflösung von Anforderungen des internen Netzwerks, die keinerlei Abfragen von außenstehenden Computern beantworten. Dieses Konzept wird als "Split-DNS" bezeichnet.
- Verwenden eines schreibgeschützten DNS-Servers, der keine Aktualisierungen zulässt.
- Sichern der DNS-Datenbank mithilfe von Active Directory-Sicherheit und ausschließliches Zulassen von sicheren DNS-Aktualisierungen.
- Aktivieren der Option zum Schutz vor DNS Poisoning in den erweiterten Einstellungen der Windows 2000-DNS-Konfiguration.

URL-Zeichenfolgeangriffe

In jüngster Zeit konzentrieren Angreifer ihre Bemühungen auf Angriffe, die Port 80 durchlaufen. Eine Form dieses Angriffstyps arbeitet mit einer URL-Zeichenfolge, welche die UTF-8-Codeversion (Unicode Translation Format-8) des umgekehrten oder normalen Schrägstrichs (**** bzw. **/**) verwendet; eine solche Zeichenfolge wäre beispielsweise **%c0%af**. Bei Angriffen dieser Art kann der Angreifer die Verzeichnisstruktur des Remotesystems durchlaufen und dabei wichtige Informationen zum Server oder Netzwerk gewinnen oder sogar ein Programm remote ausführen.

Beispielsweise verwendet der Nimda-Wurm eine UTF-codierte URL-Zeichenfolge, um eine TFTP-Sitzung (Trivial File Transfer Protocol) auf dem Remoteserver zu starten und seine Nutzlast auf den betroffenen Computer zu downloaden. Der Wurm installiert danach seinen eigenen TFTP-Server, downloadet den Rest der Nutzlast und beginnt dann, sich selbst auf unterschiedliche Weise zu replizieren, indem er beispielsweise Massen-E-Mails versendet, eine EML-Datei in eine Website einbettet und offene Netzwerkfreigaben angreift.

Der erste Schritt bei der Anwendung einer Strategie der umfassenden Verteidigung gegen einen URL-Zeichenfolgeangriff besteht darin, so viel wie möglich über den Angriff in Erfahrung zu bringen und sicherzustellen, dass das System mit den aktuellen Sicherheitspatches versehen wurde. Weitere Informationen dazu, wie Sie im Hinblick auf Patches auf dem aktuellen Stand bleiben, finden Sie in Kapitel 5, "Patchverwaltung".

Weitere Informationen zum Nimda-Wurm und speziellen Schutzmaßnahmen finden Sie auf der TechNet-Website. (Im Abschnitt "Weitere Informationen" am Ende dieses Kapitels finden Sie Einzelheiten dazu.)

Angriffe auf die SAM-Datei

Durch Angriffe auf die SAM-Datei (Security Accounts Manager oder Sicherheitskontenverwaltung) können Angreifer Zugriff auf Benutzernamen und Kennwörter erhalten. Sobald ein Angreifer Zugriff auf diese Informationen hat, kann er scheinbar rechtmäßig auf Ressourcen in Ihrem Netzwerk zugreifen. Das Verwalten der SAM-Datei ist also ein weiterer wichtiger Schritt zur Vorbeugung von Angriffen. Dazu können Sie die folgenden Methoden einsetzen:

- Verwenden von Systemschlüsseln (System Key oder Syskey), um eine zusätzliche Verschlüsselung der SAM-Datei zu ermöglichen.
- Deaktivieren der LAN Manager-Authentifizierung (Local Area Network oder lokales Netzwerk) und Speicherung von LAN Manager-Hashwerten durch eine Richtlinie und Verwenden anderer Authentifizierungsformen (z. B. Zertifikate und biometrische Kontrollen).
- Festlegen und Erzwingen einer Richtlinie für komplexe Kennwörter.

Pufferüberlauf

Pufferüberläufe stellen eine sehr gefährliche Methode dar, die von Angreifern dazu genutzt wird, sich Zugriff auf ein System zu verschaffen. Angreifer versuchen, Container mit einem Übermaß an Daten zu überlasten, um durch den Pufferüberlauf Vorteile zu gewinnen. Wenn beispielsweise das angegriffene Programm kein ordnungsgemäßes Bounds Checking vornimmt, verursacht dies einen Überlauf und ermöglicht dem Angreifer, beliebige Funktionen auszuführen. Häufig werden diese Überläufe im Kontext der lokalen Systemkonten ausgeführt, die über volle Administratorrechte verfügen.

Viele Überlaufangriffe sind gut dokumentiert und lassen sich mühelos aus dem Web downloaden. Bei dieser Art von Angriffen handelt es sich meistens um stackbasierte Pufferüberlaufangriffe. Der Überlauf überschreibt den gesamten Stack einschließlich der Zeiger. Dies nutzt der Angreifer aus, indem er genau die Datenmenge abstimmt,

die in den Überlauf gelangt. Dann sendet der Angreifer computerspezifischen Code zum Ausführen eines Befehls sowie eine neue Adresse für den rückweisenden Zeiger. Anschließend verwendet der Angreifer die zum Stack zurückweisende Adresse, um bei der Rückkehr des Systems zum Stack die Programmanweisungen auszuführen.

Um Pufferüberlaufangriffe zu steuern, müssen Sie folgende Aufgaben erledigen:

- Die Systeme mit den aktuellen Service Packs, Hotfixes und Patches auf dem neuesten Stand halten. Die optimale Vorgehensweise dazu finden Sie in Kapitel 5, "Patchverwaltung".
- Gute Codiermethoden implementieren und die Standardrichtlinien für Bounds Checking befolgen. Es gibt eine Reihe von Ressourcen zu diesem Thema, beispielsweise *Writing Secure Code* (englischsprachig) von Michael Howard und David LeBlanc (Microsoft Press, ISBN: 0-7356-1588-8).

Denial-of-Service-Angriffe

Ein Angreifer muss nicht unbedingt auf ein System zugreifen, um beträchtliche Probleme zu verursachen. Bei Denial-of-Service-Angriffen (DoS) werden die Ressourcen eines Systems so weit überlastet, dass sie ihre normalen Funktionen nicht mehr ausführen können. Beispiele für DoS-Angriffe sind die gleichzeitige Nutzung aller Netzwerkverbindungen eines Servers oder die Überlastung eines Mailservers durch das Senden einer größeren Menge von E-Mail-Nachrichten als dieser verarbeiten kann. DoS-Angriffe können direkte Angriffe sein oder durch Würmer, Viren oder Trojanische Pferde verursacht werden.

Bei Distributed Denial-of-Service-Angriffen (DDoS) werden vor dem Angriff Programme, so genannte Zombies, auf verschiedenen Computern installiert. An diese Zombies wird ein Befehl gesendet, mit dem der Angriff für den Angreifer gestartet wird. Auf diese Weise kann der Angriff nicht zum Angreifer zurückverfolgt werden. Die Zombies werden meist mithilfe von Würmern installiert.

Die eigentliche Gefahr bei DDoS-Angriffen liegt darin, dass der Angreifer viele angegriffene Computer als Hostrechner zur Steuerung der Zombies verwendet, die den Angriff initiieren. Wenn das angegriffene System versucht, den Angriff zurückzuschlagen, erhält es nur eine Reihe von gefälschten Adressen, die von den verschiedenen Zombies generiert wurden.

Mithilfe der folgenden Abwehrmaßnahmen können Sie diese Art von Angriffen verhindern:

- Halten Sie die Systeme stets mit den aktuellen Sicherheitspatches auf dem neuesten Stand. Die optimale Vorgehensweise dazu finden Sie in Kapitel 5, "Patchverwaltung".
- Blockieren Sie große Ping-Pakete am Router und am Firewall, um zu verhindern, dass sie das Perimeternetzwerk erreichen.
- Wenden Sie am Router Anti-Spoof-Filter an, d. h., sperren Sie alle Pakete mit Ursprungsadressen, die mit Adressen innerhalb des internen Netzwerks identisch sind.
- Filtern Sie ICMP-Meldungen am Firewall und am Router (dies kann jedoch bestimmte Verwaltungstools beeinträchtigen).
- Entwickeln Sie zusammen mit dem Internetdienstanbieter (ISP oder Internet Service Provider) einen Verteidigungsplan, der eine rasche Reaktion auf Angriffe ermöglicht, welche die Bandbreite zwischen dem ISP und Ihrem Perimeternetzwerk beeinträchtigen sollen.
- Deaktivieren Sie das Antworten auf geroutete Broadcasts (Directed Broadcasts).

Wenden Sie geeignete Router- und Firewallfilter an.

Lassen Sie ein IDS-System nach auffälligem Datenverkehr suchen und gegebenenfalls eine Warnung generieren. Konfigurieren Sie IDS so, dass im Fall von ICMP_ECHOREPLY ohne zugehörige ICMP_ECHO-Pakete eine Warnung generiert wird.

DoS und DDoS sind heute die häufigsten Arten von Angriffen im Internet. Wöchentlich werden weitere DoS-Angriffe dokumentiert und zu Problemverfolgungsdatenbanken hinzugefügt. Sie sollten sicherstellen, dass Sie immer über die aktuellsten Informationen zu diesen Angriffen und zu geeigneten Schutzmaßnahmen verfügen.

Backdoorangriffe

Um zu verhindern, dass Angreifer Systeminformationen downloaden, müssen Sie Vorkehrungen gegen die Installation eines Backdoorprogramms durch ein Trojanisches Pferd im System treffen. Dies ist eher auf dem Client ein Problem als auf einem vollständig gesicherten Server. Jedoch kann ein Angreifer mithilfe eines solchen Mechanismus die Arbeitsstation eines Benutzers oder des Administrators angreifen und dann dieses System als Ausgangsbasis für Angriffe auf das Produktionsperimeternetzwerk verwenden.

Back Orifice 2000 beispielsweise ist ein Backdoorprogramm, das es Angreifern ermöglicht, einen Computer über ein Netzwerk zu steuern, die dort ausgeführten Tastaturanschläge zu speichern und sich dann mithilfe dieser Informationen als Benutzer einer Arbeitsstation im Netzwerk auszugeben. Viele Antivirenprogramme erkennen Back Orifice; neue Versionen von Back Orifice können jedoch verschiedenartige Mutationen erstellen, die von den Antivirenprogrammen nicht entdeckt werden. Zudem wird Back Orifice im Stealth-Modus ausgeführt und nicht in der Taskliste angezeigt, da sein Speicherbedarf unter 100 Kilobyte (KB) liegt. Back Orifice ist nur eines von vielen Backdoorprogrammen. Mit folgenden Maßnahmen können Sie dazu beitragen, derartige Angriffe zu verhindern:

Ausführen eines kompletten Virenscans und regelmäßiges Aktualisieren des Antivirenprogramms mit den neuesten Signaturen.

Vorsicht bei allen Inhalten von E-Mail-Nachrichten und Einschränken der Ausführung von unbekannten Dateianlagen.

Ausführen von Tools wie beispielsweise ISS-Scanner (Internet Security Systems), um das gesamte Netzwerk auf das Vorhandensein von Angreifertools wie Back Orifice zu scannen. Dabei ist darauf zu achten, dass die Scannerdatenbank stets auf dem neuesten Stand ist.

Zurückweisen von nicht signierten Microsoft ActiveX®-Steuerelementen.

Weiterbilden der Benutzer hinsichtlich der Gefahren des Installierens unbekannter Programme, des Öffnens ungewöhnlicher Dateianlagen und des Downloadens unsignierter oder unbekannter Internetinhalte.

Schädlicher Code

Jedes ausführbare Programm stellt für eine Organisation ein potenzielles Risiko dar. Schädlicher Code kann in der Form eines Codes vorliegen, der Schaden anrichtet und sich zwischen Organisationen verbreitet (z. B. über E-Mail-Nachrichten). Er kann aber auch absichtlich innerhalb einer Organisation ausgeführt werden.

Es gibt im Wesentlichen die folgenden vier Arten von schädlichem Code:

Viren

Würmer

Trojanische Pferde

Sonstiger schädlicher Code

Tabelle 2.7: Arten von schädlichem Code

Typ	Beschreibung
Virus	Befällt andere Programme, Startsektoren, Partitionssektoren oder Dateien, die Makros unterstützen, indem sich der Virus selbst in das Medium einfügt oder an das Medium anfügt. Dann wird der Virus von dort auf andere Computer repliziert. Manche Viren werden nur repliziert, viele richten aber auch in den befallenen Systemen Schaden an.
Wurm	Kopiert sich selbst mithilfe einer E-Mail oder eines anderen Übertragungsmediums von einem Datenträger auf einen anderen oder im gesamten Netzwerk. Um sich auszubreiten, muss der Wurm auf dem Computer, auf dem er sich befindet, keine Änderungen vornehmen. Ein Wurm kann Schaden anrichten oder die Sicherheit des Computers gefährden.
Trojanisches Pferd	Repliziert sich nicht selbst. Die schädlichen Funktionen sind in anderen Programmen verborgen, die nützlich zu sein scheinen und daher weitergegeben werden (häufig als "Unterhaltungsprogramm"). Sobald sich das Trojanische Pferd in einem System befindet, wird es Schaden anrichten oder die Sicherheit des Computers verletzen. Dies kann der erste Schritt für einen unberechtigten Zugriff sein.
Sonstiger schädlicher Code	Ausführbarer Code, der absichtlich oder versehentlich Schaden in der Umgebung anrichtet. Ein Beispiel ist eine Batchdatei, die Schleifen ausführt. Bei jeder dieser Schleifen werden Systemressourcen verbraucht, bis der Computer schließlich nicht mehr normal funktionsfähig ist.

Antivirenprogramme können die Ausführung eines Großteils des schädlichen Codes verhindern, aber nicht des gesamten. Wenn Sie den Zugriff auf CD-ROM-Laufwerke, Diskettenlaufwerke und andere E/A-Geräte verhindern, können Sie den Schutz vor diesem Code verbessern. Diese Möglichkeit bietet allerdings keinen Schutz vor Code, der auf internen Systemen geschrieben wird. Code kann auch per E-Mail an einen Mitarbeiter in der Organisation gesendet werden. Auch wenn die Art der Anlage nicht zulässig ist, kann die Dateierweiterung geändert werden, um das Problem zu umgehen und den Code in die Organisation zu senden. Anschließend kann zur Ausführung des Codes die Dateierweiterung wieder zurückgeändert werden.

Das Schützen der wichtigsten System- und Datendateien vor unberechtigtem Zugriff ist ein wichtiger Bestandteil der Schutzmaßnahmen gegen schädlichen Code. Sie müssen außerdem Active Directory und Active Directory-Komponenten schützen.

Zusammenfassung

In diesem Kapitel wurden die schwerwiegendsten Bedrohungen für Ihre Umgebung und einige Maßnahmen zum Schutz vor diesen Bedrohungen aufgezeigt. In den folgenden Kapiteln erhalten Sie ausführlichere Informationen zum Schutz des Systems vor Angriffen, zum Erkennen von Angriffen und zu den geeigneten Gegenmaßnahmen.

Weitere Informationen

Writing Secure Code (englischsprachig) von Michael Howard und David LeBlanc (Microsoft Press; ISBN: 0-7356-1588-8):

http://mspress.microsoft.de/mspress/product.asp?sku=0-7356-1588-8

Informationen zum Nimda-Wurm und zu geeigneten Schutzmaßnahmen:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/nimda.asp (englischsprachig)

Request for Comments (RFCs) stehen unter folgender Adresse zur Verfügung:

http://www.rfc-editor.org/ (englischsprachig)

Originaltitel: Chapter 3 – Managing Security with Windows 2000 Group Policy

3

Verwalten von Sicherheit mit Windows 2000-Gruppenrichtlinien

Nachdem Sie den für Ihre Umgebung wahrscheinlichen Umfang an Risiken ermittelt und eine Richtlinie für die gesamte Sicherheit festgelegt haben, sollten Sie jetzt mit dem Sichern der Umgebung beginnen. In einer Windows 2000-basierten Umgebung werden dazu vorwiegend Gruppenrichtlinien verwendet.

In diesem Kapitel wird gezeigt, wie Gruppenrichtlinienobjekte (Group Policy Objects oder GPOs) durch Sicherheitsvorlagen eingerichtet werden, mit denen die Sicherheitseinstellungen in der Windows 2000-basierten Umgebung definiert werden. Außerdem wird eine einfache Struktur von Organisationseinheiten (OEs) erläutert, die die Verwendung von Gruppenrichtlinienobjekten unterstützt.

Achtung: Bevor Sie die in diesem Kapitel erläuterten Sicherheitsvorlagen in einer Produktionsumgebung implementieren, müssen Sie die Sicherheitsvorlagen erst in einer Testumgebung gründlich testen. So können Sie sicherstellen, dass die Server weiterhin wie erwartet funktionieren.

Die Bedeutung von Gruppenrichtlinien

Mithilfe von Sicherheitsrichtlinien sollen die Verfahren zum Konfigurieren und Verwalten der Sicherheit in einer Umgebung definiert werden. Mithilfe von Windows 2000-Gruppenrichtlinien können technische Anforderungen Ihrer Sicherheitsrichtlinie für alle Arbeitsstationen und Server in den Active Directory-Domänen umgesetzt werden. Sie können Gruppenrichtlinien zusammen mit der Struktur Ihrer Organisationseinheiten verwenden, um bestimmte Sicherheitseinstellungen für bestimmte Serverrollen zu definieren.

Wenn Sie Gruppenrichtlinien zum Implementieren von Sicherheitseinstellungen verwenden, können Sie sicherstellen, dass alle an der Richtlinie vorgenommenen Änderungen auf alle Server angewendet werden, die diese Richtlinie verwenden, und dass neue Server automatisch die neuen Einstellungen erhalten.

Anwenden von Gruppenrichtlinien

Um Gruppenrichtlinien sicher und effizient zu verwenden, müssen Sie wissen, wie diese angewendet werden. Ein Benutzer- oder Computerobjekt kann mehreren Gruppenrichtlinienobjekten zugeordnet werden. Diese Gruppenrichtlinienobjekte werden nacheinander angewendet und die Einstellungen akkumuliert. Wenn es dabei zu Konflikten kommt, werden standardmäßig ältere Einstellungen durch neuere außer Kraft gesetzt.

Die erste Richtlinie, die angewendet wird, ist das lokale Gruppenrichtlinienobjekt. Auf jedem Computer unter Windows 2000 ist ein lokales Gruppenrichtlinienobjekt gespeichert. Standardmäßig werden nur die Knoten unter **Sicherheitseinstellungen** konfiguriert. Einstellungen in anderen Teilen des lokalen Gruppenrichtlinienobjekts werden weder aktiviert noch deaktiviert. Das lokale Gruppenrichtlinienobjekt wird auf jedem Server in **%systemroot%\System32\GroupPolicy** gespeichert.

Nach dem lokalen Gruppenrichtlinienobjekt werden nachfolgende Gruppenrichtlinienobjekte auf den Standort, die Domäne, die übergeordnete Organisationseinheit und schließlich auf die untergeordnete Organisationseinheit angewendet. In der folgenden Abbildung ist dargestellt, wie die einzelnen Richtlinien angewendet werden:

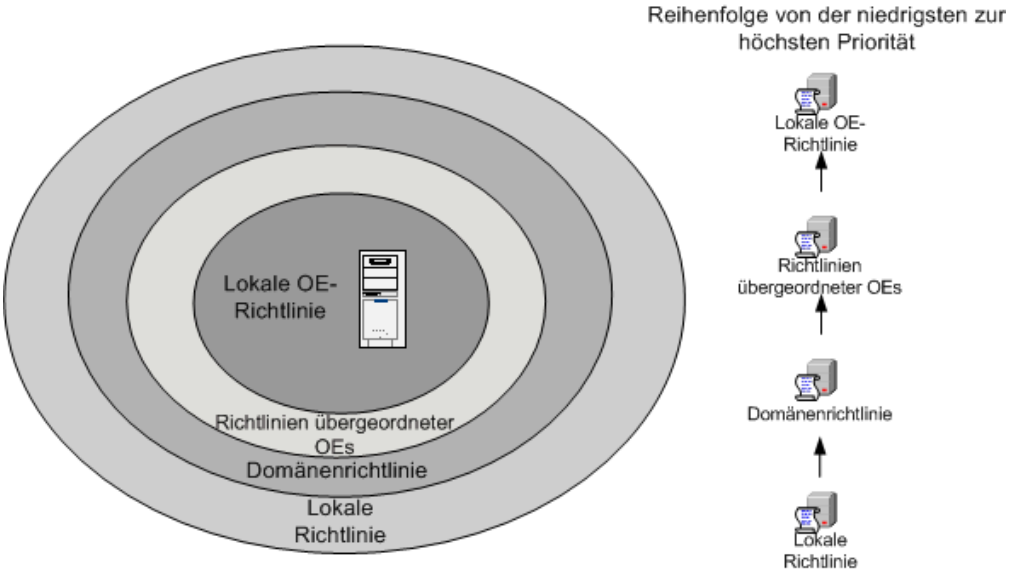


Abbildung 3.1: Hierarchie der Anwendung von Gruppenrichtlinienobjekten

Auf jeder Ebene, auf der mehrere Gruppenrichtlinienobjekte definiert sind, legt ein Administrator die Reihenfolge fest, in der die Gruppenrichtlinienobjekte angewendet werden.

Die in einer Gruppenrichtlinie definierten Einstellungen werden auf einen Benutzer oder Computer angewendet, wenn a) die Gruppenrichtlinie auf den entsprechenden Container angewendet wird und b) er in der Zugriffssteuerungsliste (DACL oder Discretionary Access Control List) für das Gruppenrichtlinienobjekt mindestens mit der Berechtigung **Gruppenrichtlinie übernehmen** enthalten ist.

Anmerkung: Standardmäßig hat die integrierte Gruppe **Authentifizierte Benutzer** die Berechtigung **Gruppenrichtlinie übernehmen**. In dieser Gruppe sind alle Benutzer und Computer der Domäne enthalten.

Sicherstellen der Anwendung von Gruppenrichtlinien

Gruppenrichtlinieneinstellungen befinden sich (teilweise) in Active Directory. Das bedeutet, dass Änderungen an der Gruppenrichtlinie nicht sofort angewendet werden. Domänencontroller müssen zuerst die Änderungen an der Gruppenrichtlinie auf andere Domänencontroller replizieren. Dies kann innerhalb eines Standorts bis zu 15 Minuten dauern. Bei Replikationen mit anderen Standorten kann es erheblich länger dauern. Nachdem die Änderungen repliziert wurden, dauert es wieder eine Weile (fünf Minuten bei Domänencontrollern und 90 Minuten plus oder minus einer Abweichung von 30 Minuten bei anderen Computern), bis die Änderungen der Richtlinie auf dem Zielcomputer aktualisiert wurden.

Bei Bedarf können Sie erzwingen, dass beide Aktionen sofort durchgeführt werden.

▶ **So erzwingen Sie die Replikation des Domänencontrollers**

1. Öffnen Sie **Active Directory-Standorte und -Dienste**, erweitern Sie **Standorte**, erweitern Sie dann **<Standortname>**, und erweitern Sie anschließend **Server**.
2. Erweitern Sie **<Name des 1. Domänencontrollers>** und **<Name des 2. Domänencontrollers>**, und wählen Sie dann für jeden Server **NTDS-Einstellungen** aus.
3. Klicken Sie im rechten Bereich mit der rechten Maustaste auf den Verbindungsobjektnamen, und wählen Sie **Jetzt replizieren** aus. Dadurch wird die sofortige Replikation zwischen den Domänencontrollern erzwungen.
4. Wiederholen Sie die Schritte 2 und 3 für alle Domänencontroller.

▶ **So aktualisieren Sie die Richtlinie manuell auf einem Server**

Geben Sie an der Eingabeaufforderung des Servers **Secedit /refreshpolicy machine_policy /enforce** ein. Mit diesem Befehl wird der Server aufgefordert, Active Directory auf Aktualisierungen der Richtlinie zu überprüfen und diese ggf. sofort zu downloaden.

▶ **So überprüfen Sie die effektiven Richtlinieneinstellungen**

1. Starten Sie **Lokale Sicherheitsrichtlinie**.
2. Klicken Sie unter **Sicherheitseinstellungen** auf **Lokale Richtlinien**, und klicken Sie dann auf **Sicherheitsoptionen**.
3. Sehen Sie sich im rechten Bereich die Spalte **Effektive Einstellung** an, um zu überprüfen, ob die richtigen Sicherheitseinstellungen angewendet wurden.

Anmerkung: Da Sie Sicherheitseinstellungen mithilfe von Gruppenrichtlinien anwenden werden, ist es sehr wichtig, dass Sie deren Eigenschaften und Interaktionen genau kennen. Das englischsprachige Microsoft-Whitepaper "Windows 2000 Group Policy" enthält ausführlichere Informationen zur Bereitstellung von Gruppenrichtlinien. Weitere Informationen finden Sie im gleichnamigen Abschnitt am Ende dieses Kapitels.

Struktur der Gruppenrichtlinien

Konfigurationseinstellungen für Gruppenrichtlinien werden an zwei Orten gespeichert:

Gruppenrichtlinienobjekte befinden sich in Active Directory.

Sicherheitsvorlagendateien befinden sich im lokalen Dateisystem.

Änderungen des Gruppenrichtlinienobjekts werden direkt in Active Directory gespeichert. Änderungen an den Sicherheitsvorlagendateien müssen anschließend wieder in das Gruppenrichtlinienobjekt in Active Directory importiert werden, bevor sie angewendet werden können.

Anmerkung: In diesem Betriebshandbuch finden Sie Vorlagen, mit denen Sie Ihre Gruppenrichtlinienobjekte ändern können. Wenn Sie Änderungen vornehmen und die Gruppenrichtlinienobjekte direkt ändern, stimmen diese nicht mehr mit den Vorlagendateien überein. Sie sollten also die Vorlagendateien ändern und wieder in das Gruppenrichtlinienobjekt importieren.

Im Lieferumfang von Windows 2000 sind eine Reihe von Sicherheitsvorlagen enthalten. Die folgenden Vorlagen können in einer Umgebung mit niedriger Sicherheit angewendet werden.

- **Basicwk.inf** – für Windows 2000 Professional
- **Basicsv.inf** – für Windows 2000 Server
- **Basicdc.inf** – für Windows 2000-basierte Domänencontroller

Für eine höhere Sicherheit auf Windows 2000-basierten Computern stehen weitere Vorlagen zur Verfügung. Diese enthalten weitere Sicherheitseinstellungen, zusätzlich zu denen aus den Basisvorlagen:

- **Securedc.inf** und **Hisecdc.inf** – für Domänencontroller
- **Securews.inf** und **Hisecws.inf** – für Mitgliedsserver und Arbeitsstationen

Diese Vorlagen werden als inkrementelle Vorlagen bezeichnet, da vor ihrem Einsatz zunächst die Basisvorlagen übernommen werden müssen. Für dieses Handbuch wurden auf der Grundlage von **Hisecdc.inf** und **Hisecws.inf** neue Sicherheitsvorlagen erstellt. Ziel ist die Erstellung einer sehr restriktiven Umgebung, die dann selektiv weiter geöffnet werden kann, um die erforderlichen Funktionalitäten sicherzustellen. Die Wahrung der Sicherheit bleibt dabei von größter Bedeutung.

Anmerkung: Die standardmäßigen Windows 2000-Sicherheitsvorlagen sind als INF-Dateien im Ordner **%SystemRoot%\Security\Templates** gespeichert.

Format der Sicherheitsvorlagen

Vorlagendateien sind textbasierte Dateien. Änderungen an den Vorlagendateien können über das MMC-Snap-In Sicherheitsvorlagen oder mithilfe eines Texteditors wie Editor vorgenommen werden. In der folgenden Tabelle ist dargestellt, welche Abschnitte der Richtlinie welchen Abschnitten der Vorlagendateien zugeordnet sind.

Tabelle 3.1: Abschnitte der Sicherheitsvorlage und die entsprechenden Abschnitte der Gruppenrichtlinie

Abschnitt der Richtlinie	Abschnitt der Vorlage
Kontorichtlinie	[System Access]
Überwachungsrichtlinie	[System Log] [Security Log] [Application Log]
Benutzerrechte	[Privilege Rights]
Sicherheitsoptionen	[Registry Values]
Ereignisprotokoll	[Event Audit]
Eingeschränkte Gruppen	[Group Membership]
Systemdienste	[Service General Setting]
Registrierung	[Registry Keys]
Dateisystem	[File Security]

Einige Abschnitte in der Sicherheitsvorlagendatei, wie [File Security] und [Registry Keys], enthalten spezielle Zugriffssteuerungslisten (ACLs oder Access Control Lists). Diese Zugriffssteuerungslisten sind Zeichenfolgen, die mithilfe von SDDL (Security Descriptor Definition Language) definiert wurden.
Informationen zum Bearbeiten von Sicherheitsvorlagen mit SDDL finden Sie auf der MSDN-Website.
Weitere Informationen finden Sie außerdem im gleichnamigen Abschnitt am Ende dieses Kapitels.

Testumgebung

Es ist wichtig, dass Sie alle Änderungen der Sicherheit Ihrer IT-Systeme in einer Testumgebung beurteilen, bevor Sie sie an der Produktionsumgebung vornehmen. Die Testumgebung sollte die Produktionsumgebung möglichst genau nachbilden. Zumindest sollten zur Testumgebung mehrere Domänencontroller und alle Mitgliedsserverrollen gehören, die auch in der Produktionsumgebung vorhanden sind.

Das Testen ist notwendig, um festzustellen, ob die Umgebung auch nach den Änderungen noch funktionsfähig ist. Das Testen ist außerdem wichtig, um sicherzustellen, dass sie den Sicherheitsgrad wie beabsichtigt erhöht haben. Sie sollten alle Änderungen sorgfältig überprüfen und eine Schwachstellenanalyse (Vulnerability Assessment) in der Testumgebung durchführen.

Anmerkung: Bevor eine Schwachstellenanalyse in der Organisation durchgeführt wird, sollten die dafür zuständigen Personen über eine entsprechende schriftliche Genehmigung verfügen.

Überprüfen der Domänenumgebung

Vor dem Implementieren von Gruppenrichtlinien in der Produktionsumgebung sollte die Domänenumgebung stabil und funktionsfähig sein. Zu den wichtigsten Bereichen in Active Directory, die überprüft werden sollten, zählen die DNS-Server, die Replikation von Domänencontrollern und die Zeitsynchronisierung. Sie sollten eine Testumgebung auch zur Unterstützung einer stabilen Produktionsumgebung verwenden.

Überprüfen der DNS-Konfiguration

Die DNS-Namensauflösung ist wichtig für die ordnungsgemäße Funktionsfähigkeit von Servern und Domänencontrollern. Wenn für eine Domäne mehrere DNS-Server implementiert wurden, sollte jeder DNS-Server getestet werden. Sie sollten die folgenden Tests durchführen:

Auf Domänencontrollern:

Führen Sie **dcdiag /v** und **netdiag /v** im ausführlichen Modus aus, um DNS auf allen Domänencontrollern zu testen, und überprüfen Sie die Ausgabe auf Fehler. DCDIAG und NETDIAG finden Sie auf der Windows 2000-Installations-CD im Verzeichnis **Supporttools**

Beenden und starten Sie den Anmeldedienst, und überprüfen Sie das Ereignisprotokoll auf Fehler. Der Anmeldedienst registriert für den Domänencontroller dynamisch Dienstaufzeichnungen (Service Records) im DNS und generiert Fehlermeldungen, wenn DNS-Eintäge nicht erfolgreich registriert werden können. Diese Dienstaufzeichnungen finden Sie in der Datei **netlogon.dns** im Verzeichnis **%SystemRoot%\System32\Config**.

Überprüfen Sie auf Mitgliedsservern mithilfe von **nslookup** oder **netdiag /v**, ob DNS ordnungsgemäß funktioniert.

Replikation von Domänencontrollern

Vor dem Implementieren von Gruppenrichtlinien muss die Replikation zwischen mehreren Domänencontrollern ordnungsgemäß funktionieren. Wenn die Replikation nicht ordnungsgemäß funktioniert, werden Änderungen an den Gruppenrichtlinien nicht auf alle Domänencontroller angewendet. Dies kann zu Inkonsistenzen zwischen Servern führen, die auf Domänencontrollern nach Aktualisierungen von Gruppenrichtlinien suchen. Die Server, die den Domänencontroller abfragen, auf dem die Änderung vorgenommen wurde, werden aktualisiert, während Server, die Domänencontroller abfragen, die noch auf die Replikation der Gruppenrichtlinie warten, nicht aktualisiert werden.

Erzwingen und Überprüfen der Replikation mithilfe von Repadmin

Repadmin ist ein Befehlszeilenprogramm, das im Verzeichnis **Support** auf der Windows 2000-CD enthalten ist. Mithilfe von Repadmin können Sie die Verzeichnisreplikationspartner des Zielservers ermitteln und dann über einen Befehl den Quellserver mit dem Zielserver synchronisieren. Dazu wird der Objekt-GUID (Globally Unique Identifier oder global eindeutiger Bezeichner) des Quellservers verwendet.

▶ **So verwenden Sie Repadmin, um die Replikation zwischen zwei Domänencontrollern zu erzwingen**

1. Geben Sie an der Eingabeaufforderung eines Domänencontrollers Folgendes ein:
   repadmin /showreps <destination_server_name>
2. Suchen Sie im Abschnitt "Inbound Neighbors" der Ausgabe nach der Verzeichnispartition, die synchronisiert werden muss, und suchen Sie nach dem Quellserver, mit dem der Zielserver synchronisiert werden soll. Notieren Sie sich den Wert des Objekt-GUIDs für den Zielserver.
3. Starten Sie die Replikation, indem Sie den folgenden Befehl eingeben:
   repadmin /sync
   <Verzeichnispartition_DN> <Zielserver_Name> <Quellserver_objectGuid>

Anmerkung: Sobald Sie den Objekt-GUID der Domänencontroller kennen, könnten Sie eine Batchdatei erstellen, die das Tool Repadmin verwendet, um die Replikation zwischen Servern zu starten und Statusinformationen zum Ergebnis der Replikation zu liefern.

Zentrale Sicherheitsvorlagen

Es ist sehr wichtig, dass für die Produktion verwendete Sicherheitsvorlagen an einem sicheren Ort gespeichert werden, auf den nur die Administratoren zugreifen können, zu deren Aufgaben das Implementieren von Gruppenrichtlinien gehört. Standardmäßig werden Sicherheitsvorlagen im Ordner **%SystemRoot%\security\templates** auf jedem Domänencontroller gespeichert. Dieser Ordner wird nicht auf anderen Domänencontrollern repliziert. Deshalb müssen Sie einen Domänencontroller auswählen, auf dem die Masterkopie der Sicherheitsvorlagen gespeichert ist, so dass bei den Vorlagen keine Probleme mit der Versionskontrolle entstehen.

Konfiguration der Systemzeit

Es ist sehr wichtig, dass die Systemzeit korrekt ist und dass alle Server dieselbe Zeitquelle verwenden. Der Windows 2000-Dienst W32Time ermöglicht die Zeitsynchronisierung von Windows 2000-basierten Computern in einer Active Directory-Domäne. Mit dem Dienst W32Time wird sichergestellt, dass die Uhren von Windows 2000-basierten Clients mit den Domänencontrollern in einer Domäne synchronisiert werden. Dies ist für die Kerberos-Authentifizierung erforderlich. Die Synchronisierung der Systemzeit hilft aber auch bei der Analyse von Ereignisprotokollen.

Der Dienst W32Time synchronisiert die Uhren mithilfe von SNTP (Simple Network Time Protocol), wie in RFC 1769 beschrieben. In einer Windows 2000-Gesamtstruktur wird die Systemzeit folgendermaßen synchronisiert:

- Der PDC-Emulator (Primary Domain Controller oder Primärer Domänencontroller) Betriebsmaster in der Stammdomäne der Gesamtstruktur ist die maßgebliche Zeitquelle für die Organisation.
- Alle PDC-Betriebsmaster in anderen Domänen der Gesamtstruktur folgen der Hierarchie von Domänen, wenn Sie einen PDC-Emulator auswählen, mit dem sie die Systemzeit synchronisieren.
- Alle Domänencontroller in einer Domäne synchronisieren ihre Systemzeit mit dem PDC-Emulator Betriebsmaster in ihrer Domäne als maßgeblichen Zeitpartner.
- Alle Mitgliedsserver und Clientdesktopcomputer verwenden den authentifizierenden Domänencontroller als maßgeblichen Zeitpartner.

Um die Genauigkeit der Systemzeit sicherzustellen, sollte der PDC-Emulator in der Stammdomäne der Gesamtstruktur mit einem externen SNTP-Zeitserver synchronisiert werden. Sie können dies konfigurieren, indem Sie den folgenden Befehl für die Netzwerkzeit ausführen, <server_liste> steht dabei für Ihre Serverliste:

```
net time /setsntp:<server_liste>
```

Anmerkung: Wenn sich der PDC-Emulator im Stamm der Gesamtstruktur hinter einem Firewall befindet, müssen Sie möglicherweise im Firewall UDP-Port 123 öffnen, damit der PDC-Emulator eine Verbindung mit einem SNTP-Zeitserver im Internet herstellen kann.

Wenn im Netzwerk ältere Windows-Betriebssysteme verwendet werden, können die Uhren auf diesen Computern mithilfe des folgenden Befehls in einem Anmeldeskript synchronisiert werden, <Zeitserver> steht dabei für einen Domänencontroller im Netzwerk:

```
net time \\<Zeitserver> /set /yes
```

Anmerkung: Auch die Uhren von Computern, auf denen keine Windows-Betriebssysteme ausgeführt werden, sollten mit externen Zeitquellen synchronisiert werden, damit protokollierte Ereignisse basierend auf der Systemzeit analysiert werden können. Weitere Informationen finden Sie im Microsoft Knowledge Base-Artikel D42387, "Konfigurieren eines Zeitservers in Windows".

Entwurf und Implementierung von Richtlinien

Um Gruppenrichtlinien effektiv einzusetzen, müssen Sie genau bestimmen, wie sie angewendet werden. Um das Anwenden und Überprüfen der Sicherheitseinstellungen von Gruppenrichtlinien zu vereinfachen, wird empfohlen, die Sicherheitseinstellungen auf zwei Ebenen anzuwenden:

Domänenebene. Für die gemeinsamen Sicherheitsanforderungen, wie Kontorichtlinien und Überwachungsrichtlinien, die für alle Server erzwungen werden müssen.

Ebene der Organisationseinheiten. Für spezielle Sicherheitsanforderungen von Servern, die nicht für alle Server im Netzwerk gelten. Beispielsweise weichen die Sicherheitsanforderungen für Infrastrukturserver von denen der Server mit IIS ab.

Gruppenrichtlinieneinstellungen, die Auswirkungen auf die Sicherheit haben, sind in mehrere Abschnitte unterteilt.

Tabelle 3.2: Abschnitte von Gruppenrichtlinien und deren Zweck

Abschnitt der Richtlinie	Beschreibung
Kontorichtlinie\Kennwortrichtlinie	Konfiguration von Kennwortalter, -länge und -komplexität
Kontorichtlinie\Kontosperrungsrichtlinie	Konfiguration der Sperrdauer, Sperrschwelle und Zurücksetzungszähler
Kontorichtlinie\Kerberos-Richtlinie	Konfiguration der Lebensdauer von Tickets
Lokale Richtlinien\Überwachungsrichtlinie	Aktivieren/deaktivieren der Aufzeichnung bestimmter Ereignisse
Lokale Richtlinien\Benutzerrechte	Definition von Rechten wie lokales Anmelden, Zugriff über das Netzwerk usw.
Lokale Richtlinien\Sicherheitsoptionen	Ändern von Registrierungswerten, die relevant für die Sicherheit sind
Ereignisprotokoll	Erfolgs- und Fehlerüberwachung aktiviert
Eingeschränkte Gruppen	Administratoren können steuern, wer zu einer bestimmten Gruppe gehört.
Systemdienste	Steuert den Startmodus für alle Dienste.
Registrierung	Konfiguration von Berechtigungen für Registrierungsschlüssel
Dateisystem	Konfiguration von Berechtigungen für Ordner, Unterordner und Dateien

Alle Computer verfügen über eine vordefinierte lokale Richtlinie. Wenn eine Active Directory-Domäne neu erstellt wird, werden außerdem Standardrichtlinien für die Domäne und die Domänencontroller erstellt. Bevor Sie eine Standardrichtlinie ändern, sollten Sie die enthaltenen Einstellungen dokumentieren, so dass Sie bei einem Problem den vorherigen Zustand problemlos wieder herstellen können.

Serverrollen

Für dieses Handbuch wurden mehrere Serverrollen definiert und Sicherheitsvorlagen erstellt, um die Sicherheit dieser Server zu erhöhen.

Tabelle 3.3: Windows 2000-Serverrollen

Serverrolle	Beschreibung	Sicherheitsvorlagen
Windows 2000-Domänencontroller	Ein Active Directory-Domänencontroller	**BaselineDC.inf**
Windows 2000-Anwendungsserver	Ein gesperrter Mitgliedsserver, auf dem ein Dienst, beispielsweise Exchange 2000, installiert werden kann. Damit der Dienst ordnungsgemäß funktioniert, muss die Sicherheit gelockert werden.	**Baseline.inf**
Windows 2000-Datei- und -Druckserver	Ein gesperrter Datei- und Druckserver	**Baseline.inf** und **File and Print Incremental.inf**
Windows 2000-Infrastrukturserver	Ein gesperrter DNS-, WINS- (Windows Internet Name Service) und DHCP-Server	**Baseline.inf** und **Infrastructure Incremental.inf**
Windows 2000-IIS-Server	Ein gesperrter IIS-Server	**Baseline.inf** und **IIS Incremental.inf**

Für diese Serverrollen gelten unterschiedliche Sicherheitsanforderungen. Die geeigneten Sicherheitseinstellungen für die einzelnen Serverrollen werden in Kapitel 4, "Sichern von Servern basierend auf ihrer Rolle", detailliert erläutert.

Anmerkung: In diesem Handbuch wird davon ausgegangen, dass Server bestimmte definierte Rollen ausführen. Wenn diese Rollen denen Ihrer Server nicht entsprechen oder wenn Sie Mehrzweckserver verwenden, sollten Sie die hier definierten Einstellungen als Leitfaden für das Erstellen eigener Sicherheitsvorlagen verwenden. Sie sollten dabei jedoch bedenken, dass ein Server mit vielen verschiedenen Rollen anfälliger für Angriffe ist.

Active Directory-Struktur zur Unterstützung der Serverrollen

Wie bereits erwähnt, können Sie Gruppenrichtlinien auf verschiedene Arten, mit mehreren Gruppenrichtlinienobjekten und auf unterschiedlichen Ebenen der Hierarchie anwenden. Für dieses Handbuch wurde eine Reihe von Gruppenrichtlinieneinstellungen definiert, mit denen Sie die verschiedenen Serverrollen sichern können. Sie müssen sicherstellen, dass die Active Directory-Struktur das Anwenden dieser Einstellungen zulässt.

Um das Sichern der Windows 2000-basierten Umgebung zu erleichtern, wurden einige Sicherheitsvorlagen vordefiniert, die Sie in die Gruppenrichtlinienobjekte importieren können. Wenn Sie diese Sicherheitsvorlagen unverändert verwenden möchten, müssen Sie sicherstellen, dass die Active Directory-Struktur entsprechend konfiguriert ist. Die in diesem Handbuch definierten Gruppenrichtlinienobjekte sind für die in der folgenden Abbildung dargestellte Struktur von Organisationseinheiten vorgesehen.

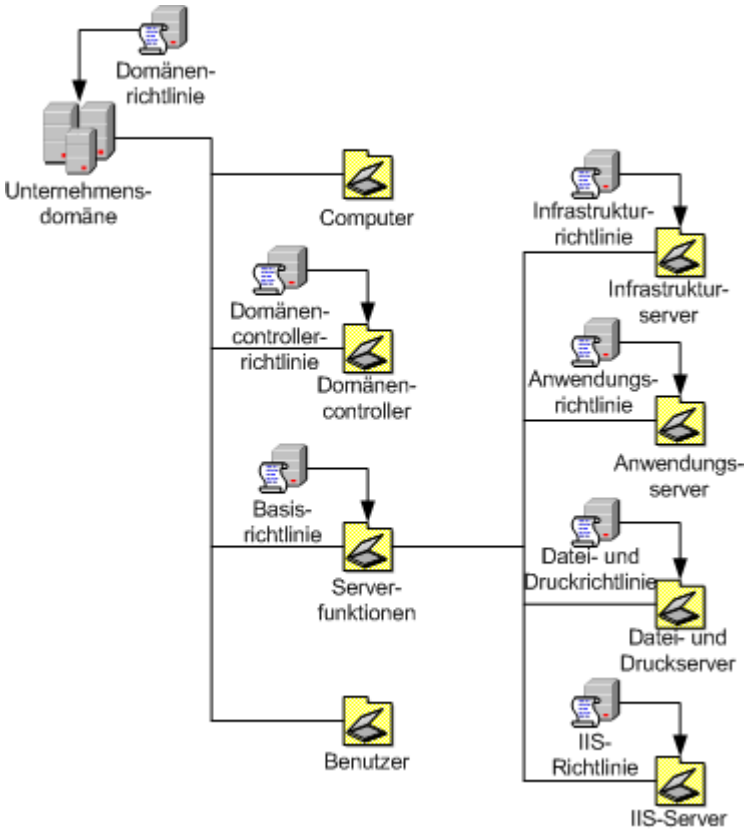


Abbildung 3.2: Struktur von Organisationseinheiten für definierte Gruppenrichtlinienobjekte

---

Anmerkung: Die Domänenstruktur ist hier ohne Bedeutung, da Gruppenrichtlinien für Domänen und Organisationseinheiten nur für die Domäne gelten, in der sie definiert werden. Die Standortstruktur ist ebenfalls ohne Bedeutung, da in diesem Handbuch keine Gruppenrichtlinienobjekte auf Standortebene definiert werden.

So erstellen Sie die Struktur von Organisationseinheiten

1. Starten Sie **Active Directory-Benutzer und –Computer**.
2. Klicken Sie mit der rechten Maustaste auf den Domänennamen, wählen Sie **Neu** aus, und wählen dann **Organisationseinheit** aus.
3. Geben Sie **Mitgliedsserver** ein, und klicken Sie dann auf **OK**.
4. Klicken Sie mit der rechten Maustaste auf **Mitgliedsserver**, wählen Sie **Neu** aus, und wählen Sie dann **Organisationseinheit** aus.
5. Geben Sie **Anwendungsserver** ein, und klicken Sie dann auf **OK**.
6. Wiederholen Sie die Schritte 5 und 6 für **Datei- und Druckserver**, **IIS-Server** und **Infrastrukturserver**.

Sie sollten sich die Struktur von Organisationseinheiten genauer ansehen.

Richtlinien auf Domänenebene

Wenn eine Windows 2000-Domäne erstellt wird, wird eine standardmäßige Domänenrichtlinie erstellt. Wenn Sie Sicherheitseinstellungen auf die gesamte Domäne anwenden möchten, haben Sie die folgenden Möglichkeiten:

- Erstellen Sie eine zusätzliche Richtlinie, und verknüpfen Sie diese oberhalb der Standardrichtlinie
- Ändern Sie die vorhandene Standardrichtlinie

Das Ändern der vorhandenen Richtlinie ist im Allgemeinen einfacher. Wenn Sie jedoch stattdessen eine zusätzliche Domänenrichtlinie erstellen, haben Sie den Vorteil, dass Sie die zusätzliche Richtlinie bei Problemen wieder deaktivieren können, so dass die standardmäßige Domänenrichtlinie wieder die Kontrolle übernimmt.

Sie dürfen nicht vergessen, dass Domänen häufig Clientcomputer und Benutzer ebenso wie Server enthalten. Wenn Sie also spezielle Server sperren möchten, ist es häufig nicht möglich, diese Einstellungen auf Domänenebene zu definieren. In der Praxis ist es meisten sinnvoll, die Sicherheitseinstellungen für Server auf die Einstellungen zu beschränken, die auf Domänenebene festgelegt werden müssen.

In diesem Betriebshandbuch werden keine Einstellungen auf Domänenebene definiert, da viele der Einstellungen, z. B. die Länge von Kennwörtern, entsprechend der Richtlinie für die gesamte Sicherheit Ihrer Organisation geändert werden. In Kapitel 4, "Sichern von Servern basierend auf ihrer Rolle", finden Sie jedoch einige allgemeine Empfehlungen zu diesem Thema.

Anmerkung: Die Kennwort- und Kontorichtlinien haben nur Auswirkungen auf Domänenkonten, wenn Sie auf Domänenebene festgelegt werden (d. h., dass Sie pro Domäne nur eine Kennwort- und eine Kontorichtlinie konfigurieren können). Wenn diese Richtlinien auf der Ebene der Organisationseinheiten oder auf einer anderen Ebene festgelegt werden, haben sie nur Einfluss auf lokale Konten. Weitere Informationen finden Sie im englischsprachigen Knowledge Base-Artikel Q259576, "Group Policy Application Rules for Domain Controllers".

Organisationseinheit der Mitgliedsserver

Viele der Sicherheitseinstellungen, die Sie für Mitgliedsserver definieren, sollten für alle Mitgliedsserver gelten. Um diesen Vorgang zu vereinfachen, wurde die Basissicherheitsvorlage **Baseline.inf** erstellt, die Sie in ein Gruppenrichtlinienobjekt importieren und auf die Organisationseinheit der Mitgliedsserver anwenden können. Diese Einstellungen gelten dann für die Organisationseinheit der Mitgliedsserver und alle untergeordneten Organisationseinheiten.

Organisationseinheiten der Domänencontroller

In Windows 2000 ist standardmäßig eine Organisationseinheit der Domänencontroller integriert. Wenn ein Server zu einem Domänencontroller wird, wird er automatisch in dieser Organisationseinheit platziert und sollte daraus nicht entfernt werden, da dies für Benutzer zu Anmelde- und Zugriffsproblemen führen kann.

Mit diesem Handbuch wird Ihnen die Sicherheitsvorlage **BaselineDC.inf** zur Verfügung gestellt, die Sie in ein Gruppenrichtlinienobjekt importieren und auf die Organisationseinheit der Domänencontroller anwenden können. Sie können diese Vorlage zusätzlich zum standardmäßigen Gruppenrichtlinienobjekt für Domänencontroller anwenden oder einfach die Einstellungen im Gruppenrichtlinienobjekt für Domänencontroller ändern.

Organisationseinheiten einzelner Serverrollen

Die Organisationseinheiten einzelner Serverrollen sind der Organisationseinheit für Mitgliedsserver untergeordnet. Dies bedeutet, dass diese Server standardmäßig die Einstellungen übernehmen, die in der Basisrichtlinie für Mitgliedsserver definiert sind.

Wenn Sie die Basisrichtlinie verwenden, um die Mitgliedsserver zu sichern, müssen Sie Änderungen vornehmen, die für jede einzelne Serverrolle gelten. Sie können dies erreichen, indem Sie jeder Organisationseinheit für Serverrollen eigene Gruppenrichtlinienobjekte zuweisen.

In diesem Handbuch werden Sicherheitsvorlagen zur Verfügung gestellt, die Sie in die Gruppenrichtlinienobjekte für die einzelnen Organisationseinheiten der Serverrollen importieren können. Serverrollen werden in Kapitel 4, "Sichern von Servern basierend auf ihrer Rolle", detailliert erläutert.

Importieren der Sicherheitsvorlagen

Mit dem folgenden Verfahren werden die in diesem Handbuch enthaltenen Sicherheitsvorlagen in die in diesem Kapitel beschriebene Struktur von Organisationseinheiten importiert. Bevor Sie das folgende Verfahren auf einem Domänencontroller implementieren, müssen Sie den Inhalt der im Lieferumfang dieses Handbuchs enthaltenen Datei **SecurityOps.exe** extrahieren.

Achtung: Mit den Sicherheitsvorlagen in diesem Handbuch soll die Sicherheit in einer Umgebung erhöht werden. Es ist möglich, dass durch die Installation der Vorlagen dieses Handbuchs ein Teil der Funktionalität der Umgebung verloren geht. Dazu könnte der Ausfall unternehmenswichtiger Anwendungen gehören. Es ist daher UNBEDINGT ERFORDERLICH, dass Sie diese Vorlagen testen, bevor Sie sie in einer Produktionsumgebung bereitstellen. Wenn es für die Umgebung erforderlich ist, sollten Sie die entsprechenden Änderungen vornehmen. Sichern Sie alle Domänencontroller und Server, bevor Sie die neuen Sicherheitseinstellungen übernehmen. Der Systemstatus muss in der Sicherung enthalten sein, da im Systemstatus die Registrierungsdaten gespeichert sind. Auf Domänencontrollern sind darin außerdem alle Active Directory-Objekte enthalten.

Anmerkung: Wenn Sie Windows 2000 Service Pack 2 verwenden, müssen Sie den im englischsprachigen Knowledge Base-Artikel Q295444, "SCE Cannot Alter a Service's SACL Entry in the Service's Registry Key", beschriebenen Hotfix anwenden, bevor Sie den Vorgang fortsetzen. Wenn dieser Hotfix nicht angewendet wurde, können mit den Gruppenrichtlinienvorlagen keine Dienste deaktiviert werden.

Importieren der Basisrichtlinie für Domänencontroller

1. Klicken Sie in **Active Directory-Benutzer und –Computer** mit der rechten Maustaste auf **Domänencontroller**, und wählen Sie dann **Eigenschaften** aus.
2. Klicken Sie auf der Registerkarte **Gruppenrichtlinie** auf **Neu**, um ein neues Gruppenrichtlinienobjekt hinzuzufügen.
3. Geben Sie **BaselineDC Policy** ein, und drücken Sie die EINGABETASTE.
4. Klicken Sie mit der rechten Maustaste auf **BaselineDC Policy**, und wählen Sie **Kein Vorrang** aus.

Anmerkung: Dies ist erforderlich, da mit der Standardrichtlinie für Domänencontroller für alle Einstellungen, mit Ausnahme des Kontenmanagement (Account Management), die Überwachungsrichtlinie **Keine Überwachung** festgelegt wird. Da die Standardrichtlinie für Domänencontroller eine höhere Priorität hat, wird die Einstellung **Keine Überwachung** wirksam.

5. Klicken Sie auf **Bearbeiten**.
6. Erweitern Sie **Windows-Einstellungen**, klicken Sie mit der rechten Maustaste auf **Sicherheitseinstellungen**, und wählen Sie **Richtlinie importieren** aus.

Anmerkung: Wenn **Richtlinie importieren** nicht im Menü angezeigt wird, schließen Sie das Fenster **Gruppenrichtlinie**, und wiederholen Sie die Schritte 4 und 5.

7. Wechseln Sie im Dialogfeld **Richtlinie importieren von** zum Ordner **C:\SecurityOps\Templates**, und doppelklicken Sie auf **BaselineDC.inf**.
8. Schließen Sie **Gruppenrichtlinie**, und klicken Sie dann auf **Schließen**.
9. Erzwingen Sie die Replikation zwischen den Domänencontrollern, so dass alle Domänencontroller über die Richtlinie verfügen.
10. Überprüfen Sie im Ereignisprotokoll, ob die Richtlinie gedownloadet wurde und ob der Server mit den anderen Domänencontrollern in der Domäne kommunizieren kann.
11. Starten Sie alle Domänencontroller einzeln neu, um sicherzustellen, dass die Domänencontroller erfolgreich gestartet werden können.

Importieren der Richtlinien für Mitgliedsserver

1. Klicken Sie in **Active Directory-Benutzer und -Computer** mit der rechten Maustaste auf **Mitgliedsserver**, und wählen Sie dann **Eigenschaften** aus.
2. Klicken Sie auf der Registerkarte **Gruppenrichtlinie** auf **Neu**, um ein neues Gruppenrichtlinienobjekt hinzuzufügen.
3. Geben Sie **Baseline Policy** ein, und drücken Sie die EINGABETASTE.
4. Klicken Sie auf **Bearbeiten**.
5. Erweitern Sie **Windows-Einstellungen**, klicken Sie mit der rechten Maustaste auf **Sicherheitseinstellungen**, und wählen Sie **Richtlinie importieren** aus.

Anmerkung: Wenn **Richtlinie importieren** nicht im Menü angezeigt wird, schließen Sie das Fenster **Gruppenrichtlinie**, und wiederholen Sie die Schritte 4 und 5.

6. Wechseln Sie im Dialogfeld **Richtlinie importieren von** zum Ordner **C:\SecurityOps\Templates**, und doppelklicken Sie auf **Baseline.inf**.
7. Schließen Sie **Gruppenrichtlinie**, und klicken Sie dann auf **Schließen**.
8. Wiederholen Sie die Schritte 1 bis 7 mit den folgenden Organisationseinheiten und Sicherheitsvorlagendateien:

Organisationseinheit	Sicherheitsvorlage
Datei- und Druckserver	File and Print Incremental.inf
IIS-Server	IIS Incremental.inf
Infrastrukturserver	Infrastructure Incremental.inf

9. Erzwingen Sie die Replikation zwischen den Domänencontrollern, so dass alle Domänencontroller über die Richtlinie verfügen.
10. Verschieben Sie einen Server für jede Rolle in die entsprechende Organisationseinheit, und downloaden Sie auf dem Server die Richtlinie mit dem Befehl **secedit**.
11. Überprüfen Sie im Ereignisprotokoll, ob die Richtlinie gedownloadet wurde und ob der Server mit den Domänencontrollern und mit anderen Servern in der Domäne kommunizieren kann. Nachdem Sie einen Server in der Organisationseinheit erfolgreich getestet haben, verschieben Sie die übrigen Server in die Organisationseinheit, und wenden Sie die Sicherheitsvorlage an.
12. Starten Sie die Server neu, um sicherzustellen, dass sie erfolgreich gestartet werden können.

Wahren der Sicherheit von Gruppenrichtlinieneinstellungen

Wenn Sie Sicherheitseinstellungen mithilfe von Gruppenrichtlinien anwenden, müssen Sie sicherstellen, dass die Einstellungen selbst so sicher wie möglich sind. Dies wird im Allgemeinen dadurch erreicht, dass die Berechtigungen für die Gruppenrichtlinienobjekte und die Organisationseinheiten sowie für die Domänen, auf die die Einstellungen angewendet werden, entsprechend festgelegt werden. Mit den Vorlagen in diesem Handbuch werden die standardmäßigen Active Directory-Berechtigungen nicht geändert. Sie müssen dies manuell vornehmen.

Gruppenrichtlinieneinstellungen, die für übergeordnete Container definiert wurden, können möglicherweise durch Einstellungen für untergeordnete Container überschrieben werden. Wenn Sie die Option **Kein Vorrang** für das Gruppenrichtlinienobjekt verwenden, können Sie verhindern, dass die Einstellungen übergeordneter Container überschrieben werden.

Anmerkung: Legen Sie **Kein Vorrang** nicht für die Basisrichtlinie von Mitgliedsservern fest. Andernfalls werden durch die Richtlinien für die Serverrollen nicht die entsprechenden Dienste und Einstellungen aktiviert.

Sie sollten nicht nur die Serverrollen auf der Ebene der Organisationseinheiten unterteilen, sondern auch die entsprechenden getrennten Administratorfunktionen erstellen und diesen ausschließlich die Administratorrechte für die entsprechenden Organisationseinheiten zuweisen. Dadurch können Sie sicherstellen, dass ein Angreifer, der über die Administratorrechte für den IIS-Server verfügt, nicht auch Zugriff auf den Infrastrukturserver usw. erhält.

Nur Administratoren auf Domänenebene oder auf einer höheren Ebene sollten über die Berechtigung verfügen, die Mitglieder einer Organisationseinheit zu ändern. Wenn ein Administrator auf der Ebene der Organisationseinheiten einen Server aus der Organisationseinheit entfernen kann, ist er auch in der Lage, die Sicherheitseinstellungen zu ändern.

Ihre Arbeit ist nicht abgeschlossen, wenn die Richtlinie auf die Server angewendet wurde. Sie sollten die Server regelmäßig auf Folgendes überprüfen:

Wurde die richtige Richtlinie auf den Server angewendet?

Wurde eine Einstellung der Richtlinie von einem Administrator geändert und so der Sicherheitsgrad der Server reduziert?

Wurden Aktualisierungen oder Änderungen von Richtlinien auf alle Server angewendet?

Wenn Sie überprüfen, ob die Einstellungen im Gruppenrichtlinienobjekt wie erwartet angewendet wurden, können Sie davon ausgehen, dass die Server ordnungsgemäß gesichert sind. Es gibt mehrere Methoden, mit denen Sie die Gruppenrichtlinie auf einem Server untersuchen können, um zu überprüfen, ob sie ordnungsgemäß festgelegt wurde.

Ereignisse im Ereignisprotokoll

Wenn die Richtlinie erfolgreich gedownloadet wurde, wird im Ereignisprotokoll ein Ereignis mit den folgenden Informationen angezeigt:

Typ: Informationen

Quelle: SceCli

Ereignis-ID: 1704

Beschreibung: Die Sicherheitsrichtlinien in den Gruppenrichtlinienobjekten wurden erfolgreich angewendet

Es kann eine Weile dauern, bis diese Meldung nach dem Anwenden der Richtlinie angezeigt wird. Wenn keine erfolgreiche Ereignisprotokollmeldung angezeigt wird, müssen Sie **secedit /refreshpolicy machine_policy /enforce** ausführen, und dann den Server neu starten, um den Download der Richtlinie zu erzwingen. Überprüfen Sie das Ereignisprotokoll nach dem Neustart noch einmal auf den erfolgreichen Download der Richtlinie.

Anmerkung: Wenn für Dienste in einem Gruppenrichtlinienobjekt **Deaktiviert** festgelegt ist, und der Server einmal neu gestartet wird, werden die Dienste normalerweise neu gestartet, bevor die Einstellungen im Gruppenrichtlinienobjekt wirksam werden. Indem Sie den Server ein zweites Mal neu starten, stellen Sie sicher, dass die Dienste, die deaktiviert wurden, nicht gestartet werden.

Überprüfen der Richtlinie mithilfe der MMC "Lokale Sicherheitsrichtlinie"

Sie können das erfolgreiche Anwenden der Richtlinie auch anhand der effektiven Richtlinieneinstellungen auf dem lokalen Server überprüfen.

▶ **So überprüfen Sie die effektiven Richtlinieneinstellungen**

1. Starten Sie die MMC **Lokale Sicherheitsrichtlinie**.
2. Klicken Sie unter **Sicherheitseinstellungen** auf **Lokale Richtlinien**, und klicken Sie dann auf **Sicherheitsoptionen**.
3. Sehen Sie sich im rechten Bereich die Spalte **Effektive Einstellung** an.

In der Spalte **Effektive Einstellung** sollten die Einstellungen angezeigt werden, die in der Vorlage für die Rolle des ausgewählten Servers konfiguriert wurden.

Überprüfen der Richtlinie mithilfe von Befehlszeilentools

Es gibt auch zwei Befehlszeilentools, mit denen Sie die Richtlinieneinstellungen überprüfen können.

Secedit

Dieses Tool ist in Windows 2000 enthalten und kann verwendet werden, um die Unterschiede zwischen der Vorlagedatei und der Richtlinie des Computers anzuzeigen. Verwenden Sie die folgende Befehlszeile, um eine Vorlage mit der aktuellen Richtlinie auf einem Computer zu vergleichen:

```
secedit /analyze /db secedit.sdb /cfg <Vorlagenname>
```

Anmerkung: Wenn Sie die in diesem Handbuch enthaltenen Vorlagen anwenden und dann den oben angegebenen Befehl ausführen, wird eine Fehlermeldung generiert, die besagt, dass der Zugriff verweigert wird. Dies ist das aufgrund der zusätzlichen Sicherheit zu erwartende Ergebnis. Dennoch wird eine Protokolldatei mit den Ergebnissen der Analyse generiert.

GPResult

Im Resource Kit zu *Windows 2000 Server – Die technische Referenz* (Microsoft Press, ISBN: 3-86063-273-6) ist ein Tool mit dem Namen GPResult enthalten, mit dem die auf einen Server angewendeten Richtlinien angezeigt werden können. Verwenden Sie die folgende Befehlszeile, um eine Liste der auf einen Server angewendeten Richtlinien abzurufen:

```
Gpresult /c
```

Anmerkung: GPResult wird im Abschnitt "Behandeln von Problemen mit Gruppenrichtlinien" weiter unten in diesem Kapitel ausführlich behandelt.

Überwachen von Gruppenrichtlinien

Es ist möglich, Änderungen der Gruppenrichtlinie zu überwachen. Durch das Überwachen von Richtlinienänderungen können Sie nachverfolgen, wer Richtlinieneinstellungen ändert oder versucht, sie zu ändern. Das Überwachen des Erfolgs und des Fehlschlagens von Richtlinienänderungen wird in den Basissicherheitsvorlagen aktiviert.

Behandeln von Problemen mit Gruppenrichtlinien

Die Gruppenrichtlinie wird zwar automatisch angewendet, es ist aber dennoch möglich, dass sie auf dem Server anders als erwartet ist. Der häufigste Grund dafür ist, dass die Gruppenrichtlinie auf verschiedenen Ebenen konfiguriert werden kann. Dieser Abschnitt enthält einige Richtlinien, die Sie für die Behandlung von Problemen mit Gruppenrichtlinien verwenden können.

Anmerkung: Wenn Sie ein bestimmtes Problem mit der Gruppenrichtlinie haben, das in diesem Kapitel nicht behandelt wird, sollten Sie in der Microsoft Knowledge Base nach einem entsprechenden Artikel suchen. Die wichtigsten Knowledge Base-Artikel zum Thema Gruppenrichtlinien sind im Abschnitt "Weitere Informationen" am Ende dieses Kapitels und im englischsprachigen Whitepaper "Troubleshooting Group Policy" aufgeführt.

Tools im Resource Kit

GPResult und GpoTool sind zwei Tools aus dem Resource Kit zu *Windows 2000 Server – Die technische Referenz*, die Ihnen die Behandlung von Problemen mit Gruppenrichtlinien erleichtern.

Anmerkung: Diese Tools sind auch online verfügbar. Lesen Sie dazu den Abschnitt "Weitere Informationen" am Ende dieses Kapitels.

GPResult

Mit diesem Tool wird eine Liste zur Verfügung gestellt, in der alle Gruppenrichtlinienobjekte, die auf einen Computer angewendet wurden, die Angabe des Domänencontrollers, von dem die Gruppenrichtlinienobjekte stammen, sowie Datum und Uhrzeit der letzten Anwendung der Gruppenrichtlinien aufgeführt sind.

Wenn Sie GPResult auf einem Server ausführen, um sicherzustellen, dass die richtigen Gruppenrichtlinienobjekte vorhanden sind, verwenden Sie die Option **/c**, damit nur Informationen zu den Computereinstellungen angezeigt werden.

Wenn GPResult mit der Option **/c** verwendet wird, werden die folgenden allgemeinen Informationen zur Verfügung gestellt:

- Betriebssystem
  - Typ (Professional, Server, Domänencontroller)
  - Buildnummer und Informationen zu Service Packs
  - Installation der Terminaldienste und der von ihnen verwendeten Modi
- Computerinformationen
  - Computername und -standort in Active Directory (falls vorhanden)
  - Domänenname und -typ (Windows NT oder Windows 2000)
  - Standortname

GPResult mit der Option **/c** stellt außerdem die folgenden Informationen zur Gruppenrichtlinie zur Verfügung:

- Zeitpunkt der letzten Anwendung der Richtlinie und Informationen zum Domänencontroller, der die Richtlinie für den Benutzer und den Computer angewendet hat
- Die vollständige Liste der angewendeten Gruppenrichtlinienobjekte und deren Details, einschließlich einer Zusammenfassung der Erweiterungen, die in den einzelnen Gruppenrichtlinienobjekten enthalten sind
- Angewendete Registrierungseinstellungen und deren Details
- Umgeleitete Ordner und deren Details
- Softwaremanagementinformationen, einschließlich zugewiesener und veröffentlichter Anwendungen
- Informationen zu Datenträgerkontingenten
- IP-Sicherheitseinstellungen
- Skripts

GpoTool

Mit diesem Befehlszeilentool können Sie den Zustand der Gruppenrichtlinienobjekte auf Domänencontrollern überprüfen. Dazu gehört Folgendes:

- **Überprüfen der Konsistenz der Gruppenrichtlinienobjekte**. Das Tool liest die verbindlichen und optionalen Eigenschaften von Verzeichnisdiensten (Version, Anzeigename, Erweiterungs-GUIDs und Daten des Windows 2000-Systemdatenträgers (System Volume oder SYSVOL) in der Datei **Gpt.ini**), vergleicht Verzeichnisdienste und SYSVOL-Versionsnummern und führt weitere Konsistenzprüfungen durch. Die Nummer der Funktionalitätsversion muss 2 sein, die Benutzer-/Computerversion größer als 0, wenn die Erweiterungseigenschaft GUIDs enthält.
- **Überprüfen der Replikation der Gruppenrichtlinienobjekte**. Das Tool liest die Instanzen des Gruppenrichtlinienobjekts der Domänencontroller und vergleicht sie (ausgewählte Eigenschaften des Gruppenrichtliniencontainers und ein vollständiger rekursiver Vergleich der Gruppenrichtlinienvorlage).

Anzeigen von Informationen zu einem bestimmten Gruppenrichtlinienobjekt. Zu den Informationen gehören Eigenschaften, auf die über das Snap-In Gruppenrichtlinie nicht zugegriffen werden kann, z. B. Funktionalitätsversionen und Erweiterungs-GUIDs.

Suchen von Gruppenrichtlinienobjekten. Eine Befehlszeilenoption kann basierend auf dem Anzeigenamen oder dem GUID nach Richtlinien suchen. Die Suche führt auch bei partiellen Übereinstimmungen zu einem Ergebnis.

Bevorzugte Domänencontroller. Standardmäßig werden alle verfügbaren Domänencontroller in der Domäne verwendet. Diese Einstellung kann mit der bereitgestellten Liste von Domänencontrollern über die Befehlszeile überschrieben werden.

Bereitstellen domänenübergreifender Unterstützung. Es gibt eine Befehlszeilenoption, mit der Richtlinien in unterschiedlichen Domänen überprüft werden können.

Ausführen im ausführlichen Modus. Wenn es keine Probleme mit den Richtlinien gibt, zeigt das Tool eine Bestätigungsmeldung an. Bei Fehlern werden Informationen zu den fehlerhaften Richtlinien ausgedruckt. Mit einer Befehlszeilenoption können ausführliche Informationen zu allen Richtlinien verarbeitet werden.

Verwenden Sie die folgende Befehlszeile, um Informationen zu einer Gruppenrichtlinie abzurufen und um über Fehler in der Richtlinie informiert zu werden:

```
GPOTool /gpo:<gpo name>
```

Fehler im Ereignisprotokoll der Gruppenrichtlinie

Einige Fehler im Ereignisprotokoll der Gruppenrichtlinie weisen auf spezielle Probleme in der Umgebung hin. Durch die im Folgenden dargestellten Probleme wird verhindert, dass die Gruppenrichtlinie ordnungsgemäß angewendet wird:

Auf einem Domänencontroller wird die Warnung 1202 zusammen mit dem Fehler 1000 angezeigt. Dies bedeutet im Allgemeinen, dass ein Domänencontroller aus der Organisationseinheit der Domänencontroller in eine andere Organisationseinheit verschoben wurde, die nicht mit dem standardmäßigen Gruppenrichtlinienobjekt für Domänencontroller verknüpft ist.

Wenn ein Administrator versucht, eines der standardmäßigen Gruppenrichtlinienobjekte zu öffnen, wird der folgende Fehler zurückgegeben:

Das Gruppenrichtlinienobjekt konnte nicht geöffnet werden.

Möglicherweise verfügen Sie nicht über die erforderlichen Rechte.

Details: Unbekannter Fehler

Im Ereignisprotokoll werden die Ereignisse 1000, 1001 und 1004 angezeigt. Dies ist auf eine fehlerhafte Datei **registry.pol** zurückzuführen. Wenn Sie die Datei **registry.pol** unter SYSVOL löschen, neu starten und eine Änderung auf dem Server vornehmen, sollte der Fehler behoben werden.

Zusammenfassung

Windows 2000-Gruppenrichtlinien bieten die Möglichkeit, in einer Windows 2000-basierten Umgebung einheitliche Einstellungen zur Verfügung zu stellen. Um Gruppenrichtlinien effektiv bereitzustellen, sollten Sie wissen, wo Gruppenrichtlinienobjekte angewendet werden, und sicher sein, dass alle Server die entsprechenden Einstellungen erhalten und dass Sie die erforderliche Sicherheit für die Gruppenrichtlinienobjekte definiert haben.

Weitere Informationen

Microsoft Whitepaper zu Gruppenrichtlinien:

http://www.microsoft.com/windows2000/techinfo/howitworks/management/grouppolwp.asp (englischsprachig)

Microsoft Whitepaper zum Behandeln von Problemen mit Gruppenrichtlinien:

http://www.microsoft.com/Windows2000/techinfo/howitworks/management/gptshoot.asp (englischsprachig)

Knowledge Base-Artikel zum Behandeln von Problemen mit Gruppenrichtlinien:

http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q250842 (englischsprachig)

http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q216359 (englischsprachig)

Dateiformat administrativer Vorlagen:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/policy/policyref_17hw.asp (englischsprachig)

Security Descriptor Definition Language (SDDL):

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/Security/security_descriptor_definition_language.asp (englischsprachig)

Weitere Tools und Informationen zu Gruppenrichtlinien finden Sie in folgenden Quellen:

Im Resource Kit zu Windows 2000 Server – Die technische Referenz (Microsoft Press, ISBN: 3-86063-273-6)

http://mspress.microsoft.de/mspress/product.asp?sku=3-86063-273-6

oder online unter:

http://www.microsoft.com/windows2000/techinfo/reskit/default.asp (englischsprachig)

Originaltitel: Chapter 4 – Securing Servers Based on Role

4

Sichern von Servern basierend auf ihrer Rolle

Im vorherigen Kapitel wurde erläutert, wie Gruppenrichtlinien verwendet werden können, um Sicherheitseinstellungen auf Servern zu definieren. In diesem Kapitel werden die Einzelheiten behandelt: Basisrichtlinien, die für alle Mitgliedsserver und Domänencontroller im Unternehmen definiert werden können, und weitere Änderungen, die auf bestimmte Serverrollen angewendet werden.

Diese Vorgehensweise ermöglicht Administratoren, Server mithilfe zentraler Basisrichtlinien zu sperren, die einheitlich auf alle Server im Unternehmen angewendet werden. Die Basisrichtlinien lassen nur minimale Funktionalität zu, ermöglichen aber eine Kommunikation der Server mit anderen Computern in der Domäne sowie die Authentifizierung der Server durch Domänencontroller. Auf der Grundlage dieses sicheren Status können zusätzliche inkrementelle Richtlinien angewendet werden, so dass jeder Server nur die durch seine Rolle definierten Tasks ausführen kann. Durch die Risikomanagementstrategie (Risk Management) wird bestimmt, ob diese Änderungen für die Umgebung angemessen sind.

In diesem Betriebshandbuch wird die Implementierung von Richtlinien folgendermaßen unterteilt:

Domänenweite Richtlinie. Deckt allgemeine Sicherheitsanforderungen ab, wie z. B. Kontorichtlinien, die für alle Server und Arbeitsstationen erzwungen werden müssen.

Domänencontroller-Richtlinie. Richtlinien, die für die Organisationseinheit der Domänencontroller gelten. Besonders die Konfigurationseinstellungen haben Auswirkungen auf die Überwachungsrichtlinie, Sicherheitsoptionen und die Dienstkonfiguration.

Basisrichtlinie für Mitgliedsserver. Gemeinsame Einstellungen für alle Mitgliedsserver, einschließlich Überwachungsrichtlinien, Dienstkonfiguration, den Zugriff auf die Registrierung beschränkende Richtlinien, Dateisystem sowie andere spezielle Sicherheitseinstellungen, wie das Löschen der Auslagerungsdatei des virtuellen Arbeitsspeichers beim Herunterfahren des Systems.

Richtlinien für Serverrollen. Es werden vier unterschiedliche Serverrollen definiert: Anwendungsserver, Datei- und Druckserver, Infrastrukturserver und IIS-Server. Für jede Rolle werden bestimmte Sicherheitsanforderungen und -konfigurationen beschrieben.

In diesem Kapitel werden diese Richtlinien und andere Einstellungen behandelt, die für bestimmte Serverrollen definiert werden sollten. Weitere Informationen dazu, wie mithilfe von Gruppenrichtlinien Sicherheitseinstellungen angewendet werden, finden Sie in Kapitel 3, "Verwalten von Sicherheit mit Windows 2000-Gruppenrichtlinien".

Domänenrichtlinie

In diesem Betriebshandbuch werden keine Einstellungen auf Domänenebene erzwungen, da viele dieser Einstellungen, z. B. die Länge von Kennwörtern, entsprechend der Richtlinie für die gesamte Sicherheit Ihrer Organisation geändert werden. Es ist jedoch sehr wichtig, diese Einstellungen richtig zu definieren.

Kennwortrichtlinie

Für alle Server in der Domäne werden standardmäßige Kennwortrichtlinien erzwungen. In der folgenden Tabelle sind die Einstellungen für eine standardmäßige Kennwortrichtlinie und empfohlene minimale Einstellungen für eine Umgebung aufgeführt.

Tabelle 4.1: Standardeinstellungen und empfohlene Einstellungen für Kennwortrichtlinien

Richtlinie	Standardeinstellung	Empfohlene minimale Einstellung
Kennwortchronik erzwingen	Gespeicherte Kennwörter: 1	Gespeicherte Kennwörter: 24
Maximales Kennwortalter	42 Tage	42 Tage
Minimales Kennwortalter	0 Tage	2 Tage
Minimale Kennwortlänge	0 Zeichen	8 Zeichen
Kennwörter müssen den Komplexitätsanforderungen entsprechen	Deaktiviert	Aktiviert
Kennwörter für alle Domänenbenutzer mithilfe umkehrbarer Verschlüsselung speichern	Deaktiviert	Deaktiviert

Komplexitätsanforderungen

Wenn die Einstellung **Kennwörter müssen den Komplexitätsanforderungen entsprechen** der Gruppenrichtlinie aktiviert ist, müssen die Kennwörter mindestens 6 Zeichen lang sein (die empfohlene Länge ist jedoch 8 Zeichen). Das Kennwort muss auch Zeichen aus mindestens drei der folgenden Klassen enthalten:

Lateinische Großbuchstaben	A, B, C, … Z
Lateinische Kleinbuchstaben	a, b, c, … z
Arabische Zahlen	0, 1, 2, … 9
Zeichen, die nicht alphanumerisch sind, z. B. Satzzeichen	

Anmerkung: Eine Kennwortrichtlinie sollte nicht nur auf Servern unter Windows 2000 erzwungen werden, sondern auch auf allen anderen Geräten, bei denen ein Kennwort für die Authentifizierung erforderlich ist. Netzwerkgeräte wie Router und Switches sind sehr anfällig für einen Angriff, wenn einfache Kennwörter verwendet werden. Angreifer versuchen möglicherweise, die Kontrolle über diese Netzwerkgeräte zu übernehmen, um Firewalls zu umgehen.

Kontosperrungsrichtlinie

Eine effektive Kontosperrungsrichtlinie kann dazu beitragen, das Erraten der Kennwörter Ihrer Konten durch Angreifer zu verhindern. In der folgenden Tabelle sind die Einstellungen für eine standardmäßige Kontosperrungsrichtlinie und empfohlene minimale Einstellungen für eine Umgebung aufgeführt.

Tabelle 4.2: Standardeinstellungen und empfohlene Einstellungen für Kontorichtlinien

Richtlinie	Standardeinstellung	Empfohlene minimale Einstellung
Kontosperrdauer	Nicht definiert	30 Minuten
Kontensperrungsschwelle	0	Ungültige Anmeldeversuche: 5
Kontosperrungszähler zurücksetzen nach	Nicht definiert	30 Minuten

Mit den hier aufgeführten minimalen Einstellungen wird ein Konto, für das innerhalb von 30 Minuten 5 ungültige Anmeldeversuche unternommen wurden, für 30 Minuten gesperrt (anschließend wird es auf 0 ungültige Anmeldeversuche zurückgesetzt, und neue Anmeldeversuche können unternommen werden). Vor Ablauf der 30 Minuten kann das Konto nur wieder aktiviert werden, indem die Sperrung von einem Administrator aufgehoben wird. Um den Sicherheitsgrad in einer Organisation zu erhöhen, sollte die Kontosperrdauer verlängert und die Kontensperrungsschwelle gesenkt werden.

Anmerkung: Die Kennwort- und Kontenrichtlinien **müssen** auf Domänenebene festgelegt werden. Wenn diese Richtlinien auf der Ebene der Organisationseinheiten oder auf einer anderen Ebene in Active Directory festgelegt werden, haben sie Auswirkungen auf lokale Konten und nicht auf Domänenkonten. Für eine Domäne ist nur eine Kontorichtlinie möglich. Weitere Informationen finden Sie im Knowledge Base-Artikel D42198, "Konfigurieren von Kontorichtlinien im Active Directory".

Basisrichtlinie für Mitgliedsserver

Nachdem Sie die Einstellungen auf Domänenebene konfiguriert haben, sollten Sie die gemeinsamen Einstellungen für alle Mitgliedsserver definieren. Dazu wird ein Gruppenrichtlinienobjekt der Organisationseinheit für Mitgliedsserver verwendet, das als Basisrichtlinie bezeichnet wird. Mit einem gemeinsamen Gruppenrichtlinienobjekt wird das Konfigurieren bestimmter Sicherheitseinstellungen auf allen Servern automatisiert. Sie müssen außerdem einige zusätzliche Sicherheitseinstellungen manuell anwenden, die nicht mithilfe von Gruppenrichtlinien angewendet werden können.

Basisgruppenrichtlinie für Mitgliedsserver

Die Konfiguration der in diesem Handbuch verwendeten Basisrichtlinie ist von der Richtlinie **hisecws.inf** abgeleitet, die Teil der Server- und Arbeitsstationsinstallation ist. Mit **hisecws.inf** werden u. a. die folgenden Bereiche abgedeckt:

- **Überwachungsrichtlinie**. Bestimmt, wie die Überwachung auf den Servern erfolgt.
- **Sicherheitsoptionen**. Bestimmen mithilfe von Registrierungswerten spezielle Sicherheitseinstellungen.
- **Zugriffssteuerungslisten für die Registrierung**. Bestimmen, wer auf die Registrierung zugreifen kann.
- **Zugriffssteuerungslisten für Dateien**. Bestimmen, wer auf das Dateisystem zugreifen kann.
- **Dienstkonfiguration**. Bestimmt, welche Dienste gestartet, beendet, deaktiviert usw. werden.

Für dieses Handbuch wurde **hisecws.inf** zur Erhöhung der Sicherheit geändert. Mit der Basisrichtlinie für Mitgliedsserver, **baseline.inf**, kann ein Server erstellt werden, der in Produktionsumgebungen Angriffen gegenüber deutlich widerstandsfähiger ist.

Zu **hisecws.inf** wurde Folgendes hinzugefügt:

Registrierungswerte, die die Sicherheit betreffen

Dienstkonfiguration

Restriktivere Zugriffssteuerungslisten für Dateien

Verbesserte Überwachungskonfiguration

Basisüberwachungsrichtlinie für Mitgliedsserver

Die Einstellungen für die Anwendungs-, Sicherheits- und Systemereignisprotokolle werden in der Richtlinie konfiguriert und auf alle Mitgliedsserver in der Domäne angewendet. Für die Größe der einzelnen Protokolle sind 10 Megabyte (MB) festgelegt, und jedes Protokoll ist so konfiguriert, dass Ereignisse nicht überschrieben werden. Deshalb ist es für einen Administrator wichtig, die Protokolle zu überprüfen und zu archivieren oder ggf. zu löschen.

Anmerkung: Wenn ein Verwaltungssystem die Protokolle regelmäßig auf bestimmte Ereignisse überprüft und die Details extrahiert und an eine Verwaltungsdatenbank weiterleitet, werden die notwendigen Daten aufgezeichnet. Deshalb können Sie für die Protokolldateien festlegen, dass sie überschrieben werden.

In der folgenden Tabelle werden die Einstellungen dargestellt, die in der Basisüberwachungsrichtlinie für Mitgliedsserver definiert sind.

Tabelle 4.3: Einstellungen der Basisüberwachungsrichtlinie für Mitgliedsserver

Richtlinie	Computereinstellung
Kontoanmeldeereignisse überwachen	Erfolg, Fehler
Kontenmanagement (Account Management) überwachen	Erfolg, Fehler
Active Directory-Zugriff überwachen	Fehler
Anmeldeereignisse überwachen	Erfolg, Fehler
Objektzugriffsversuche überwachen	Erfolg, Fehler
Richtlinienänderungen überwachen	Erfolg, Fehler
Rechteverwendung überwachen	Fehler
Prozessverfolgung überwachen	Keine Überwachung
Systemereignisse überwachen	Erfolg, Fehler
Gastzugriff auf Anwendungsprotokoll beschränken	Aktiviert
Gastzugriff auf Sicherheitsprotokoll beschränken	Aktiviert
Gastzugriff auf Systemprotokoll beschränken	Aktiviert
Aufbewahrungsmethode des Anwendungsprotokolls	Ereignisse nie überschreiben (Protokoll manuell löschen)
Aufbewahrungsmethode des Sicherheitsprotokolls	Ereignisse nie überschreiben (Protokoll manuell löschen)
Aufbewahrungsmethode des Systemprotokolls	Ereignisse nie überschreiben (Protokoll manuell löschen)
System bei Erreichen der max. Sicherheitsprotokollgröße herunterfahren	Nicht definiert

Anmerkung: Für die Aufbewahrungsmethode ist die Richtlinieneinstellung **Manuell** angegeben. Dies bedeutet, dass Ereignisse nicht überschrieben werden (das Protokoll wird manuell gelöscht).

Basisrichtlinie der Sicherheitsoptionen für Mitgliedsserver

Die folgenden Sicherheitsoptionen sind in der Basisgruppenrichtlinie konfiguriert.

Tabelle 4.4: Einstellungen der Basisrichtlinie der Sicherheitsoptionen für Mitgliedsserver

Option	Einstellung
Weitere Beschränkungen für anonyme Verbindungen	Kein Zugriff ohne explizite anonyme Berechtigung
Serveroperatoren das Einrichten von geplanten Tasks erlauben (Nur für Domänencontroller)	Deaktiviert
Herunterfahren des Systems ohne Anmeldung zulassen	Deaktiviert
Auswerfen von NTFS-Wechselmedien zulassen	Administratoren
Leerlaufzeitspanne bis zur Trennung der Sitzung	15 Minuten
Zugriff auf globale Systemobjekte prüfen	Deaktiviert

Option	Einstellung
Die Verwendung des Sicherungs- und Wiederherstellungsrechts überprüfen	Deaktiviert
Benutzer nach Ablauf der Anmeldezeit automatisch abmelden	Nicht definiert (siehe Anmerkung)
Benutzer automatisch abmelden, wenn die Anmeldezeit überschritten wird (lokal)	Aktiviert
Auslagerungsdatei des virtuellen Arbeitspeichers beim Herunterfahren des Systems löschen	Aktiviert
Clientkommunikation digital signieren (immer)	Aktiviert
Clientkommunikation digital signieren (wenn möglich)	Aktiviert
Serverkommunikation digital signieren (immer)	Aktiviert
Serverkommunikation digital signieren (wenn möglich)	Aktiviert
STRG+ALT+ENTF-Anforderung zur Anmeldung deaktivieren	Deaktiviert
Letzten Benutzernamen nicht im Anmeldedialog anzeigen	Aktiviert
LAN Manager-Authentifizierungsebene	Nur NTLMv2-Antworten senden, LM & NTLM verweigern
Nachricht für Benutzer, die sich anmelden wollen	
Nachrichtentitel für Benutzer, die sich anmelden wollen	
Anzahl zwischenzuspeichernder vorheriger Anmeldungen (für den Fall, dass der Domänencontroller nicht verfügbar ist)	0 Anmeldungen
Systemwartung des Computerkontokennworts nicht gestatten	Deaktiviert
Anwendern das Installieren von Druckertreibern nicht erlauben	Aktiviert
Anwender vor Ablauf des Kennworts zum Ändern des Kennworts auffordern	14 Tage
Wiederherstellungskonsole: Automatische administrative Anmeldungen zulassen	Deaktiviert
Wiederherstellungskonsole: Kopieren von Disketten und Zugriff auf alle Laufwerke und alle Ordner zulassen	Deaktiviert
Administrator umbenennen	Nicht definiert
Gastkonto umbenennen	Nicht definiert
Zugriff auf CD-ROM-Laufwerke auf lokal angemeldete Benutzer beschränken	Aktiviert
Zugriff auf Diskettenlaufwerke auf lokal angemeldete Benutzer beschränken	Aktiviert

Option	Einstellung
Sicherer Kanal: Daten des sicheren Kanals digital verschlüsseln oder signieren (immer)	Aktiviert
Sicherer Kanal: Daten des sicheren Kanals digital verschlüsseln (wenn möglich)	Aktiviert
Sicherer Kanal: Daten des sicheren Kanals digital signieren (wenn möglich)	Aktiviert
Sicherer Kanal: Starker Sitzungsschlüssel erforderlich (Windows 2000 oder höher)	Aktiviert
Systempartition sichern (nur für RISC-Plattformen)	Nicht definiert
Unverschlüsseltes Kennwort senden, um Verbindung mit SMB-Servern von Drittanbietern herzustellen	Deaktiviert
System sofort herunterfahren, wenn Sicherheitsüberprüfungen nicht protokolliert werden können	Aktiviert (siehe zweite Anmerkung)
Verhalten beim Entfernen von Smartcards	Computer sperren
Standardberechtigungen globaler Systemobjekte (z. B. symbolischer Verknüpfungen) verstärken	Aktiviert
Verhalten bei der Installation von nichtsignierten Treibern	Installation nicht zulassen
Verhalten bei der Installation von nichtsignierten Dateien (außer Treibern)	Warnen, aber Installation zulassen

Anmerkung: In der standardmäßigen Domänenrichtlinie ist **Benutzer nach Ablauf der Anmeldezeit automatisch abmelden** deaktiviert. Um diese Option zu konfigurieren, müssen Sie die standardmäßige Domänenrichtlinie bearbeiten. Deshalb ist diese Option in der Basisrichtlinie zu diesem Handbuch nicht definiert.

Anmerkung: Wenn Sie die Anzahl der Objekte, die Sie überwachen, deutlich erhöhen, wird möglicherweise das Sicherheitsprotokoll gefüllt und ein Herunterfahren des Systems erzwungen. Das System kann dann erst wieder verwendet werden, wenn ein Administrator das Protokoll löscht. Um dies zu verhindern, sollten Sie entweder die in der Tabelle aufgeführte Option zum Herunterfahren deaktivieren, oder vorzugsweise das Sicherheitsprotokoll vergrößern.

Einige der hier festgelegten Optionen müssen genauer erläutert werden, da sie direkte Auswirkungen auf die Kommunikation der Server in der Domäne haben und außerdem einen Einfluss auf die Serverleistung haben können.

Weitere Beschränkungen für anonyme Verbindungen

Standardmäßig ermöglicht Windows 2000 anonymen Benutzern das Ausführen bestimmter Aktivitäten, z. B. das Auflisten der Namen von Domänenkonten und Netzwerkfreigaben. So kann ein Angreifer diese Konten und Freigabenamen auf einem Remoteserver anzeigen, ohne sich mit einem Benutzerkonto zu authentifizieren. Um den anonymen Zugriff besser zu sichern, kann **Kein Zugriff ohne explizite anonyme Berechtigung** konfiguriert werden. Dadurch wird die Gruppe **Jeder** aus dem anonymen Benutzertoken entfernt. Anonymer Zugriff auf einen Server ist nicht mehr zulässig, und expliziter Zugriff auf Ressourcen ist dann erforderlich.

Anmerkung: Ausführliche Informationen zu den möglichen Auswirkungen auf die Umgebung finden Sie in Knowledge Base-Artikel D246261, "Verwenden des Registrierungswertes restrictanonymous in Windows 2000".

LAN Manager-Authentifizierungsebene

Bei den Betriebssystemen Microsoft Windows 9*x* und Windows NT® kann nicht Kerberos für die Authentifizierung verwendet werden. Deshalb verwenden diese Betriebssysteme standardmäßig das NTLM-Protokoll für die Netzwerkauthentifizierung in einer Windows 2000-Domäne. Mithilfe von NTLMv2 können Sie ein sicheres Authentifizierungsprotokoll für Windows 9*x* und Windows NT erzwingen. Beim Anmelden bietet NTLMv2 einen sicheren Kanal, mit dem der Authentifizierungsvorgang geschützt wird.

Anmerkung: Wenn Sie NTLMv2 bei herkömmlichen Clients und Servern verwenden, werden Windows 2000-basierte Clients und Server weiterhin mit Windows 2000-Domänencontroller über Kerberos authentifiziert. Informationen zum Aktivieren von NTLMv2 finden Sie im englischsprachigen Knowledge Base-Artikel Q239869, "How to Enable NTLM 2 Authentication for Windows 95/98/2000 and NT". Für Windows NT 4.0 ist Service Pack 4 erforderlich, um NTLMv2 zu unterstützen. Auf Windows 9*x*-Plattformen muss der Verzeichnisdienstclient installiert sein, damit NTLMv2 unterstützt wird.

Auslagerungsdatei des virtuellen Arbeitspeichers beim Herunterfahren des Systems löschen

Wichtige Informationen aus dem realen Arbeitsspeicher können in regelmäßigen Abständen in der Auslagerungsdatei gespeichert werden. Dadurch werden unter Windows 2000 Multitaskingfunktionen unterstützt. Wenn Sie diese Option aktivieren, löscht Windows 2000 die Auslagerungsdatei beim Herunterfahren des Systems und löscht alle in der Datei gespeicherten Informationen. Abhängig von der Größe der Auslagerungsdatei kann es mehrere Minuten dauern, bis das System vollständig heruntergefahren wurde.

Client- und Serverkommunikation digital signieren

Durch das Implementieren digitaler Signaturen in sehr sicheren Netzwerken können Sie den Identitätswechsel von Clients und Servern verhindern (so genannte Sitzungsübernahmen oder Man-in-the-Middle-Angriffe). Durch SMB-Signaturen (Server Message Block) werden der Benutzer und der Server mit den Daten authentifiziert. Wenn der Benutzer oder der Server nicht authentifiziert wird, findet keine Datenübertragung statt. Wenn SMB-Signaturen implementiert sind, kann es durch das Signieren und Überprüfen der Pakete zwischen den Servern zu einem Leistungsverlust von bis zu 15 % kommen. Weitere Informationen zum Leistungsverlust finden Sie im englischsprachigen Knowledge Base-Artikel Q161372, "How to Enable SMB Signing in Windows NT".

Weitere Sicherheitsoptionen

Für dieses Handbuch wurden zusätzliche Registrierungswerte zur Basissicherheitsvorlage hinzugefügt, die nicht in der Datei für administrative Vorlagen (ADM) definiert sind. Dies bedeutet, dass die Registrierungswerte in den Tabellen 4.5 bis 4.11 nicht dargestellt werden, wenn Sie das MMC-Snap-In (Microsoft Management Console) **Sicherheitsvorlagen** laden und die Vorlage **baseline.inf** anzeigen. Stattdessen können diese Einstellungen mithilfe eines Texteditors zu der INF-Datei hinzugefügt und auf den Server angewendet werden, wenn die Richtlinie gedownloadet wird.

Anmerkung: Weitere Informationen zu den Beziehungen zwischen INF- und ADM-Dateien finden Sie im Knowledge Base-Artikel D43831, "Speicherort von ADM-Dateien (Administrative Vorlagen) in Windows 2000".

Diese Einstellungen wurden in die Sicherheitsvorlage **Baseline.inf** eingebettet, um die Änderungen zu automatisieren. Wenn die Richtlinie entfernt wird, werden diese Einstellungen nicht automatisch ebenfalls entfernt, sondern müssen manuell geändert werden.

Sicherheitsüberlegungen in Bezug auf Netzwerkangriffe

Einige Denial-of-Service-Angriffe können eine Bedrohung für den TCP/IP-Stack auf Windows 2000-basierten Servern darstellen. Mit diesen Registrierungseinstellungen können Sie den Windows 2000-TCP/IP-Stack vor normalen Denial-of-Service-Netzwerkangriffen besser schützen. Informationen zu diesen Einstellungen finden Sie im englischsprachigen Knowledge Base-Artikel Q315669, "HOW TO: Harden the TCP/IP Stack Against Denial of Service Attacks in Windows 2000".

Die folgenden Registrierungsschlüssel wurden als Unterschlüssel von **HKLM\System\CurrentControlSet\Services\Tcpip|Parameters** zur Vorlagendatei hinzugefügt:

Tabelle 4.5: TCP/IP-Parameter, die durch die Basisrichtlinie für Mitgliedsserver zur Registrierung hinzugefügt wurden

Schlüssel	Format	Wert (dezimal)
EnableICMPRedirect	DWORD	0
EnableSecurityFilters	DWORD	1
SynAttackProtect	DWORD	2
EnableDeadGWDetect	DWORD	0
EnablePMTUDiscovery	DWORD	0
KeepAliveTime	DWORD	300.000
DisableIPSourceRouting	DWORD	2
TcpMaxConnectResponseRetransmissions	DWORD	2
TcpMaxDataRetransmissions	DWORD	3
NoNameReleaseOnDemand	DWORD	1
PerformRouterDiscovery	DWORD	0
TCPMaxPortsExhausted	DWORD	5

Windows Sockets-Anwendungen wie FTP-Server und Webserver verfügen über eigene Verbindungsversuche, die von **Afd.sys** verarbeitet werden. **Afd.sys** wurde geändert, so dass jetzt eine große Anzahl von Verbindungen im halb offenen Zustand unterstützt wird, ohne dass den eigentlichen Clients der Zugriff verweigert wird. Dazu muss der Administrator einen dynamischen Rückstand konfigurieren können. Die

neue Version von **Afd.sys** unterstützt vier neue Registrierungsparameter, die verwendet werden können, um das Verhalten des dynamischen Rückstands zu steuern. Weitere Informationen zu diesen Einstellungen finden Sie im englischsprachigen Knowledge Base-Artikel Q142641, "Internet Server Unavailable Because of Malicious SYN Attacks".

Die folgenden Registrierungsschlüssel wurden als Unterschlüssel von **HKLM\System\CurrentControlSet\Services\AFD\Parameters** zur Vorlagendatei hinzugefügt:

Tabelle 4.6: **Afd.sys**-Einstellungen, die durch die Basisrichtlinie für Mitgliedsserver zur Registrierung hinzugefügt wurden

Schlüssel	Format	Wert (dezimal)
DynamicBacklogGrowthDelta	DWORD	10
EnableDynamicBacklog	DWORD	1
MinimumDynamicBacklog	DWORD	20
MaximumDynamicBacklog	DWORD	20000

Deaktivieren der automatischen Generierung von 8.3-Dateinamen

Windows 2000 unterstützt 8.3-Dateinamenformate aufgrund der Abwärtskompatibilität mit 16-Bit-Anwendungen. Dies bedeutet, dass ein Angreifer nur acht Zeichen benötigt, um auf eine Datei zu verweisen, deren Name 20 Zeichen lang ist. Wenn Sie keine 16-Bit-Anwendungen mehr verwenden, können Sie dieses Feature deaktivieren. Durch das Deaktivieren der Generierung kurzer Namen auf einer NTFS-Partition wird außerdem die Leistung beim Auflisten von Verzeichnissen erhöht.

Der folgende Registrierungsschlüssel wurde als Unterschlüssel von **HKLM\System\CurrentControlSet\Control\FileSystem** zur Vorlagendatei hinzugefügt:

Tabelle 4.7: Einstellung zum Entfernen der 8.3-Dateinamenerstellung, die durch die Basisrichtlinie für Mitgliedsserver zur Registrierung hinzugefügt wurde

Schlüssel	Format	Wert (dezimal)
NtfsDisable8dot3NameCreation	DWORD	1

Anmerkung: Wenn Sie diese Einstellung auf einen vorhandenen Server anwenden, auf dem sich bereits Dateien mit automatisch generierten 8.3-Dateinamen befinden, werden diese Dateien nicht entfernt. Um die vorhandenen 8.3-Dateinamen zu entfernen, müssen Sie die Dateien vom Server kopieren, sie an ihrem ursprünglichen Speicherort löschen und die Dateien dann an ihren ursprünglichen Speicherort zurück kopieren.

Deaktivieren der Lmhash-Erstellung

Windows 2000-basierte Server können Computer authentifizieren, auf denen alle vorherigen Versionen von Windows ausgeführt werden. Vorherige Versionen von Windows verwenden jedoch nicht Kerberos für die Authentifizierung, deshalb unterstützt Windows 2000 Lan Manager (LM), Windows NT (NTLM) und NTLM, Version 2, (NTLMv2). Das LM-Hash ist verglichen mit dem NTLM-Hash unsicherer und deshalb anfälliger für Brute Force-Angriffe. Wenn für keinen der Clients LM-Authentifizierung erforderlich ist, sollten Sie die Speicherung von LM-Hashes deaktivieren. Windows 2000 Service Pack 2 bietet eine Registrierungseinstellung, mit der die Speicherung von LM-Hashes deaktiviert werden kann.

Der folgende Registrierungsschlüssel wurde als Unterschlüssel von **HKLM\System\CurrentControlSet\Control\Lsa** zur Vorlagendatei hinzugefügt:

Tabelle 4.8: Einstellung zum Deaktivieren der Lmhash-Erstellung, die durch die Basisrichtlinie für Mitgliedsserver zur Registrierung hinzugefügt wurde

Schlüssel	Format	Wert (dezimal)
NoLMHash	DWORD	1

Anmerkung: Um die Speicherung von LM-Hashes mit dieser Registrierungseinstellung zu deaktivieren, muss Windows 2000 Service Pack 2 oder höher ausgeführt werden.

Weitere Informationen finden Sie im englischsprachigen Knowledge Base-Artikel Q147706, "How to Disable LM Authentication on Windows NT".

Konfigurieren von NTLMSSP-Sicherheit

Über den NTLM-Sicherheitsdienst (NTLM Security Support Provider oder NTLMSSP) können Sie die Sicherheitseinstellungen angeben, die bei serverseitigen Netzwerkverbindungen für Anwendungen mindestens erforderlich sind.

Durch die Basisrichtlinie für Mitgliedsserver wird sichergestellt, dass die Verbindung nicht hergestellt wird, wenn die Vertraulichkeit der Nachricht erforderlich ist, aber 128-Bit-Verschlüsselung nicht ausgehandelt wird.

Der folgende Registrierungsschlüssel wurde als Unterschlüssel von **HKLM\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0** zur Vorlagendatei hinzugefügt:

Tabelle 4.9: Einstellung zur Konfiguration von NTLMSSP-Sicherheit, die durch die Basisrichtlinie für Mitgliedsserver zur Registrierung hinzugefügt wurde

Schlüssel	Format	Wert (hex)
NtlmMinServerSec	DWORD	0x20000000

Deaktivieren von AutoRun

AutoRun beginnt Daten von einem Laufwerk zu lesen, sobald ein Medium eingelegt wurde. Deshalb beginnen die Ausführung der Installationsdatei von Programmen und die Tonwiedergabe von Audiomedien sofort. Damit potenziell schädliche Programme nicht gestartet werden, wenn ein Medium eingelegt wird, wird durch die Gruppenrichtlinie AutoRun auf allen Laufwerken deaktiviert.

Der folgende Registrierungsschlüssel wurde als Unterschlüssel von **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer** zur Vorlagendatei hinzugefügt:

Tabelle 4.10: Einstellung zum Deaktivieren von AutoRun auf allen Laufwerken, die durch die Basisrichtlinie für Mitgliedsserver zur Registrierung hinzugefügt wurde

Schlüssel	Format	Wert (hex)
NoDriveTypeAutoRun	DWORD	0xFF

Basisrichtlinie für Registrierungs-ACLs von Mitgliedsservern

Durch die Basisrichtlinie für Mitgliedsserver werden die in **hisecws.inf** definierten Zugriffsteuerungslisten (ACLs oder Access Control Lists) für die Registrierung nicht geändert. Sie sollten in der Umgebung sorgfältige Tests durchführen, bevor Sie Änderungen vornehmen.

Durch die in **hisecws.inf** definierten ACLs wird im Wesentlichen die Gruppe **Hauptbenutzer** geändert, die standardmäßig aus Gründen der Abwärtskompatibilität mit Windows NT 4.0-basierten Umgebungen erstellt wird. Mit der Vorlage wird sichergestellt, dass die Gruppe **Hauptbenutzer** über dieselben Berechtigungen verfügt, wie die Gruppe **Benutzer** in Windows 2000.

Anmerkung: Die Gruppe **Hauptbenutzer** wird auf Domänencontrollern nicht definiert.

Basisrichtlinie für Datei-ACLs von Mitgliedsservern

Um das Dateisystem weiter zu sichern, sollten Sie sicherstellen, das restriktivere Berechtigungen auf Verzeichnisse und Dateien angewendet werden, die auf allen Mitgliedsservern in der Domäne vorhanden sind. In der Basissicherheitsvorlage für Mitgliedsserver sind alle Zugriffssteuerungslisten enthalten, die auch in der Vorlage **hisecws.inf** enthalten sind. Darüber hinaus enthält sie Einstellungen für eine Reihe von Ordnern und Dateien.

Anmerkung: Informationen zu den standardmäßigen Registrierungs- und Dateiberechtigungen in Windows 2000 finden Sie im englischsprachigen Whitepaper "Default Access Control Settings in Windows 2000" auf der TechNet-Website. Im Abschnitt "Weitere Informationen" am Ende dieses Kapitels finden Sie einen Link zu diesem Whitepaper.

In der folgenden Tabelle sind die Ordner aufgeführt, die zusätzlich zu den in **hisecws.inf** definierten Ordnern durch die Basisrichtlinie für Mitgliedsserver gesichert werden.

Tabelle 4.11: Einstellungen zum Sichern wichtiger Verzeichnisse, die in der Basisrichtlinie für Mitgliedsserver definiert sind

Gesicherte Ordner	Angewendete Berechtigungen
%systemdrive%\	Administratoren: Vollzugriff System: Vollzugriff Authentifizierte Benutzer: Lesen und Ausführen, Ordnerinhalt auflisten und Lesen
%SystemRoot%\Repair %SystemRoot%\Security %SystemRoot%\Temp %SystemRoot%\system32\Config %SystemRoot%\system32\Logfiles	Administratoren: Vollzugriff Ersteller/Besitzer: Vollzugriff System: Vollzugriff
%systemdrive%\Inetpub	Administratoren: Vollzugriff System: Vollzugriff Jeder: Lesen und Ausführen, Ordnerinhalt auflisten und Lesen

Anmerkung: Mit **%SystemRoot%** werden der Pfad und der Ordnername definiert, in dem sich die Windows-Systemdateien befinden, mit **%systemdrive%** wird das Laufwerk mit **%SystemRoot%** definiert.

Auf dem Server gibt es außerdem viele Dateien, die weiter gesperrt werden sollten. Durch die Basisrichtlinie für Mitgliedsserver werden die ACLs für die standardmäßigen Windows-Startdateien geändert. Außerdem werden die ACLs für viele ausführbare Dateien geändert, die über die Eingabeaufforderung ausgeführt werden können. Diese Dateien sind in Anhang A aufgeführt.

Basisdienstrichtlinie für Mitgliedsserver

Bei der Erstinstallation von Windows 2000 Server werden die Standarddienste erstellt und so konfiguriert, dass sie beim Systemstart ausgeführt werden. Einige dieser Dienste müssen in vielen Umgebungen nicht ausgeführt werden, und da jeder Dienst einen potenziellen Angriffspunkt darstellt, sollten Sie nicht erforderliche Dienste deaktivieren.

Mit der Basisrichtlinie für Mitgliedsserver werden nur die Dienste aktiviert, die für einen Windows 2000-Mitgliedsserver erforderlich sind, um zu einer Windows 2000-Domäne zu gehören und grundlegende Verwaltungsdienste bereitzustellen.

Tabelle 4.12: Durch die Basisrichtlinie für Mitgliedsserver aktivierte Dienste

Dienst	Starttyp	Grund für die Aufnahme in die Basisrichtlinie für Mitgliedsserver
COM+-Ereignisdienste	Manuell	Ermöglicht die Verwaltung von Komponentendiensten
DHCP-Client	Automatisch	Ist für Aktualisierungsdatensätze im dynamischen DNS erforderlich
Überwachung verteilter Verknüpfungen (Client)	Automatisch	Wird zum Verwalten von Verknüpfungen auf NTFS-Datenträgern verwendet
DNS-Client	Automatisch	Ermöglicht die Auflösung von DNS-Namen
Ereignisprotokoll	Automatisch	Ermöglicht die Anzeige von Ereignisprotokollmeldungen im Ereignisprotokoll
Verwaltung logischer Datenträger	Automatisch	Ist erforderlich, um sicherzustellen, dass die Informationen zu dynamischen Datenträgern aktuell sind
Verwaltungsdienst für die Verwaltung logischer Datenträger	Manuell	Ist für die Datenträgerverwaltung erforderlich
Netlogon	Automatisch	Ist für die Beteiligung an der Domäne erforderlich
Netzwerkverbindungen	Manuell	Ist für die Netzwerkkommunikation erforderlich
Leistungsprotokolle und Warnungen	Manuell	Sammelt Leistungsdaten für Computer, schreibt sie in Protokolle oder löst Warnungen aus
Plug & Play	Automatisch	Ist für Windows 2000 erforderlich, um Systemhardware zu identifizieren und zu verwenden
Geschützter Speicher	Automatisch	Ist erforderlich, um vertrauliche Daten wie private Schlüssel zu schützen
Remoteprozeduraufruf (RPC)	Automatisch	Ist für interne Prozesse in Windows 2000 erforderlich
Remote-Registrierungsdienst	Automatisch	Ist für das Dienstprogramm Hfnetchk erforderlich (siehe Anmerkung)

Dienst	Starttyp	Grund für die Aufnahme in die Basisrichtlinie für Mitgliedsserver
Sicherheitskontenverwaltung	Automatisch	Speichert Kontoinformationen für lokale Sicherheitskonten
Server	Automatisch	Ist für das Dienstprogramm Hfnetchk erforderlich (siehe Anmerkung)
Systemereignisbenachrichtigung	Automatisch	Ist erforderlich, um Einträge in den Ereignisprotokollen aufzuzeichnen
TCP/IP-NetBIOS-Hilfsprogramm	Automatisch	Ist für die Softwareverteilung in Gruppenrichtlinien erforderlich (kann auch für die Verteilung von Patches verwendet werden)
Treiber für Windows-Verwaltungsinstrumentation	Manuell	Ist erforderlich, um Leistungswarnungen mithilfe von Leistungsdatenprotokollen und Warnungen zu implementieren
Windows-Zeitgeber	Automatisch	Ist erforderlich, damit die Kerberos-Authentifizierung einheitlich funktioniert
Arbeitsstation	Automatisch	Ist für die Beteiligung an einer Domäne erforderlich

Anmerkung: Mit dem Tool **Hfnetchk** können Sie überprüfen, welche Patches auf den einzelnen Servern in der Organisation installiert wurden. Die Verwendung dieses Tools wird in Kapitel 5, "Patchverwaltung", beschrieben.

Bei diesen Einstellungen wird von einer reinen und standardmäßigen Windows 2000-basierten Umgebung ausgegangen (eine Ausnahme bildet das Tool Hfnetchk). Wenn in der Umgebung auch Windows NT 4.0-Computer vorhanden sind (oder auf allen Mitgliedsservern andere Tools installiert sind), müssen für die Kompatibilität möglicherweise andere Dienste vorhanden sein. Wenn Sie andere Dienste aktivieren, können wiederum Abhängigkeiten bestehen, die weitere Dienste erforderlich machen. Dienste, die für eine bestimmte Serverrolle notwendig sind, können zu der Richtlinie für diese Serverrolle hinzugefügt werden.

In Anhang B sind alle Dienste einer standardmäßigen Windows 2000-Installation aufgeführt. In Anhang C sind die zusätzlichen Dienste aufgeführt, die zu einer Standardinstallation hinzugefügt werden können.

In der Basisrichtlinie für Mitgliedsserver nicht enthaltene wichtige Dienste

Die Basisrichtlinie für Mitgliedsserver soll so restriktiv wie möglich sein. Aus diesem Grund wurden mehrere Dienste deaktiviert, die in Ihrer Umgebung möglicherweise erforderlich sind. Einige der bekanntesten sind im Folgenden aufgeführt.

SNMP-Dienst

Häufig muss für Verwaltungsanwendungen ein Agent auf jedem Server installiert werden. In der Regel verwenden diese Agents SNMP, um Warnungen an einen zentralen Verwaltungsserver weiterzuleiten. Wenn Verwaltungs-Agents erforderlich sind, sollten Sie überprüfen, ob für die Agents der SNMP-Dienst gestartet sein muss.

WMI-Dienste

Der WMI-Dienst (Windows Management Instrumentation oder Windows-Verwaltungsinstrumentation) ist in der Basisrichtlinie für Mitgliedsserver deaktiviert. Um logische Datenträger über die Computerverwaltung verwalten zu können, müssen Sie den WMI-Dienst aktivieren. Viele andere Anwendungen und Tools verwenden ebenfalls WMI.

Nachrichtendienst und Warnungsdienst

Diese Dienste hängen zwar nicht explizit voneinander ab, sie arbeiten jedoch zusammen, um administrative Warnungen zu senden. Der Nachrichtendienst sendet Warnungen, die durch den Warnungsdienst ausgelöst wurden. Wenn Sie Leistungsprotokolle und Warnungen verwenden, um Warnungen auszulösen, müssen Sie diese Dienste aktivieren.

Basisrichtlinie für Domänencontroller

Alle in der Domäne erstellten Domänencontroller werden automatisch der Organisationseinheit für Domänencontroller zugeordnet. Domänencontroller sollten nicht aus der Organisationseinheit für Domänencontroller entfernt werden, da auf diese Organisationseinheit spezielle Sicherheits-ACLs angewendet wurden.

Die Organisationseinheit für Domänencontroller ist eine übergeordnete Organisationseinheit und übernimmt deshalb nicht die in der Basisrichtlinie für Mitgliedsserver definierten Einstellungen. Daher wurde eine gesonderte Basisrichtlinie für Domänencontroller erstellt.

Die Konfigurationseinstellungen, die in der Basisrichtlinie für Domänencontroller implementiert sind, haben Auswirkungen auf die folgenden Abschnitte der Richtlinie:

- Überwachungsrichtlinie
- Sicherheitsoptionen
- Dienstkonfiguration

Anmerkung: Datei-ACLs, mit Ausnahme der in Anhang A aufgeführten System32-Dateien, und Registrierungs-ACLs wurden in diese Gruppenrichtlinie nicht aufgenommen, da sie definiert und implementiert werden, wenn ein Server unter Windows 2000 zu einem Domänencontroller heraufgestuft wird. Eine Sicherheitsvorlage mit dem Namen **Defltdc.inf** wird angewendet, wenn ein Windows 2000-basierter Server zu einem Domänencontroller heraufgestuft wird. Mit dieser Vorlage werden ACLs auf das Dateisystem und Registrierungsschlüssel für zusätzlich erstellte Dienste angewendet, um einen Domänencontroller zu unterstützen.

Basisrichtlinien für die Überwachung und Sicherheitsoptionen für Domänencontroller

Die Überwachungsrichtlinie und die Sicherheitsoptionen, die für die Domänencontroller konfiguriert werden, stimmen mit denen in der Basisrichtlinie überein (im Abschnitt "Basisrichtlinie für Mitgliedsserver" finden Sie Einzelheiten zu diesen Einstellungen).

Basisdienstrichtlinie für Domänencontroller

Bei den Diensten, die gestartet werden, handelt es sich um dieselben Dienste, die in der Basiskonfiguration für Mitgliedsserver definiert sind. Zusätzlich sind einige Dienste erforderlich, um die Funktionen des Domänencontrollers zu unterstützen.

Tabelle 4.13: Durch die Basisdienstrichtlinie für Domänencontroller aktivierte Dienste (zusätzlich zu den durch die Basisrichtlinie für Mitgliedsserver festgelegten Diensten)

Dienst	Starttyp	Grund für die Aufnahme in die Basisrichtlinie für Domänencontroller
Verteiltes Dateisystem	Automatisch	Ist für die Active Directory-Sysvol-Freigabe erforderlich
DNS-Server	Automatisch	Ist für das in Active Directory integrierte DNS erforderlich
Dateireplikation	Automatisch	Wird für die Dateireplikation zwischen Domänencontrollern benötigt
Kerberos-Schlüsselverteilungscenter	Automatisch	Ermöglicht Benutzern die Anmeldung am Netzwerk mithilfe von Kerberos, Version 5
NTLM-Sicherheitsdienst	Automatisch	Ermöglicht Clients die Anmeldung mithilfe der NTLM-Authentifizierung
RPC-Locator	Automatisch	Ermöglicht Domänencontrollern die Bereitstellung des RPC-Namensdienstes

In der Basisrichtlinie für Domänencontroller nicht enthaltene wichtige Dienste

Die Basisrichtlinie für Domänencontroller soll so restriktiv wie möglich sein. Aus diesem Grund wurden mehrere Dienste deaktiviert, die in Ihrer Umgebung möglicherweise erforderlich sind. Einige der bekanntesten, die Sie möglicherweise benötigen, sind im Folgenden aufgeführt.

Simple Mail Transport Protocol (SMTP)

Die standortübergreifende Replikation kann mithilfe von RPC oder SMTP erfolgen. Wenn Sie in Ihrer Umgebung SMTP für die Replikation verwenden, müssen Sie den SMTP-Dienst aktivieren.

Standortübergreifender Meldungsdienst

Dieser Dienst wird für die E-Mail-basierte Replikation zwischen Standorten verwendet. Jeder Transport, der für die Replikation verwendet werden soll, wird in einer gesonderten Add-In-DLL (Dynamic Link Library) definiert. Diese Add-In-DLLs werden in den standortübergreifenden Meldungsdienst geladen. Der standortübergreifende Meldungsdienst leitet Sende- und Empfangsanforderungen an die Add-In-DLLs des entsprechenden Transports weiter, der dann die Meldungen an den standortübergreifenden Meldungsdienst auf dem Zielcomputer weiterleitet. Wenn Sie in Ihrer Umgebung SMTP für die Replikation verwenden, müssen Sie diesen Dienst aktivieren.

IIS-Verwaltungsdienst

Wenn der SMTP-Dienst gestartet wurde, muss auch der IIS-Verwaltungsdienst gestartet werden, da der SMTP-Dienst vom IIS-Verwaltungsdienst abhängt.

Überwachung verteilter Verknüpfungen (Server)

Dieser Dienst wird verwendet, um Dateien auf NTFS-Datenträgern in einer Domäne zu überwachen. Er wird von Computern aufgerufen, auf denen der Dienst **Überwachung verteilter Verknüpfungen (Client)** ausgeführt wird. Diese Computer versuchen in regelmäßigen Abständen, den Dienst **Überwachung verteilter Verknüpfungen (Server)** abzurufen, auch wenn er deaktiviert wurde.

Anmerkung: Wenn Sie das Dienstprogramm dcdiag aus den Windows 2000-Supporttools ausführen, überprüft es, ob alle Dienste gestartet wurden, die normalerweise auf Domänencontrollern ausgeführt werden. Da einige Dienste durch die Basisrichtlinie für Domänencontroller deaktiviert wurden, meldet dcdiag Fehler. Dies ist ganz normal und deutet nicht auf ein Problem mit der Konfiguration hin.

Weitere grundlegende Sicherheitsaufgaben

Es können nicht alle Aufgaben, die zur Erhöhung der Sicherheit von Mitgliedsservern und Domänencontrollern erforderlich sind, mithilfe von Gruppenrichtlinien durchgeführt werden. Es gibt eine Reihe zusätzlicher Schritte, die Sie ausführen sollten, um die Sicherheit der Server insgesamt zu erhöhen.

Sichern vordefinierter Konten

Zu Windows 2000 gehören einige vordefinierte Benutzerkonten, die nicht gelöscht, aber umbenannt werden können. Zwei der am häufigsten verwendeten vordefinierten Konten in Windows 2000 sind das Administratorkonto und das Gastkonto. Auf Domänencontrollern und Mitgliedsservern ist das Gastkonto standardmäßig deaktiviert. Sie sollten diese Einstellung nicht ändern. Das vordefinierte Administratorkonto sollte umbenannt und die Beschreibung geändert werden, damit Angreifer einen Remoteserver nicht mithilfe eines bekannten Namens gefährden können. Viele schädliche Skripts verwenden das vordefinierte Administratorkonto als ersten Angriffspunkt auf einem Server.

Anmerkung: Das vordefinierte Administratorkonto kann mithilfe von Gruppenrichtlinien umbenannt werden. Diese Einstellung wurde nicht in die Basisrichtlinien implementiert, da Sie einen Namen wählen sollten, der unbekannt ist.

Sichern des lokalen Administratorkontos

Jeder Mitgliedsserver verfügt über eine lokale Kontendatenbank und ein lokales Administratorkonto, das Vollzugriff auf den Server gewährt. Deshalb ist dieses Konto sehr wichtig. Sie sollten dieses Konto umbenennen und sicherstellen, dass das Kennwort dafür komplex ist. Sie sollten außerdem sicherstellen, dass die lokalen Administratorkennwörter nicht auf andere Mitgliedsserver repliziert werden. Andernfalls kann ein Angreifer, der sich den Zugriff auf einen Mitgliedsserver verschafft hat, mit demselben Kennwort auch auf alle anderen Mitgliedsserver zugreifen.

Sie sollten die lokalen Administratorkonten nicht in die Gruppe **Domänen-Admins** aufnehmen, da sie dadurch mehr Berechtigungen erhalten, als für die Verwaltung von Mitgliedsservern erforderlich. Aus demselben Grund muss sichergestellt werden, dass nur lokale Konten für die Verwaltung von Mitgliedsservern verwendet werden.

Sichern von Dienstkonten

Windows 2000-Dienste werden üblicherweise mit dem lokalen Systemkonto ausgeführt, sie können aber auch mit einem Domänenbenutzerkonto oder einem lokalen Konto ausgeführt werden. Sie sollten möglichst immer lokale Konten statt Domänenbenutzerkonten verwenden. Ein Dienst wird immer im Sicherheitskontext des Dienstkontos ausgeführt. Wenn also ein Angreifer einen Dienst auf einem Mitgliedsserver gefährdet, kann das Dienstkonto für einen Angriff auf einen Domänencontroller verwendet werden. Wenn Sie festlegen, welches Konto als Dienstkonto verwendet werden soll, sollten Sie sicherstellen, dass nur die Rechte zugewiesen werden, die für einen erfolgreichen Betrieb des Dienstes erforderlich sind. In der folgenden Tabelle werden die Rechte einzelner Dienstkontotypen erläutert.

Tabelle 4.14: Rechte von Windows 2000-Konten in unterschiedlichen Umgebungen

Authentifizierung beim Ausführen des Dienstes auf Windows 2000-basierten Computern	Alle Windows 2000-basierten Server innerhalb der Gesamtstruktur	Anwendungen in mehreren Gesamtstrukturen mit NTLM-Vertrauensstellungen zwischen den Domänen
Dienstkonto für lokale Benutzer	Keine Netzwerkressourcen, nur lokaler Zugriff mit den Rechten des Kontos	Keine Netzwerkressourcen, nur lokaler Zugriff mit den Rechten des Kontos
Dienstkonto für Domänenbenutzer	Netzwerkzugriff als Domänenbenutzer, lokaler Zugriff mit den Rechten des Benutzers	Netzwerkzugriff als Domänenbenutzer, lokaler Zugriff mit den Rechten des Benutzers
Lokales System	Netzwerkzugriff als Benutzer, der mit dem Computerkonto authentifiziert wurde, lokaler Zugriff unter **Lokales System**	Keine Netzwerkressourcen aus anderen Gesamtstrukturen, lokaler Zugriff unter **Lokales System**

Alle Windows 2000-Standarddienste werden unter **Lokales System** ausgeführt, und diese Einstellung sollte nicht geändert werden. Alle zusätzlich zum System hinzugefügten Dienste, für die die Verwendung von Domänenkonten erforderlich ist, sollten vor ihrer Bereitstellung sorgfältig geprüft werden.

Überprüfen der Basiskonfiguration

Nachdem die Sicherheitseinstellungen zum ersten Mal auf einen Server angewendet wurden, sollten Sie überprüfen, ob bestimmte Sicherheitseinstellungen ordnungsgemäß konfiguriert wurden. Das Microsoft Security Baseline Analyzer Tool führt auf den Servern eine Reihe von Tests durch und warnt Sie vor möglichen Sicherheitsproblemen.

Überprüfen der Portkonfiguration

Sie sollten die endgültige Portkonfiguration überwachen und wissen, welche TCP- und UPD-Ports von den Servern unter Windows 2000 überwacht werden. Nachdem die Basisrichtlinien angewendet wurden, kann der Befehl **netstat** ausgeführt werden, um für jede Netzwerkschnittstellenkarte anzuzeigen, welche Ports der Server überwacht. In der Tabelle ist die erwartete Ausgabe von **netstat** für einen Mitgliedsserver dargestellt, auf den die Basisrichtlinie für Mitgliedsserver angewendet wurde:

Tabelle 4.15: Ports, die ein Mitgliedsserver überwacht, nachdem die Basisrichtlinie für Mitgliedsserver angewendet wurde

Protokoll	Lokale Adresse	Remoteadresse	Status
TCP	0.0.0.0:135	0.0.0.0:0	ABHÖREN
TCP	0.0.0.0:445	0.0.0.0:0	ABHÖREN
TCP	<IP-Adresse>:139	0.0.0.0:0	ABHÖREN
UDP	<IP-Adresse>:137	*.*	Nicht zutreffend
UDP	<IP-Adresse>:138	*.*	Nicht zutreffend
UDP	0.0.0.0:445	*.*	Nicht zutreffend
UDP	0.0.0.0:1027	*.*	Nicht zutreffend
UDP	0.0.0.0:1045	*.*	Nicht zutreffend

Sichern der Serverrollen

Nachdem Sie die Basisrichtlinie angewendet haben, sind die Server viel sicherer. Jetzt müssen Sie möglicherweise zusätzliche Einstellungen aktivieren, um die Funktionen der Basisrichtlinie zu erweitern. Für dieses Handbuch wurden vier unterschiedliche Mitgliedsserverrollen definiert:

Windows 2000-Anwendungsserver. Die sicherste und am stärksten gesperrte Serverrolle. Mit dem sicheren Anwendungsserver soll ein Server bereitgestellt werden, auf dem eine Anwendung wie Exchange oder SQL Server installiert werden kann. Diese Serverrolle kann nur für die Authentifizierung mit Domänencontrollern kommunizieren. Diese Rolle bildet die Grundlage für die anderen Rollen.

Windows 2000-Datei- und Druckserver. Damit soll die Sicherheit von Servern, die als Datei- und Druckserver dienen, deutlich erhöht werden.

Windows 2000-Infrastrukturserver. Damit soll die Sicherheit von Servern, die als DNS-, DHCP- und WINS-Server dienen, deutlich erhöht werden.

Windows 2000-IIS-Server. Damit soll die Sicherheit von Servern, die als IIS-Server dienen, deutlich erhöht werden. Für diese Rolle werden eine abgewandelte Version der Richtlinie für Anwendungsserver sowie das IIS Lockdowntool und das Tool URLScan verwendet.

Anmerkung: Die Anwendungsserverrolle wurde bewusst stark eingeschränkt. Um bestimmte Anwendungen zu installieren und auszuführen, müssen Sie möglicherweise die hier definierten Sicherheitseinstellungen ändern.

Anmerkung: Es ist möglich, die Vorlagen dieses Handbuchs zu ändern, um Vorlagen für andere Rollen zu erstellen. Dabei ist es sehr wichtig, die geänderten Vorlagen umfassend zu testen, um den gewünschten Sicherheitsgrad sicherzustellen.

Windows 2000-Anwendungsserverrolle

Die Einstellungen für die Anwendungsserverrolle hängen von der Anwendung ab, die Sie bereitstellen. Aus diesem Grund bleiben die Einstellungen der Basisrichtlinie für Mitgliedsserver unverändert. Deshalb ist die Anwendungsserverrolle stark eingeschränkt: Um bestimmte Anwendungen zu installieren und auszuführen, müssen Sie die hier definierten Sicherheitseinstellungen ändern. Die einfachste Methode ist es, eine neue Organisationseinheit für die Anwendung unter der Organisationseinheit für Anwendungsserver zu erstellen. Erstellen Sie dann eine Gruppenrichtlinie, mit der die Basiseinstellungen geändert werden, und importieren Sie die Richtlinie in die neue Organisationseinheit.

Windows 2000-Datei- und Druckserverrolle

Normalerweise nutzen in einer Unternehmensumgebung alle Benutzer Datei- und Druckdienste. Dementsprechend kann es sehr schwierig sein, eine möglichst hohe Sicherheit für die Serverrolle sicherzustellen. Durch die Datei- und Druckserverrichtlinie wird Folgendes ermöglicht:

Aktivieren des Spoolerdienstes, der zum Drucken verwendet wird.

Deaktivieren der Einstellung der Sicherheitsrichtlinie **Clientkommunikation digital signieren (immer)**. Wenn diese Einstellung nicht deaktiviert ist, können Clients zwar drucken, aber die Druckerwarteschlange kann nicht angezeigt werden. Bei dem Versuch, die Druckerwarteschlange anzuzeigen, wird eine Meldung ausgegeben: "Zugriff verweigert; keine Verbindung möglich"

Anmerkung: Der Spoolerdienst wird auf allen einen Druckauftrag startenden Computern sowie auf Druckservern verwendet. Die Standardeinstellungen der Basisrichtlinien für Mitgliedsserver und Domänencontroller führen dazu, dass auf diesen Computern keine Druckaufträge gestartet werden können.

Windows 2000-Infrastrukturserverrolle

Die Infrastrukturserverrolle unterstützt DNS-, DHCP- und WINS-Netzwerkdienste. Damit diese drei Dienste auf einem Mitgliedsserver ausgeführt werden können, werden durch die Richtlinie für Infrastrukturserver, zusätzlich zu den Diensten in der Basisrichtlinie für Mitgliedsserver, die folgenden Dienste aktiviert:

Tabelle 4.16: Dienste, die durch die Richtlinie für die Infrastrukturserverrolle hinzugefügt werden

Dienst	Starttyp	Grund für die Aufnahme in die Richtlinie für die Infrastrukturserverrolle
DHCPServer	Automatisch	Um Clients DHCP-Dienste bereitzustellen
DNS	Automatisch	Um Clients DNS-Dienste bereitzustellen
NTLMSSP	Automatisch	Um RPC-Programme zu sichern, die keine Named Pipes für den Transport verwenden
WINS	Automatisch	Um Clients (WINS-Dienste) bereitzustellen

Windows 2000-IIS-Serverrolle

Mit der IIS-Serverrolle werden die Funktionen von Webservern auf Windows 2000-basierten Servern bereitgestellt. Durch die Gruppenrichtlinie für die IIS-Serverrolle werden die folgenden Dienste zur Basisrichtlinie für Mitgliedsserver hinzugefügt:

Tabelle 4.17: Dienste, die durch die Richtlinie für die IIS-Serverrolle hinzugefügt werden

Dienst	Starttyp	Grund für die Aufnahme in die Richtlinie für die IIS-Serverrolle
IISAdmin	Automatisch	Verwaltung des Webservers
W3SVC	Automatisch	Stellt Webserverfunktionen bereit

Außerdem wird durch die Gruppenrichtlinie für die IIS-Serverrolle der Registrierungswert **SynAttackProtect** auf **1** festgelegt.

Das IIS Lockdowntool

IIS-Server bieten viele Funktionen. Um eine möglichst hohe Sicherheit für IIS-Server zu erzielen, sollten Sie sich jedoch auf die erforderlichen Funktionen beschränken. Dies geht am einfachsten mit dem IIS Lockdowntool. Das IIS Lockdowntool ist ein Dienstprogramm, das in hohem Maße konfiguriert werden kann und mit dem Sie die erforderlichen Funktionen des Webservers angeben können. Es entfernt dann alle Funktionen, die für einen bestimmten Webserver nicht erforderlich sind. Sie sollten natürlich alle Änderungen sorgfältig testen, bevor diese in einer Produktionsumgebung implementiert werden.

Anmerkung: Das IIS Lockdowntool steht als Teil des Security Toolkits und auf der Microsoft-Website zum Thema Sicherheit zur Verfügung. Weitere Informationen finden Sie im gleichnamigen Abschnitt am Ende dieses Kapitels.

Das IIS Lockdowntool kann viele Schritte ausführen, um Webserver zu sichern. Dazu zählen u. a. folgende:

- Sperren von Dateien
- Deaktivieren von Diensten und Komponenten
- Installieren von URLScan
- Entfernen unnötiger ISAPI-DLL-Skriptzuordnungen (Internet Server Application Programming Interface)
- Entfernen nicht erforderlicher Verzeichnisse
- Ändern von ACLs

Sie können das IIS Lockdowntool verwenden, um verschiede Arten von IIS-Serverrollen zu sichern. Für jeden Server sollten Sie die restriktivste Rolle auswählen, die die Anforderungen des Webservers erfüllt.

So sichern Sie einen statischen Webserver mit dem IIS Lockdowntool

1. Starten Sie **IISLockd.exe**.
2. Klicken Sie auf **Next**.
3. Wählen Sie **I agree** aus, und klicken Sie dann auf **Next**.
4. Wählen Sie **Static Web server** aus, und klicken Sie dann auf **Next**.
5. Stellen Sie sicher, dass **Install URLScan filter on the server** ausgewählt ist, und klicken Sie dann auf **Next**.
6. Klicken Sie auf **Next**.
7. Wenn das Dialogfeld **Digital Signature Not Found** angezeigt wird, klicken Sie auf **Yes**.
8. Klicken Sie auf **Next**.
9. Klicken Sie auf **Finish**.

Wenn Sie den IIS-Server als statischen Webserver einrichten, werden die folgenden Änderungen vorgenommen:

Die Skriptzuordnung für die Index Server-Weboberfläche (IDQ, HTW, IDA) wird deaktiviert.

Die Skriptzuordnung für Internet Data Connector (IDC) wird deaktiviert.

Die Skriptzuordnung für serverseitige Include-Dateien (SHTML, SHTM, STM) wird deaktiviert.

Die Skriptzuordnung für die HTR-Skripterstellung wird deaktiviert.

Die ASP-Skriptzuordnung (Active Server Pages) wird deaktiviert.

Die Skriptzuordnung für das Internetdrucken (PRINTER) wird deaktiviert.

Das virtuelle Verzeichnis für Drucker wird entfernt.

Web Distributed Authoring and Versioning (WebDAV) wird deaktiviert.

Die Dateiberechtigungen werden so festgelegt, dass anonyme IIS-Benutzer nicht in Verzeichnisse mit Webinhalten schreiben können.

Die Dateiberechtigungen werden so festgelegt, dass anonyme IIS-Benutzer keine Systemprogramme ausführen können.

Der URLScan-Filter wird auf dem Server installiert.

Das virtuelle Verzeichnis für Skripts wird entfernt.

Das virtuelle Verzeichnis **MSADC** wird entfernt.

Das virtuelle Verzeichnis **IIS Samples** wird entfernt.

Das virtuelle Verzeichnis **IISAdmin** wird entfernt.

Das virtuelle Verzeichnis **IISHelp** wird entfernt.

Anmerkung: Weitere Informationen zu URLScan finden Sie in Kapitel 6, "Überwachung und Erkennung von Eindringversuchen".

Weitere Sicherheitseinstellungen für die IIS-Serverrolle

Das IIS Lockdowntool erhöht deutlich die Sicherheit von IIS-Servern. Es gibt jedoch weitere Schritte, durch die die Server mit dem IIS-Dienst von Windows 2000 weiter gesichert werden können.

Festlegen von Beschränkungen für IP-Adressen/DNS-Adressen

Mit dieser Einstellung wird sichergestellt, dass nur Systeme mit bestimmten IP-Adressen oder DNS-Namen auf den Webserver zugreifen können. Das Festlegen von Beschränkungen für IP- und DNS-Adressen erfolgt selten, ist aber eine weitere Möglichkeit zur Beschränkung von Websites auf bestimmte Benutzer. Wenn jedoch für die Beschränkungen DNS-Namen anstelle von IP-Adressen verwendet werden, muss IIS eine DNS-Suche durchführen, die sehr zeitintensiv sein kann.

Verwenden eines lokalen anonymen Kontos

Standardmäßig ist das anonyme Konto, das für den Zugriff auf IIS verwendet wird, ein Domänenkonto mit dem Namen **IUSR**_*Computername*. Zur Erhöhung der Sicherheit sollten Sie das Standardkonto deaktivieren und durch ein lokales Konto ersetzen. Dabei sollten Sie die Richtlinien für sichere Kennwörter beachten. Wenn dann ein Angreifer das Kennwort für das Konto ermittelt hat, kann er nur auf das lokale System zugreifen. Es ist wichtig, die auf diese Weise konfigurierten IIS-Server sorgfältig zu testen, da für einige Webanwendungen statt eines lokalen Kontos ein Domänenkonto erforderlich sein kann.

Anmerkung: Sie können das Konto **IUSR**_*Computername* löschen, Sie können das Konto jedoch auch deaktivieren und als "Lockvogelkonto" bestehen lassen.

Implementieren von IPSec-Filtern für mehrfach vernetzte Webserver

Das im Lieferumfang von Windows 2000 enthaltene IPSec-Richtlinienmodul ist ein nützliches Tool zum Erhöhen der Sicherheit der Webarchitektur insgesamt, insbesondere aber der Sicherheit der Webserver. Normalerweise wird die IPSec-Richtlinie für die Schaffung eines sicheren Kommunikationsweges zwischen zwei Hoststandorten oder zwei Remotestandorten verwendet. Sie kann aber auch aufgrund ihrer Protokoll- und Portfilterfunktionen verwendet werden.

Sie können Filterlisten zusammen mit Filteraktionen verwenden, um den Datenverkehr zu und von einem Webserver zu steuern. Sie könnten z. B. zwei Filterlisten erstellen: eine für den Datenverkehr von allen Zielen für Port 80 und eine für den Datenverkehr von allen Zielen für alle Ports. Dann definieren Sie Filteraktionen, die den Datenverkehr zulassen, der mit der ersten Filterliste übereinstimmt, und den Datenverkehr blockieren, der mit der zweiten Filterliste übereinstimmt.

IPSec-Richtlinien werden mithilfe von Gruppenrichtlinien implementiert. Sie wurden nicht in die Richtlinien in diesem Handbuch aufgenommen, da sie je nach Umgebung anders implementiert werden.

Änderungen an der empfohlenen Umgebung

Die Empfehlungen in diesem Kapitel sollen Ihnen das Erstellen einer deutlich sichereren Umgebung für Windows 2000-basierte Server erleichtern. Einige der Änderungen sind jedoch möglicherweise für Ihre Umgebung nicht geeignet. Im Folgenden werden zwei Fälle betrachtet, in denen 1) weitere administrative Funktionen erforderlich sind und 2) das Dienstprogramm Hfnetchk nicht verwendet wird.

Änderungen der Verwaltungsfunktionen

Durch die standardmäßigen Basisrichtlinien für Mitgliedsserver und Domänencontroller bietet die Umgebung weniger Remoteverwaltungsfunktionen (und auch weniger lokale Verwaltungsfunktionen). Die Remoteverwaltung über das MMC-Snap-In (Microsoft Management Console) **Computerverwaltung** funktioniert nicht mit den standardmäßigen Basisrichtlinien, da einige MMC-bezogene Dienste deaktiviert sind.

Mit den Basisrichtlinien werden der Serverdienst und der Remote-Registrierungsdienst aktiviert. Dadurch kann das Snap-In **Computerverwaltung** eine Remoteverbindung mit anderen Computern herstellen und die folgenden Elemente verwalten:

- Freigegebene Ordner
- Lokale Benutzer und Gruppen
- Alles unter **Speicherverwaltung** außer **Logische Laufwerke** und **Wechselmedienverwaltung**
- Geräte-Manager
- Ereignisanzeige
- Leistungsprotokolle und Warnungen

WMI ist in den Basisrichtlinien nicht aktiviert. Dadurch werden die folgenden Elemente nicht verwaltet:

- WMI
- **Logische Laufwerke** unter **Speicherverwaltung**

Wenn eine lokale oder Remoteverwaltung für diese Elemente erforderlich ist, sollten Sie den WMI-Dienst aktivieren.

Auf die Wechselmedienverwaltung ist kein Remotezugriff möglich, wenn nur die Dienste der Basisrichtlinie für Mitgliedsserver gestartet wurden. Wenn der Wechselmediendienst auf dem Remoteserver nicht gestartet wird, generiert der Remoteserver im Ereignisprotokoll eine DCOM-Fehlermeldung, die darauf hinweist, dass der Dienst nicht verfügbar ist.

Anmerkung: Wenn Sie die oben aufgeführten Dienste aktivieren, um die Verwaltung zu ermöglichen, sollten Sie sie nur in der inkrementellen Richtlinie für die Serverrolle aktivieren, für die die Dienste erforderlich sind.

Anmerkung: Für einige Verwaltungsprogramme kann es erforderlich sein, die Sicherheitseinstellungen auf dem Client zu ändern, auf dem Sie das Tool ausführen. Beispielsweise verwenden einige Tools möglicherweise NTLM-Authentifizierung, und mit der Basisrichtlinie werden die Server so konfiguriert, dass nur NTLM, Version 2, zulässig ist. Weitere Informationen dazu finden Sie im Abschnitt "LAN Manager-Authentifizierungsebene" in diesem Kapitel.

Änderungen der Sicherheit bei fehlender Implementierung von Hfnetchk

Mit dem Tool **Hfnetchk** können Sie überprüfen, welche Patches auf den einzelnen Servern in der Organisation installiert wurden. Es ist sehr empfehlenswert, ein Tool wie Hfnetchk zu verwenden, da Sie damit die Sicherheit der Umgebung insgesamt erhöhen können.

Wenn Sie jedoch Hfnetchk nicht implementieren, können Sie den Remote-Registrierungsdienst und den Serverdienst in der Basisrichtlinie für Mitgliedsserver deaktivieren. In der Basisrichtlinie für Domänencontroller können Sie den Remote-Registrierungsdienst deaktivieren.

Wenn Sie diese Dienste in der Basisrichtlinie für Mitgliedsserver deaktivieren, müssen Sie sie für einige Serverrollen aktivieren:

Tabelle 4.18: Dienste, die zu den Gruppenrichtlinienobjekten für Serverrollen hinzugefügt werden müssen, wenn der Remote-Registrierungsdienst und der Serverdienst in der Basisrichtlinie für Mitgliedsserver deaktiviert wurden

Serverrolle	Zu aktivierender Dienst	Grund
Datei- und Druckserver	Server	Um Dateifreigaben zu ermöglichen
Infrastrukturserver	Server	Damit WINS ordnungsgemäß funktioniert
Infrastrukturserver	Remote-Registrierung	Damit der WINS-Manager den Status der WINS-Server anzeigen kann

Wenn Sie den Serverdienst und den Remote-Registrierungsdienst deaktivieren, können Sie nur sehr wenige der Remoteverwaltungsfunktionen nutzen.

Zusammenfassung

Windows 2000-basierte Server bieten standardmäßig eine große Anzahl von Funktionen. Jedoch sind viele dieser Funktionen nicht für alle Server erforderlich. Indem Sie die Tasks definieren, die die Server ausführen, können Sie die Elemente deaktivieren, die nicht erforderlich sind, und auf diese Weise die Sicherheit der Umgebung erhöhen. Mithilfe der in diesem Kapitel empfohlenen Schritte können Sie die Sicherheit der Umgebung bereits deutlich erhöhen.

Weitere Informationen

Informationen zum Sichern des Windows 2000-TCP/IP-Stacks:

http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/website/dosrv.asp (englischsprachig)

Whitepaper zu den standardmäßigen Zugriffssteuerungseinstellungen in Windows 2000:

http://www.microsoft.com/windows2000/techinfo/planning/security/secdefs.asp (englischsprachig)

Microsoft Security Toolkit (englischsprachig):

http://www.microsoft.com/germany/themen/security/default.htm

Glossar der Windows 2000-Dienste

http://www.microsoft.com/windows2000/techinfo/howitworks/management/w2kservices.asp (englischsprachig)

Originaltitel: Chapter 5 – Patch Management

5

Patchverwaltung

Betriebssysteme und Anwendungen sind in vielen Fällen äußerst komplex. Sie können sich aus Millionen von Codezeilen zusammensetzen, die von vielen verschiedenen Programmierern geschrieben wurden. Es ist überaus wichtig, dass die Software zuverlässig funktioniert und die Sicherheit bzw. Stabilität der IT-Umgebung nicht beeinträchtigt. Um die Gefahr von Problemen zu minimieren, werden Programme vor der Veröffentlichung umfassend getestet. Angreifer suchen jedoch permanent nach Schwachstellen in der Software, und es ist nicht möglich, alle zukünftigen Angriffe vorherzusehen.

Softwareunternehmen geben Patches für Schwachstellen im Code oder in der Implementierung heraus, die erst nach der Veröffentlichung des Produkts aufgedeckt werden. Diese Probleme treten mehr und mehr im Bereich der Sicherheit auf, da die Zahl der Angreifer steigt, die angewandten Methoden komplizierter werden und neuer schädlicher Code erstellt wird, mit dem Sicherheitslücken ausgenutzt werden. Patches können jedoch auch einfach dazu dienen, dem Produkt Funktionalität hinzuzufügen

Sicherheitspatches sind für die meisten Organisationen mit besonderen Schwierigkeiten verbunden. Nachdem eine Schwachstelle in der Software bekannt gegeben wurde, werden die Informationen im Allgemeinen von Angreifern sofort im Internet verbreitet. Softwareunternehmen versuchen daher, so bald wie möglich ein Sicherheitspatch zu veröffentlichen. Bevor Sie den Patch bereitstellen, ist die Sicherheit, von der Sie abhängig sind und die Sie von der Software erwarten, möglicherweise in hohem Maße beeinträchtigt.

Ob Ihr Unternehmen über Tausende von Computern oder nur über eine geringe Anzahl von Computern verfügt, es kann äußerst schwierig und zeitaufwändig sein, alle verfügbaren Patches zu verwalten, zu bestimmen, welche Patches für Ihre Umgebung relevant sind, und abzuschätzen, wie viele Tests vor der Bereitstellung durchgeführt werden können.

Dieses Kapitel soll Ihnen dabei helfen, die Sicherheit Ihrer Windows 2000-basierten Server aufrechtzuerhalten. Die beschriebenen Prozesse können jedoch auch zur Patchverwaltung für alle Softwareaktualisierungen angewandt werden. Sie sollten sich mit dem speziellen Hersteller in Verbindung setzen, um sich über Einzelheiten zu den jeweiligen Softwareaktualisierungen zu informieren.

Terminologie

In diesem Handbuch haben die Begriffe "Patch", "Service Pack" und "Hotfix" die gleiche Bedeutung und werden für Änderungen an der Software nach der Veröffentlichung verwendet. Die Begriffe sind austauschbar, da der Bereitstellungsprozess in allen drei Fällen derselbe ist. Jeder Begriff kann jedoch genauer definiert werden:

Service Packs

Mit Service Packs werden die Produkte auf dem aktuellsten Stand gehalten, bekannte Probleme werden behoben, und mitunter wird auch die Funktionalität des Computers erweitert. Sie enthalten Tools, Treiber und Updates, einschließlich Erweiterungen, die nach der Veröffentlichung des Produkts entwickelt wurden. Sie liegen zum einfachen Downloaden in gepackter Version vor.

Service Packs sind produktspezifisch, d. h. für jedes Produkt gibt es separate Service Packs. Für verschiedene Versionen desselben Produkts wird jedoch im Allgemeinen dasselbe Service Pack verwendet. Für die Aktualisierung von Windows 2000 Server und von Windows 2000 Professional wird z. B. dasselbe Service Pack verwendet.

Service Packs sind zudem kumulativ – jedes neue Service Pack enthält alle Fixes der früheren Service Packs sowie alle neuen Fixes und Systemänderungen, die seitdem empfohlen wurden. Sie müssen vor dem Installieren des neuesten Service Packs kein früheres Service Pack installieren.

Hotfixes oder QFEs

Quick Fix Engineering (QFE) ist eine Microsoft-Gruppe, die Hotfixes bzw. Codepatches für Produkte herstellt. Die Hotfixes werden einzelnen Kunden bei schwerwiegenden Problemen bereitgestellt, für die keine Problemumgehung (workaround) möglich ist. Gelegentlich werden Hotfixes in technischen Dokumentationen als QFEs bezeichnet.

Für Hotfixes werden keine umfassenden Regressionstests durchgeführt, und sie sind sehr problemspezifisch. Sie sollten nur dann einen Hotfix anwenden, wenn bei Ihnen exakt das Problem auftritt, das mit dem Hotfix behoben werden soll, und wenn Sie die aktuelle Softwareversion mit dem neuesten Service Pack verwenden.

In regelmäßigen Abständen werden mehrere Hotfixes in Service Packs integriert. In diesen Fällen werden sie umfassend getestet und allen Kunden zur Verfügung gestellt.

Sicherheitspatches

Mit Sicherheitspatches sollen Sicherheitslücken beseitigt werden. Angreifer, die ins System einzudringen versuchen, können diese Sicherheitslücken ausnutzen. Sicherheitspatches ähneln Hotfixes, werden jedoch unter den entsprechenden Bedingungen als zwingend erforderlich angesehen und müssen umgehend bereitgestellt werden.

Viele veröffentlichte Sicherheitsupdates sind für clientseitige Probleme (meist für Probleme mit dem Browser) vorgesehen. In manchen Fällen sind sie für eine Serverinstallation relevant, in anderen nicht. Um Ihre derzeitige Clientbasis zu aktualisieren, benötigen Sie Clientpatches, und um einen Clientinstallationsbereich auf einem Server zu aktualisieren, benötigen Sie den Administratorpatch.

Patchverwaltung in Ihrer Organisation

Auf welche Art und Weise Sie die Patchverwaltung implementieren, hängt in hohem Maße von der Größe und Komplexität Ihrer Organisation ab. Sie müssen jedoch wissen, wie wichtig die Patchverwaltung ist und wie sie sich in die gesamte Risikomanagementstrategie (Risk Management) Ihres Unternehmens einfügt. Wenn Sie sich z. B. dazu entschließen, die Risiken um jeden Preis zu minimieren, können Sie eine Strategie verfolgen, nach der alle Produktionssysteme heruntergefahren werden, sobald eine neue Schwachstelle in Ihrer Software entdeckt wird. Sie haben anschließend die Möglichkeit, die Systeme erst dann neu zu starten, nachdem für das Sicherheitspatch umfassende Tests durchgeführt wurden und nachdem es in der gesamten Organisation bereitgestellt wurde. Dieser Prozess ist sowohl sehr zeitaufwändig als auch teuer und von daher für viele Organisationen nicht praktikabel.

Sie müssen für den gesamten Prozess der Patchverwaltung die Risiken gegen die Kosten für die entsprechenden Gegenmaßnahmen abwägen. Nachdem eine Sicherheitslücke bekannt gegeben wurde, vergeht möglicherweise etwas Zeit, bevor ein Patch veröffentlich wird. Sie müssen das von der Schwachstelle ausgehende erhöhte Risiko abschätzen und entscheiden, welche Maßnahmen vor den Tests und der Bereitstellung eines Patches ergriffen werden sollen. Diese Maßnahmen können z. B. darin bestehen, Dienste zu deaktivieren, Systeme offline zu schalten oder den Zugriff nach Bedarf auf interne Benutzer oder andere Gruppen zu beschränken. Nach der Veröffentlichung eines Patches müssen Sie das Risiko einer sofortigen Bereitstellung gegen die Kosten abwägen, die entstehen, wenn Dienste für die Zeit, in der Sie Tests durchführen. Stellen Sie sicher, dass der Patch keine negativen Auswirkungen auf das System hat, deaktiviert oder ungeschützt bleiben. Wenn Sie sich zum Durchführen von Tests entscheiden, müssen Sie ermitteln, wie viele Tests akzeptabel sind, bevor die Risiken der Nichtbereitstellung größer sind als die der Bereitstellung.

Anmerkung: Ihre Organisation sollte einen Prozess zum Änderungsmanagement (Change Management) implementieren. Das Microsoft Operations Framework (MOF) enthält einen Prozess zum Änderungsmanagement, der dem Prozess in Ihrer Organisation zugrunde gelegt werden kann. Am Ende dieses Kapitels finden Sie im Abschnitt "Weitere Informationen" einen Hyperlink zum MOF.

Beurteilen der aktuellen Umgebung

Patches werden in einer Organisation häufig uneinheitlich angewendet. Darüber hinaus wird nicht dokumentiert, warum, wann und wo sie bereitgestellt wurden. Bevor Sie die Sicherheit Ihrer Umgebung richtig verwalten können, müssen Sie den aktuellen Status genau kennen. Für eine Patchverwaltung müssen Sie mindestens über die folgenden Informationen verfügen:

Welche Systeme werden in Ihrer Umgebung verwendet?

- Betriebssystem, einschließlich Version
- Patchstufe (Version des Service Packs, Hotfixes und andere Änderungen)
- Funktion
- Anwendungen
- Besitz- und Kontaktinformationen

Über welchen Hardwarebestand verfügen Sie in Ihrer Umgebung, und wie hoch ist der entsprechende Wert?

Welches sind die bekannten Risiken, und welchen Prozess wenden Sie an, um neue Risiken oder veränderte Risiken zu erkennen.

Welches sind die bekannten Schwachstellen, und welchen Prozess wenden Sie an, um neue oder veränderte Schwachstellen zu erkennen.

Welche Gegenmaßnahmen wurden angewandt?

Sie sollten auf jeden Fall diese Informationen sämtlichen Benutzern zur Verfügung stellen, die an dem Prozess der Patchverwaltung beteiligt sind. Sie sollten außerdem sicherstellen, dass die Informationen immer aktuell sind.

Wenn Sie Ihren Bestand, die Schwachstellen, die Risiken und die Konfiguration Ihrer Umgebung kennen, können Sie feststellen, welche Risiken und Schwachstellen für Ihr Unternehmen relevant sind.

Systeme für Sicherheitsupdates

In vielen Umgebungen kann es von Vorteil sein, über spezielle Computer zu verfügen, auf denen Sie zahlreiche Schritte des Patchverwaltungsprozesses ausführen können. Diese Systeme stellen spezielle Speicherorte zum Speichern von Sicherheitstools, Patches, Hotfixes, Service Packs und Dokumentationen zur Verfügung. Auf diesen Systemen können Sie Patches analysieren, abrufen und bereitstellen. In diesem Handbuch werden diese Systeme als "Systeme für Sicherheitsupdates" bezeichnet.

Sie sollten sicherstellen, dass sich Ihre Systeme für Sicherheitsupdates auf mindestens einem dedizierten Computer befinden, der umfassend gesteuert und gesichert werden kann, da die Systeme zum Bereitstellen und Verwalten von Sicherheitspatches für alle Systeme in Ihrer Umgebung verwendet werden. Bei den Systemen für Sicherheitsupdates muss es sich normalerweise nicht um Server mit einer hohen Leistung handeln, da die Verarbeitungslast im Allgemeinen sehr gering ist. Diese Computer müssen jedoch eine hohe Verfügbarkeit aufweisen, damit Ihre Umgebung mit den neuesten Patches auf dem aktuellsten Stand gehalten werden kann.

Um ein System für Sicherheitsupdates ordnungsgemäß bereitstellen zu können, muss der Computer über direkten oder indirekten Internetzugriff verfügen, damit die neuesten Patchinformationen aus vertrauenswürdigen Quellen gedownloadet werden können. Zudem muss der Computer Zugriff auf jeden Computer haben, der auf dem aktuellsten Stand gehalten werden soll.

Weiter unten in diesem Kapitel werden Beispiele und Beispielskripts verwendet, die von einem System für Sicherheitsupdates ausgeführt werden sollten.

Anmerkung: Im MOF werden Updatesysteme im Zusammenhang mit dem Prozess zum Versionsmanagement (Release Management) vorgestellt.

Kommunikation

Wenn Ihr Unternehmen klein ist, muss möglicherweise nur eine Person damit beauftragt werden, die Patches auf dem neuesten Stand zu halten, Patches zu testen und zu installieren sowie die verschiedenen Protokolldateien zu lesen. In größeren Umgebungen sind normalerweise mehrere Personen für verschiedene Aspekte der Sicherheit zuständig. Es ist äußerst wichtig, dass alle an der Patchverwaltung beteiligten Personen effektiv miteinander kommunizieren. So kann sichergestellt werden, dass Entscheidungen ohne doppelten Aufwand getroffen und keine Schritte des Prozesses vergessen werden.

Patch- und Änderungsmanagement

Die Patchverwaltung ist nur ein Teil des Änderungsmanagements. Wenn Sie in Ihrer Organisation bereits über einen Prozess für das Änderungsmanagement verfügen, müssen Sie nicht den gesamten Prozess der Patchverwaltung neu erstellen. Es kann jedoch sehr nützlich sein, dieses Kapitel mit speziellen Informationen zum Prozess der Patchverwaltung zu lesen.

Ein zuverlässiges Verfahren zur Kontrolle von Änderungen ist durch Folgendes gekennzeichnet: einen identifizierter Besitzer für die Änderung, eine Option für Feedback zur Änderung, eine Überwachungsliste für Änderungen, eine festgelegte Ankündigungs- und Überprüfungsdauer, Testverfahren und einen genauen Alternativplan.

Microsoft Security Toolkit

Das Microsoft Security Toolkit kann sehr hilfreich sein, wenn Sie die erforderlichen Service Packs und Hotfixes downloaden möchten, um Ihre Server auf dem aktuellsten Stand zu halten. Es enthält wichtige Sicherheitsinformationen, aktuelle Service Packs sowie wichtige Sicherheitspatches für Windows NT 4.0, Windows 2000, IIS und Internet Explorer. Zudem enthält es das Benachrichtigungstool für wichtige Aktualisierungen (Critical Update notification tool). Mit diesem Tool können Sie zur Windows Update-Site wechseln, um sicherzustellen, dass alle neuesten Patches installiert sind. Das Security Toolkit ist über TechNet verfügbar.

Patchverwaltungsprozesse

Der Prozess der Patchverwaltung ist anhand eines Flussdiagramms in Abbildung 5.1 dargestellt.

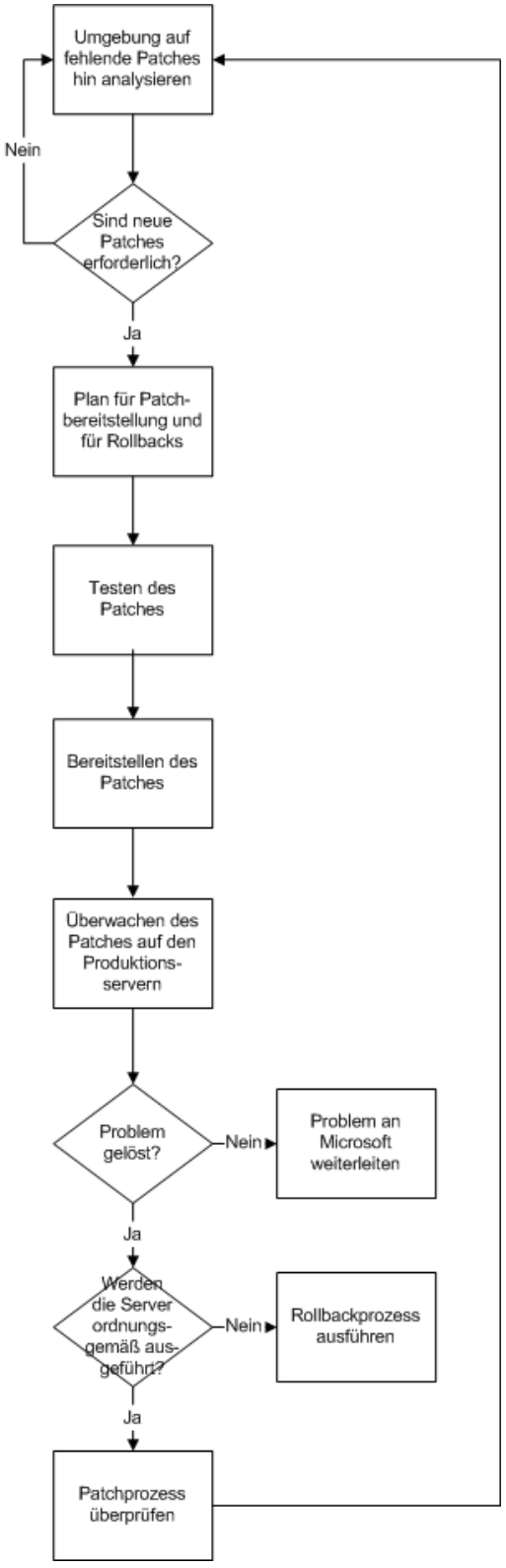


Abbildung 5.1: Patchverwaltungsprozess

Die einzelnen Schritte ausführlicher erläutert:

Analysieren. Analysieren Sie die aktuelle Umgebung und die potenziellen Risiken. Ermitteln Sie, welche Patches Sie bereitstellen müssen, um die Risiken für Ihre Umgebung zu reduzieren.

Planen. Ermitteln Sie, welche Patches für die ermittelten potenziellen Risiken und Schwachstellen bereitgestellt werden sollten. Bestimmen Sie die Personen, die die Tests und die Bereitstellung sowie die damit verbundenen Schritte durchführen sollen.

Testen. Gehen Sie die verfügbaren Patches durch, und teilen Sie diese für Ihre Umgebung in Kategorien ein. Testen Sie alle gefundenen Patches, um sicherzustellen, dass sie in Ihrer Umgebung ohne unerwünschte Nebeneffekte ordnungsgemäß ausgeführt werden können. Machen Sie sich mit der Funktion des Patches und mit seinen Auswirkungen auf die Umgebung vertraut. Überprüfen Sie, ob der Patch wie geplant ausgeführt werden kann.

Bereitstellen. Stellen Sie die richtigen Patches bereit, um die Sicherheit Ihrer Umgebung zu gewährleisten.

Überwachen. Überprüfen Sie nach dem Bereitstellen der Patches alle Systeme, um sicherzustellen, dass keine unerwünschten Nebeneffekte aufgetreten sind.

Überprüfen. Während des laufenden Prozesses müssen Sie regelmäßig neu herausgegebene Patches sowie Ihre Umgebung überprüfen und feststellen, welche Patches für Ihr Unternehmen erforderlich sind. Wenn Sie dabei neue Patches finden, die erforderlich sind, müssen Sie noch einmal mit Schritt 1 beginnen.

Anmerkung: Sie sollten auf jeden Fall vor dem Bereitstellen der Patches alle Produktionssysteme sichern.

Analysieren der Umgebung in Bezug auf fehlende Patches

Während eines laufenden Prozesses müssen Sie sicherstellen, dass Sie in Bezug auf Patches auf dem aktuellsten Stand sind. In einigen Fällen wird ein neuer Patch veröffentlicht, den Sie auf allen Servern installieren müssen. In anderen Fällen wird ein neuer Server online geschaltet, und Sie müssen darauf die entsprechenden Patches installieren. Sie sollten alle Server fortlaufend analysieren, um sicherzustellen, dass sie über die erforderlichen neuesten Patches verfügen. Es gibt eine Reihe von Tools, die Sie hierfür verwenden können.

Microsoft Network Security Hotfix Checker (Hfnetchk)

Hfnetchk ist ein Befehlszeilenprogramm, mit dem Sie überprüfen können, ob die aktuelle Konfiguration auf den Servern auf dem neuesten Stand ist und die Server über alle entsprechenden Sicherheitspatches verfügen. Mit diesem Tool wird eine XML-Datenbank (Extensible Markup Language) direkt von Microsoft gedownloadet, die eine Liste der neuesten Hotfixes enthält, mit denen Sie gegebenenfalls die Sicherheit Ihrer Server gewährleisten können. Wenn Sie über keine Verbindung mit dem Internet verfügen, verwendet Hfnetchk eine lokale XML-Datenbank. Diese Datenbank ist jedoch möglicherweise nicht aktuell.

Anmerkung: Um Hfnetchk verwenden zu können, müssen Sie über Administratorzugriff auf die Computer verfügen, die auf fehlende Patches hin überprüft werden (entweder als lokaler Administrator oder als Domänenadministrator).

Das Tool enthält eine Reihe von Befehlszeilenoptionen, die in der folgenden Tabelle aufgelistet sind.

Tabelle 5.1: Hfnetchk-Optionen

Hfnetchk-Option	Funktion
-about	Informationen zu Hfnetchk.
-h <hostname>	Gibt den NetBIOS-Namen des Computers an, der gescannt werden soll. Die Standardeinstellung ist **localhost**.
-fh <hostfile>	Gibt den Namen einer Datei an, die den NetBIOS-Namen des Computers enthält, der gescannt werden soll. Ein Name pro Zeile, max. 256 pro Datei.
-i <ipaddress>	Gibt die IP-Adresse eines Computers an, der gescannt werden soll.
-fip <ipfile>	Gibt den Namen einer Datei an, die Adressen enthält, die gescannt werden sollen. Ein IP-Adresse pro Zeile, max. 256 pro Datei.
-r <range>	Gibt den IP-Adressbereich an, der gescannt werden soll; der Adressbereich beginnt mit **ipaddress1** und endet mit **ipaddress2**. **ipaddress1** und **ipaddress2** sind im Bereich enthalten.
-d >domain_name>	Gibt den Namen der Domäne an, die gescannt werden soll. Alle Computer in der Domäne werden gescannt.
-n <network>	Alle Systeme auf dem lokalen Netzwerk werden gescannt (alle Hosts in der Netzwerkumgebung).
-history <level>	Für normalen Betrieb nicht erforderlich.
-t <threads>	Anzahl der zum Ausführen der Scans verwendeten Threads. Es sind Werte von 1 bis 128 möglich. Der Standardwert ist **64**.
-o <output>	Gibt das gewünschte Ausgabeformat an. (**tab**) Ausgaben im tabstoppgetrennten Format. (**wrap**) Ausgaben mit Zeilenumbrüchen. Die Standardeinstellung ist **wrap**.
-x <datasource>	Gibt die XML-Datenquelle mit den Hotfixinformationen an. Bei dem Speicherort kann es sich um einen XML-Dateinamen, eine komprimierte XML-CAB-Datei oder einen URL handeln. Der Standardwert ist **mssecure.cab** auf der Microsoft-Website.
-s <suppress>	Die Meldungen NOTE (ANMERKUNG) und WARNING (WARNUNG) werden nicht angezeigt. 1 = nur die Meldungen NOTE unterdrücken, 2 = Meldungen NOTE und WARNING unterdrücken. Standardmäßig werden alle Meldungen angezeigt.
-z	Die Registrierung wird nicht überprüft.
-nosum	Die Prüfsumme der Datei wird nicht berechnet. Beim Prüfsummentest wird die Prüfsumme von Dateien berechnet. Dies kann zu einer hohen Belastung des Netzwerks führen. Mithilfe dieser Option wird der Scanvorgang beschleunigt, und die benötigte Bandbreite ist geringer. Die Dateiversionen werden weiterhin überprüft.
-b	Der Status von Hotfixes, die zur Erfüllung minimaler Sicherheitsstandards benötigt werden, wird angezeigt.
-v	Die Details zu den Meldungen Patch NOT Found (Patch nicht gefunden), WARNING (WARNUNG) und NOTE (ANMERKUNG) werden angezeigt. Standardmäßig im Tabmodus aktiviert.
-f <outfile>	Gibt den Namen der Datei an, in der die Ergebnisse gespeichert werden sollen. Standardmäßig ist die Anzeige auf dem Bildschirm aktiviert.
-u <username>	Gibt den optionalen Benutzernamen für die Anmeldung an einem Remotecomputer an.
-p <password>	Gibt das Kennwort für einen Benutzernamen an.
-?	Zeigt ein Hilfemenü an.

Wenn Sie Hfnetchk zum Überprüfen des Patchstatus verwenden, sollten Sie sicherstellen, dass es regelmäßig ausgeführt wird. In den meisten Umgebungen sollte ein Zeitplan für eine regelmäßige Ausführung erstellt werden.

Anmerkung: Weitere Informationen zur Verwendung von Hfnetchk finden Sie im englischsprachigen Knowledge Base-Artikel Q303215 "Microsoft Network Security Hotfix Checker (Hfnetchk.exe) Tool Is Available".

Patchverwaltungsskript

Dieses Handbuch enthält ein Patchverwaltungsskript, **hfnetchk.cmd**, mit dem mehrere Server auf fehlende Patches hin überprüft werden. Die Ergebnisse werden in einer Protokolldatei aufgezeichnet, die in einem datenbasierten Ordner gespeichert wird. Das Skript verwendet Hfnetchk, um Server zu scannen, und das Skript **movelog.vbs**, um die Dateien in die entsprechenden Ordner zu verschieben. Mit der Zeit dienen die Ordner als Verlaufsprotokolle, die Sie bei Ihren Analysen und Überprüfungen heranziehen können, um für die Umgebung mehr Sicherheit zu gewährleisten.

Anmerkung: Für das in diesem Handbuch enthaltene Skript ist **Hfnetchk.exe**, Version 3.32 oder höher, erforderlich.

Nach dem Downloaden und Extrahieren der in diesem Handbuch enthaltenen Skripts erhalten Sie die folgende Ordnerstruktur für das Patchverwaltungsskript:

Tabelle 5.2: Ordnerstruktur für das Patchverwaltungsskript

Ordner	Beschreibung
C:\SecurityOps	Dies ist der Stammordner für alle in diesem Handbuch enthaltenen Dateien.
C:\SecurityOps\PatchMgmt	Dieser Ordner enthält das Patchverwaltungsskript, **hfnetchk.cmd**, das Skript **movelog.vbs** und die Unterordner für die Unterstützungsdateien und -protokolle. In diesem Ordner muss auch die Datei **mssecure.xml** gespeichert werden.
C:\SecurityOps\PatchMgmt\Hfnetchk	In diesem Ordner muss das Dienstprogramm **hfnetchk.exe** nach dem Download von der Microsoft-Website gespeichert werden. Ausführliche Anweisungen finden Sie weiter unten.
C:\SecurityOps\PatchMgmt\ServerLists	In diesem Ordner erstellen und speichern Sie Textdateien mit einer Auflistung der Servergruppen, die auf fehlende Patches hin gescannt werden sollen.
C:\SecurityOps\PatchMgmt\Logs	In diesem Ordner werden nach dem Ausführen von **hfnetchk.cmd** die Protokolldateien erstellt. Das Skript erstellt einen Unterordner mit dem aktuellen Datum, in dem die Protokolldatei gespeichert wird. Beispiel: **\SecurityOps\PatchMgmt\Logs\2002117**

Anmerkung: Wenn Sie die in diesem Handbuch enthaltenen Dateien auf einer anderen Partition als **C:** installieren, müssen Sie in der Datei **hfnetchk.cmd** die Pfade bearbeiten, um die Partition verwenden zu können.

So richten Sie das Skript "Hfnetchk.cmd" auf einem System für Sicherheitsupdates ein und verwenden es

1. Führen Sie **SecurityOps.exe** aus, um die in diesem Handbuch enthaltenen Skriptdateien zu extrahieren und die in Tabelle 5.2 aufgeführte Ordnerstruktur zu erstellen.
2. Downloaden und extrahieren Sie das Dienstprogramm Hfnetchk von http://www.microsoft.com/Downloads/Release.asp?ReleaseID=31154 (englischsprachig), und speichern Sie **hfnetchk.exe** im Ordner **C:\SecurityOps\PatchMgmt\Hfnetchk**. Ist der Computer, der das Skript ausführt, nicht mit dem Internet verbunden, müssen Sie zusätzlich die Datei **Mssecure.xml** von http://download.microsoft.com/download/xml/security/1.0/nt5/en-us/mssecure.cab (englischsprachig) downloaden. **Mssecure.xml** sollte im Ordner **C:\SecurityOps\PatchMgmt** gespeichert werden.
3. Erstellen Sie im Ordner **C:\SecurityOps\PatchMgmt\ServerLists** eine Textdatei mit einer Serverliste. Die Textdatei enthält die NetBIOS-Namen der Server (durch Zeilenumbrüche getrennt), die Sie überprüfen möchten.

   Anmerkung: Ist zwischen dem Servernamen und dem Zeilenumbruch ein Leerzeichen, führt **Hfnetchk.exe**, Version 3.32, für den Server keinen Scanvorgang durch. Stellen Sie vor dem Ausführen von Hfnetchk sicher, dass keine Zeile mit einem Leerzeichen endet.
4. Starten Sie eine Eingabeaufforderung, wechseln Sie zum Ordner **C:\SecurityOps\PatchMgmt**, und starten Sie mithilfe der folgenden Befehlszeile das Skript:

   ```
   Hfnetchk.cmd serverlist.txt
   ```

   Wobei **serverlist.txt** der Name der Textdatei mit der Serverliste ist.

   Anmerkung: Es wird ein Dialogfeld angezeigt, in dem Sie gefragt werden, ob Sie die Datei **mssecure.xml** downloaden möchten. Klicken Sie auf **Ja**.
5. Wechseln Sie zum Ordner **C:\SecurityOps\PatchMgmt\Logs**, öffnen Sie den Ordner mit dem aktuellen Datum, und öffnen Sie die Datei mit dem gleichen Namen wie die Datei **serverlist.txt**.
6. Prüfen Sie in der Protokolldatei, welche Patches auf den Servern fehlen.

   Anmerkung: Wenn das Patchverwaltungsskript zweimal an einem Tag ausgeführt wird, wird die Protokolldatei der ersten Ausführung überschrieben.

Arbeiten mit mehreren Serverlisten

Bei einem Netzwerk großen Umfangs verfügen Sie wahrscheinlich über unterschiedliche Servertypen. Möglicherweise möchten Sie in Ihrer Risikomanagementstrategie festlegen, dass einige Server häufiger als andere auf fehlende Patches hin überprüft werden sollen. Wenn Sie mehrere Serverlisten verwenden, können Sie für das Patchverwaltungsskript einen Zeitplan festlegen, nach dem die unterschiedlichen Servertypen in unterschiedlichen Abständen gescannt werden. Mehrere Serverlisten sind auch in den Fällen nützlich, in denen verschiedene Administratoren für unterschiedliche Servergruppen verantwortlich sind.

Beim Verwenden von mehreren Listen können Sie für jede Gruppe von Administratoren separate Berichte über fehlende Patches erstellen.

Als Beispiel sollten Sie für ein einfaches Netzwerk, wie in Abbildung 5.2 gezeigt, sechs Dateien mit Serverlisten erstellen, um verschiedenen Administratorgruppen Patchberichte bereitzustellen.

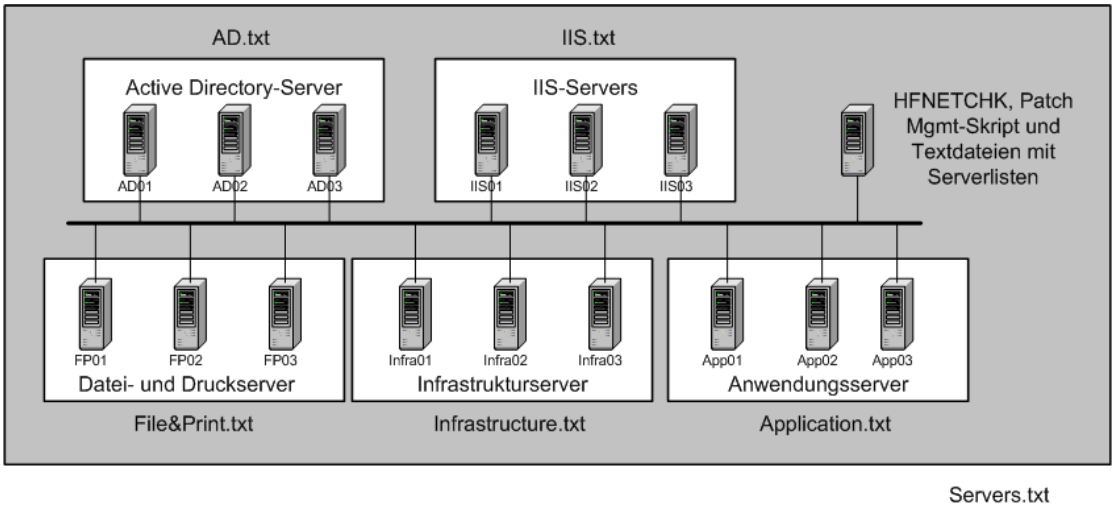


Abbildung 5.2: Dateien mit Serverlisten für ein einfaches Netzwerk

In diesem Beispiel würden die Dateien mit Serverlisten für jeden Servertyp die Namen dieser Server enthalten. **File&Print.txt** enthält z. B. lediglich die folgenden Namen:

```
FP01
FP02
FP03
```

Die sechste Datei, **Servers.text**, enthält alle Server in der Umgebung. Das Sicherheitsteam könnte mithilfe der Ergebnisse dieses Scanvorgangs sicherstellen, dass jede Gruppe ihre Server in Bezug auf die aktuellsten Patches auf dem neuesten Stand hält.

Erstellen eines Zeitplanes für das Patchverwaltungsskript

Um sicherzustellen, dass **hfnetchk.cmd** in regelmäßigen Abständen ausgeführt wird, sollten Sie für das Tool einen Zeitplan erstellen. Hierfür kann der Taskplaner oder der AT-Befehl verwendet werden. Durch Verwendung mehrerer Serverlisten können Sie sicherstellen, dass unterschiedliche Server zu unterschiedlichen Zeitpunkten überprüft werden.

Anmerkung: Der Zeitplandienst ist in den Basisrichtlinien für Mitgliedsserver und Domänencontroller standardmäßig deaktiviert. Sie müssen den Dienst aktivieren, wenn Sie für das Patchverwaltungsskript einen Zeitplan erstellen möchten.

Weitere Methoden zum Ermitteln von Hotfixversionen

Wenn Sie das Tool hfnetchk in manchen Teilen der Umgebung nicht verwenden können oder möchten, können Sie auch auf andere Arte und Weise ermitteln, ob Hotfixes installiert wurden.

Am einfachsten ist es, in der Registrierung unter dem Schlüssel **HKLM\Software\Microsoft\Windows Nt\Currentversion\hotfix** nachzusehen. Jeder neu installierte Hotfix verfügt normalerweise über einen Schlüssel mit einem Namen beginnend mit Q, der dem Knowledge Base-Artikel zu diesem Hotfix entspricht. Bei einigen älteren Hotfixes und bei Hotfixes für einige Anwendungen ist dies jedoch nicht der Fall.

Es gibt zwei weitere kostenlose Tools von Microsoft, mit denen Sie diese Informationen sammeln können:

Qfecheck.exe /v. Gibt die Version des Service Packs und die installierten Hotfixes an. Qfecheck gibt zudem an, ob der Patch ordnungsgemäß installiert wurde.

Hotfix.exe -l. Zeigt die installierten Hotfixes an.

Plan

Nicht jedes Risiko oder jede Schwachstelle stellt für Ihre Umgebung eine tatsächliche Gefahr dar. Wenn Sie über potenzielle neue Schwachstellen von Betriebssystemen oder Anwendungen lesen, sollten Sie abschätzen, ob diese Schwachstellen auf Ihre Umgebung zutreffen. Wenn die Schwachstelle z. B. für den FTP-Dienst von Windows 2000 gilt und Sie diesen Dienst nie aktivieren, trifft das Problem auf Sie nicht zu. Wenn Sie auf Risiken und Schwachstellen reagieren, die auf Ihre Umgebung nicht zutreffen, verbrauchen Sie unnötig wertvolle Ressourcen und beeinträchtigen möglicherweise die Stabilität Ihrer Umgebung, ohne einen Vorteil zu erzielen.

Wenn neue Risiken und Schwachstellen entdeckt werden, sollten Sie alle diesbezüglichen unterstützenden Informationen lesen. So können Sie eine vernünftige Entscheidung darüber treffen, ob für Ihre Umgebung ein tatsächliches Risiko besteht, und ermitteln, wie Sie auf angemessene Weise reagieren können. Die Reaktion kann darin bestehen, keine Maßnahmen zu ergreifen, den betreffenden Dienst zu deaktivieren oder einen Patch bereitzustellen.

Anmerkung: Wenn Sie einen Plan zum Bereitstellen eines neuen Patches erstellen, sollten Sie auch einen Rollbackplan erstellen.

Anmerkung: Damit Sie über neue Patches immer auf dem Laufenden sind, sollten Sie sicherstellen, dass Sie regelmäßig Sicherheitsbulletins von Microsoft erhalten. Auf der Microsoft Security-Website können Sie sich registrieren, um diese Sicherheitsbulletins zu erhalten. Den entsprechenden Hyperlink finden Sie im Abschnitt "Weitere Informationen" am Ende dieses Kapitels.

Kategorisieren von Patches

Wenn ein neuer Patch zur Verfügung gestellt wird, sollten Sie jedes Mal ermitteln, wie wichtig dieser Patch für Ihre Umgebung ist. So können Sie festlegen, wie schnell er bereitgestellt werden muss und wie viele Tests durchgeführt werden können.

Die Sicherheitsbulletins von Microsoft enthalten Bewertungen in Bezug auf die einzelnen Schwachstellen. Die unterschiedlichen Bewertungen sind in der folgenden Tabelle angegeben.

Tabelle 5.3: Von Microsoft definierte Bewertung der Schwachstellen

Computertyp	Bewertung		
	Schwerwiegend (Critical)	Mittelschwere (Moderate)	Gering (Low)
Internetserver	Websitefehler, Denial-of-Service oder Verweigerung des Vollzugriffs	Schwierig zu nutzende, ungewöhnliche Konfiguration oder vorübergehende Auswirkungen	Eingeschränkte Auswirkungen, wie z. B. Veröffentlichung von Skripts
Interne Server	Erhöhte Privilegien, Datenveröffentlichung oder -änderung. Überwachung schwierig	Datenveröffentlichung, Datenänderung oder Denial-of-Service mit Möglichkeit der Überwachung	Ungezielter oder unvollständiger Datendiebstahl, ungezielte oder unvollständige Datenänderung, eingeschränkter Denial-of-Service
Clientsysteme	Ausführen von beliebigem Code ohne Benutzeraktion, Remoteausweitung von Berechtigungen	Lokale Ausweitung von Berechtigungen; ungezielte Datenveröffentlichung oder ungezielter Denial-of-Service; Ausnutzung von Benutzeraktionen	Eingeschränkter oder unvollständiger Datendiebstahl, eingeschränkte oder unvollständige Datenänderung, feindliche Websiteangriffe

In dem Bewertungssystem werden die Schwachstellen nach den potenziellen negativen Auswirkungen bei Ausnutzung der Schwachstelle sowie nach der Wahrscheinlichkeit für die Ausnutzung kategorisiert.

Sie können dieses Bewertungssystem als Leitfaden zum Kategorisieren von Patches verwenden. Das Bewertungssystem von Microsoft ist jedoch nur eine allgemeine Schätzung in Bezug auf die potenziellen Auswirkungen für Millionen von Computern weltweit. Der jeweilige Schweregrad basiert auf früheren Erfahrungen und subjektiven Einschätzungen. Daher sind möglicherweise keine exakten Vorhersagen bezüglich der Auswirkungen auf Ihre Umgebung möglich. Letztendlich müssen Sie die Patches auf der Basis Ihrer eigenen Umgebung kategorisieren.

Testen der Patches

Wie für jedes Softwareprogramm gilt auch für Patches, dass sie möglicherweise nicht in jeder Umgebung optimal funktionieren. Im Idealfall sollten Sie alle Patches umfassend testen, die Sie in Ihrer Umgebung installieren möchten. Viele Sicherheitspatches müssen jedoch schnell installiert werden, um möglicherweise schwerwiegende Probleme zu beheben. In vielen Fällen wird das jeweilige Testverfahren für Sie ein Kompromiss sein zwischen der Notwendigkeit, ein Sicherheitsproblem zu lösen, und der Notwendigkeit, sicherzustellen, dass der Patch in Ihrer Umgebung stabil ist.

Wie viele Tests angemessen sind, hängt von der jeweiligen Kategorisierung des Patches ab. Die folgende Tabelle zeigt mithilfe der Kategorisierungen von Microsoft die Tests, die Sie für den einzelnen Patchtyp mindestens durchführen sollten.

Tabelle 5.4: Erforderliche Tests für Patches

Patchtyp	Erforderliche Tests
Sicherheitspatches für schwerwiegende Probleme	Beurteilen des Patches Beurteilen der Servervorgänge (eingeschränkt)
Sicherheitspatches für mittelschwere Probleme	Beurteilen des Patches Installieren des Patches in einer Testumgebung Beurteilen der Servervorgänge (vollständig) Überprüfen des Deinstallationsverfahrens
Sicherheitspatches für geringe Probleme	Beurteilen des Patches Installieren des Patches in einer Testumgebung Beurteilen der Servervorgänge (vollständig) Beurteilen der Anwendungsvorgänge Überprüfen des Deinstallationsverfahrens

Bei Ihrem Risikomanagement müssen Sie ermitteln, wie gründlich Sie jeden Schritt ausführen müssen. Wenn Sie einige dieser Phasen aus Gründen der Dringlichkeit überspringen, sollten Sie sie dennoch in einer Testumgebung ausführen, um potenzielle Probleme zu erkennen, bevor diese auf schon bereitgestellten Systemen auftreten.

Alle Tests sollten auf Servern durchgeführt werden, die den Produktionsservern so weit wie möglich entsprechen.

Beurteilen des Patches

Ihre Patchbeurteilung sollte mindestens die folgenden Schritte enthalten:

Bestimmen des Patchbesitzers. Für alle Patches sollten Sie einen Besitzer bestimmen, der für die Bewertung des Patches verantwortlich ist.

Lesen der Dokumentation. Bevor ein Service Pack, Hotfix oder Sicherheitspatch angewendet wird, sollten alle relevanten Dokumentationen gelesen sowie ein zweites Mal geprüft werden. Der Prüfvorgang ist äußerst wichtig, da so weitgehend vermieden wird, dass eine einzelne Person bei der Bewertung des Updates wichtige und relevante Punkte übersieht.

Überprüfen der Patchkategorie. Es ist möglich, dass bei weiterer Beurteilung des Patches die jeweilige Kategorie geändert werden muss. Dies wirkt sich auf andere Aspekte der Tests aus.

Achten Sie beim Lesen der Dokumentation auf Folgendes:

Ist das Update relevant und löst es ein ausstehendes Problem?

Führt die Anwendung des Updates zu anderen Problemen, die negative Auswirkungen auf das Produktionssystem haben?

Ist das Update mit Abhängigkeiten verbunden? (Müssen für das Update z. B. bestimmte Features aktiviert bzw. deaktiviert werden?)

Müssen Sie vor dem Bereitstellen des Updates bestimme Aktionen ausführen?

Neben der Durchsicht der zusammen mit den Updates veröffentlichten Dokumentation sollten Sie auf der Website des Technischen Supports von Microsoft nach zusätzlichen Informationen zum Update suchen, die nach der Veröffentlichung des Updates herausgegeben wurden. Auf der TechNet-Website werden Sicherheitsbulletins in einer suchfähigen (nach Produktname und Service Pack geordneten) Datenbank bereitgestellt. Die Sicherheitsbulletins enthalten wichtige Informationen, die herangezogen werden sollten.

Installieren

Sie sollten sicherstellen, dass der Patch wie erwartet installiert wird. Außerdem müssen Sie wissen, ob ein Neustart erforderlich ist, wie viel Speicherplatz benötigt wird (einschließlich eines Deinstallationsordners), welche Optionen Ihnen zur Verfügung stehen usw. Wenn Sie den Patch installieren, sollten Sie auch alle unterstützenden Dokumentationen lesen, um zusätzliche Informationen zu erhalten.

Serveroptionen

Nachdem der Patch installiert wurde, müssen Sie sicherstellen, dass der Server weiterhin ordnungsgemäß ausgeführt werden kann. Es kann auch nützlich sein, das Ereignisprotokoll und den Systemmonitor auf unerwartete Ergebnisse hin zu überprüfen. Testen Sie alle Serverfunktionen, und stellen Sie sicher, dass alle Funktionen ordnungsgemäß ausgeführt werden können. Wie lang Sie den Server zur Überprüfung aller Funktionen ausführen sollten, hängt davon ab, wie hoch in Bezug auf die jeweilige Schwachstelle das Risiko auf dem Server sein darf. Wenn Probleme auftreten, müssen Sie sicherstellen, dass diese Probleme dokumentiert werden und dass Sie die Vor- und Nachteile der Anwendung des Patches ausgewertet haben. Aufgetretene Probleme sollten so bald wie möglich an Microsoft weitergegeben werden.

Anmerkung: Mithilfe von Microsoft Operations Manager können Sie Informationen im Ereignisprotokoll und Systemmonitor sammeln.

Anwendungsvorgänge

Beim Testverfahren ist es äußerst wichtig, den Patch mit allen Anwendungen zu testen, die auf dem Server gemeinsam verwendet werden, und sicherzustellen, dass Sie alle Probleme in Bezug auf Abhängigkeiten kennen. Nach dem Installieren des Patches sollten Sie überprüfen, ob alle Anwendungen wie zuvor ausgeführt werden können.

Deinstallieren

Es ist möglich, dass nach dem Installieren des Patches trotz Ihrer Tests Probleme auftreten, die eine Deinstallation des Patches erforderlich machen. Es sollte daher getestet werden, ob die Deinstallation ordnungsgemäß funktioniert. Nach dem Deinstallieren sollten Sie überprüfen, ob der Server weiterhin wie erwartet ausgeführt werden kann, und die Leistungsindikatoren des Ereignisprotokolls und des Systemmonitors weiter beobachten.

Erstellen eines Alternativplanes

Auch wenn die Tests ohne Zwischenfall durchgeführt werden können, besteht die Möglichkeit, dass Probleme auftreten, wenn Sie den Patch in der gesamten Organisation bereitstellen. Sie benötigen daher einen Aktionsplan, um den ursprünglichen Zustand des Systems wiederherzustellen, der vor dem Bereitstellen des Patches bestand. In einigen Fällen wird vor der Installation ein Sicherungssnapshot des Servers erstellt, damit beim Auftreten von Problemen der Server sehr schnell wiederhergestellt werden kann. Führen Sie unabhängig von der Art Ihres Alternativplanes umfassende Tests durch.

Bereitstellen der Patches

Wenn bei Ihren Tests keine Probleme aufgetreten sind, können Sie nun den Patch in der gesamten Organisation bereitstellen. Hierfür haben Sie mehrere Möglichkeiten, wie z. B. die folgenden:

Manuell

Gruppenrichtlinien

Skripts

Anmerkung: Weitere Informationen zum Bereitstellen von Patches finden Sie im englischsprachigen TechNet-Artikel "Best Practices for Applying Service Packs, Hotfixes and Security Patches". Den entsprechenden Hyperlink finden Sie im Abschnitt "Weitere Informationen" am Ende dieses Kapitels.

Manuell

Eine manuelle Installation von Hotfixes ist in den meisten Organisationen die häufigste Installationsmethode. Dabei wird lediglich auf jedem Server die ausführbare Datei für den entsprechenden Hotfix ausgeführt. Wenn Ihre Organisation über eine große Anzahl von Servern verfügt, ist diese Option möglicherweise nicht praktikabel.

Die Namen der meisten Hotfixes enthalten wichtige Informationen zum Fix. Ein typischer Name für einen Hotfix ist z. B. **Q292435_W2K_SP3_x86_en.EXE**. Der Name enthält die folgenden Informationen:

Q292435 ist die Nummer des Knowledge Base-Artikels, in dem Sie weitere Informationen zum Hotfix finden.

W2K ist das Produkt, für das der Hotfix vorgesehen ist (Microsoft Windows 2000)

SP3 ist das Service Pack, in dem der Hotfix enthalten ist.

x86 ist die vorgesehene Prozessorarchitektur.

en steht für die Sprache (Englisch).

Anmerkung: Hotfixes mit dem Dateinamen **QXXXXXX.exe** ohne den Zusatz "W2K_SP3_x86" wurden speziell für Anwendungen wie Internet Explorer entwickelt.

Hotfixes unterstützen auch einige Befehlszeilenoptionen, mit denen das Verhalten bei der Installation des Hotfixes gesteuert werden kann.

Tabelle 5.5: Optionen für ausführbare Hotfix-Dateien

Option	Beschreibung
-y	Deinstallation ausführen
-f	Schließen oder Herunterfahren von Anwendungen erzwingen
-n	Kein Deinstallationsverzeichnis erstellen
-z	Nach der Installation des Updates keinen Neustart durchführen
-q	Stiller Modus – keine Benutzeroberfläche
-m	Unbeaufsichtigter Modus
-l	Installierte Hotfixes auflisten

Anmerkung: Anwendungsspezifische Hotfixes mit dem Namen **QXXXXXX.exe** unterstützen normalerweise nicht alle oben genannten Optionen.

Wenn Sie für die Installation von mehreren Hotfixes ein Skript erstellen möchten, können Sie die Optionen **-q** und **-z** verwenden, damit der Hotfix ohne eine Benutzeroberfläche installiert und kein Neustart erzwungen wird.

Wenn Sie mehrere Hotfixes installieren, müssen Sie normalerweise den Computer vor jeder neuen Installation neu starten. Dies liegt daran, dass gesperrte oder geöffnete Dateien nicht ersetzt werden können, so dass sie in eine Warteschlange gelegt und erst nach dem Neustart des Systems ersetzt werden. QChain ist ein Tool, mit dem Sie mehrere Hotfixes für einen einzigen Neustart miteinander verbinden können, anstatt zwischen den einzelnen Installationen einen Neustart durchführen zu müssen. Führen Sie für QChain das Hotfixinstallationsprogramm mit der Option **-z** aus, damit nach der Installation kein Neustart durchgeführt wird. Führen Sie anschließend **QChain.exe** aus, und starten Sie den Computer neu.

Anmerkung: QChain ist über TechNet verfügbar. Weitere Informationen finden Sie im Abschnitt "Weitere Informationen" am Ende dieses Kapitels.

Wenn nach dem Anwenden eines Service Packs und von Patches zusätzliche Komponenten hinzugefügt werden, wie z. B. DNS, müssen Sie das Service Pack und die Patches erneut anwenden, um sicherzustellen, dass die neue Komponente mit dem richtigen Patch ausgeführt wird.

Gruppenrichtlinien

Windows 2000 unterstützt Softwareverteilungen mithilfe von Gruppenrichtlinien. Patches werden normalerweise nicht als Windows Installer-Paket bereitgestellt. Sie können jedoch die ausführbare Datei zusammen mit einer ZAP-Datei verwenden.

Anwendungen ohne Windows Installer-Pakete müssen eine ZAP-Datei verwenden, in der das vorhandene Installationsprogramm beschrieben wird. Eine ZAP-Datei ist eine Textdatei (ähnlich einer INI-Datei), die Informationen zur Installation eines Programms enthält sowie Anwendungseigenschaften und die von der Anwendung zu installierenden Einstiegspunkte.

Eine ZAP-Datei kann jedoch nur einem Benutzer zugewiesen werden, d. h., wenn Sie eine Gruppenrichtlinie für die Verteilung des Hotfixes einrichten, müssen Sie sich mit dem Benutzerkonto, dem die ZAP-Datei zugewiesen wurde, am Computer anmelden.

Anmerkung: Weitere Informationen zum Erstellen einer ZAP-Datei und zum Zuweisen der ZAP-Datei mithilfe von Gruppenrichtlinien finden Sie im englischsprachigen Knowledge Base-Artikel Q231747, "How to Publish non-MSI Programs with .zap Files".

Skripts

Möglicherweise möchten Sie zum Verteilen von Patches Ihre eigenen VBScripts oder Batchdateien erstellen. Dabei könnte es sich um Anmelde- oder Startskripts handeln, mit denen von einem zentralen Server aus der aktuelle Patchstatus und anschließend die Updates überprüft werden.

Ihre Skripts können QChain einschließen, damit sichergestellt ist, dass nur ein einziger Neustart durchgeführt wird, wenn mehrere Hotfixes erforderlich sind.

Überwachen

Nachdem Sie die Patches in Ihrer Produktionsumgebung installiert haben, müssen Sie die Server weiter überwachen. Sie sollten in jedem Fall die Leistungsindikatoren des Ereignisprotokolls und des Systemmonitors auf Probleme hin überprüfen. Wenn Ihnen in den folgenden Wochen weitere Probleme auf dem Computer auffallen, sollten Sie Tests durchführen, um sicherzustellen, dass die Probleme nicht mit dem bereitgestellten Patch zusammenhängen. Wenn Sie einen Patch implementiert haben, für den aufgrund eines schwerwiegenden Problems keine umfassenden Tests durchgeführt wurden, sollten Sie den Patch in einer Testumgebung hinterher weiter testen, um sicherzustellen, dass kein Problem übersehen wurde.

Neben der Überwachung vorhandener Server ist es sehr wichtig, dass Sie die Umgebung als Ganzes überwachen, um sicherzustellen, dass keine neuen Server ohne die entsprechenden aktuellen Patches ins Netzwerk gestellt werden. Neue Server sollten immer das neueste Build erhalten, und Sie sollten dies durch Überwachung der Umgebung sicherstellen.

Überprüfen

Sie können nur dann sicher sein, dass alle Vorgänge ordnungsgemäß ausgeführt werden, wenn Sie diese überprüfen. Nach Abschluss des Patchverwaltungsprozesses für einzelne Patches sollten Sie eine Überprüfung durchführen, um sicherzustellen, dass der Patch ordnungsgemäß bereitgestellt wurde und alle Verfahren wie erwartet durchgeführt werden konnten. So können Sie sicherstellen, dass der Prozess auch weiterhin wie erwartet durchgeführt wird. Beim Überprüfen des Patchverwaltungsprozesses sollten Sie wiederholt Analysen durchführen, um festzustellen, ob weitere Änderungen an der Umgebung vorgenommen werden müssen. In dem Fall muss der Patchverwaltungsprozess von vorne beginnen.

Clientseitige Patchverwaltung

In diesem Kapitel wird der serverseitige Prozess der Patchverwaltung behandelt. Sie sollten sich jedoch darüber im Klaren sein, dass häufig über einen clientseitigen Zugriff Viren ins System gelangen und andere Risiken für die Unternehmenssicherheit entstehen.

Die meisten der weiter oben besprochenen Punkte beziehen sich auch auf die clientseitige Verwaltung, es gibt jedoch einige Unterschiede. Meist bestehen die Unterschiede nicht so sehr in der Funktion des Patches, sondern mehr in der Art des Prozesses, mit dem Ihr Unternehmen ermittelt, welche Patches erforderlich sind, und die Patches testet und bereitstellt.

Es gibt eine Reihe von speziellen Tools, die Ihnen bei der clientseitigen Patchverwaltung helfen.

Windows Update

Wenn Sie eine Windows XP-Clientbasis ausführen, stellt Windows Update eine einfache Möglichkeit dar, nach Fixes zu suchen und Fixes anzuwenden. Wenn Sie zur Windows Update-Website wechseln, wird der Computer gescannt, und sicherheitsrelevante oder andere Patches, die nicht installiert wurden, werden aufgelistet und können gedownloadet werden.

Um Windows Update auszuführen, müssen Sie für den lokalen Computer über Administratorrechte verfügen. Daher kann das Tool in vielen Umgebungen nicht eingesetzt werden.

Unternehmensversion von Windows Update

Die Site zur Unternehmensversion von Windows Update stellt einen umfassenden Katalog von Updates bereit, die in einem Unternehmensnetzwerk verteilt werden können. Es handelt sich um eine umfassende Site mit Windows Update-Inhalten und Gerätetreibern mit dem Microsoft WHQL-Logo (Windows Hardware Quality Lab).

Die Unternehmensversion von Windows Update ermöglicht Ihnen Folgendes:

Suchen nach den neuesten Software- und Treiberupdates durch Eingabe eines Schlüsselwortes, eines Betriebssystems, eines Updatetyps, eines Komponententyps, einer Sprache, eines Bereitstellungsdatums oder eines Herstellers, so dass Sie die für Ihr Unternehmen relevanten Updates leicht finden können.

Downloaden einzelner Updates nach Bedarf oder Auswählen mehrerer Updates zum Downloaden in einem Paket, das als Ganzes im Netzwerk verteilt werden kann.

Verwenden des Downloadverlaufsprotokolls mit Informationen zu bereits gedownloadeten Updates und deren Speicherort.

Lesen der Datei "Wichtige Hinweise" (Readme.txt o.ä.) mit detaillierten Informationen zu jedem Update, bevor Sie das Update downloaden. Die Datei "Wichtige Hinweise" ist in jedem Downloadpaket enthalten und enthält Hyperlinks zu relevanten Websites mit weiteren Informationen.

Microsoft Baseline Security Analyzer

Dies ist eine Anwendung, die auf der TechNet-Website gedownloadet und mit der sichergestellt werden kann, dass Windows 2000- und Windows XP-basierte Systeme sicher und auf dem neuesten Stand sind. Der Baseline Security Analyzer scannt mindestens ein System und gibt einen Bericht z. B. über die folgenden Probleme zurück: fehlende Sicherheitspatches, unsichere Kennwörter, Internet Explorer- und Outlook Express-Sicherheitseinstellungen und Office-Makroschutzeinstellungen. Die Anwendung enthält Informationen zum vorliegenden Sicherheitsproblem und zur Behebung des Problems sowie Hyperlinks zu zusätzlichen Informationen.

Weitere Tools

Wenn Sie die in diesem Kapitel bislang beschriebenen Empfehlungen befolgen, können Sie Patches in Ihrer Organisation effektiv verwalten. Es gibt jedoch eine Reihe von zusätzlichen Tools, mit denen Sie den Prozess der Patchverwaltung noch weiter automatisieren können.

SMS

Wenn Sie in Ihrer Organisation Microsoft Systems Management Server (SMS) bereitgestellt haben, können Sie viele der oben dargestellten Phasen vereinfachen.

Das Microsoft Security Toolkit enthält ein SMS-Importdienstprogramm, mit dem die Verteilung und Installation von empfohlenen IIS-Sicherheitsfixes automatisiert werden kann. Mithilfe von SMS können Sie ermitteln, für welche Computer die Sicherheitsfixes erforderlich sind, und die Fixes anschließend bereitstellen. Mithilfe der Softwarebereitstellungsfeatures von SMS können Sie in Ihrer Umgebung Patches auf allen Computern verteilen, die über den SMS-Client verfügen. Wenn Sie für den Patch ein Softwarepaket erstellen, können Sie für alle Computer in Ihrer Umgebung oder für eine Sammlung von Computern eine Aktualisierung erzwingen. Einer der Hauptvorteile ist, dass Sie überwachen können, auf welchen Computern der Patch installiert ist. Die Softwarepakete kann jedoch in den meisten Fällen nur ein SMS-Administrator oder eine Person mit Kenntnissen in Bezug auf die Erstellung von SMS-Paketen verteilen.

Tools von Drittanbietern

Es sind einige Tools von Drittanbietern verfügbar, die die Patchverwaltung vereinfachen. Sie bieten diverse Features, die über die kostenlosen Tools von Microsoft zurzeit nicht verfügbar sind. Dazu gehört die Möglichkeit, Fixes bereitzustellen und dabei einen Statusbericht zu erhalten, Gruppen von Computern mit ähnlichen Updateanforderungen zu erstellen, andere Produkte zu unterstützen, die weiter oben nicht beschrieben sind, und für administrative Aufgaben GUI-Befehlsbereiche (Graphical User Interface oder Grafische Benutzeroberfläche) zu verwenden. Sie sollten abschätzen, ob diese Features in Ihrer Umgebung erforderlich sind.

Service Pack and Hotfix Utility von der Polaris Group

Dieses Tool bietet eine benutzerfreundliche GUI und unterstützt alle Microsoft-Produkte. Das Bereitstellen von Service Packs und Hotfixes kann mit diesem Tool automatisiert werden, so dass alle Computer nach einem zuvor angegebenen Unternehmensstandard ausgeführt werden.

http://www.polarisgroup.com/solutions (englischsprachig)

Shavlik Hfnetchkpro

Dieses Tool baut auf der hfnetchk-Technologie auf. Es verfügt über eine GUI und ermöglicht das Erstellen eines Scanverlaufsprotokolls. Dies ist mit der Befehlszeilenversion nicht möglich.

http://www.shavlik.com/nshc.htm (englischsprachig)

Bindview Security Advisor

Dieses Tool von Bindview verfügt über eine GUI, die das Überprüfen von nicht kompatiblen Computern vereinfacht. Es bietet zudem einen Updatedienst, der über neu herausgegebene Patches informiert.

http://www.bindview.com/Solutions/Security/SecAdvisor_bvCtrlW2k.cfm (englischsprachig)

Security Expressions von Pedestal Software

Mit diesem Tool können Administratoren Sperrungs-Sicherheitsrichtlinien für Windows- und UNIX-Computer implementieren. Darüber hinaus kann nach Hotfixes gesucht werden, die gegebenenfalls automatisch gedownloadet und installiert werden.

http://www.pedestalsoftware.com/secexp/index.htm (englischsprachig)

Zusammenfassung

Die meisten IT-Sicherheitsverletzungen sind auf Systeme zurückzuführen, die in Bezug auf Sicherheitspatches nicht auf dem neuesten Stand sind und deren Sicherheitslücken ausgenutzt werden. Eine zuverlässige Patchverwaltung ist überaus wichtig, wenn Sie die bestehenden Sicherheitsrisiken reduzieren möchten. Wenn Sie die Patchverwaltung ernst nehmen, können Sie die mit Sicherheitsverletzungen verbunden Kosten deutlich reduzieren.

Weitere Informationen

Weitere Informationen zu Hfnetchk:

http://support.microsoft.com/default.aspx?scid=kb;EN-US;q303215 (englischsprachig)

Downloaden von Hfnetchk:

http://www.microsoft.com/downloads/release.asp?releaseid=31154 (englischsprachig)

Downloaden von **mssecure.cab**:

http://download.microsoft.com/download/xml/security/1.0/nt5/en-us/mssecure.cab (englischsprachig)

Weitere Informationen zum Erstellen einer ZAP-Datei für die Verwendung mit Gruppenrichtlinien finden Sie unter:

http://support.microsoft.com/default.aspx?scid=http%3a%2f%2fwww.microsoft.com%2fIntlKB%2fGermany%2fsupport%2fkb%2fd41%2fd41635.htm

oder unter

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnexnt00/html/ewn0085.asp (englischsprachig)

Download von und Informationen zu **Qfecheck.exe**:

http://support.microsoft.com/default.aspx?scid=http%3a%2f%2fwww.microsoft.com%2fIntlKB%2fGermany%2fsupport%2fkb%2fd44%2fd44863.htm

Informationen zu **Hotfix.exe**:

http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q184305 (englischsprachig)

Informationen zu Qchain und Downloaden der ausführbaren Datei:

http://support.microsoft.com/default.aspx?scid=http%3a%2f%2fwww.microsoft.com%2fIntlKB%2fGermany%2fsupport%2fkb%2fd296%2fd296861.htm

Informationen zum Sicherheitsbewertungssystem von Microsoft:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/policy/rating.asp (englischsprachig)

Regelmäßig veröffentlichte Sicherheitsbulletins:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp (englischsprachig)

Microsoft Security Toolkit (englischsprachig):

http://www.microsoft.com/germany/themen/security/default.htm

Microsoft Operations Framework (MOF):

http://www.microsoft.com/germany/ms/technetdatenbank/overview.asp?siteid=495298

Optimale Vorgehensweisen zum Anwenden von Service Packs, Hotfixes und Sicherheitspatches:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/bpsp.asp (englischsprachig)

Referenzen/Hyperlinks

Microsoft TechNet Security-Website:
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/itsolutions/security/bestprac/secthret.asp (englischsprachig)

Microsoft Security Best Practices:
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/itsolutions/security/bestprac/secthret.asp (englischsprachig)

How to Publish non-MSI Programs with .zap Files (D41635):

http://support.microsoft.com/default.aspx?scid=http%3a%2f%2fwww.microsoft.com%2fIntlKB%2fGermany%2fsupport%2fkb%2fd41%2fd41635.htm

Originaltitel: Chapter 6 – Auditing and Intrusion Detection

6

Überwachung und Erkennung von Eindringversuchen

In einer sicheren Umgebung sollten Sie Überprüfungen in Bezug auf Eindringversuche und Angriffe durchführen. Nach dem Einrichten eines sicheren Systems kann nicht davon ausgegangen werden, dass keine Angriffe stattfinden können.

Das Überwachen von Eindringversuchen ist aus mehreren Gründen sehr wichtig. Im Folgenden werden einige der Gründe genannt:

- Eine funktionsfähige Computerumgebung ist der Gefahr möglicher Angriffe ausgesetzt. Unabhängig davon, wie hoch die Sicherheit Ihrer Computerumgebung ist, besteht immer das Risiko eines Angriffs.
- Erfolgreiche Angriffe sind häufig das Ergebnis einer Reihe erfolgloser Angriffe. Wenn Sie Ihre Umgebung nicht auf Angriffe hin überprüfen, können Sie mögliche Angriffe nicht vor ihrer erfolgreichen Durchführung aufspüren.
- Je früher Sie feststellen, dass ein erfolgreicher Angriff stattgefunden hat, desto einfacher ist die Schadensbegrenzung.
- Nach einem Angriff müssen Sie wissen, welcher Schaden verursacht wurde.
- Durch Überwachung und Erkennung von Eindringversuchen können Sie leichter ermitteln, wer für den Angriff verantwortlich ist.
- Durch die Kombination von Überwachung und Erkennung von Eindringversuchen können Sie Informationen leichter zueinander in Beziehung setzen und Angriffsmuster erkennen.
- Durch eine regelmäßige Überprüfung von Sicherheitsprotokollen können Sie unbekannte Probleme, die mit der Sicherheitskonfiguration zusammenhängen, leichter erkennen. Dazu gehören z. B. falsche Berechtigungen oder unsichere Einstellungen zur Kontosperrung.
- Nach einer Angriffserkennung kann durch eine Überwachung ermittelt werden, welche Netzwerkressourcen gefährdet wurden.

In diesem Kapitel wird gezeigt, wie Sie die Umgebung überwachen sollten, so dass Sie mit größter Wahrscheinlichkeit alle Angriffe entdecken. Außerdem wird die Überwachung von Eindringversuchen erläutert, einschließlich der Verwendung von Systemen zur Erkennung von Eindringversuchen. Dabei handelt es sich um Software, mit der Verhaltensweisen gefunden werden, die auf Angriffe hindeuten.

Überwachung

Im Rahmen Ihrer Sicherheitsstrategie sollten Sie ermitteln, in welchem Ausmaß Ihre Umgebung überwacht werden sollte. Bei der Überwachung sollten sowohl erfolgreiche als auch erfolglose Angriffe erkannt werden, die eine Gefahr für Ihr Netzwerk darstellen oder für Ressourcen, die Sie bei Ihrer Risikobeurteilung als wertvoll eingestuft haben.

Wenn Sie eine Entscheidung über das Ausmaß der Überwachung treffen, sollten Sie Folgendes beachten: Je mehr Sie überwachen, desto mehr Ereignisse werden generiert und desto schwieriger kann es sein, wichtige Ereignisse ausfindig zu machen. Wenn Sie eine umfassende Überwachung durchführen, sollten Sie auf jeden Fall den Einsatz zusätzlicher Tools erwägen, wie z. B. Microsoft Operations Manager, damit Sie wichtigere Ereignisse herausfiltern können.

Überwachungsereignisse können in zwei Kategorien eingeteilt werden: in Erfolgsereignisse und Fehlerereignisse. Ein Erfolgsereignis zeigt an, dass ein Benutzer erfolgreich auf eine Ressource zugegriffen hat. Ein Fehlerereignis zeigt an, dass ein Versuch unternommen wurde, der fehlgeschlagen ist. Fehlerereignisse sind sehr nützlich bei der Überwachung von Angriffsversuchen in Ihrer Umgebung. Die Interpretation von Erfolgsereignissen ist sehr viel schwieriger. Die meisten erfolgreichen Überwachungsereignisse sind lediglich ein Indiz für normale Aktivitäten. Ein Angreifer, der erfolgreich auf ein System zugreifen kann, generiert jedoch ebenfalls ein Erfolgsereignis. Ein Ereignismuster ist in vielen Fällen ebenso wichtig wie die Ereignisse selbst. Eine Reihe von Fehlern und ein darauf folgendes Erfolgsereignis könnten z. B. auf einen versuchten Angriff hinweisen, der schließlich erfolgreich war.

Sie sollten Überwachungsereignisse möglichst immer mit anderen Informationen zu den Benutzern in Ihrer Umgebung in Beziehung setzen. Wenn Benutzer z. B. in Urlaub gehen, können Sie ihre Konten während ihrer Abwesenheit deaktivieren und die erneute Aktivierung überwachen.

Aktivieren der Überwachung

Die Überwachung wird mithilfe von Gruppenrichtlinien für einen Standort, eine Domäne, Organisationseinheit oder einen lokalen Computer aktiviert. Die Einstellungen der Überwachungsrichtlinien finden Sie in:

Computerkonfiguration\Windows-Einstellungen\Sicherheits-einstellungen\Lokale Richtlinien\Überwachungsrichtlinien

Sie sollten die Überwachung normalerweise auf der oberen Ebene der Active Directory-Hierarchie implementieren, um eine Einheitlichkeit in Bezug auf die Überwachungseinstellungen aufrechtzuerhalten. In diesem Handbuch wird die Überwachung auf der Ebene der Organisationseinheit der Mitgliedsserver und Domänencontroller implementiert (weitere Informationen finden Sie in Kapitel 4, "Sichern von Servern basierend auf ihrer Rolle").

Möglicherweise verfügen Sie über Server, die von der Domäne getrennt sein sollen. Die Überwachung kann auf diesen Computern konfiguriert werden, indem die Gruppenrichtlinien für den lokalen Computer bearbeitet oder das Dienstprogramm **Auditpol.exe** im Resource Kit zu Windows 2000 Server verwendet wird.

Anmerkung: Um auf die Gruppenrichtlinien für einen lokalen Computer zuzugreifen, müssen Sie MMC (Microsoft Management Console) starten. Fügen Sie anschließend das Snap-In Gruppenrichtlinien hinzu, und setzen Sie den Fokus des Snap-Ins auf den lokalen Computer.

Definieren von Ereignisprotokolleinstellungen

Jedes durch eine Überwachung generierte Ereignis wird in der Ereignisanzeige angezeigt. Sie sollten festlegen, wie das Ereignisprotokoll die generierten Ereignisse speichern soll. Alle Einstellungen können direkt in der Ereignisanzeige oder in den Gruppenrichtlinien definiert werden. Für dieses Handbuch wurden die Einstellungen für die Ereignisanzeige über Gruppenrichtlinien definiert. Einzelheiten zu den empfohlenen Einstellungen finden Sie in Kapitel 4, "Sichern von Servern basierend auf ihrer Rolle".

Möglicherweise möchten Sie die in den Gruppenrichtlinien definierten Einstellungen ändern oder die Einstellungen auf einer anderen Ebene anwenden, beispielsweise wenn das Sicherheitsprotokoll zahlreiche Einträge zu Servern mit IIS enthält, die dazu führen, dass das System heruntergefahren wird. Um dies zu verhindern, sollten die Gruppenrichtlinien auf der Ebene der Organisationseinheit der Server mit IIS geändert werden, um ein umfangreicheres Sicherheitsprotokoll zu erhalten. Sie können auch die Richtlinie ändern, damit das System nicht heruntergefahren wird, wenn das Sicherheitsprotokoll voll ist. Mit dem folgenden Verfahren können Sie Sicherheitsprotokolleinstellungen in den Gruppenrichtlinien definieren:

So ändern Sie mithilfe von Gruppenrichtlinien die Ereignisprotokolleinstellungen für eine Organisationseinheit

1. Klicken Sie auf **Start**, zeigen Sie auf **Programme**, wählen Sie **Verwaltung** und dann **Active Directory-Benutzer und -Computer** aus.
2. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf die Organisationseinheit, für die Sie die Überwachungsrichtlinie definieren möchten, und klicken Sie dann auf **Eigenschaften**.
3. Wählen Sie die Registerkarte **Gruppenrichtlinien** aus, wählen Sie das Gruppenrichtlinienobjekt aus, das Sie bearbeiten möchten, und klicken Sie anschließend auf **Bearbeiten**.
4. Wechseln Sie im Gruppenrichtlinien-Editor zu **Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Ereignisprotokolle\Einstellungen für Ereignisprotokolle**.
5. Ändern Sie die Einstellungen je nach Anforderungen.

Wenn Sie die Einstellungen für die Ereignisanzeige aus den Gruppenrichtlinien entfernen, können Sie sie stattdessen direkt in der Ereignisanzeige definieren. Es wird jedoch empfohlen, die Einstellungen für die Ereignisanzeige in den Gruppenrichtlinien zu definieren, um sicherzustellen, dass Sie auf ähnlichen Computern über einheitliche Einstellungen verfügen.

Zu überwachende Ereignisse

Windows 2000 bietet mehrere Überwachungskategorien für Sicherheitsereignisse. Wenn Sie für Ihr Unternehmen eine Überwachungsstrategie entwerfen, müssen Sie entscheiden, ob die folgenden Kategorien der Sicherheitsüberwachungsereignisse eingeschlossen werden sollen:

Anmeldeereignisse

Kontoanmeldeereignisse

Objektzugriff

Verzeichnisdienstzugriff

Rechteverwendung

Prozessnachverfolgung

Systemereignisse

Richtlinienänderung

In den folgenden Abschnitten werden einige häufige Ereigniskennungen beschrieben, die zurückgegeben werden, wenn die Überwachung für bestimmte Kategorien aktiviert ist.

Anmerkung: Tools für die Suche nach und für das Sammeln von Ereignisprotokollinformationen werden im Abschnitt "Passive Erkennungsmethoden" weiter unten in diesem Kapitel beschrieben.

Anmeldeereignisse

Wenn Sie Anmeldeereignisse überwachen, wird jedes Mal, wenn sich ein Benutzer an einem Computer an- oder abmeldet, im Sicherheitsprotokoll dieses Computers ein Ereignis generiert. Auch wenn ein Benutzer eine Verbindung mit einem Remoteserver herstellt, wird im Sicherheitsprotokoll des Remoteservers ein Anmeldeereignis generiert. Anmeldeereignisse werden erstellt, wenn die Anmeldesitzung und das Token erstellt bzw. gelöscht werden.

Anmeldeereignisse können nützlich sein, um Versuche interaktiver Anmeldungen an Servern zu überwachen oder von einem bestimmten Computer ausgehende Angriffe zu untersuchen. Bei Erfolgsüberwachungen wird ein Überwachungseintrag generiert, wenn ein Anmeldeversuch erfolgreich ist. Bei Fehlerüberwachungen wird ein Überwachungseintrag generiert, wenn ein Anmeldeversuch fehlschlägt.

Anmerkung: Zu den Anmeldeereignissen gehören sowohl Computer- als auch Benutzeranmeldeereignisse. Wenn versucht wird, von einem Windows NT- oder Windows 2000-basierten Computer eine Netzwerkverbindung herzustellen, werden für das Computerkonto und das Benutzerkonto jeweils separate Protokolleinträge für Sicherheitsereignisse generiert. Bei Windows 9*x*-basierten Computern enthält das Verzeichnis keine Computerkonten, und für Netzwerkanmeldeereignisse werden keine Einträge für Computeranmeldeereignisse generiert.

In den Basisrichtlinien der Mitgliedsserver und Domänencontroller ist die Überwachung für Erfolgs- und Fehleranmeldereignisse aktiviert. Daher werden die folgenden Ereigniskennungen für interaktive Anmeldevorgänge angezeigt sowie für Terminaldiensteanmeldungen, bei denen eine Verbindung mit Computern hergestellt wird, die Terminaldienste ausführen.

Tabelle 6.1: Im Ereignisprotokoll angezeigte Anmeldeereignisse

Ereigniskennung	Beschreibung
528	Ein Benutzer hat sich erfolgreich an einem Computer angemeldet.
529	Der Anmeldeversuch ist mit einem unbekannten Benutzernamen oder einem bekannten Benutzernamen mit einem falschen Kennwort erfolgt.
530	Der Anmeldeversuch mithilfe des Benutzerkontos erfolgte außerhalb der zulässigen Zeit.
531	Ein Anmeldeversuch ist mithilfe eines deaktivierten Kontos erfolgt.
532	Ein Anmeldeversuch ist mithilfe eines abgelaufenen Kontos erfolgt.
533	Der Benutzer darf sich an diesem Computer nicht anmelden.
534	Der Benutzer hat versucht, sich mit einem unzulässigen Anmeldetyp anzumelden (z. B. Netzwerkanmeldung, interaktive Anmeldung, Batchanmeldung, Dienstanmeldung oder interaktive Remoteanmeldung).

Ereigniskennung	Beschreibung
535	Das Kennwort für das angegebene Konto ist abgelaufen.
536	Der Netzwerkanmeldedienst ist nicht aktiviert.
537	Der Anmeldeversuch ist aus anderen Gründen fehlgeschlagen.
538	Ein Benutzer hat sich abgemeldet.
539	Das Konto wurde zu dem Zeitpunkt gesperrt, als der Anmeldeversuch erfolgte. Dieses Ereignis kann darauf hinweisen, dass ein erfolgloser Kennwortangriff gestartet und das Konto daraufhin gesperrt wurde.
540	Erfolgreiche Netzwerkanmeldung. Dieses Ereignis zeigt an, dass ein Remotebenutzer erfolgreich eine Verbindung vom Netzwerk zu einer lokalen Ressource auf dem Server hergestellt hat. Dabei wurde ein Token für den Netzwerkbenutzer generiert.
682	Ein Benutzer hat die Verbindung zu einer getrennten Terminaldienstesitzung wiederhergestellt. Dieses Ereignis kann darauf hinweisen, dass die Verbindung zu einer vorhergehenden Terminaldienstesitzung hergestellt wurde.
683	Ein Benutzer hat die Verbindung zu einer Terminaldienstesitzung getrennt, ohne sich abzumelden. Dieses Ereignis wird generiert, wenn ein Benutzer über das Netzwerk mit einer Terminaldienstesitzung verbunden ist. Es wird auf dem Terminalserver angezeigt.

Die folgenden Sicherheitsereignisse können mithilfe von Einträgen für Anmeldeereignisse diagnostiziert werden:

Lokaler Anmeldeversuch ist fehlgeschlagen. Folgende Ereigniskennungen zeigen fehlgeschlagene Anmeldeversuche an: 529, 530, 531, 532, 533, 534 und 537. Die Ereigniskennungen 529 und 534 werden angezeigt, wenn ein Angreifer die falsche Kombination aus Benutzername und Kennwort für ein lokales Konto eingegeben hat. Diese Ereignisse können auch auftreten, wenn ein Benutzer sein Kennwort vergessen hat oder das Netzwerk über die Netzwerkumgebung durchsucht. In einer Umgebung mit großem Umfang kann es sich als schwierig erweisen, diese Ereignisse effektiv zu interpretieren. Grundsätzlich sollten Sie diesen Mustern nachgehen, wenn sie wiederholt oder gemeinsam mit anderen ungewöhnlichen Vorkommnissen auftreten. Beispielsweise kann die Ereigniskennung 528 infolge mehrerer Ereignisse der Kennung 529 mitten in der Nacht auf einen erfolgreichen Kenntwortangriff hinweisen (oder nur auf einen übermüdeten Administrator).

Kontomissbrauch. Die Ereigniskennungen 530, 531, 532 und 533 können den Missbrauch eines Benutzerkontos anzeigen. Die Ereigniskennungen weisen darauf hin, dass die Kombination Konto/Kennwort zwar richtig eingegeben wurde, andere Beschränkungen aber die erfolgreiche Anmeldung verhindern. Wenn möglich, sollten Sie diesen Ereignissen nachgehen und ermitteln, ob ein Missbrauch vorliegt oder ob die aktuellen Beschränkungen geändert werden müssen. Beispielsweise kann es nötig sein, die Anmeldezeiten bestimmter Konten zu verlängern.

Kontosperrungen. Die Ereigniskennung 539 zeigt an, dass das Konto gesperrt wurde. Das kann darauf hinweisen, dass ein Kennwortangriff fehlgeschlagen ist. Sie sollten nach früheren Ereignissen der Kennung 529 desselben Benutzerkontos suchen, um das Muster der versuchten Anmeldungen erkennen zu können.

Angriffe auf Terminaldienste. Terminaldienstesitzungen können im verbundenen Status verbleiben. Auch nach Beendung der Sitzung wird dadurch ein Fortsetzen aktiver Prozesse ermöglicht. Die Ereigniskennung 683 zeigt an, dass ein Benutzer sich nicht von der Terminaldienstesitzung abgemeldet hat. Die Ereigniskennung 682 zeigt an, dass eine Verbindung zu einer zuvor getrennten Sitzung aufgenommen wurde.

Kontoanmeldeereignisse

Wenn sich ein Benutzer an einer Domäne anmeldet, wird die Anmeldung auf einem Domänencontroller verarbeitet. Wenn Sie Kontoanmeldeereignisse auf Domänencontrollern überwachen, wird dieser Anmeldeversuch auf dem Domänencontroller aufgezeichnet, der das Konto überprüft. Kontoanmeldeereignisse werden bei der Überprüfung der Benutzerinformationen durch ein Authentifizierungspaket erstellt. Bei der Verwendung von Domäneninformationen werden die Kontoanmeldeereignisse nur in den Ereignisprotokollen der Domänencontroller generiert. Wenn die angegebenen Anmeldeinformationen lokale SAM-Datenbankinformationen (Security Accounts Manager oder Sicherheitskontenverwaltung) sind, werden die Kontoanmeldeereignisse im Sicherheitsereignisprotokoll des Servers erstellt.

Da das Kontoanmeldeereignis auf jedem gültigen Domänencontroller in der Domäne aufgezeichnet werden kann, müssen Sie zur Analyse sämtlicher Kontoanmeldeereignisse in der Domäne sicherstellen, dass Sie die Sicherheitsprotokolle domänencontrollerübergreifend konsolidieren.

Anmerkung: Vergleichbar den Anmeldeereignissen gehören auch zu den Kontoanmeldeereignissen sowohl Computer- als auch Benutzeranmeldeereignisse.

In den Basisrichtlinien der Mitgliedsserver und Domänencontroller ist die Überwachung für Erfolgs- und Fehlerereignisse bei der Kontoanmeldung aktiviert. Daher werden die folgenden Ereigniskennungen für Netzwerkanmeldevorgänge und Terminaldiensteauthentifizierung angezeigt:

Tabelle 6.2: Im Ereignisprotokoll angezeigte Kontoanmeldeereignisse

Ereigniskennung	Beschreibung
672	Ein Authentifizierungsdienstticket (AS oder Authentication Service) wurde erfolgreich ausgestellt und überprüft.
673	Ein Ticketerteilunsdienst-Ticket (TGS oder Ticket Granting Service) wurde erteilt.
674	Ein Sicherheitsprincipal wurde als AS-Ticket oder TGS-Ticket erneuert.
675	Vorbestätigung ist fehlgeschlagen.
676	Anfrage für Authentifizierungsticket ist fehlgeschlagen.
677	Ein TGS-Ticket wurde nicht erteilt.
678	Ein Konto wurde erfolgreich einem Domänenkonto zugeordnet.
680	Gibt das für den erfolgreichen Anmeldeversuch verwendete Konto an. Dieses Ereignis zeigt auch das zur Authentifizierung des Kontos verwendete Authentifizierungspaket an.
681	Der Versuch einer Domänenkontoanmeldung wurde unternommen.
682	Ein Benutzer hat die Verbindung zu einer getrennten Terminaldienstesitzung wiederhergestellt.
683	Ein Benutzer hat die Verbindung zu einer Terminaldienstesitzung getrennt, ohne sich abzumelden.

Für jedes dieser Ereignisse zeigt das Ereignisprotokoll detaillierte Informationen zu jeder speziellen Anmeldung an. Die folgenden Sicherheitsereignisse können mithilfe von Einträgen für Kontoanmeldeereignisse diagnostiziert werden:

Domänenanmeldeversuch ist fehlgeschlagen. Die Ereigniskennungen 675 und 677 zeigen fehlgeschlagene Domänenanmeldeversuche an.

Zeitsynchronisierungsaspekte. Die Zeit des Clientcomputers unterscheidet sich von der Zeit des Authentifizierungsdomänencontrollers um mehr als fünf Minuten (standardmäßig). Die Ereigniskennung 675 wird im Sicherheitsprotokoll angezeigt.

Angriffe auf Terminaldienste. Terminaldienstesitzungen können im verbundenen Status verbleiben. Auch nach Beendigung der Terminalserversitzung wird dadurch ein Fortsetzen aktiver Prozesse ermöglicht. Die Ereigniskennung 683 zeigt an, dass ein Benutzer sich nicht von der Terminaldienstesitzung abgemeldet hat. Die Ereigniskennung 682 zeigt an, dass eine Verbindung zu einer zuvor getrennten Sitzung aufgenommen wurde. Definieren Sie in der Konsole zur Terminaldienstekonfiguration in den Eigenschaften des RDP-TCP-Protokolls die Option **Zeitraum zum Beenden getrennter Sitzungen**, um Abbrüche zu verhindern oder abgebrochene Sitzungen zu beenden.

Kontenmanagement

Mit der Überwachung des Kontenmanagements (Account Management) wird festgelegt, wann Benutzer oder Gruppen erstellt, geändert oder gelöscht werden. Mit dieser Überwachung kann ermittelt werden, wann ein Sicherheitsprincipal erstellt wurde und wer die Aufgabe ausgeführt hat.

In den Basisrichtlinien der Mitgliedsserver und Domänencontroller ist die Überwachung für Erfolgs- und Fehlerereignisse beim Kontenmanagement aktiviert. Daher wird die Aufzeichnung der folgenden Ereigniskennungen im Sicherheitsprotokoll angezeigt:

Tabelle 6.3: Im Ereignisprotokoll angezeigte Kontenmanagementereignisse

Ereigniskennung	Beschreibung
624	Benutzerkonto wurde erstellt.
625	Benutzerkontotyp wurde geändert.
626	Benutzerkonto wurde aktiviert.
627	Versuch einer Kennwortänderung wurde unternommen.
628	Benutzerkontokennwort wurde festgelegt.
629	Benutzerkonto wurde deaktiviert.
630	Benutzerkonto wurde gelöscht.
631	Globale Gruppe mit aktivierter Sicherheit wurde erstellt.
632	Globales Gruppenmitglied mit aktivierter Sicherheit wurde hinzugefügt.
633	Globales Gruppenmitglied mit aktivierter Sicherheit wurde entfernt.
634	Globale Gruppe mit aktivierter Sicherheit wurde gelöscht.
635	Lokale Gruppe mit aktivierter Sicherheit wurde erstellt.
636	Lokales Gruppenmitglied mit aktivierter Sicherheit wurde hinzugefügt.
637	Lokales Gruppenmitglied mit aktivierter Sicherheit wurde entfernt.
638	Lokale Gruppe mit aktivierter Sicherheit wurde gelöscht.
639	Lokale Gruppe mit aktivierter Sicherheit wurde geändert.
641	Globale Gruppe mit aktivierter Sicherheit wurde geändert.
642	Benutzerkonto wurde geändert.
643	Domänenrichtlinien wurden geändert.
644	Benutzerkonto wurde gesperrt.

Die folgenden Kontenmanagementereignisse können mithilfe von Sicherheitsprotokolleinträgen diagnostiziert werden:

Erstellung eines Benutzerkontos. Die Ereigniskennungen 624 und 626 zeigen das Erstellen und Aktivieren von Benutzerkonten an. Wenn die Kontoerstellung auf bestimmte Individuen in der Organisation begrenzt ist, können Sie diese Ereignisse verwenden, um Kontoerstellungen durch unberechtigte Benutzer zu erkennen.

Benutzerkontokennwort wurde geändert. Die Änderung eines Kennwortes durch eine andere Person als den Benutzer kann darauf hindeuten, dass ein Konto von einem anderen Benutzer übernommen wurde. Achten Sie auf die Ereigniskennungen 627 und 628. Sie zeigen an, dass eine Kennwortänderung erfolgreich durchgeführt wurde. Überprüfen Sie die Einzelheiten, um zu ermitteln, ob ein anderes Konto die Änderungen veranlasst hat und ob das Konto ein Mitglied des Helpdesks oder eines anderen Serviceteams ist, das Benutzerkontokennwörter zurücksetzt.

Benutzerkontostatus wurde geändert. Es ist möglich, dass ein Angreifer seine Spuren zu verwischen versucht, indem er das zum Angriff verwendete Konto deaktiviert oder löscht. Alle Vorkommnisse der Ereigniskennungen 629 und 630 sollten untersucht werden, um sicherzustellen, dass sie autorisierte Transaktionen darstellen. Achten Sie auf die Ereigniskennung 629 kurz nach Vorkommnissen der Ereigniskennung 626. Dies kann darauf hindeuten, dass ein deaktiviertes Konto aktiviert, verwendet und anschließend wieder deaktiviert wurde.

Änderung von Sicherheitsgruppen. Mitgliedschaftsänderungen für Domänenadministratoren, Administratoren, Operatorengruppen oder benutzerdefinierte globale, universale oder lokale Domänengruppen, denen administrative Funktionen übertragen wurden, sollten überprüft werden. Änderungen globaler Gruppenmitgliedschaften werden in Ereignissen mit den Kennungen 632 und 633 aufgezeichnet. Änderungen lokaler Domänengruppenmitgliedschaften werden in Ereignissen mit den Kennungen 636 und 637 aufgezeichnet.

Kontosperrung. Bei der Sperrung eines Kontos werden zwei Ereignisse auf dem Betriebsmaster des PDC-Emulators protokolliert. Ein Ereignis der Kennung 644 zeigt an, dass der Kontoname gesperrt wurde. Zur Angabe des gesperrten Kontos wird daraufhin ein Ereignis der Kennung 642 aufgezeichnet. Dieses Ereignis wird nur am PDC-Emulator protokolliert.

Objektzugriff

Sämtliche Objekte in einem Windows 2000-basierten Netzwerk mit einer Systemzugriffskontrollliste (SACL oder System Access Control List) können überwacht werden. Eine SACL enthält eine Liste der Benutzer und Gruppen, deren Aktionen auf dem Objekt überwacht werden sollen. Fast jedes Objekt, das ein Benutzer in Windows 2000 ändern kann, verfügt über eine SACL. Dies beinhaltet Dateien und Ordner auf NTFS-Laufwerken, Druckern und Registrierungsschlüssel.

Eine SACL setzt sich aus Zugriffskontrolleinträgen (ACEs oder Access Control Entries) zusammen. Jeder ACE enthält drei Informationen:

Den zu überwachenden Sicherheitsprincipal

Die zu überwachenden Zugriffstypen, Zugriffsmaske genannt

Ein Flag zur Kennzeichnung, ob der Zugriff zur Überwachung fehlgeschlagen ist, erfolgreich war oder beides

Wenn Ereignisse im Sicherheitsprotokoll aufgeführt werden sollen, müssen Sie zuerst **Objektzugriffsversuche überwachen** aktivieren und dann die SACL für jedes zu überwachende Objekt definieren.

In Windows 2000 werden Überwachungen generiert, sobald ein Handle zu einem Objekt geöffnet wird. Windows 2000 verwendet ein Kernelmodus-Sicherheitsteilsystem, das Programmen den Zugriff nur durch den Kernel gewährt. Dadurch wird verhindert, dass Programme das Sicherheitssystem umgehen. Da der Kernelspeicherplatz von Benutzermodusprogrammen isoliert ist, verweist ein Programm auf ein Objekt mithilfe einer Datenstruktur, die Handle genannt wird. Dies ist ein Beispiel für einen typischen Zugriffsversuch:

1. Ein Benutzer weist ein Programm zum Zugreifen auf ein Objekt an (z. B. **Datei** und dann **Öffnen**).
2. Das Programm fordert vom System ein Handle zur Angabe der gewünschten Zugriffsart an (Lesen, Schreiben etc.).
3. Das Sicherheitsteilsystem vergleicht die DACL auf dem angeforderten Objekt mit dem Token des Benutzers und sucht nach Einträgen in der DACL, die entweder mit dem Benutzer oder einer Gruppe, zu der der Benutzer gehört, übereinstimmen. Zudem verfügt das Sicherheitsteilsystem über die Zugriffsrechte, die das Programm fordert.
4. Das System vergleicht die SACL auf dem angeforderten Objekt mit dem Token des Benutzers und sucht nach Einträgen in der SACL, die entweder mit den vom Programm zurückgegebenen Rechten oder den vom Programm angeforderten Rechten übereinstimmen. Wenn eine übereinstimmende Fehlerüberwachungs-ACE mit einem angeforderten, aber nicht gewährten Zugriff übereinstimmt, wird ein Fehlerüberwachungsereignis generiert. Wenn eine übereinstimmende Erfolgsüberwachungs-ACE mit einem gewährten Zugriff übereinstimmt, wird ein Erfolgsüberwachungsereignis generiert.

5. Wenn ein Zugriff gewährt wird, gibt das System ein Handle an das Programm zurück, das dann das Handle zum Zugreifen auf das Objekt verwenden kann.

An dieser Stelle muss darauf hingewiesen werden, dass während der Überwachung und der Generierung des Ereignisses *noch keine Veränderungen am Objekt vorgenommen werden*. Für die Auswertung von Überwachungsereignissen ist dies unbedingt erforderlich. Schreibüberwachungen werden generiert, noch bevor in eine Datei geschrieben wird. Leseüberwachungen werden generiert, noch bevor eine Datei gelesen wird.

Wie bei jeder Überwachung ist es auch hier wichtig, eine Zielvorgabe für die Überwachung von Objektzugriffen zu definieren. Bestimmen Sie in Ihrer Überwachungsplanung, welche Objekttypen überwacht werden müssen und welche Zugriffstypen (Erfolg, Fehler oder beide) Sie für jeden überwachten Objekttyp überwachen möchten. Ein allzu breit gefächerter Überwachungsansatz wird sich deutlich auf die Systemleistung auswirken und mehr Informationen als nötig oder sinnvoll sammeln.

Im Allgemeinen möchten Sie sicher alle Zugriffe auf die ausgewählten Objekte, auch von nicht vertrauenswürdigen Konten, überwachen. Hierzu fügen Sie die Gruppe **Jeder** zur SACL für die zu überwachenden Objekte hinzu. Mit der Überwachung von erfolgreichen Objektzugriffen sollten Sie vorsichtig umgehen, denn dies kann zu einer Vielzahl von Überwachungseinträgen im Sicherheitsprotokoll führen. Wenn Sie aber beispielsweise das Löschen einer wichtigen Datei untersuchen, werden Sie Erfolgsüberwachungsereignisse überprüfen müssen, um zu ermitteln, welches Benutzerkonto die Datei gelöscht hat.

Die Basisrichtlinien der Mitgliedsserver und Domänencontroller legen sowohl die Erfolgs- als auch die Fehlerüberwachung für Objektzugriffe fest. Jedoch werden für die Objekte selbst keine SACLs festgelegt. Diese müssen Sie entsprechend den Bedürfnissen Ihrer Umgebung selbst festlegen. Die SACLs können direkt an den Objekten oder mithilfe von Gruppenrichtlinien definiert werden. Wenn sich das zu überwachende Objekt auf mehreren Computern befindet, sollten Sie die SACLs durch Gruppenrichtlinien definieren.

Durch die Überwachung des Objektzugriffs werden die folgenden Ereignisse im Sicherheitsprotokoll angezeigt:

Tabelle 6.4: Im Ereignisprotokoll angezeigte Objektzugriffsereignisse

Ereigniskennung	Beschreibung
560	Für ein bereits bestehendes Objekt wurde Zugriff gewährt.
562	Ein Handle zu einem Objekt wurde geschlossen.
563	Ein Objekt wurde in der Absicht geöffnet, es zu löschen. (Hiervon machen Dateisysteme Gebrauch, wenn der FILE_DELETE_ON_CLOSE-Flag festgelegt ist.)
564	Ein geschütztes Objekt wurde gelöscht.
565	Für einen bereits bestehenden Objekttyp wurde Zugriff gewährt.

Wenn Sie bestimmte Objektzugriffsereignisse suchen, werden Sie diese meist in Ereignissen mit der Ereigniskennung 560 finden. Suchen Sie in den Ereignisdetails, denn dort finden Sie nützliche Informationen zu den jeweiligen gesuchten Ereignissen. Tabelle 6.5 zeigt einige Aktionen, die Sie möglicherweise durchführen müssen, und bietet Informationen zu deren Ausführung.

Tabelle 6.5: Informationen zu Schlüsselüberwachungsaktionen für Objektzugriffsereignisse der Kennung 560

Überwachungsaktion	Informationen zur Ausführung
Suchen einer bestimmten Datei, eines bestimmten Ordners oder eines bestimmten Objekts	Suchen Sie in den Details zur Ereigniskennung 560 nach dem vollständigen Pfad der Datei oder des Ordners, deren oder dessen Aktionen Sie überprüfen möchten.
Ermitteln von Aktionen eines bestimmten Benutzers	Definieren Sie einen Filter, der den Benutzer in einem Ereignis der Kennung 560 identifiziert.
Ermitteln von an einem bestimmten Computer ausgeführten Aktionen	Definieren Sie einen Filter, der das Computerkonto identifiziert, für das ein Ereignis der Kennung 560 ausgeführt wurde.

Verzeichnisdienstzugriff

Aktive Verzeichnisobjekte sind mit SACLs verbunden und können so überwacht werden. Wie zuvor bereits erwähnt, können durch die Überwachung des Kontenmanagements auch Benutzer- und Gruppenkonten von Active Directory überwacht werden. Wenn Sie jedoch Änderungen von Objekten in anderen Namenskontexten überwachen möchten (z. B. im Konfigurations- und Schemanamenskontext), muss der Objektzugriff überwacht und die SACL für die zu überwachenden Container definiert werden. Überwachungseinträge werden generiert, sobald in der SACL eines Active Directory-Objekts aufgeführte Benutzer auf dieses Objekt zugreifen möchten.

Die SACL für Container und Objekte kann im Konfigurationsnamenskontext (und in anderen Namenskontexten) mithilfe des Snap-Ins ADSIEDIT MMC geändert werden. Dies wird durch das Anzeigen des erforderlichen Kontextes in der ADSIEDIT-Konsole mit anschließender Änderung der SACL für das Objekt im Dialogfeld **Erweiterte Sicherheitseinstellungen** erreicht.

Das Auffinden bestimmter Ereignisse für den Verzeichnisdienstzugriff gestaltet sich aufgrund der großen Volumen der stattfindenden (generell unbedenklichen) Ereignisse sehr schwierig. Deshalb überwachen Basisrichtlinien der Mitgliedsserver und Domänencontroller nur fehlgeschlagene Ereignisse des Verzeichnisdienstzugriffs. Dies trägt zur leichteren Identifizierung von Angreifern bei, die einen unautorisierten Zugriff auf Active Directory versuchen.

Ein versuchter Verzeichniszugriff wird im Sicherheitsprotokoll als Verzeichnisdienstereignis mit der Kennung 565 angezeigt. Nur durch Untersuchung der Details des Sicherheitsereignisses kann ermittelt werden, welchem Objekt das Ereignis zugeordnet werden kann.

Rechteverwendung

Benutzer in einer IT-Umgebung üben definierte Benutzerrechte aus. Wenn Sie sowohl Erfolge als auch Fehler der Rechteverwendung überwachen, wird bei jedem Ausüben von Benutzerrechten durch einen Benutzer ein Ereignis generiert.

Auch wenn Sie die Rechteverwendung überwachen, werden nicht alle Benutzerrechte überwacht. Standardmäßig sind die folgenden Benutzerrechte von der Überwachung ausgeschlossen:

Umgehen der durchsuchenden Überprüfung

Debuggen von Programmen

Erstellen eines Tokenobjekts

Ersetzen eines Tokens auf Prozessebene

Generieren von Sicherheitsüberwachungen

Sichern von Dateien und Verzeichnissen

Wiederherstellen von Dateien und Verzeichnissen

Das Standardverhalten, das Sicherungs- und Wiederherstellungsrecht von Benutzern nicht zu überwachen, kann durch Aktivieren der Sicherheitsoption **Die Verwendung des Sicherungs- und Wiederherstellungsrechts überprüfen** der Gruppenrichtlinien außer Kraft gesetzt werden.

Die Erfolgsüberwachung der Rechteverwendung erstellt eine sehr große Anzahl von Einträgen im Sicherheitsprotokoll. Deshalb überwachen Basisrichtlinien der Mitgliedsserver und Domänencontroller nur fehlgeschlagene Versuche bei der Rechteverwendung.

Die folgenden Ereignisse werden bei aktivierter Überwachung der Rechteverwendung generiert:

Tabelle 6.6: Im Ereignisprotokoll angezeigte Rechteverwendungsereignisse

Ereigniskennung	Beschreibung
576	Bestimmte Rechte wurden zum Zugriffstoken eines Benutzers hinzugefügt. (Dieses Ereignis wird generiert, sobald sich der Benutzer anmeldet.)
577	Ein Benutzer hat versucht, einen privilegierten Systemdienstevorgang auszuführen.
578	Rechte wurden in Bezug auf ein bereits geöffnetes Handle für ein geschütztes Objekt verwendet.

Es folgenden einige Beispiele von Ereignisprotokolleinträgen, die bei der Verwendung bestimmter Benutzerrechte bestehen können:

Als Teil des Betriebssystems handeln. Achten Sie auf die Ereigniskennungen 577 oder 578 mit dem angezeigten Recht `SeTcbPrivilege`. Das Benutzerkonto, das dieses Benutzerrecht verwendet hat, wird in den Ereignisdetails angezeigt. Dieses Ereignis kann auf einen Benutzerversuch hindeuten, Sicherheitsrechte durch Handeln als Teil des Betriebssystems zu erhöhen. Dies gilt beispielsweise für den **GetAdmin**-Angriff, bei dem ein Benutzer versucht hat, sein Konto zur Administratorengruppe hinzuzufügen, die dieses Recht verwendet. Die einzigen Einträge für dieses Ereignis sollten die für das Systemkonto und weitere dem Benutzerrecht zugewiesene Dienstkonten sein.

Systemzeit ändern. Achten Sie auf die Ereigniskennungen 577 oder 578 mit dem angezeigten Recht `SeSystemtimePrivilege`. Das Benutzerkonto, das dieses Benutzerrecht verwendet hat, wird in den Ereignisdetails angezeigt. Dieses Ereignis kann auf einen Benutzerversuch hindeuten, die Systemzeit zu ändern, um den tatsächlichen Zeitpunkt eines Ereignisses zu verschleiern.

Erzwingen des Herunterfahrens von einem Remotesystem aus. Achten Sie auf die Ereigniskennungen 577 und 578 mit dem angezeigten Benutzerrecht `SeRemoteShutdownPrivilege`. Die Sicherheits-ID (SID), der das Benutzerrecht zugeordnet ist, und der Benutzername des Sicherheitsprincipals, der das Recht zugeordnet hat, sind in den Ereignisdetails enthalten.

Laden und Entladen von Gerätetreibern. Achten Sie auf die Ereigniskennungen 577 oder 578 mit dem angezeigten Recht `SeLoadDriverPrivilege`. Das Benutzerkonto, das dieses Benutzerrecht verwendet hat, wird in den Ereignisdetails angezeigt. Dieses Ereignis kann auf einen Benutzerversuch hindeuten, eine unautorisierte Version eines Gerätetreibers oder ein Trojanisches Pferd zu laden.

Verwalten von Überwachungs- und Sicherheitsprotokollen. Achten Sie auf die Ereigniskennungen 577 oder 578 mit dem angezeigten Recht `SeSecurityPrivilege`. Das Benutzerkonto, das dieses Benutzerrecht verwendet hat, wird in den Ereignisdetails angezeigt. Dieses Ereignis tritt auf, wenn das Ereignisprotokoll gelöscht wird und wenn Ereignisse zur Rechteverwendung in das Sicherheitsprotokoll geschrieben werden.

Herunterfahren des Systems Achten Sie auf die Ereigniskennungen 577 mit dem angezeigten Recht `SeShutdownPrivilege`. Das Benutzerkonto, das dieses Benutzerrecht verwendet hat, wird in den Ereignisdetails angezeigt. Dieses Ereignis tritt auf, wenn ein Versuch unternommen wurde, den Computer herunterzufahren.

Übernehmen des Besitzes von Dateien und anderen Objekten. Achten Sie auf die Ereigniskennungen 577 oder 578 mit dem angezeigten Recht `SeTakeOwnershipPrivilege`. Das Benutzerkonto, das dieses Benutzerrecht verwendet hat, wird in den Ereignisdetails angezeigt. Dieses Ereignis kann auf einen versuchten Angriff mit dem Ziel hindeuten, aktuelle Sicherheitseinstellungen durch Übernahme des Besitzes eines Objekts zu umgehen.

Prozessnachverfolgung

Wenn für Prozesse auf Windows 2000-basierten Computern detaillierte Prozessnachverfolgungsinformationen überwacht werden, werden im Ereignisprotokoll Versuche der Erstellung und Beendigung von Prozessen anzeigt. Auch der Versuch eines Prozesses, ein Handle zu einem Objekt zu generieren oder indirekten Zugriff auf ein Objekt zu erhalten, wird aufgezeichnet.

Aufgrund der sehr großen Anzahl der erstellten Überwachungseinträge ermöglichen die Basisrichtlinien der Mitgliedsserver und Domänencontroller keine Überwachung zum Zweck der Prozessnachverfolgung. Wenn Sie dennoch Erfolge und Fehler überwachen, wird die folgende Ereigniskennung im Ereignisprotokoll aufgezeichnet:

Tabelle 6.7: Im Ereignisprotokoll angezeigte Prozessnachverfolgungsereignisse

Ereigniskennung	Beschreibung
592	Ein neuer Prozess wurde erstellt.
593	Ein Prozess wurde beendet.
594	Ein Handle zu einem Objekt wurde dupliziert.
595	Ein indirekter Zugriff auf ein Objekt wurde erhalten.

Systemereignisse

Systemereignisse werden generiert, wenn ein Benutzer oder ein Prozess Aspekte der Computerumgebung ändert. Sie können Versuche überwachen, Systemänderungen (wie das Herunterfahren des Computers) oder eine Änderung der Systemzeit vornehmen.

Wenn Sie Systemereignisse überwachen, können Sie auch den Zeitpunkt des Löschens des Sicherheitsprotokolls überwachen. Dies ist sehr wichtig, denn Angreifer versuchen oft, ihre Spuren zu verwischen, nachdem sie Änderungen in einer Umgebung vorgenommen haben.

Die Basisrichtlinien der Mitgliedsserver und Domänencontroller überwachen Ereignisse auf Erfolg oder Fehler. Dies führt zu folgenden Ereigniskennungen im Ereignisprotokoll:

Tabelle 6.8: Im Ereignisprotokoll angezeigte Systemereignisse

Ereigniskennung	Beschreibung
512	Windows wird gestartet.
513	Windows wird heruntergefahren.
514	Ein Authentifizierungspaket wurde von der lokalen Sicherheitsautorität (LSA oder Local Security Authority) geladen.
515	Ein vertrauenswürdiger Anmeldevorgang wurde bei der lokalen Sicherheitsautorität registriert.
516	Die für das Einreihen von Sicherheitsereignismeldungen in Warteschlangen zugewiesenen internen Ressourcen sind ausgelastet. Dies führt zu einem Verlust von Sicherheitsereignismeldungen.
517	Das Sicherheitsprotokoll wurde gelöscht.
518	Die Sicherheitskontenverwaltung hat ein Benachrichtigungspaket geladen.

Die Ereigniskennungen können zur Erfassung einiger Sicherheitsprobleme verwendet werden:

Herunterfahren/Neustarten des Computers. Die Ereigniskennung 513 kennzeichnet das Herunterfahren von Windows. Es ist wichtig, den Zeitpunkt zu kennen, zu dem Server heruntergefahren oder neugestartet wurden. Es gibt eine Reihe legitimer Gründe, wie z. B. die Installation eines Treibers oder einer Anwendung, die einen Neustart erforderlich machen, sowie das Herunterfahren oder Neustarten zu Wartungszwecken. Jedoch kann auch ein Angriff den Neustart eines Servers erzwingen, um während des Starts Zugriff auf das System zu erhalten. Alle Fälle, in denen der Computer heruntergefahren wurde, sollten für einen Vergleich mit dem Ereignisprotokoll notiert werden.

Viele Angriffe führen zu einem Neustart des Computers. Anhand der Ereignisprotokolle können Sie ermitteln, wann ein Server neugestartet wurde und ob der Neustart ein geplanter Vorgang war. Die Ereigniskennung 513 kennzeichnet das Starten von Windows, ebenso wie eine Reihe anderer Ereignisse, die im Systemprotokoll automatisch generiert werden. Dies beinhaltet auch die Ereigniskennung 6005, die den Start des Ereignisprotokolldienstes kennzeichnet.

Achten Sie zusätzlich zu diesem Eintrag auf ein oder zwei unterschiedliche Ereignisprotokolleinträge im Systemprotokoll. Wenn das vorhergehende Herunterfahren ein geplanter Vorgang war (z. B. wenn der Administrator den Computer neugestartet hat), wird die Ereigniskennung 6006 (Der Ereignisprotokolldienst wurde beendet) im Systemprotokoll aufgezeichnet. Anhand der Details des Eintrags können Sie ermitteln, welcher Benutzer das Herunterfahren initiiert hat.

Wenn es sich hingegen um einen unerwarteten Neustart (Ereigniskennung 6008) handelt, war das vorhergehende Herunterfahren des Systems um <*Zeit*> am <*Datum*> unerwartet. Dies kann auf einen DoS-Angriff (Denial-of-Service) hinweisen, aufgrund dessen der Computer herunterfahren wurde. Jedoch kann der Grund für das Herunterfahren ebenso eine Unterbrechung der Stromzufuhr sein oder ein Fehler des Gerätetreibers.

Wenn der Neustart aufgrund eines Bluescreens erfolgt ist (Ereigniskennung 1001), wird dies im Systemprotokoll mit der Quellangabe **Save Dump** aufgezeichnet. Die eigentliche Bluescreen-Fehlermeldung kann in den Ereignisdetails überprüft werden.

Anmerkung: Damit die Einträge der Ereigniskennung 1001 eingeschlossen werden, muss das Kontrollkästchen **Ereignis in das Systemprotokoll eintragen** in den Wiederherstellungseinstellungen der Systemsteuerung aktiviert sein.

Ändern oder Löschen des Sicherheitsprotokolls Um nicht entdeckt zu werden, versucht ein Angreifer möglicherweise die Sicherheitsprotokolle zu ändern, die Überwachung während eines Angriffs zu deaktivieren oder die Sicherheitsprotokolle zu löschen. Wenn Ihnen im Systemprotokoll größere Zeitblöcke ohne Einträge auffallen, sollten Sie nach den Ereigniskennungen 612 und 517 suchen, um zu ermitteln, welcher Benutzer die Überwachungsrichtlinie geändert hat. Sämtliche Vorkommnisse mit der Ereigniskennung 517 sollten mit einem physischen Protokoll verglichen werden, das die Zeiten aufführt, zu denen das Sicherheitsprotokoll gelöscht wurde. Ein unautorisiertes Löschen des Sicherheitsprotokolls kann der Versuch sein, Ereignisse, die in dem vorherigen Sicherheitsprotokoll vorhanden waren, zu verbergen. In den Ereignisdetails ist der Name des Benutzers enthalten, der das Protokoll gelöscht hat.

Richtlinienänderung

Die Überwachungsrichtlinien definieren, welche Umgebungsänderungen überwacht werden, und sie helfen Ihnen beim Ermitteln von Angriffen auf Ihre Umgebung. Ein versierter Angreifer wird jedoch versuchen, die Überwachungsrichtlinien zu ändern, damit von ihm vorgenommene Änderungen nicht überwacht werden.

Wenn Sie die Überwachung von Richtlinienänderungen aktivieren, werden Änderungsversuche an den Überwachungsrichtlinien, anderen Richtlinien und Benutzerrechten verfolgt. Die Basisrichtlinien der Mitgliedsserver und Domänencontroller überwachen erfolgreiche und fehlgeschlagene Richtlinienänderungen. Diese Ereignisse werden im Ereignisprotokoll festgehalten.

Tabelle 6.9: Im Ereignisprotokoll angezeigte Richtlinienänderungsereignisse

Ereigniskennung	Beschreibung
608	Ein Benutzerrecht wurde zugewiesen.
609	Ein Benutzerrecht wurde entfernt.
610	Eine Vertrauensstellung mit einer anderen Domäne wurde erstellt.
611	Eine Vertrauensstellung mit einer anderen Domäne wurde entfernt.
612	Eine Überwachungsrichtlinie wurde geändert.
768	Zwischen einem Namespaceelement in einer Gesamtstruktur und einem Namespaceelement in einer anderen Gesamtstruktur wurde ein Konflikt entdeckt. (Tritt auf, wenn ein Namespaceelement in einer Gesamtstruktur sich mit einem Namespaceelement in einer anderen Gesamtstruktur überschneidet.)

Die zwei wichtigsten Ereignisse, auf die Sie hier achten sollten, sind die Ereignisse mit den Kennungen 608 und 609. Eine Reihe versuchter Angriffe kann zum Aufzeichnen dieser Ereignisse führen. Die folgenden Beispiele generieren ein Ereignis mit der Kennung 608, wenn ein Benutzerrecht zugeordnet wird, oder ein Ereignis mit der Kennung 609, wenn ein Benutzerrecht entfernt wird. In den Ereignisdetails ist die Sicherheits-ID (SID) aufgeführt, der das Benutzerrecht zugeordnet ist, sowie der Benutzername des Sicherheitsprincipals, der das Recht zugeordnet hat.

Als Teil des Betriebssystems handeln. Achten Sie auf die Ereigniskennungen 608 und 609 mit dem angezeigten Benutzerrecht `seTcbPrivilege` in den Ereignisdetails.

Hinzufügen von Arbeitsstationen zur Domäne. Achten Sie auf Ereignisse mit dem angezeigten Benutzerrecht `SeMachineAccountPrivilege` in den Ereignisdetails.

Sichern von Dateien und Verzeichnissen. Achten Sie auf Ereignisse mit dem angezeigten Benutzerrecht `SeBackupPrivilege` in den Ereignisdetails.

Umgehen der durchsuchenden Überprüfung. Achten Sie auf Ereignisse mit dem angezeigten Benutzerrecht `SeChangeNotifyPrivilege` in den Ereignisdetails. Dieses Benutzerrecht ermöglicht Benutzern das Durchsuchen einer Verzeichnisstruktur auch dann, wenn sie keine anderen Zugriffsrechte für das Verzeichnis besitzen.

Systemzeit ändern. Achten Sie auf Ereignisse mit dem angezeigten Benutzerrecht `SeSystemtimePrivilege` in den Ereignisdetails. Dieses Benutzerrecht ermöglicht einem Sicherheitsprincipal das Ändern der Systemzeit und somit das Verschleiern des Zeitpunktes eines Ereignisses.

Erstellen von dauerhaft freigegebenen Objekten. Achten Sie auf Ereignisse mit dem angezeigten Benutzerrecht `SeCreatePermanentPrivilege` in den Ereignisdetails. Der Inhaber dieses Rechtes kann Datei- und Druckfreigaben erstellen.

Debuggen von Programmen. Achten Sie auf Ereignisse mit dem angezeigten Benutzerrecht `SeDebugPrivilege` in den Ereignisdetails. Der Inhaber dieses Rechtes kann mit jedem beliebigen Prozess eine Verbindung herstellen. Dieses Recht ist standardmäßig nur Administratoren zugewiesen.

Erzwingen des Herunterfahrens von einem Remotesystem aus. Achten Sie auf Ereignisse mit dem angezeigten Benutzerrecht `SeRemoteShutdownPrivilege` in den Ereignisdetails.

Erhöhen der Zeitplanungspriorität. Achten Sie auf Ereignisse mit dem angezeigten Benutzerrecht `SeIncreaseBasePriorityPrivilege` in den Ereignisdetails. Ein Benutzer mit diesem Recht kann Prozessprioritäten ändern.

Laden und Entladen von Gerätetreibern. Achten Sie auf Ereignisse mit dem angezeigten Benutzerrecht `SeLoadDriverPrivilege` in den Ereignisdetails. Ein Benutzer mit diesem Benutzerrecht könnte ein als Gerätetreiber getarntes Trojanisches Pferd laden.

Verwalten von Überwachungs- und Sicherheitsprotokollen. Achten Sie auf Ereignisse mit dem angezeigten Benutzerrecht `SeSecurityPrivilege` in den Ereignisdetails. Ein Benutzer mit diesem Benutzerrecht kann das Sicherheitsprotokoll anzeigen und löschen.

Ein Prozessebenentoken ersetzen. Achten Sie auf Ereignisse mit dem angezeigten Benutzerrecht `SeAssignPrimaryTokenPrivilege` in den Ereignisdetails. Ein Benutzer mit diesem Benutzerrecht kann den mit einem gestarteten Unterprozess verbundenen Standardtoken ändern.

Wiederherstellen von Dateien und Verzeichnissen. Achten Sie auf Ereignisse mit dem angezeigten Benutzerrecht `SeRestorePrivilege` in den Ereignisdetails.

Herunterfahren des Systems. Achten Sie auf Ereignisse mit dem angezeigten Benutzerrecht `SeShutdownPrivilege` in den Ereignisdetails. Ein Benutzer mit diesem Benutzerrecht kann das System herunterfahren, um die Installation eines neuen Gerätetreibers zu initialisieren.

Übernehmen des Besitzes von Dateien und anderen Objekten. Achten Sie auf Ereignisse mit dem angezeigten Benutzerrecht `SeTakeOwnershipPrivilege` in den Ereignisdetails. Ein Benutzer mit diesem Benutzerrecht kann auf beliebige Objekte oder Dateien auf dem NTFS-Datenträger zugreifen, indem er deren Besitz übernimmt.

Anmerkung: Diese Überwachungsereignisse zeigen nur, dass das Benutzerrecht einem bestimmten Sicherheitsprincipal zugewiesen wurde. Sie geben keinen Aufschluss darüber, ob der Sicherheitsprincipal mithilfe des jeweiligen Benutzerrechtes eine Aufgabe ausgeführt hat. Mithilfe der Überwachungsereignisse kann ermittelt werden, wann die Richtlinien für die Benutzerrechte geändert wurden.

Anmerkung: Weitere Informationen zur Verwendung von Benutzerrechten finden Sie im englischsprachigen Buch *Writing Secure Code* von Michael Howard und David LeBlanc (Microsoft Press, ISBN: 0-7356-1588-8).

Schützen von Ereignisprotokollen

Um Ereignisprotokolleinträge für zukünftige Referenzzwecke beizubehalten, sollten Sie unbedingt einige Schritte durchführen, um die Sicherheit der Ereignisprotokolle zu gewährleisten. Diese Schritte sollten Folgendes beinhalten:

Definieren Sie für die Speicherung, das Überschreiben und die Wartung sämtlicher Ereignisprotokolle eine Richtlinie. Diese Richtlinie sollte alle erforderlichen Ereignisprotokolleinstellungen definieren, und sie sollte durch die Gruppenrichtlinie erzwungen werden.

Stellen Sie sicher, dass die Richtlinie auch die Behandlung von vollständigen Ereignisprotokollen und insbesondere des Sicherheitsprotokolls enthält. Ein vollständiges Sicherheitsprotokoll sollte das Herunterfahren des Servers erfordern. Für einige Umgebungen mag sich diese Praxis als hinderlich erweisen, aber sie sollte doch in Betracht gezogen werden.

Verhindern Sie Gastzugriffe auf die Ereignisprotokolle, indem Sie die Sicherheitsrichtlinieneinstellungen aktivieren, so dass lokale Gäste am Zugriff auf System, Anwendungen und Sicherheitsprotokolle gehindert werden.

Stellen Sie sicher, dass für Systemereignisse sowohl Erfolgs- als auch Fehlerüberwachung erfolgt. So können Sie ermitteln, ob Versuche unternommen wurden, den Inhalt des Sicherheitsprotokolls zu löschen.

- Sämtliche Sicherheitsprincipals mit der Möglichkeit zur Ansicht oder Änderung von Überwachungseinstellungen müssen komplexe Kennwörter verwenden oder Authentifizierungsverfahren aus zwei Faktoren (z. B. Smartcard-Anmeldung), um Angriffe gegen diese Konten mit dem Ziel des Zugriffs auf Überwachungsinformationen zu verhindern.

Diese Einstellungen sind in den Gruppenrichtlinienobjekten der Mitgliedsserver und Domänencontroller in Kapitel 4, "Sichern von Servern basierend auf ihrer Rolle", definiert.

Zusätzlich zu diesen Schritten sollten Sie einige weitere praktische Überprüfungen durchführen, um sicherzustellen, dass die Ereignisprotokollinformationen so sicher wie möglich sind:

Ihr Sicherheitsplan sollte auch die physische Sicherheit aller Server enthalten, um sicherzustellen, dass ein Angreifer während des Überwachungsprozesses keinen physischen Zugriff auf den Computer erhalten kann. Ein Angreifer kann Überwachungseinträge entfernen, indem er physische Ereignisprotokolldateien (EVT-Dateien) auf dem lokalen Festplatten-Teilsystem ändert oder löscht.

Implementieren Sie eine Methode zum Entfernen oder Speichern der Ereignisprotokolle an einem anderen Ort als dem physischen Server. Geplante Tasks können verwendet werden, um Ereignisprotokolle auf CD-Rs (einmal beschreibbare Datenträger, die mehrfach gelesen werden können) in regelmäßigen Abständen oder an anderen Speicherorten im Netzwerk als auf dem Server zu schreiben. Wenn die Sicherungen auf ein externes Medium wie Sicherungsbänder oder CD-Rs kopiert werden, sollte das Medium im Fall eines Brandes oder anderer Naturkatastrophen aus dem Geschäftsgebäude entfernt werden.

Anmerkung: Wird der Gastzugriff auf Ereignisprotokolle gesperrt, wird nur der Zugriff von Benutzern, die nicht Domänenmitglieder sind, auf Ereignisprotokolle verhindert. Standardmäßig können alle Benutzer in einer Domäne auf die System- und Anwendungsprotokolle zugreifen. Nur der Zugriff auf das Sicherheitsprotokoll unterliegt Beschränkungen. Sicherheitsprincipals mit dem zugewiesenen Benutzerrecht zum Verwalten von Überwachungs- und Sicherheitsprotokollen können auf das Sicherheitsprotokoll zugreifen. Standardmäßig ist dieses Recht nur Administratoren und Exchange-Servern des Unternehmens vorbehalten.

Andere optimale Überwachungspraktiken

Neben der Konfiguration der Überwachung gibt es andere Praktiken, die für eine effektive Überwachung der Sicherheit Ihrer Serverumgebung implementiert werden sollten. Dies schließt Folgendes ein:

Planen von regelmäßigen Überprüfungen der Ereignisprotokolle

Überprüfen anderer Anwendungsprotokolldateien

Überwachen installierter Dienste und Treiber

Überwachen offener Ports

Planen von regelmäßigen Überprüfungen der Ereignisprotokolle

Wie bereits erwähnt, sollten das Sicherheitsprotokoll und andere Ereignisprotokolle auf keine austauschbaren Datenträger geschrieben oder an einem zentralen Speicherort zur Überprüfung konsolidiert werden. Die Überprüfung der Protokolle ist der am häufigsten vergessene Überwachungsschritt.

Sie müssen sicherstellen, dass die Stellenbeschreibung einer Person oder eines Teams die Überprüfung der Ereignisprotokolle als reguläre Aufgabe ausweisen. Die Überprüfung von Ereignisprotokollen kann als tägliche oder wöchentliche Aufgabe geplant werden, abhängig vom Umfang der im Sicherheitsprotokoll gesammelten Daten. Dies basiert in der Regel auf dem im Netzwerk implementierten Überwachungsumfang. Je mehr Ereignisse in der Überwachung vorgesehen sind, desto größer wird das Ausmaß der Protokolleinträge sein. Wenn Sie regelmäßige Ereignisprotokollprüfungen planen, erreichen Sie damit Folgendes:

Schnellere Erkennung von Sicherheitsproblemen. Wenn eine tägliche Überprüfung der Ereignisprotokolle durchgeführt wird, sollte kein Sicherheitsereignis älter als 24 Stunden sein. Dadurch werden Sicherheitslücken schnell erkannt und geschlossen.

Zuständigkeiten definieren. Wenn eine regelmäßige Überprüfung der Ereignisprotokolle notwendig ist, kann der überprüfenden Person die Gesamtverantwortung für die Identifizierung potenzieller Angriffe übertragen werden.

Das Risiko von überschriebenen Ereignissen und Serverabstürzen minimieren. Wenn ein Ereignisprotokoll überprüft wird, können Ereignisse in der Protokolldatei zum Zweck zukünftiger Überprüfungen archiviert und aus dem aktuellen Protokoll entfernt werden. Dies vermindert das Risiko der Überfüllung von Ereignisprotokollen.

Überprüfen anderer Anwendungsprotokolldateien

Zusätzlich zur Überprüfung der Windows 2000-Ereignisprotokolle nach Sicherheitsereignissen sollten auch die Protokolle anderer Anwendungen überprüft werden. Diese Anwendungsprotokolle können wichtige Informationen zu potenziellen Angriffen enthalten, die in den Ereignisprotokollen gefundene Informationen ergänzen können. Abhängig von Ihrer Umgebung kann es nötig sein, eine oder mehrere dieser Protokolldateien anzuzeigen:

Internet-Informationsdienste (IIS oder Internet Information Services). Mit Internet-Informationsdienste werden Protokolldateien erstellt, die Verbindungsversuche zu Web-, FTP-, NTP- (Network Time Protocol) und SMTP-Diensten nachverfolgen. Jeder Dienst, der in Internet-Informationsdienste ausgeführt wird, behält separate Protokolldateien bei und speichert die Protokolldateien im erweiterten Protokolldateiformat des W3C im Ordner **%WinDir%\System32\Logfiles**. Jeder Dienst behält außerdem einen separaten Ordner bei, um Protokollinformationen weiter aufzuschlüsseln. Internet-Informationsdienste kann auch so konfiguriert werden, dass die Protokolle in einer ODBC-kompatiblen Datenbank (wie z. B. Microsoft SQL Server) gespeichert werden.

Internet Security und Acceleration Server (ISA Server). ISA Server bietet Protokolle für Paketfilter, den ISA Server-Firewalldienst und den ISA Server-Webproxydienst. Ebenso wie bei Internet-Informationsdienste werden auch hier die Protokolle standardmäßig im erweiterten Protokolldateiformat des W3C gespeichert. Alternativ können sie aber auch in einer ODBC-kompatiblen Datenbank aufgezeichnet werden. Die ISA Server-Protokolldateien werden standardmäßig unter **C:\Programme\Microsoft ISA Server\ISALogs** gespeichert.

Paketfilterprotokolle: z. B.	IPPEXT20020416.log
Firewalldienstprotokolle: z. B.	FWEXT20020416.log
Webproxydienstprotokoll: z. B.	WEBEXT20020416.log

Internetauthentifizierungsdienst (IAS). Der Internetauthentifizierungsdienst (IAS oder Internet Authentication Service) zentralisiert die Authentifizierung und Kontoführung für die Authentifizierung von Remotezugriffen mithilfe des RADIUS-Protokolls (Remote Authentication Dial-In User Service). Standardmäßig werden Anfragen zur Kontoführung, Anfragen zur Authentifizierung und periodische Statusanfragen in der Datei **IASlog.log** protokolliert. Diese Datei befindet sich im Ordner **%WinDir%\System32\Logfiles**. Alternativ kann die Protokolldatei auch in einem Datenbank-kompatiblen Format und nicht im IAS-Format gesichert werden.

Anwendungen von Drittanbietern. Viele Anwendungen von Drittanbietern implementieren lokale Protokollierungsfunktionen, um detaillierte Anwendungsinformationen bereitzustellen. Weitere Informationen finden Sie in der Hilfedatei Ihrer jeweiligen Anwendung.

Anmerkung: Alle Computer, die Protokolldateien beibehalten, sollten synchronisierte Uhren verwenden. Dadurch kann ein Administrator Ereignisse zwischen Computern und Diensten vergleichen und somit aufdecken, welche Aktionen durch einen Angreifer ausgeführt wurden. Weitere Informationen zur Zeitsynchronisierung finden Sie im Abschnitt "Die Wichtigkeit der Zeitsynchronisierung" weiter unten in diesem Kapitel.

Überwachen installierter Dienste und Treiber

Viele Angriffe gegen einen Computer werden durch Angriffe auf Dienste implementiert, die auf dem Zielcomputer installiert sind. Bei vielen Angriffen werden auch gültige Treiber durch Treiberversionen mit einem Trojanischen Pferd ersetzt, wodurch der Angreifer Zugriff auf den Zielcomputer erhält.

Mit den folgenden Tools können auf Computern installierte Dienste und Treiber überwacht werden:

Die Konsole Dienste. Die MMC-Konsole Dienste wird verwendet, um Dienste des lokalen Computers oder eines Remotecomputers zu überwachen und dem Administrator das Konfigurieren, Anhalten, Beenden, Starten und Neustarten aller installierten Dienste zu ermöglichen. Ermitteln Sie mithilfe dieser Konsole, ob Dienste, die für den automatischen Start konfiguriert wurden, nicht gestartet werden.

Netsvc.exe. Das Resource Kit zu Windows 2000 Server enthält dieses Befehlszeilentool. Es ermöglicht einem Administrator das Starten, Beenden, Anhalten, Fortsetzen und Abfragen des Status von Diensten von einem Remotecomputer aus mithilfe einer Befehlszeile.

SvcMon.exe. Dieses Tool überwacht Dienste auf lokalen Computern und Remotecomputern im Hinblick auf Statusänderungen (Starten oder Anhalten). Zum Erkennen dieser Änderungen implementiert das Tool zur Diensteüberwachung ein Abrufsystem. Wenn ein überwachter Dienst angehalten oder gestartet wird, werden Sie vom Tool zur Diensteüberwachung per E-Mail benachrichtigt. Die Server, Überwachungsintervalle und Dienste müssen für das Überwachen mithilfe des Tools Diensteüberwachung (**smconfig.exe**) konfiguriert werden.

Drivers.exe. Dieses Tool zeigt alle installierten Gerätetreiber des Computers an, auf dem das Tool ausgeführt wird. Die Ausgabe des Tools beinhaltet Informationen zum Dateinamen des Treibers, zur Größe des Treibers auf dem Datenträger und zum Datum, an dem der Treiber verknüpft wurde. Anhand des Verknüpfungsdatums können kürzlich installierte Treiber identifiziert werden. Wenn ein aktualisierter Treiber nicht kürzlich installiert wurde, kann dies auf einen ersetzten Treiber hindeuten. Setzen Sie diese Informationen immer mit einem Systemneustartereignis in der Ereignisanzeige in Bezug.

Anmerkung: Nicht alle Dienste (wie z. B. der Arbeitsstationsdienst) können direkt angehalten werden; sie können jedoch abgefragt werden. Wenn der Benutzer viele aktive Verbindungen hat, können Sie die Dienste im Remoteverfahren nicht zum Herunterfahren zwingen. Die Dienste können jedoch angehalten oder abgefragt werden. Einige Dienste hängen von anderen Diensten ab. Derartige Dienste können erst dann heruntergefahren werden, wenn der jeweils abhängige Dienst bereits heruntergefahren wurde.

Überwachen offener Ports

Angriffe erfolgen oft durch Ausführen eines Portscans, wobei bekannte Dienste auf dem Zielcomputer identifiziert werden. Sie sollten auf die Überwachung offener Ports auf Ihren Servern viel Sorgfalt verwenden. In der Regel werden Sie die Ports selbst scannen müssen, um zu ermitteln, auf welche Ports zugegriffen werden kann.

Wenn ein Portscan durchgeführt wird, sollte dieser sowohl lokal auf dem Zielcomputer als auch von einem Remotecomputer aus durchgeführt werden. Wenn der Zugriff auf den Computer von einem öffentlichen Netzwerk aus erfolgen kann, sollte der Portscan von einem externen Computer aus durchgeführt werden, um sicherzustellen, dass Ihr Firewall den Zugriff nur auf gewünschte Ports gewährt.

Netstat.exe ist ein Befehlszeilen-Dienstprogramm, das offene Ports sowohl für TCP als auch für UDP anzeigen kann. Der **Netstat**-Befehl verwendet die folgende Syntax:

```
NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]
```

Dabei gilt:

-a. Zeigt alle Verbindungen und überwachenden Ports an.

-e. Zeigt Ethernet-Statistiken an. Kann mit der **-s**-Option kombiniert werden.

-n. Zeigt Adressen und Portnummern im numerischen Format an.

-p *proto*. Zeigt Verbindungen für das durch **proto** angegebene Protokoll an; **proto** kann TCP oder UDP sein. In Verbindung mit der **-s**-Option zur Anzeige von Protokollstatistiken kann **proto** TCP, UDP oder IP sein.

-r. Zeigt die Routingtabelle an.

-s. Zeigt Protokollstatistiken an. Standardmäßig werden Statistiken für TCP, UDP und IP angezeigt; die **-p**-Option kann verwendet werden, um eine Teilmenge der Standardmenge anzugeben.

interval. Zeigt ausgewählte Statistiken mit einigen Sekunden Pause zwischen jeder Anzeige erneut an. Drücken Sie STRG+C, um das erneute Anzeigen von Statistiken anzuhalten. Erfolgt keine Angabe, druckt **netstat** die aktuellen Konfigurationsinformationen einmal.

Wenn Sie die offenen TCP- und UDP-Ports des lokalen Computers aufführen, werden Portnummern basierend auf den Einträgen in der Dienstedatei im Ordner **\%WinDir%\System32\Drivers\Etc** in Namen übersetzt. Wenn Sie nur die Portnummern angezeigt bekommen möchten, verwenden Sie die **-n**-Option.

Wenn offene, nicht erkannte Ports entdeckt werden, sollten Sie diese untersuchen, um zu ermitteln, ob der entsprechende Dienst auf dem Computer benötigt wird. Wird der Dienst nicht benötigt, sollten Sie ihn deaktivieren oder entfernen, damit der Computer diesen Port nicht mehr überwacht. Einige Dienste wurden in den Basisrichtlinien der Mitgliedsserver und Domänencontroller deaktiviert. Diese Richtlinien sind in diesem Handbuch enthalten.

Weil viele Server durch Firewalls oder Paketfilterungsrouter geschützt werden, wird empfohlen, den Portscan von einem Remotecomputer aus durchzuführen. Viele verfügbare Tools von Drittanbietern (teilweise Freeware) können Remoteportscans durchführen. Der Remoteportscan zeigt, welche Ports für externe Benutzer verfügbar sind, sobald sie eine Verbindung zum Computer herstellen.

Anmerkung: Portscanvorgänge können auch verwendet werden, um Ihr Programm zur Erkennung von Eindringversuchen zu überprüfen und um sicherzustellen, dass es den ausgeführten Portscan erkennt. Weitere Informationen zu Systemen zur Erkennung von Eindringversuchen finden Sie im Abschnitt "Aktive Erkennungsmethoden" weiter unten in diesem Kapitel.

Überwachen von Eindringversuchen und Sicherheitsereignissen

Das Überwachen von Eindringversuchen und Sicherheitsereignissen beinhaltet sowohl passive als auch aktive Tasks. Viele Eindringversuche werden erst nach dem eigentlichen Angriff bei der Überprüfung der Protokolldateien entdeckt. Die Entdeckung nach erfolgtem Angriff wird häufig als *passive* Erkennung von Eindringversuchen bezeichnet. Nur durch eine Überprüfung der Protokolldateien kann der Angriff erkannt und aufgrund der Protokollinformationen rekonstruiert werden.

Andere Eindringversuche können während des Angriffs erkannt werden. Diese Methode, bekannt als *aktive* Erkennung von Eindringversuchen, sucht nach bekannten Angriffsmustern oder Befehlen und verhindert die Ausführung dieser Befehle.

Dieser Abschnitt befasst sich mit Tools, die zur Implementierung beider Formen der Erkennung von Eindringversuchen verwendet werden können, um Ihr Netzwerk vor Angriffen zu schützen.

Die Wichtigkeit der Zeitsynchronisierung

Wenn sowohl Eindringversuche als auch Sicherheitsereignisse zwischen mehreren Computern überwacht werden, ist eine Synchronisierung der Computeruhren unabdingbar. Synchronisierte Zeit ermöglicht einem Administrator die Rekonstruktion der Ereignisse während eines Angriffs auf mehrere Computer. Ohne synchronisierte Zeit kann nur sehr schwer ermittelt werden, wann bestimmte Ereignisse eintrafen und in welcher Verbindung sie zueinander stehen. Weitere Informationen zur Zeitsynchronisierung finden Sie in Kapitel 3, "Verwalten von Sicherheit mit Windows 2000-Gruppenrichtlinien".

Passive Erkennungsmethoden

Passive Systeme zur Erkennung von Eindringversuchen beinhalten die manuelle Überprüfung von Ereignisprotokollen und Anwendungsprotokollen. Die Überwachung beinhaltet die Analyse und Erkennung von Angriffsmustern in Ereignisprotokolldaten. Es gibt verschiedene Tools, Dienstprogramme und Anwendungen, die bei der Auswertung von Ereignisprotokollen hilfreich sein können. Dieser Abschnitt führt vor, wie jedes Tool zur Koordination von Informationen verwendet werden kann.

Ereignisanzeige

Das Windows 2000-Sicherheitsprotokoll kann mithilfe der MMC-Konsole Ereignisanzeige von Windows 2000 angezeigt werden. Die Ereignisanzeige ermöglicht die Anzeige der Anwendungs-, Sicherheits- und Systemprotokolle. Zum Suchen nach bestimmten Ereignissen in der Ereignisanzeige können Filter definiert werden.

So definieren Sie Filter in der Ereignisanzeige

1. Wählen Sie das betreffende Ereignisprotokoll in der Konsolenstruktur aus.
2. Wählen Sie im Menü **Ansicht** die Option **Filter** aus.
3. Wählen Sie die Filterparameter aus.

Im Dialogfeld **Eigenschaften** können Sie auf der Registerkarte **Filter** die folgenden Attribute für Filterereigniseinträge definieren:

Ereignistypen. Der Filter kann auf Informationen, Warnmeldungen, Fehler, Erfolgsüberwachungen, Fehlerüberwachungen oder eine Kombination aus den Ereignistypen beschränkt werden.

Ereignisquelle. Der bestimmte Dienst oder Treiber, der das Ereignis generiert hat.

Kategorie. Der Filter kann auf bestimmte Kategorien von Ereignissen beschränkt werden.

Ereigniskennung. Wenn Ihnen die Kennung des gesuchten Ereignisses bekannt ist, kann der Filter die Auflistung auf diese bestimmte Ereigniskennung beschränken.

Benutzer. Sie können die Ereignisanzeige auf Ereignisse beschränken, die durch einen bestimmten Benutzer generiert wurden.

Computer. Sie können die Ereignisanzeige auf Ereignisse beschränken, die durch einen bestimmten Computer generiert wurden.

Datumsintervalle. Sie können die Ereignisanzeige auf Ereignisse beschränken, die in einen bestimmten Zeitrahmen fallen.

Wenn der Filter angewendet wird, kann die gefilterte Ereignisliste in eine durch Kommas oder Tabstopps getrennte Auflistung exportiert und anschließend in eine Datenbankanwendung importiert werden.

Tool für Ausgabeereignisprotokolle (Dumpel.exe)

Das Ausgabeereignisprotokoll ist ein Befehlszeilentool. Es ist enthalten im Resource Kit zu *Windows 2000 Server – Die technische Referenz – Zusatzband 1* (Microsoft Press, ISBN: 3-86063-924-2). Es gibt ein Ereignisprotokoll für ein lokales System oder ein Remotesystem in einer durch Tabstopps getrennten Textdatei aus. Diese Datei kann anschließend zur weiteren Untersuchung in eine Kalkulationstabelle oder eine Datenbank importiert werden. Dieses Tool kann auch verwendet werden, um nach bestimmten Ereignistypen zu filtern oder diese auszufiltern.

Das Tool **dumpel.exe** verwendet die folgende Syntax:

dumpel -f *file* [**-s** *server*] [**-l** *log* [**-m** *source*]] [**-e** *n1 n2 n3...*] [**-r**] [**-t**] [**-d** *x*]

Wobei:

-f *file*. Gibt den Dateinamen der Augabedatei an. Es gibt keine Standardeinstellung für **-f**, d. h. Sie müssen die Datei angeben.

-s *server*. Gibt den Namen des Servers an, für den das Ereignisprotokoll ausgegeben werden soll. Führende umgekehrte Schrägstriche beim Servernamen sind optional.

-l *log*. Gibt an, welches Protokoll (System, Anwendung, Sicherheit) ausgegeben werden soll. Wird ein ungültiger Protokollname angegeben, wird das Anwendungsprotokoll ausgegeben.

-m *source*. Gibt an, in welche Quelle (z. B. Umleitung (rdr), Seriennummer usw.) Datensätze ausgegeben werden sollen. Es kann nur eine Quelle angegeben werden. Wird diese Option nicht verwendet, werden alle Ereignisse ausgegeben. Wenn eine Quelle verwendet wird, die nicht in der Registrierung enthalten ist, wird das Anwendungsprotokoll nach Datensätzen dieses Typs durchsucht.

-e *n1 n2 n3*. Filtert nach der Ereigniskennung *nn* (bis zu zehn können festgelegt werden). Wenn die **-r**-Option nicht verwendet wird, werden nur Datensätze dieser Typen ausgegeben. Wenn **-r** verwendet wird, werden alle Datensätze außer Datensätze dieser Typen ausgegeben. Wird diese Option nicht verwendet, werden alle Ereignisse vom angegebenen *Quellennamen* ausgewählt. Diese Option kann nicht ohne die **-m**-Option verwendet werden.

-r. Gibt an, ob nach bestimmten Quellen oder Datensätzen gefiltert werden soll oder ob diese ausgefiltert werden sollen.

-t. Gibt an, dass einzelne Zeichenfolgen durch Tabstopps getrennt werden. Wenn **-t** nicht verwendet wird, werden Zeichenfolgen durch Leerzeichen getrennt.

-d *x*. Gibt Ereignisse der letzten *x* Tage aus.

Anmerkung: Dumpel.exe kann nur Inhalte von System-, Anwendungs- und Sicherheitsprotokolldateien abrufen. **Dumpel.exe** kann nicht verwendet werden, um Inhalte der Ereignisprotokolle des Datenreplikationsdienstes, des DNS- oder des Verzeichnisdienstes abzurufen.

EventCombMT

EventCombMT ist ein Multithreadtool zum Analysieren der Ereignisprotokolle mehrerer Server zur gleichen Zeit. Es erstellt für jeden Server einen separaten Ausführungsthread, der in den Suchkriterien enthalten ist. Das Tool ermöglicht Folgendes:

Eine oder mehrere zu findende Ereigniskennungen definieren. Sie können eine Ereigniskennung oder viele durch Leerzeichen getrennte Ereigniskennungen einschließen.

Einen Bereich von zu findenden Ereigniskennungen definieren. Die Endpunkte sind im Bereich eingeschlossen. Wenn Sie z. B. nach allen Ereignissen zwischen und einschließlich den Ereigniskennungen 528 und 540 suchen möchten, würden Sie den Bereich als 528 > ID < 540 definieren. Dieses Feature ist sehr nützlich, denn die meisten Anwendungen, die in das Ereignisprotokoll schreiben, verwenden einen sequenziellen Bereich von Ereignissen.

Die Suche auf bestimmte Ereignisprotokolle beschränken. Sie können die System-, Anwendungs- und Sicherheitsprotokolle durchsuchen. Wird die Suche lokal auf einem Domänencontroller ausgeführt, können Sie auch FRS-, DNS- und AD-Protokolle durchsuchen.

Die Suche auf bestimmte Ereignismeldungstypen beschränken. Sie können die Suche auf Fehler, Informationen, Warnungen, Erfolgsüberwachungen, Fehlerüberwachungen oder Erfolgsereignisse beschränken.

Die Suche auf bestimmte Ereignisquellen beschränken. Sie können die Suche auf Ereignisse bestimmter Ereignisquellen beschränken.

In einer Ereignisbeschreibung nach einem bestimmten Text suchen. Sie können bei jedem Ereignis nach einem bestimmten Text suchen. Die ist nützlich, wenn Sie bestimmte Benutzer oder Gruppen überwachen möchten.

Anmerkung: Suchlogik (z. B. AND, OR oder NOT) kann dem Text nicht hinzugefügt werden. Begrenzen Sie auch keinen Text mit Anführungszeichen.

Definieren Sie vom aktuellen Datum und der aktuellen Zeit rückläufige Zeitintervalle. Dadurch können Sie die Suche auf Ereignisse der letzten Woche, des letzten Tages oder des letzten Monats beschränken.

Installieren des Tools

Zur Installation des Tools extrahieren Sie den Inhalt der selbstausführenden Datei **SecurityOps.exe**. Die Datei ist im Lieferumfang dieses Handbuchs enthalten. Durch dieses Vorgehen wird der Ordner **C:\SecurityOps\EventComb** erstellt. Sobald die Dateien extrahiert sind, kann das Tool EventCombMT durch Doppelklicken auf die Datei **EventCombMT.exe** ausgeführt werden.

Ausführen des Tools EventComb

Der erste Schritt zum Verwenden des Tools EventComb ist das Definieren der Computer, die in die Ereignisprotokollsuche eingeschlossen werden.

So fügen Sie Computern zur Suche hinzu

1. Das Dienstprogramm EventCombMT stellt die automatische Erkennung der richtigen Domäne im Feld **Domain** sicher. Wenn Sie Ereignisprotokolle in einer anderen Domäne durchsuchen möchten, geben Sie den neuen Domänennamen manuell im Feld **Domain** ein.
2. Zum Hinzufügen von Computern zur Suchliste klicken Sie mit der rechten Maustaste auf das Feld unter **Select To Search/Right Click to Add**. Das Kontextmenü wird wie in Abbildung 6.1 angezeigt:

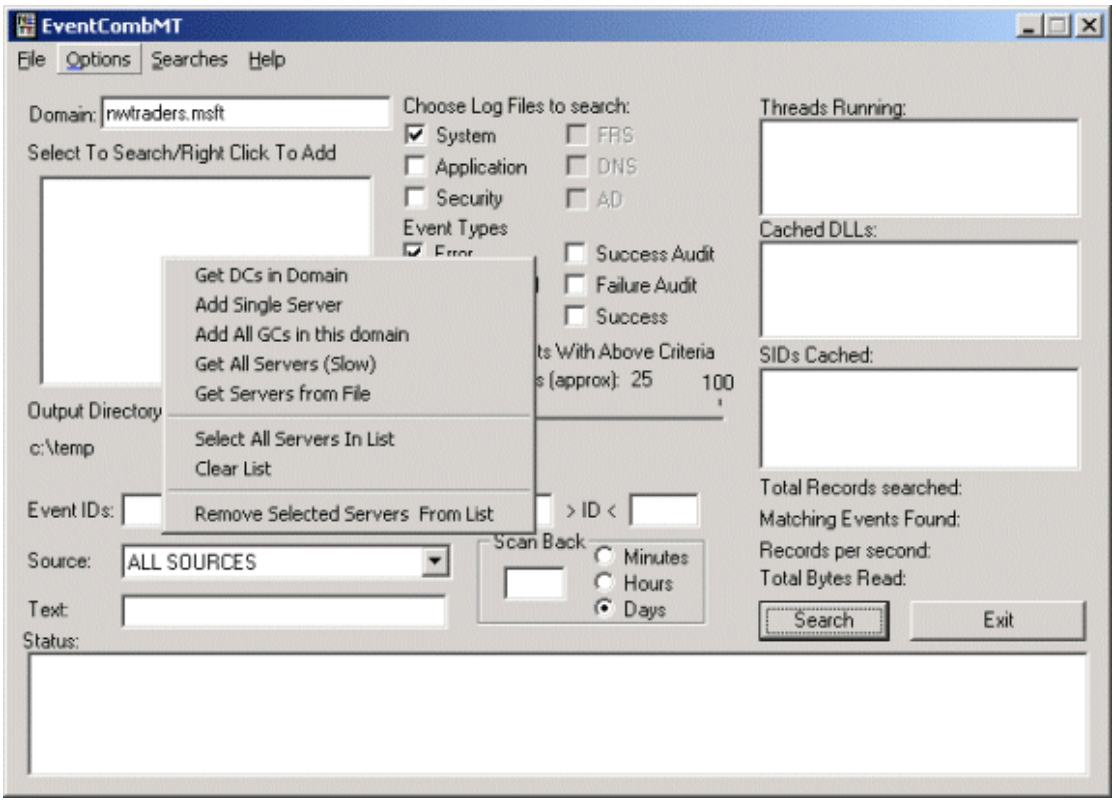


Abbildung 6.1: Hinzufügen von Computern zur Suchliste, die nicht automatisch erkannt wurden

Die folgenden Optionen stehen zur Verfügung:

Get DCs in Domain. Fügt alle Domänencontroller für die aktuelle Domäne zur Auflistung hinzu.

Add Single Server. Ermöglicht es Ihnen, den Namen eines Servers oder einer Arbeitsstation zur Liste hinzuzufügen.

Add all GCs in this domain. Ermöglicht es Ihnen, alle Domänencontroller in der ausgewählten Domäne hinzuzufügen, die als globale Katalogserver konfiguriert wurden.

Get All Servers. Fügt alle in der Domäne gefundenen Server mithilfe eines Suchdienstes hinzu. Die Server schließen alle Domänencontroller aus.

Get Servers from File. Ermöglicht es Ihnen, eine Datei zu importieren, die alle im Suchbereich enthaltenen Server auflistet. Jeder Server sollte auf einer separaten Zeile in die Textdatei eingegeben werden.

3. Sobald die Server zur Liste hinzugefügt wurden, müssen Sie die Server auswählen, auf denen die Suche ausgeführt werden soll. Sobald ein Server ausgewählt ist, wird er in der Liste hervorgehoben dargestellt. Mithilfe der Kombination STRG+Klicken können Sie mehrere Server auswählen.

Angeben der zu suchenden Ereignisprotokolle und Ereignistypen

Sobald Sie die Server ausgewählt haben, die in die Ereignisprotokollsuche eingeschlossen werden sollen, können Sie die Suche durch Auswahl der zu berücksichtigenden Ereignisprotokolle und Ereignistypen einschränken.

Im Dienstprogramm EventCombMT können Sie für die Suche aus den folgenden Ereignisprotokollen auswählen:

System

Application

Security

FRS (File Replication Service Log oder Dateireplikationsdienst-Protokoll)

DNS (DNS-Serverprotokoll)

AD (Verzeichnisdienstprotokoll)

Sie können auch die Ereignistypen auswählen, die bei der Suche berücksichtigt werden sollen:

Error. Wird in den Anwendungs- und Systemprotokollen aufgezeichnet und auch in den FRS-, DNS- und Verzeichnisdienstprotokollen angezeigt.

Informational. Wird in den Anwendungs- und Systemprotokollen aufgezeichnet und auch in den FRS-, DNS- und Verzeichnisdienstprotokollen angezeigt.

Warning. Wird in den Anwendungs- und Systemprotokollen aufgezeichnet und auch in den FRS-, DNS- und Verzeichnisdienstprotokollen angezeigt.

Success Audit. Wird im Sicherheitsprotokoll oder im Anwendungsprotokoll angezeigt, wenn die Anwendung im Anwendungsprotokoll Erfolgsüberwachungen registriert. Beispielsweise fügt Active Directory Migration Tool (ADMT) Protokolle über Erfolgsüberwachungen zum Anwendungsprotokoll hinzu.

Failure Audit. Wird im Sicherheitsprotokoll oder im Anwendungsprotokoll angezeigt, wenn die Anwendung im Anwendungsprotokoll Fehlerüberwachungen registriert. Beispielsweise fügt ADMT Protokolle über Fehlerüberwachungen zum Anwendungsprotokoll hinzu.

Success. Der Typ tritt selten auf und wird in den Anwendungs- und Systemprotokollen aufgezeichnet ebenso wie in den FRS-, DNS- und Verzeichnisdienstprotokollen angezeigt. In der Ereignisanzeige werden Erfolgsereignisse als Informationsereignistyp angezeigt.

Anmerkung: Wenn Sie über genaue Angaben der Ereignisprotokolle und Ereigniskennungen sowie des Ereignistyps der Ereigniskennung verfügen, fügen Sie diese Informationen zu den Kriterien Ihrer Suche hinzu. Dies trägt zur Beschleunigung des Suchvorgangs bei.

Sichern von Suchvorgängen

EventCombMT ermöglicht Ihnen das Sichern und erneute Laden von Suchvorgängen. Dies kann hilfreich sein, wenn Sie mit EventCombMT häufig Ihre Server mit IIS nach einem Ereignissatz und Ihre Domänencontroller nach einem anderen durchsuchen.

Suchkriterien werden in der Registrierung unter folgendem Pfad gesichert: **HKLM\Software\Microsoft\EventCombMT**. Die Kriterien können einfach bearbeitet werden.

Dateien mit Suchergebnissen

Die Ergebnisse des Suchvorgangs werden standardmäßig im Ordner **C:\Temp** gesichert. Die Ergebnisse enthalten eine Zusammenfassungsdatei (**EventCombMT.txt**), und für jeden in der Ereignisprotokollsuche aufgeführten Computer wird eine separate Textdatei (***ComputerName-EreignisProtokollName*_LOG.txt**) generiert. Diese unterschiedlichen Textdateien beinhalten alle Ihren Suchkriterien entsprechende Ereignisse aus den Ereignisprotokollen.

Beispiele für das Verwenden von EventCombMT

Zur Verdeutlichung der Verwendungsweise von EventCombMT erfahren Sie nun, wie das Tool so konfiguriert werden kann, dass Sie Neustarts des Domänencontrollers und Kontoabmeldevorgänge erkennen.

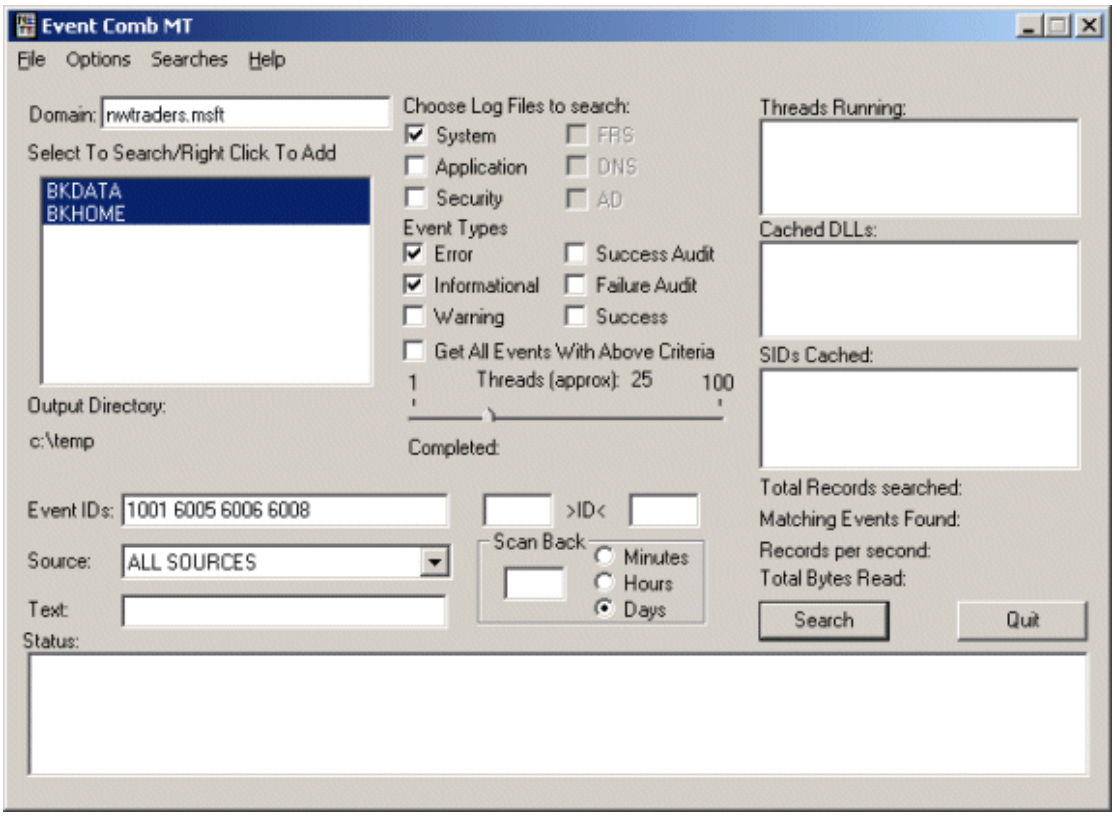
So verwenden Sie EventCombMT zum Suchen nach Neustarts von Domänencontrollern

1. Das Tool EventCombMT stellt die Konfiguration der Domäne mit dem richtigen Domänennamen sicher.
2. Klicken Sie mit der rechten Maustaste auf das Feld **Select to Search/Right Click to Add** unter dem Domänennamen. Klicken Sie anschließend auf **Get DCs in Domain**.

Anmerkung: Wenn Sie nach Ereignissen wie z. B. Kontoanmeldungs- und Kontenmanagementereignissen suchen, stellen Sie sicher, dass Sie alle Domänencontroller durchsuchen. Da Windows 2000 für das Kontenmanagement ein Multimastermodell verwendet, kann ein Konto auf jedem Domänencontroller in der Domäne hinzugefügt, geändert oder gelöscht werden. Ebenso kann die Authentifizierung von jedem beliebigen Domänencontroller in der Domäne überprüft werden. Deshalb können Sie nicht mit Sicherheit sagen, auf welchem Domänencontroller ein bestimmter Aktualisierungs- oder Authentifizierungsversuch vorgenommen wurde.

---

3. Klicken Sie mit der rechten Maustaste auf das Feld **Select to Search/Right Click to Add**, und klicken Sie anschließend auf **Select All Servers in List**.
4. Wählen Sie im Abschnitt **Choose Log Files to search** des Tools nur **System** aus.
5. Wählen Sie im Abschnitt **Event Types** des Tools **Error** und **Informational** aus.
6. Geben Sie im Feld **Event IDs** die folgenden Ereigniskennungen ein: **1001 6005 6006 6008**
7. Bevor Sie auf die Schaltfläche **Search** klicken, stellen Sie sicher, dass Ihre Suchkriterien wie in der Abbildung unten gezeigt angegeben sind. Klicken Sie anschließend auf **Search**.



Sobald die Suche abgeschlossen ist, werden die Resultate im Protokollverzeichnis angezeigt. Dieses Verzeichnis sollte sich nach Abschluss der Suche automatisch öffnen.

So überprüfen Sie Protokolleinträge

1. Wählen Sie **Open Log Directory** im Menü **File** aus.
2. Doppelklicken Sie im Ordner **C:\Temp** auf die Ausgabedatei eines Domänencontrollers, um die einzelnen Ereignisse anzuzeigen, die das Tool EventCombMT protokolliert hat. Die Ausgabe sollte ähnlich wie die folgende aussehen:

```
1001,INFORMATIONAL,Save Dump,Wed Nov 28 05:45:50 2001,,The computer has
rebooted from a bugcheck.  The bugcheck was:  0x000000d1 (0x00000004,
0x00000002, 0x00000000, 0x84c983dc).  A dump was saved in:
C:\WINDOWS\MEMORY.DMP.
6005,INFORMATIONAL,EventLog,Wed Nov 28 05:45:46 2001,,The Event log service was
started.
6008,ERROR,EventLog,Wed Nov 28 05:45:46 2001,,The previous system shutdown at
5:33:47 AM on 11/28/2001 was unexpected.
6005,INFORMATIONAL,EventLog,Tue Nov 27 14:10:53 2001,,The Event log service was
started.
6006,INFORMATIONAL,EventLog,Tue Nov 27 14:09:26 2001,,The Event log service was
stopped.
6005,INFORMATIONAL,EventLog,Tue Nov 27 10:11:37 2001,,The Event log service was
started.
```

Die Ereignisse mit der Kennung 6006 zeigen ein geplantes Herunterfahren durch einen Benutzer mit Benutzerrechten zum Herunterfahren des Domänencontrollers an. Die Ereignisse mit der Kennung 6005 zeigen das Starten eines Ereignisprotokolldienstes an. Dies tritt auf, sobald ein Start erfolgt.

Die Ereignisse mit der Kennung 6008 und 1001 zeigen an, dass der Computer entweder ausgeschaltet wurde, ohne heruntergefahren worden zu sein, dass er neugestartet wurde, weil er gesperrt wurde, oder dass ein Bluescreen aufgetreten ist. Ist ein Ereignis mit der Kennung 1001 vorhanden, ist ein Bluescreen aufgetreten. Die zugeordneten Debuginformationen und Referenzen zur Debugdatei sind eingeschlossen.

Die Ereignisse, die vom Tool EventCombMT zurückgegeben werden, sollten mit der bekannten Zeit des Herunterfahrens verglichen werden. Unstimmige Ereignisse sollten untersucht werden, um sicherzustellen, dass kein Angriff auf den Server stattgefunden hat.

EventCombMT enthält einige vorkonfigurierte Suchvorgänge, die zum Suchen nach Sicherheitsereignissen verwendet werden können. Beispielsweise gibt es unter ihnen einen vordefinierten Suchvorgang, der nach Kontosperrungsereignissen sucht.

So verwenden Sie EventCombMT zum Suchen nach Kontosperrungen

1. Das Tool EventCombMT stellt die Konfigurierung der Domäne mit dem richtigen Domänennamen sicher.
2. Klicken Sie mit der rechten Maustaste auf das Feld **Select to Search/Right Click to Add** unter dem Domänennamen, und klicken Sie anschließend auf **Get DCs in Domain**.
3. Klicken Sie mit der rechten Maustaste auf das Feld **Select to Search/Right Click to Add**, und klicken Sie anschließend auf **Select All Servers in List**.
4. Klicken Sie im Menü **Searches** auf **Built In Searches**, und klicken Sie anschließend auf **Account Lockouts**. Das Dienstprogramm EventCombMT wird konfiguriert.
5. Klicken Sie auf **Search**.
6. Sobald die Suche abgeschlossen ist, werden die Resultate im Protokollverzeichnis angezeigt. Dieses Verzeichnis sollte sich nach Abschluss der Suche automatisch öffnen.

Anmerkung: Andere in EventCombMT enthaltene vordefinierte Suchvorgänge sind Dateireplikationsdienst-Suchen und Active Directory-Suchen nach doppelten SIDs und NETLOGON DNS-Registrierungsfehlern, Festplattenfehlern und DNS-Schnittstellenfehlern. Sie können auch eigene Suchvorgänge definieren und sichern.

Ereigniszusammenstellung

Eines der Hauptziele der Überwachung ist die Identifizierung von Angriffen auf Ihr Netzwerk. Ein Angreifer versucht möglicherweise, mehrere Computer und Geräte im Netzwerk zu beeinträchtigen. Sie müssen also in der Lage sein, Informationen von vielen Computern zu koordinieren und zu konsolidieren.

Wenn Ihre Protokolldienstprogramme in eine Datenbank importieren, ist die Koordination der Informationen vieler Protokolle einfacher. Solange die Uhrzeit auf allen Computer synchronisiert ist, können Sie nach Zeitfeldern sortieren und so das Nachverfolgen von Ereignissen in einem bestimmten Zeitraum erleichtern.

Die folgenden Abschnitte stellen einige der Tools und Dienstprogramme vor, die zum Sammeln von Ereignisprotokollinformationen an einer zentralen Stelle verwendet werden können.

Skripterstellung

Es können Skripts geschrieben werden, die Ereignisprotokollinformationen von Remotecomputern sammeln und sie an einer zentralen Stelle speichern. Durch die Verwendung der Skripterstellung können Sie mithilfe von **Geplante Tasks** bestimmen, wann Skripts ausgeführt werden und welche Schritte durchgeführt werden sollen, sobald das Ereignisprotokoll erfolgreich an die zentrale Stelle kopiert wurde.

Ein einfaches Beispiel ist die Erstellung einer Batchdatei, die die Datei **Dumpel.exe** aus dem Resource Kit zu Windows 2000 Server verwendet und mithilfe von **Geplante Tasks** in der Systemsteuerung in regelmäßigen Intervallen gestartet wird.

Das Resource Kit zu *Windows 2000 Server – Die technische Referenz – Zusatzband 1* beinhaltet **Eventquery.pl**, ein Perl-Skript, das Ereignisse aus den Protokollen der Ereignisanzeige auf lokalen Computern und Remotecomputern unter Windows 2000 anzeigt und zur Suche nach bestimmten Ereignissen zahlreiche Filter bietet.

Anmerkung: Zur Verwendung dieses Skripts muss ActivePerl aus dem Resource Kit zu Windows 2000 Server installiert sein.

Microsoft Operations Manager

Microsoft Operations Manager 2000 bietet einen umfassenden Satz von Tools, die Unternehmen eine eingehende Analyse der vordefinierten Ereignismeldungen und Leistungsüberwachung von Windows 2000 und den zugehörigen Anwendungen ermöglichen. Operations Manager kann mithilfe von Intelligent Agents auf Remotecomputern Ereignisse und Leistungsdaten an einer Stelle sammeln, speichern und melden. Administratoren wird so die zentrale Überprüfung der gesammelten Informationen ermöglicht.

Das wichtigste Verwaltungspaket von Operation Manager sammelt im System auftretende Ereignisse, Anwendungen und Sicherheitsprotokolle und fasst die Ergebnisse in einem zentralen Ereignisrepository zusammen.

Anmerkung: Operations Manager speichert Informationen in einer SQL-Datenbank und bietet verschiedene Methoden des Abrufens und des Analysierens archivierter Daten. Administratoren können Operations Manager Administrator Console, Web Console oder Operations Manager Reporting zum Anzeigen, Drucken und Veröffentlichen von Daten verwenden. Jede Ansicht beinhaltet vordefinierte Ansichten zum Analysieren archivierter Daten und ermöglicht die Definition benutzerdefinierter Ansichten und Berichte.

Lösungen von Drittanbietern zur Sammlung von Ereignisprotokollen

Es stehen verschiedene Produkte von Drittanbietern zur Verfügung, die eine zentralisierte Sammlung und Überwachung von Ereignisprotokollen bieten. Bei der Bewertung von Drittanbieterprodukten sollten Sie die folgenden Features in Ihre Beurteilungskriterien aufnehmen:

Unterstützung für alle Windows 2000-Protokolle. Zusätzlich zur Unterstützung für Anwendungs-, Sicherheits- und Systemprotokolle sollten auch DNS Server-, Verzeichnisdienst- und Dateireplikationsdienst-Protokolle unterstützt werden.

Verwenden eines Datenbank-Backends. Das Tool sollte das Speichern der Ereignisprotokolle in einer Datenbankstruktur ermöglichen, so dass vorherige Ereignisprotokolleinträge zu Trendanalyse- und Korrelationszwecken zwischen mehreren Servern überwacht werden können.

Such- und Meldefunktionalität. Das Tool sollte Ihnen das Suchen nach bestimmten Ereignissen auf der Basis vorgegebener Kriterien bieten. Die Ergebnisse sollten in einer lesbaren Form dargestellt sein.

Es folgen einige Produkte von Drittanbietern, die Möglichkeiten zur Ereignissammlung beinhalten:

Event Log Monitor – TNT Software (www.tntsoftware.com; englischsprachig)

Event Archiver – Dorian Software Creations (www.doriansoft.com; englischsprachig)

LogCaster – RippleTech (www.rippletech.com; englischsprachig)

Aktive Erkennungsmethoden

Aktive Systeme zur Erkennung von Eindringversuchen analysieren eingehenden Netzwerkverkehr auf der Anwendungsebene und suchen nach bekannten Angriffsmethoden und verdächtiger Nutzlast auf der Anwendungsebene. Wird ein verdächtiges Paket empfangen, löscht das System zur Erkennung von Eindringversuchen normalerweise das Paket und fügt der Protokolldatei einen Eintrag hinzu. Einige Systeme zur Erkennung von Eindringversuchen alarmieren zudem den jeweiligen Administrator, wenn ein schwerwiegender Angriff erkannt wird.

Überwachen eines HTTP-Zugriffs mithilfe von URLScan

Wenn Ihre Organisation über Hosts für Websites verfügt, erhalten einige Ihrer Server eingehenden HTTP-Verkehr. Jedoch muss nicht der gesamte Verkehr rechtmäßig sein. UrlScan ist ein ISAPI-Filter zur Analyse eingehender HTTP-Pakete und kann verdächtigen Verkehr ablehnen.

UrlScan schützt einen Server vor Angriffen, indem HTTP-Anforderungen ausgewählter IIS-Dienstfeatures gefiltert und abgelehnt werden. UrlScan ist standardmäßig so konfiguriert, dass Anforderungen nach statischen HTML-Dateien (einschließlich Grafiken) akzeptiert werden. Die folgenden Anforderungstypen werden abgelehnt:

CGI-Seiten (EXE)

WebDAV

FrontPage-Servererweiterungen

Index Server

Internetdruckdienst

Serverseitige Includedateien

UrlScan kann als Endpunktsystem zur Erkennung von Eindringversuchen implementiert werden, indem der ISAPI-Filter auf allen Servern mit IIS des Netzwerkes installiert wird. Eine weitere Möglichkeit besteht darin, den ISAPI-Filter von UrlScan auf einem Computer mit ISA Server am Netzwerkperimeter als Netzwerksystem zur Erkennung von Eindringversuchen zu installieren. Wenn Sie einen Computer mit ISA Server als Firewall verwenden, sollten Sie eine Kombination der beiden Lösungen in Betracht ziehen. Hindern Sie am Netzwerkperimeter den gesamten unerwünschten Verkehr am Eindringen in Ihr Netzwerk. An den Endpunktservern mit IIS können mithilfe von URLScan Regelsätze basierend auf dem Format des am Webserver bereitgestellten Inhalts implementiert werden.

Es sollten am ISA Server entspechene Webveröffentlichungsregeln implementiert werden, die mithilfe von Zielsätzen nur die Anfragen durchlassen, die genauen URL und Pfad beinhalten.

UrlScan wird mithilfe einer Datei namens **UrlScan.ini** konfiguriert, die sich im Ordner **%WinDir%\system32\inetsrv\Urlscan** befindet. Diese Datei hat mehrere Abschnitte.

Der Abschnitt [Options] definiert, wie der Server mit IIS sowohl gültige als auch ungültige Webanforderungen behandelt. Die definierbaren Optionen beinhalten:

UseAllowVerbs. **0** oder **1** sind zugelassene Werte. Wenn **1** als Standardwert festgelegt ist, liest UrlScan den Abschnitt **AllowVerbs** der Datei **UrlScan.ini** und lehnt sämtliche Anforderungen ab, die ein HTTP-Verb beinhalten, das nicht explizit aufgeführt ist. Im Abschnitt **AllowVerbs** muss die Groß-/Kleinschreibung beachtet werden. Wenn **0** festgelegt ist, liest UrlScan den Abschnitt **DenyVerbs** der Datei **UrlScan.ini** und lehnt sämtliche Anforderungen ab, die ein aufgeführtes HTTP-Verb beinhalten. Im Abschnitt **DenyVerbs** muss die Groß-/Kleinschreibung nicht beachtet werden.

UseAllowExtensions. **0** oder **1** sind zugelassene Werte. Wenn **1** festgelegt ist, liest UrlScan den Abschnitt **AllowExtensions** der Datei **UrlScan.ini** und weist sämtliche Anforderungen ab, die eine mit dem URL verbundene Dateierweiterung beinhalten, die nicht explizit aufgeführt ist. Wenn **0** als Standardwert festgelegt ist, liest UrlScan den Abschnitt **DenyExtensions** der Datei **UrlScan.ini** und lehnt alle Anforderungen ab, in denen eine mit der Anforderung verbundene Dateierweiterung aufgeführt ist. In den Abschnitten **AllowExtensions** und **DenyExtensions** muss die Groß-/Kleinschreibung nicht beachtet werden.

NormalizeUrlBeforeScan. **0** oder **1** sind zugelassene Werte. Wenn **1** als Standardwert festgelegt ist, führt UrlScan die gesamte Analyse an den angeforderten URLs aus, nachdem IIS sie decodiert und normalisiert hat. Wenn **0** als Standardwert festgelegt ist, führt UrlScan die gesamte Analyse an den ursprünglichen URLs aus, wie sie vom Client gesendet wurden. Nur ein erfahrener Administrator mit einem umfangreichen Wissen über das Analysieren von URLs sollte diese Option auf **0** festlegen, da der Server mit IIS dadurch wahrscheinlich Kanonisierungsangriffen ausgeliefert wird, die die ordnungsgemäße Analyse von URL-Erweiterungen umgehen.

VerifyNormalization. **0** oder **1** sind zugelassene Werte. Wenn **1** als Standardwert festgelegt ist, überprüft UrlScan die Normalisierung der URL. Diese Aktion schützt vor Kanonisierungsangriffen, bei denen eine URL eine doppelt codierte Zeichenfolge enthält (beispielsweise ist die Zeichenfolge "%252e" ein doppelt codiertes '.'-Zeichen, denn "%25" decodiert ein '%'-Zeichen, die erste Decodierung von "%252e" ergibt "%2e", das in einem zweiten Schritt zu '.' decodiert werden kann). Wenn **0** festgelegt ist, wird diese Überprüfung nicht durchgeführt.

AllowHighBitCharacters. **0** oder **1** sind zugelassene Werte. Wenn **1** festgelegt ist, lässt UrlScan jedes Byte im URL zu. Wenn **0** als Standardwert festgelegt wurde, lehnt UrlScan jede Anforderung ab, deren URL ein Zeichen außerhalb des ASCII-Zeichensatzes enthält. Dieses Feature kann als Schutz gegen Unicode- und UTF-8-basierte Angriffe dienen. Es wird jedoch auch rechtmäßige Anforderungen an Server mit IIS ablehnen, die keine ASCI-Codepage verwenden.

AllowDotInPath. **0** oder **1** sind zugelassene Werte. Wenn **0** als Standardwert festgelegt ist, lehnt UrlScan sämtliche Anforderungen ab, die mehrere Instanzen des Punktzeichens (**.**) verwenden. Wenn **1** festgelegt ist, führt UrlScan diesen Test nicht aus. Weil UrlScan auf einer Ebene arbeitet, auf der IIS den URL noch nicht analysiert hat, ist es nicht immer möglich zu ermitteln, ob das Punktzeichen eine Erweiterung markiert oder Teil des Verzeichnispfades oder Dateinamens des URL ist. In Bezug auf die Erweiterungsanalyse geht UrlScan immer davon aus, dass eine Erweiterung den Teil eines URL darstellt, der nach dem letzten Punkt in der Zeichenfolge beginnt und am ersten Fragezeichen oder Schrägstrich nach dem Punkt oder dem Ende der Zeichenfolge endet. Das Festlegen von **AllowDotInPath** auf **0** bietet Schutz für den Fall, dass ein Angreifer Pfadinformationen verwendet, um die richtige Erweiterung der Anforderung zu verbergen (z. B. "**/path/TrueURL.asp/BogusPart.htm**").

Anmerkung: Das Festlegen von **AllowDotInPath** auf **0** führt auch dazu, dass UrlScan sämtliche Anforderungen ablehnt, die einen Punkt in einem Verzeichnisnamen enthalten.

RemoveServerHeader. **0** oder **1** sind zugelassene Werte. Wenn **1** festgelegt ist, entfernt UrlScan die Serverheader in sämtlichen Antworten. Wenn **0** als Standardwert festgelegt ist, führt UrlScan diese Aktion nicht aus. Bitte beachten Sie, dass dieses Feature nur zur Verfügung steht, wenn UrlScan auf einem Computer mit IIS 4.0 oder höher installiert wird.

EnableLogging. **0** oder **1** sind zugelassene Werte. Wenn **1** als Standardwert festgelegt ist, protokolliert UrlScan seine Aktionen in einer Datei namens **UrlScan.log**. Diese Datei wird in demselben Verzeichnis erstellt, das die Datei **UrlScan.dll** enthält. Wenn **0** festgelegt ist, findet keine Protokollierung statt.

PerProcessLogging. **0** oder **1** sind zugelassene Werte. Wenn **1** festgelegt ist, hängt UrlScan an den Protokolldateinamen die Prozesskennung der Datei **UrlScan.dll** an, die den IIS-Prozess hostet (z. B. **UrlScan.1234.log**). Dieses Feature ist für IIS-Versionen hilfreich, die Filter in mehr als einem Prozess gleichzeitig hosten können. Wenn **0** als Standardwert festgelegt ist, ist die Datei **UrlScan.log** die Protokolldatei.

AlternateServerName. Der zugelassene Wert ist eine Zeichenfolge, und der Standardwert ist eine leere Zeichenfolge. Wenn diese Einstellung vorhanden ist (die Zeichenfolge nicht leer ist) und **RemoveServerHeader** auf **0** festgelegt ist, ersetzt IIS seinen Standardheader in allen Antworten mit dieser Zeichenfolge. Wenn **RemoveServerHeader** auf **1** festgelegt ist, hat **AlternateServerName** keine Auswirkung. Dieses Feature steht nur zur Verfügung, wenn UrlScan auf einem Computer mit IIS 4.0 oder höher installiert ist.

AllowLateScanning. **0** oder **1** sind zugelassene Werte. Wenn **1** festgelegt ist, registriert UrlScan sich selbst als Filter geringer Priorität. Dies ermöglicht anderen Filtern, Änderungen am URL vorzunehmen, bevor UrlScan seine Analyse startet. (Beachten Sie, dass zusätzlich sichergestellt werden muss, dass UrlScan in der Filterliste auf dem Eigenschaftenblatt der ISAPI-Filter von MMC für den Server hinter den Filtern höherer Priorität aufgeführt ist.) Wenn **0** als Standardwert festgelegt ist, wird UrlScan als Filter höherer Priorität ausgeführt. Beachten Sie, dass FrontPage-Servererweiterungen erfordern, dass **1** als Standardwert festgelegt ist und UrlScan in der Filterliste zur Ladereihenfolge unten (vorzugsweise an letzter Position) aufgeführt wird.

PerDayLogging. **0** oder **1** sind zugelassene Werte. Wenn **1** als Standardwert festgelegt ist, erstellt UrlScan täglich eine neue Protokolldatei und hängt an den Protokolldateinamen ein Datum an (z. B. **UrlScan.101501.log**). Wenn **1** sowohl für **PerDayLogging** als auch für **PerProcessLogging** festgelegt ist, beinhaltet der Protokolldateiname das Datum und eine Prozesskennung (z. B. **UrlScan.101501.123.log**). Beachten Sie, dass mit PerDayLogging ein Protokoll für den aktuellen Tag erstellt wird (und das Protokoll für den vorherigen Tag geschlossen wird), sobald der erste Protokolleintrag für diesen Tag geschrieben wird. Wenn ein Tag keine UrlScan-Aktivität aufweist, wird für den Tag kein Protokoll erstellt. Wenn **0** festgelegt ist, öffnet UrlScan eine Datei namens **UrlScan.log** (oder **UrlScan.*xxx*.log**, wobei ***xxx*** die Prozesskennung ist, wenn **1** der Standardwert für **PerProcessLogging** ist).

RejectResponseUrl. Der zugelassene Wert ist eine Zeichenfolge. Der Standard ist **/<Rejected-By-UrlScan>**. Diese Zeichenfolge ist ein URL in folgendem Format: **/Pfad/Dateiname.ext**. Wenn UrlScan eine Anforderung ablehnt, wird der angegebene URL ausgeführt. Für die Analyse der Anforderung durch UrlScan muss sich der URL lokal auf der Website befinden. Der angegebene URL kann dieselbe Erweiterung haben wie der abgelehnte URL (z. B. ASP).

UseFastPathReject. **0** oder **1** sind zugelassene Werte. Wenn **1** festgelegt ist, ignoriert UrlScan RejectResponseUrl und gibt dem Client eine kurze 404-Antwort zurück, wenn eine Anforderung abgelehnt wird. Diese Vorgehensweise ist im Vergleich zur vollständigen Verarbeitung von RejectResponseUrl schneller. Wird diese Option verwendet, kann IIS jedoch keine standardmäßige 404-Antwort zurückgeben, oder viele Teile der Anforderung werden im IIS-Protokoll protokolliert. (Die UrlScan-Protokolldatei enthält noch immer vollständige Informationen zu abgelehnten Anforderungen.) Die Standardeinstellung ist das Deaktivieren von UseFastPathReject.

Der Abschnitt [AllowVerbs] beinhaltet eine Auflistung von HTTP-Verben (Methoden). Wenn **UseAllowVerbs** im Abschnitt [Options] auf **1** festgelegt ist, lehnt UrlScan sämtliche Anforderungen ab, die ein Verb enthalten, das hier nicht expliziert aufgeführt ist. Bei den Einträgen in diesem Abschnitt muss die Groß-/Kleinschreibung beachtet werden.

Der Abschnitt [DenyVerbs] beinhaltet eine Auflistung von HTTP-Verben (Methoden). Wenn **UseAllowVerbs** im Abschnitt [Options] auf **0** festgelegt ist, lehnt UrlScan sämtliche Anforderungen ab, die ein Verb enthalten, das hier aufgeführt ist. Bei den Einträgen in diesem Abschnitt muss die Groß-/Kleinschreibung nicht beachtet werden.

Der Abschnitt [DenyHeaders] beinhaltet eine Auflistung der Anforderungsheader, die abgelehnt werden, wenn sie in einer empfangenen Anforderung enthalten sind. Bei den Einträgen in diesem Abschnitt muss die Groß-/Kleinschreibung nicht beachtet werden.

Der Abschnitt [AllowExtensions] beinhaltet eine Auflistung von Dateierweiterungen. Wenn **UseAllowExtensions** im Abschnitt [Options] auf **1** festgelegt ist, werden alle Anforderungen abgelehnt, die einen URL mit einer Erweiterung enthalten, die hier nicht explizit aufgeführt ist. Bei den Einträgen in diesem Abschnitt muss die Groß-/Kleinschreibung nicht beachtet werden.

Anmerkung: Durch Hinzufügen einer leeren Erweiterung mithilfe eines Punktes und keines abschließenden Zeichens können Anforderungen ohne Erweiterungen angegeben werden (z. B. Anforderungen für eine Standardseite oder eine Verzeichnisauflistung).

Der Abschnitt [DenyExtensions] beinhaltet eine Auflistung von Dateierweiterungen. Wenn **UseAllowExtensions** im Abschnitt [Options] auf **0** festgelegt ist, werden alle Anforderungen abgelehnt, die einen URL mit einer Erweiterung enthalten, die hier aufgeführt ist. Bei den Einträgen in diesem Abschnitt muss die Groß-/Kleinschreibung nicht beachtet werden.

Anmerkung: Wenn Sie Änderungen an der Datei **UrlScan.ini** vornehmen, müssen Sie den ISA PROXY3-Dienst erneut starten, um sicherzustellen, dass ISAPI-Filter erneut geladen werden.

Überwachen/Kontollieren von HTTP-Zugriffen auf dem ISA Server

Auf dem ISA Server sollten die Webveröffentlichungsregeln, die die internen Webserver veröffentlichen, so konfiguriert werden, dass nur Anfragen die Regel passieren dürfen, die exakt (Server Name und Pfad) der Regel entsprechen. Weitere detaillierte Informationen zu dieser Thematik erhalten Sie unter der folgenden englischsprachigen Adresse:
http://www.microsoft.com/technet/prodtechnol/isa/deploy/isanimda.asp

Scannen von Netzwerken mithilfe von UrlScan mit ISA Server

Wenn UrlScan auf einem Computer mit ISA Server am Netzwerkperimeter bereitgestellt wird, muss sichergestellt werden, dass die Einstellungen der Datei **UrlScan.ini** den von Webservern hinter dem Computer mit ISA Server benötigten Verkehr zulassen. Hierzu kann eine manuelle Konfiguration der Datei **UrlScan.ini** erforderlich sein.

Wenn die Einstellungen der Datei **UrlScan.ini** auf einem Computer mit ISA Server definiert werden, sollten Sie zuerst alle auf dem Computer mit ISA Server konfigurierten Webpublishingregeln dokumentieren. Diese Regeln legen genau fest, welcher HTTP- und HTTPS-Verkehr den Computer mit ISA Server durchlaufen kann.

Sobald der gesamte Webverkehr identifiziert ist, sollten Sie ihn profilieren, um die Konfiguration der Datei **UrlScan.ini** zu ermöglichen. Wenn Sie die Einstellungen definieren, denken Sie daran, dass die Erkennung von Perimetereindringversuchen den gesamten erforderlichen Verkehr zulassen muss. Wenn es zwischen den Sicherheitskonfigurationen von zwei Webservern zu Konflikten kommt, müssen die am wenigsten restriktiven Einstellungen für das Netzwerkperimeter bereitgestellt werden. Wenn Sie beispielsweise zwei Webserver haben, die durch einen Computer mit ISA Server geschützt sind, und einen Webserver, der als Host einer ASP-basierten Website dient, während der zweite Webserver nur als Host für statischen Inhalt dient, muss durch UrlScan (auf dem Computer mit ISA Server bereitgestellt) mit ASP verbundener Verkehr zu beiden Webservern weitergeleitet werden. Sie können den Verkehr auf dem Webserver, der als Host für den statischen Inhalt dient, auch sperren, indem Sie UrlScan auf diesem Webserver implementieren.

Endpunktscannen mithilfe von UrlScan mit IIS

Sie können bestimmte Einstellungen der Datei **UrlScan.ini** definieren, um den Anforderungen der einzelnen Webserver zu entsprechen.

URLScan ist für den Schutz von Webservern sehr nützlich, denn viele Angriffe weisen gemeinsame Merkmale auf: Sie verwenden eine ungewöhnliche Anforderung. Beispielsweise kann die Anforderung sehr lang sein, eine ungewöhnliche Aktion anfordern, mithilfe eines alternativen Zeichensatzes codiert sein oder Zeichenfolgen enthalten, die in rechtmäßigen Anforderungen selten vorkommen. Durch das Herausfiltern ungewöhnlicher Anforderungen bewahrt URLScan den Server vor potenziellem Schaden.

URLScan ist sehr flexibel. Der zugehörige Standardregelsatz schützt einen Server sowohl gegen alle IIS betreffenden bekannten Sicherheitsschwachstellen als auch potenziell gegen zusätzliche, noch unbekannte Angriffsmethoden. Die Standardregeln können geändert und neue Regeln hinzugefügt werden, um die Aktionen des Tools den Anforderungen eines bestimmten Servers anzupassen. Zusätzlich zum Standardregelsatz können während der Installation des ISAPI-Filters der Datei **UrlScan.ini** die folgenden Konfigurationen im Assistenten zum IIS-Lockdowntool ausgewählt werden.

- Small Business Server 2000
- Exchange Server 5.5 (Outlook-Webzugriff)
- Exchange Server 2000 (OWA, PF-Verwaltung, IM, SMTP, NNTP)
- SharePoint Portal Server
- FrontPage-Servererweiterungen (SharePoint Team Services)
- BizTalk Server 2000
- Commerce Server 2000
- Proxyserver

Statischer Webserver

Dynamischer Webserver (ASP-aktiviert)

Andere (Server, die keiner der oben aufgeführten Rollen entsprechen)

Server, die IIS nicht benötigen

Wenn Sie eine der vorkonfigurierten Vorlagen auswählen, wird eine vordefinierte Datei **UrlScan.ini** mit den optimalen Einstellungen bereitgestellt. Akzeptieren Sie die vordefinierte Datei **UrlScan.ini**, und stellen Sie zudem sicher, dass Sie die aktuellen Microsoft Knowledge Base-Artikel nach allen Anpassungen durchsuchen, die für bestimmte Konfigurationen der Datei **Urlscan.ini** erforderlich sind.

Empfehlungen für bestimmte UrlScan-Konfigurationen

Viele Knowledge Base-Artikel bieten empfohlene Konfigurationseinstellungen, wenn UrlScan in bestimmten Umgebungen verwendet wird. Wenn Sie die Konfigurationseinstellungen von UrlScan überprüfen, sollten Sie unbedingt die folgenden Artikel berücksichtigen:

Q309394 HOW TO: Use URLScan with FrontPage 2000 (englischsprachig)

Q318290 HOW TO: Use URLScan with FrontPage 2002 (englischsprachig)

Q309505 IIS Lockdown and URLscan Configurations in Exchange Environment (englischsprachig)

Q309677 XADM: Known Issues and Fine Turning When You Use the IIS Lockdown Wizard in an Exchange 2000 Environment (englischsprachig)

Q311595 XCCC: How to Install and Configure Microsoft Security Tool Kit On a Microsoft Mobile Information Server (englischsprachig)

Q312376 HOW TO: Configure URLScan to Allow Requests with a Null Extension in IIS (englischsprachig)

Q313131 HOW TO: Use URLScan with Exchange Outlook Web Access in Exchange Server 5.5 (englischsprachig)

Q311862 How to Use The IIS Lockdown Tool with Small Business Server (englischsprachig)

Q311350 HOW TO: Create a Custom Server Type for Use with the IIS Lockdown Wizard (englischsprachig)

Features von ISA Server zur Erkennung von Eindringversuchen

ISA Server bietet ein integriertes System zur Erkennung von Eindringversuchen, das einen versuchten Angriff gegen Ihr Netzwerk erkennen kann und mit einem Satz vorkonfigurierter Aktionen oder *Alarme* reagiert. Zum Erkennen unerwünschter Eindringversuche werden Netzwerkverkehr und Protokolleinträge mit bekannten Angriffsmethoden durch ISA Server verglichen. Verdächtige Aktivitäten lösen Alarme aus, woraufhin eine Reihe von Aktionen durch ISA Server ausgeführt wird. Mögliche Aktionen beinhalten das Ausführen eines Programms, das Senden einer E-Mail-Nachricht, das Protokollieren des Ereignisses im Windows-Ereignisprotokoll, das Beenden und Starten von ISA Server-Diensten oder eine Kombination aus diesen Möglichkeiten.

Wenn die Erkennung von Eindringversuchen aktiviert ist, können Alarme für die folgenden Angriffe konfiguriert werden:

Vollständiger Port-Scan. Eine Methode, die von Angreifern zur Ermittlung offener Ports auf einem Zielcomputer oder in einem Zielnetzwerk verwendet wird. Das Modul zur Erkennung von Eindringversuchen erkennt eine Vielzahl von Versuchen der Verbindungsherstellung zu Ports und sendet einen Alarm, sobald die Anzahl der Verbindungsversuche den vom Administrator konfigurierten Schwellenwert überschreitet. ISA Server kann auch so konfiguriert werden, dass nur das Scannen bekannter Ports erkannt wird (1-2048).

IP-Half-Scan. Dieser Angriff ähnelt dem vollständigen Port-Scan-Angriff, nutzt jedoch die Tatsache, dass TCP-Kommunikation drei Schritte umfasst. Ein IP-Half-Scan sendet das dritte Paket des TCP-Dreiwegehandshakes nicht, um eine Entdeckung zu verhindern.

Land-Angriff. Einem Computer wird ein Paket mit einer gefälschten IP-Quelladresse und Portnummer gesendet, die der Zieladresse und dem Zielport entsprechen. Das gefälschte Paket lässt den Zielcomputer eine Schleife ausführen, die schließlich zum Absturz führt.

Ping-of-Death. Dieser Angriff beinhaltet eine große Anzahl außergewöhnlich großer ICMP-Echoanforderungspakete (Ping), die an einen Computer gesendet werden. Der Zielcomputer versucht, auf alle Pakete zu reagieren, wodurch ein Pufferüberlauf verursacht wird, der den Computer zum Absturz bringt.

UDP-Bomb. Ein UDP-Paket mit illegalen Werten in bestimmten Feldern führt bei einigen älteren Betriebssystemen zum Absturz, sobald das Paket empfangen wird. Wenn der Zielcomputer abstürzt, gestaltet sich die Ursachenforschung häufig schwierig.

Windows-Out-of-Band. Auch bekannt als *WinNuke*. Dies ist ein DoS-Angriff (Denial of Service), der verwendet werden kann, um Windows-Netzwerke funktionsunfähig zu machen. Ein erfolgreicher Angriff führt zum Verlust von Netzwerkverbindungen oder zum Absturz ungeschützter Computer.

Das Aktivieren der Eindringversuche ist beim ISA Server über die Eigenschaften der Paketfilter möglich. Die Einstellungen finden Sie unter den Eigenschaften für Paketfilter auf der Registerkarte **Eindringversuchserkennung**.

Zusätzliche Funktionalität zur Erkennung von Eindringversuchen kann entweder über Drittanbieterpartner für ISA Server bezogen werden oder selbst mithilfe der Anwendungsfilter-Schnittstellen aus dem Software Development Kit von ISA Server erstellt werden. Weitere Informationen finden Sie im gleichnamigen Abschnitt am Ende dieses Kapitels.

Anmerkung: Alarme bei Eindringversuchen können in der Managementkonsole von ISA Server im Ordner **Internet Security & Acceleration Server\Server und Arrays\<*Servername*>\Überwachung\Alarme** angezeigt werden.

Drittanbieterlösungen zur Erkennung von Eindringversuchen

Drittanbieterlösungen in Form von Systemen für die Erkennung von Eindringversuchen werden sowohl für Netzwerke als auch für Endpunktserver angeboten. Diese Drittanbieterlösungen bieten Protokollunterstützung über HTTP hinaus sowie Scanvorgänge nach bekannten Angriffsmethoden gegen Netzwerkcomputer.

Die folgenden Angriffstypen sollten von Systemen zur Erkennung von Eindringversuchen identifiziert werden:

Erkundungsangriffe. Dieser Angriffstyp tritt auf, wenn ein Angreifer ein Netzwerk auf der Suche nach Schwachstellen ausspioniert. Potenzielle Angriffe beinhalten sequenzielles Ping (Ping Sweeps), DNS-Zonenübertragung, E-Mail-Erkundung und das Downloaden von Websiteinhalten auf der Suche nach Skriptschwachstellen und Beispielseiten.

Ausnutzungsangriffe. Dieser Angriffstyp tritt auf, wenn Angreifer verborgene Features oder Fehler ausnutzen, um Zugriff auf das System zu erhalten. Meist identifiziert ein vorhergehender Ausnutzungsangriff die Angriffspunkte.

Denial-of-Service-Angriffe (DoS). Dieser Angriffstyp tritt auf, wenn ein Angreifer versucht, einen auf einem Computer ausgeführten Dienst durch Überlastung einer Ressource zum Absturz zu bringen. Zu diesen Ressourcen zählen z. B. Netzwerkverbindungen, die CPU oder das Festplatten-Teilsystem. Der Angreifer versucht nicht, Informationen zu sammeln, sondern setzt alles daran, Ihren Computer funktionsunfähig zu machen.

Ein gutes System zur Erkennung von Eindringversuchen sollte in der Lage sein, alle drei Angriffsformen zu erkennen. Zum Identifizieren von Angriffen werden zwei unterschiedliche Methoden verwendet:

Anomalieerkennung. Basiert auf der Auswahl eines Netzwerkcomputers als Basis. Abweichungen von der Basis können als Eindringversuch identifiziert werden. Beispielsweise kann ein Ansteigen von Anmeldeversuchen außerhalb der Spitzenzeiten auf einen gefährdeten Computer hinweisen. Der Vorteil der Anomalieerkennung ist, dass Angriffe auch ohne Vorwissen über die Ausführungsweise des Angriffs identifiziert werden können.

Signaturerkennung. Identifiziert Angriffe basierend auf bekannten Angriffsmustern. Beispielsweise verwenden viele Webserverangriffe gemeinsame Muster, die einfach zu identifizieren sind. Das Vergleichen des eingehenden Anwendungsverkehrs mit Signaturzeichenfolgen in einer Datenbank ermöglicht dem System zur Erkennung von Eindringversuchen die Identifizierung dieser Angriffe. Der Nachteil dieser Methode eines Systems zur Erkennung von Eindringversuchen liegt in der Notwendigkeit der regelmäßigen Aktualisierung der Signaturdatenbank, um auch neue Angriffssignaturen identifizieren zu können.

Im Folgenden sind einige der verfügbaren Produkte von Drittanbietern zum Testen und Bereitstellen aufgeführt:

BlackIce Defender (http://www.iss.net/products_services/hsoffice_protection/; englischsprachig)

CyberCop Scanner (http://www.pgp.com/products/cybercop-scanner/default.asp; englischsprachig)

ICEpac Security Suite (www.networkice.com/products/icepac_suite.html; englischsprachig)

Cisco Secure IDS (http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/prodlit/netra_ds.htm; englischsprachig)

eTrust Intrusion Detection (http://www3.ca.com/Solutions/Product.asp?ID=163; englischsprachig)

Snort (www.snort.org; englischsprachig)

Tripwire (www.tripwiresecurity.com; englischsprachig)

Foundstone Attacker (www.foundstone.com; englischsprachig)

Beurteilung von Schwachstellen

Zusätzlich zur passiven und aktiven Erkennung von Eindringversuchen sollten Sie Schwachstellen regelmäßig beurteilen. Beurteilungen von Schwachstellen simulieren einen Angriff auf das Netzwerk und decken die Schwachstellen auf, die sich einem Angreifer bieten.

Das regelmäßige Beurteilen von Schwachstellen ermöglicht es Ihnen, einem Angreifer beim Auffinden von Schwachstellen zuvorzukommen und die Schwachstelle Ihres Netzwerkes vor Angriffen zu sichern.

Wenn Sie Tools zur Beurteilung von Schwachstellen prüfen, schließen Sie die folgenden Anforderungen in Ihren Entscheidungsprozess ein:

Mechanismus zur Aktualisierung der Datenbank. Das Tool sollte eine automatisierte Methode zur Aktualisierung der Signaturen für Schwachstellen bieten, so dass es nicht schon nach kurzer Zeit nicht mehr aktuell ist.

Minimieren von falschen Meldungen. Das Tool sollte falsche Meldungen herausfiltern, damit Ihr Unternehmen nicht unnötig Zeit mit der Untersuchung von nicht sicherheitsbezogenen Ereignissen verliert.

Möglichkeit des Speicherns von Ergebnissen in einer Datenbank. Das Tool sollte Ihnen das Archivieren von Scanergebnissen zum Zweck von Trendanalysen und zur Erkennung von Sicherheitsänderungen ermöglichen.

Lösungen zum Erkennen von Schwachstellen. Wenn eine Schwachstelle erkannt wird, sollte das Tool eine Dokumentation mit Informationen zum Schließen der Schwachstelle bieten oder Skripts, die zum Schutz vor Schwachstellen nötige Tasks ausführen.

Viele Tools von Drittanbietern bieten Möglichkeiten zur Beurteilung von Schwachstellen in einem Windows 2000-Netzwerk. Zu diesen Tools zählen folgende:

Symantec NetRecon 3.5 (enterprisesecurity.symantec.com)

BindView Security Advisor (www.bindview.com; englischsprachig)

eEye Digital Security. Retina Network Security Scanner (http://www.eeye.com; englischsprachig)

Internet Security Systems (ISS) Internet Scanner (www.iss.net; englischsprachig)

Network Associates CyberCop (http://www.pgp.com/products/default.asp; englischsprachig)

Alternativ kann es sich auch als dienlich erweisen, die Beratungsdienstleistung eines Drittanbieters zur Beurteilung von Schwachstellen in Anspruch zu nehmen. Der Vorteil bei der Verwendung von Drittanbieterdiensten ist, dass die Teams kein Vorwissen über das Netzwerk besitzen und von demselben Ausgangspunkt wie ein externer Angreifer arbeiten. Häufig bieten diese externen Beurteilungen aufgrund der Neutralität des einschätzenden Teams die nützlichsten Informationen.

Zusammenfassung

Überwachung und Erkennung von Eindringversuchen sind Hauptbestandteile einer effektiven Verteidigung Ihrer Umgebung. Als Bestandteil Ihres Risikomanagementprozesses (Risk Management) sollten Sie ermitteln, in welchem Umfang eine Überwachung und Erkennung von Eindringversuchen für Ihre Umgebung erforderlich ist. Für die Erkennung von Eindringversuchen über mehrere Protokolle könnten Sie Tools von Drittanbietern erwägen.

Weitere Informationen

Externe Zeitserver:

ntp2.usno.navy.mil und **tock.usno.navy.mil**

Informationen zu ISA Server-Partnern:

http://www.microsoft.com/isaserver/partners (englischsprachig)

ISA Server Solution Developers Kit (SDK):

http://www.microsoft.com/isaserver/techinfo/productdoc/2000/SDKdownload.asp (englischsprachig)

Writing Secure Code (englischsprachig) von Michael Howard und David LeBlanc; Microsoft Press, ISBN: 0-7356-1588-8

http://mspress.microsoft.de/mspress/product.asp?sku=0-7356-1588-8

Originaltitel: Chapter 7 – Responding to Incidents

7

Vorgehensweise bei Vorfällen

Wie gut ist Ihre IT-Abteilung auf Sicherheitsvorfälle vorbereitet? Viele Organisationen lernen erst durch einen Angriff, wie sie bei einem Sicherheitsvorfall vorgehen sollten. Bis zu diesem Zeitpunkt können durch den Vorfall schon wesentlich höhere Kosten entstanden sein als notwendig. Die richtige Vorgehensweise bei Vorfällen sollte ein fester Bestandteil Ihrer umfassenden Sicherheitsrichtlinie und Ihrer Strategie zur Risikobegrenzung sein.

Die richtige Vorgehensweise bei Sicherheitsvorfällen hat einige direkte Vorteile. Sie kann auch zu indirekten, finanziellen Vorteilen führen. Es ist beispielsweise möglich, dass die Versicherungsgesellschaft Ihrer Organisation Vergünstigungen einräumt, wenn diese nachweislich schneller und kostengünstiger auf Angriffe reagieren kann. Wenn Sie Dienstanbieter sind, lohnt es sich u. U., einen Plan zur Vorgehensweise bei Vorfällen auszuarbeiten, denn dadurch wird Ihr Interesse für Informationssicherheit deutlich.

Minimieren der Anzahl und des Schweregrads von Sicherheitsvorfällen

In den meisten Lebensbereichen ist Vorsorge besser als Nachsorge, und dies gilt auch für die Sicherheit. Sie werden daher in erster Linie versuchen, Sicherheitsvorfällen vorzubeugen. Es ist aber unmöglich, alle Sicherheitsvorfälle zu verhindern. Dementsprechend sollten Sie bei einem Sicherheitsvorfall dafür sorgen, dass die Auswirkungen möglichst gering sind. Es gibt Vorsichtsmaßnahmen, die Sie ergreifen können, um die Anzahl und die Auswirkungen von Sicherheitsvorfällen zu minimieren. Dazu zählen folgende:

- Genaues Festlegen und Durchsetzen aller Richtlinien und Vorgehensweisen. Viele Sicherheitsvorfälle werden versehentlich durch das IT-Personal verursacht, wenn es Vorgehensweisen des Änderungsmanagements (Change Management) nicht befolgt oder nicht verstanden hat, oder wenn es Sicherheitsgeräte wie Firewalls und Authentifizierungssysteme nicht richtig konfiguriert hat. Die Richtlinien und Vorgehensweisen sollten sorgfältig getestet werden, um sicherzustellen, dass sie praktisch und verständlich sind und dass sie ein ausreichendes Maß an Sicherheit bieten.
- Bemühen um Unterstützung des Managements für Sicherheitsrichtlinien und den Umgang mit Vorfällen.
- Routinemäßiges Überwachen und Analysieren des Netzwerkverkehrs und der Systemleistung.

Routinemäßiges Überprüfen aller Protokolle und Protokollmechanismen. Dazu zählen auch Ereignisprotokolle der Betriebssysteme, anwendungsspezifische Protokolle und Protokolle für Systeme zur Erkennung von Eindringversuchen.

Routinemäßiges Beurteilen von Schwachstellen in der Umgebung. Diese Aufgabe sollte von einem dafür autorisierten Sicherheitsexperten übernommen werden.

Routinemäßiges Überprüfen von Servern, um die Installation aller aktuellen Patches sicherzustellen.

Einrichten von Sicherheitsschulungsprogrammen für IT-Mitarbeiter und Benutzer. Die größte Schwachstelle in jedem System sind nicht sensibilisierte oder arglose Benutzer – der Wurm ILOVEYOU hat diese Schwachstelle ausgenutzt.

Bereitstellen von Sicherheitsbannern, durch die Benutzer an ihre Pflichten und Beschränkungen erinnert werden, sowie einer Warnung vor möglicher strafrechtlicher Verfolgung bei Verstößen. Ohne solche Banner ist eine strafrechtliche Verfolgung möglicherweise schwierig oder unmöglich. Sie sollten sich an einen Rechtsberater wenden, um die Angemessenheit der Wortwahl auf den Sicherheitsbannern sicherzustellen.

Entwickeln, Implementieren und Durchsetzen einer Richtlinie, die komplexe Kennwörter verlangt.

Überprüfen der Sicherungs- und Wiederherstellungsverfahren. Sie sollten wissen, wo Sicherungsdateien aufbewahrt werden, wer darauf zugreifen kann und welche Verfahren zur Daten- und Systemwiederherstellung verwendet werden. Stellen Sie sicher, dass Sicherungen und Medien regelmäßig überprüft werden, indem Sie ausgewählte Daten wiederherstellen.

Bilden eines für die Computersicherheit verantwortlichen Teams (Computer Security Incident Response Team oder CSIRT). Dabei handelt es sich um eine Gruppe von Personen, die für die Behandlung aller Sicherheitsvorfälle zuständig ist. Ihr CSIRT sollte Personen mit eindeutig definierten Pflichten umfassen, damit sichergestellt wird, dass Ihre Vorgehensweise bei Vorfällen alle Bereiche abdeckt (weitere Informationen zur Zusammenstellung eines CSIRT finden Sie weiter unten in diesem Kapitel).

Schulen der für Informationssicherheit zuständigen Mitarbeiter des CSIRT zur richtigen Verwendung und Suche wichtiger Sicherheitstools. Sie sollten Laptops mit diesen Tools vorkonfigurieren, um bei Vorfällen keine Zeit mit dem Installieren und Konfigurieren von Tools zu verlieren. Diese Systeme und die dazugehörigen Tools müssen gut geschützt werden, wenn sie nicht benötigt werden.

Zusammenstellen aller wichtigen Kommunikationsinformationen. Sie sollten sicherstellen, dass Sie über die Namen aller zu benachrichtigenden Kontaktpersonen innerhalb der Organisation sowie deren Telefonnummern verfügen (einschließlich der Mitglieder des CSIRT und der für den Support aller Systeme Verantwortlichen sowie der für Pressekommunikation zuständigen Personen). Sie werden auch Informationen für Ihren Internetdienstanbieter (Internet Service Provider oder ISP) und Behörden zur Wahrung des regionalen oder nationalen Rechts benötigen. Wenden Sie sich an die Behörden zur Wahrung des regionalen Rechts, bevor sich ein Vorfall ereignet. So können Sie sicherstellen, dass Sie mit den richtigen Verfahren zum Melden von Vorfällen und zum Sammeln von Beweisen vertraut sind.

Platzieren aller Informationen zum Notfallsystem an einem zentralen Ort ohne Netzwerkanschluss, wie beispielsweise einem Notebook oder einem vom Netzwerk getrennten Computer. Diese Notfallinformationen beinhalten u. a. Folgendes: Systemkennwörter, IP-Adressen, Konfigurationsinformationen für Router, Regelsatzlisten für Firewalls, Kopien der Schlüssel von Zertifizierungsstellen, Namen und Telefonnummern von Kontaktpersonen, Verfahrensweisen für die Eskalation von Vorfällen usw. Diese Informationen müssen an einem sehr sicheren Ort und gleichzeitig schnell verfügbar aufbewahrt werden. Eine Methode zum Sichern und zum Sicherstellen einer schnellen Verfügbarkeit ist die Verschlüsselung der Informationen auf einem dedizierten in einem Tresorraum platzierten Laptop sowie das Beschränken des Zugriffs auf autorisierte Personen wie den Leiter des für die Computersicherheit verantwortlichen Teams (CSIRT) und den Leiter der IT-Abteilung (Chief Information Officer oder CIO) oder den Leiter der Technologieabteilung (Chief Technology Officer oder CTO).

Zusammenstellen der wichtigsten Mitglieder des CSIRT (Kernteam)

Das für die Computersicherheit verantwortliche Team ist die zentrale Stelle für die Behandlung von Vorfällen im Zusammenhang mit der Computersicherheit in der Umgebung. Folgende Aufgaben fallen in seinen Zuständigkeitsbereich:

- Überwachen von Systemen im Hinblick auf Sicherheitsverletzungen.
- Bereitstellen eines Kommunikationszentrums, das Berichte zu Sicherheitsvorfällen empfängt und wichtige Informationen zu Vorfällen an die entsprechenden Personen weiterleitet.
- Dokumentieren und Katalogisieren von Sicherheitsvorfällen.
- Erhöhen des Sicherheitsbewusstseins innerhalb des Unternehmens zur Vermeidung von Vorfällen.
- Unterstützen der System- und Netzwerküberwachung beispielsweise durch die Beurteilung von Schwachstellen und das Durchführen von Testangriffen.
- Sammeln von Informationen über neue Schwachstellen und über die von Angreifern eingesetzten Angriffsstrategien.
- Installieren neuer Softwarepatches.
- Analysieren und Entwickeln neuer Technologien zum Minimieren von Schwachstellen und Risiken bezüglich der Sicherheit.
- Bereitstellen von Sicherheitsberatungsdiensten.
- Kontinuierliches Verbessern und Aktualisieren der bestehenden Systeme und Verfahren.

Die ideale Struktur und Zusammensetzung des CSIRT hängt von der Art der Organisation und der Strategie des Risikomanagements (Risk Management) ab. Im Allgemeinen sollte das CSIRT allerdings einige oder alle Mitglieder des Sicherheitsteams umfassen. Innerhalb des Kernteams sind Sicherheitsexperten für die Koordination der Vorgehensweise bei Vorfällen zuständig. Die Anzahl der Mitglieder innerhalb des CSIRT wird i. d. R. von der Größe des Unternehmens und der Komplexität der Unternehmensstruktur abhängen. Stellen Sie sicher, dass genügend Mitglieder vorhanden sind, um jederzeit alle Aufgaben des Teams erfüllen zu können.

Teamleiter des CSIRT

Es ist wichtig, dass das CSIRT über einen eigenen Leiter verfügt, der die Verantwortung für die Aufgaben des Teams trägt. Der Leiter des CSIRT wird im Allgemeinen für die Aufgaben des Teams verantwortlich sein, und die Prüfung der vom Team ergriffenen Maßnahmen koordinieren. Dies kann zu Änderungen hinsichtlich der Richtlinien und Verfahren für zukünftige Vorfälle führen.

Vorfallsleiter des CSIRT

Eine Person sollte für die Koordination der weiteren Vorgehensweise bei Vorfällen verantwortlich sein. Die Vorfallleitung des CSIRT ist für einen bestimmten Vorfall oder eine Reihe von Sicherheitsvorfällen zuständig. Die Vorfallleitung koordiniert die gesamte Kommunikation im Zusammenhang mit Vorfällen und repräsentiert das gesamte CSIRT, wenn er mit Personen außerhalb des CSIRT spricht. Wer für die Vorfallleitung bestimmt wird, kann je nach Art des Vorfalls variieren. Die Vorfallleitung ist nur selten gleichzeitig die Teamleitung.

Zusätzliche Mitglieder des CSIRT

Neben den wichtigsten Mitgliedern des CSIRT (Kernteam) sollten bestimmte Personen für die Vorgehensweise bei bestimmten Vorfällen zuständig sein. Zusätzliche Mitglieder kommen aus verschiedenen Abteilungen im Unternehmen und spezialisieren sich auf bestimmte von Sicherheitsvorfällen betroffene Bereiche, die nicht direkt vom Kernteam behandelt werden. Zusätzliche Mitglieder können entweder direkt von einem Vorfall betroffen sein oder als Anlaufstelle dienen, die die Verantwortung an eine besser geeignete Person innerhalb der Abteilung überträgt. In der folgenden Tabelle werden einige zusätzliche Mitglieder und ihre Funktion aufgeführt:

Tabelle 7.1: Zusätzliche Mitglieder des CSIRT

Zusätzliches Mitglied	Beschreibung der Funktion
IT-Kontaktperson	Verantwortlich für die Koordination der Kommunikation zwischen der Vorfallleitung des CSIRT und den übrigen Mitgliedern der IT-Gruppe. Diese Person verfügt möglicherweise nicht über das technische Wissen, das für Sofortmaßnahmen bei Vorfällen erforderlich ist, ist allerdings dafür verantwortlich, innerhalb der IT-Gruppe jemanden für einen bestimmten Sicherheitsvorfall zu bestimmen.
Rechtsvertreter	In der Regel handelt es sich dabei um ein Mitglied der internen Rechtsabteilung, das mit den geltenden Richtlinien zur Vorgehensweise bei Vorfällen vertraut ist. Der Rechtsvertreter legt die Vorgehensweise bei einem Vorfall fest, um die Haftbarkeit möglichst gering zu halten und die Möglichkeiten zur strafrechtlichen Verfolgung von Tätern auszuschöpfen. Vor einem Vorfall sollte der Rechtsvertreter über die Richtlinien zum Überwachen und zur Vorgehensweise informiert werden, damit sichergestellt wird, dass das Unternehmen bei der Beseitigung oder Eingrenzung eines Vorfalls keinen rechtlichen Risiken ausgesetzt ist. Sie müssen die gesetzlichen Vorgaben zum Herunterfahren von Systemen und zur möglichen Verletzung von Vereinbarungen auf Dienstebene oder Mitgliedsvereinbarungen mit Ihren Kunden beachten. Darüber hinaus müssen Sie ein beeinträchtigtes System herunterfahren, da Sie sonst für Schäden haftbar gemacht werden könnten, die durch die auf dieses System verübten Angriffe verursacht werden. Auch jeder Kontakt mit externen Behörden zur Wahrung des Rechts und externen mit Nachforschungen betrauten Stellen sollte mit dem Rechtsvertreter koordiniert werden.

Zusätzliches Mitglied	Beschreibung der Funktion
Kommunikations-mitarbeiter	Dabei handelt es sich im Allgemeinen um ein Mitglied der PR-Abteilung. Diese Person ist zuständig für den Schutz und die Verbesserung der Unternehmensreputation. Sie stehen möglicherweise nicht in direktem Kontakt mit den Medien und den Kunden, sondern verfassen die Nachricht (während Inhalt und Zweck der Nachricht im Allgemeinen in den Verantwortungsbereich des Managements fallen). Alle Anfragen der Medien sollten an den Kommunikationsmitarbeiter weitergeleitet werden.
Management	Die Einbeziehung des Managements kann sich auf die Abteilung beschränken oder unternehmensweit erfolgen. Je nach den Auswirkungen, dem Ort, dem Schweregrad und der Art des Vorfalls können unterschiedliche Mitglieder des Managements zuständig sein. Wenn Sie eine Kontaktperson innerhalb des Managements haben, können Sie schnell herausfinden, welche Person unter den jeweiligen Umständen besonders geeignet ist. Das Management muss einer Sicherheitsrichtlinie zustimmen und diese zur Vorgabe machen. Darüber hinaus ist es dafür verantwortlich, die Gesamtauswirkungen (finanzielle und sonstige) des Vorfalls für die Organisation zu ermitteln. Das Management weist den Kommunikationsmitarbeiter an, welche Informationen an die Medien weitergegeben werden dürfen und bestimmt, inwieweit der Rechtsvertreter und die Behörden zur Wahrung des Rechts miteinander kooperieren dürfen.

Vorgehensweise des CSIRT bei Vorfällen

Bei Vorfällen wird das CSIRT die Vorgehensweise des Kernteams koordinieren und wird Kontakt zu den zusätzlichen Mitgliedern des CSIRT aufnehmen. In der folgenden Tabelle sind die Verantwortungsbereiche dieser Personen im Rahmen der Vorgehensweise bei Vorfällen dargestellt:

Tabelle 7.2: Verantwortungsbereiche des CSIRT im Rahmen der Vorgehensweise bei Vorfällen.

Aufgaben	**Funktionen**				
	Vorfallsleitung des CSIRT	IT-Kontakt-person	Rechts-vertreter	Kommunikations-mitarbeiter	Manage-ment
Erste Beurteilung	Besitzer	Berät	Keine	Keine	Keine
Erste Vorgehensweise	Besitzer	Implementiert	Aktualisiert	Aktualisiert	Aktualisiert
Sammeln rechtsgültiger Beweise	Implementiert	Berät	Besitzer	Keine	Keine
Implementieren vorläufiger Fixes	Besitzer	Implementiert	Aktualisiert	Aktualisiert	Berät
Benachrichtigen	Berater	Berät	Berät	Implementiert	Besitzer
Überprüfen hinsichtlich des vor Ort gelten-den Rechts	Aktualisierer	Aktualisiert	Implementiert	Aktualisiert	Besitzer

Aufgaben	Funktionen				
	Vorfallsleitung des CSIRT	IT-Kontakt-person	Rechts-vertreter	Kommunikations-mitarbeiter	Manage-ment
Implementieren dauerhafter Fixes	Besitzer	Implementiert	Aktualisiert	Aktualisiert	Aktualisiert
Ermitteln der finanziellen Auswirkungen auf das Unternehmen	Aktualisierer	Aktualisiert	Berät	Aktualisiert	Besitzer

Definieren eines Plans zur Vorgehensweise bei Vorfällen

Alle Mitglieder der IT-Umgebung sollten mit der Vorgehensweise bei Vorfällen vertraut sein. Während das CSIRT den Großteil der Maßnahmen bei Vorfällen ergreift, sollten alle IT-Mitarbeiter wissen, wie Vorfälle intern gemeldet werden müssen. Anwender sollten auffällige Vorkommnisse direkt oder über das Helpdesk an die IT-Mitarbeiter weitergeben und sich nicht direkt an das CSIRT wenden.

Der Plan zur Vorgehensweise bei Vorfällen sollte von allen Mitgliedern des Teams im Detail überprüft werden und für alle IT-Mitarbeiter zugänglich sein. Dadurch wird bei einem Vorfall die richtige Vorgangsweise sichergestellt.

Der Plan zur Vorgehensweise bei Vorfällen sollte folgende Schritte umfassen:

Vornehmen einer ersten Beurteilung

Melden des Vorfalls

Begrenzen des Schadens/Risikos

Identifizieren der Art und des Schweregrads der Gefährdung

Schützen der Beweise

Benachrichtigen externer Stellen

Wiederherstellen der Systeme

Zusammenstellen und Gliedern der Dokumentation zum Vorfall

Beurteilen der durch den Vorfall entstandenen Schäden und Kosten

Überprüfen der Richtlinien zur Vorgehensweise und Aktualisierung

---

Anmerkung: Aufgabenhilfe 4: Die Referenzliste zur Vorgehensweise bei Vorfällen kann während eines Vorfalls als Prüfliste verwendet werden, um die ordnungsgemäße Ausführung aller Phasen sicherzustellen.

Die Schritte müssen nicht unbedingt nacheinander vorgenommen werden. Sie werden im Laufe des Vorfalls ausgeführt. Die Dokumentation beginnt beispielsweise, wenn der Vorfall auftritt und wird bis zum Ende des Vorfalls fortgeführt. Auch die Kommunikation findet während der gesamten Dauer des Vorfalls statt.

Andere Teile des Prozesses erfolgen gleichzeitig. Durch die erste Beurteilung werden Sie beispielsweise eine allgemeine Vorstellung von der Art des Angriffs erhalten. Diese Informationen sollten verwendet werden, um den Schaden und das Risiko möglichst schnell zu begrenzen. Wenn Sie schnell handeln, können Sie für Ihr Unternehmen Zeit und Geld sparen und die Unternehmensreputation schützen. Sie benötigen allerdings nähere Einzelheiten zu Form und Ausmaß der Gefährdung, um den Schaden und das Risiko wirklich effektiv begrenzen zu können. Eine voreilige Vorgehensweise kann sogar größeren Schaden anrichten als der eigentliche Angriff. Durch das gleichzeitige Ausführen dieser Schritte werden Sie den besten Kompromiss zwischen schnellen und effektiven Maßnahmen finden.

Anmerkung: Sie sollten die Vorgehensweise bei Vorfällen unbedingt vor Auftreten eines Vorfalls testen. Andernfalls können Sie sich nicht darauf verlassen, dass die vorgesehenen Maßnahmen bei Vorfällen tatsächlich effektiv sind.

Vornehmen einer ersten Beurteilung

Viele Vorkommnisse weisen auf einen Angriff in der Organisation hin. Ein Netzwerkadministrator, der eine rechtmäßige Wartung des Systems durchführt, wird beispielsweise genauso wahrgenommen wie ein Angreifer. In anderen Fällen kann ein schlecht konfiguriertes System dazu führen, das ein System zur Erkennung von Eindringversuchen falsche Meldungen generiert, wodurch die Ermittlung echter Vorfälle erschwert wird.

Die erste Beurteilung sollte folgende Schritte beinhalten:

Das Ergreifen erster Schritte, um zu ermitteln, ob es sich um einen echten Vorfall oder eine falsche Meldung handelt.

Entwickeln einer ersten Vorstellung zur Art und zum Ausmaß des Angriffs. Diese sollte ausreichen, um den Vorfall zur weiteren Untersuchung zu melden und um mit der Begrenzung des Schadens und des Risikos zu beginnen.

Zeichnen Sie die von Ihnen ergriffenen Maßnahmen sorgfältig auf. Diese Aufzeichnungen werden später zum Dokumentieren des (echten oder falschen) Vorfalls verwendet.

Anmerkung: Obwohl falsche Meldungen weitestgehend verhindert werden sollten, ist es in jedem Fall besser, auf eine falsche Meldung zu reagieren als einen echten Vorfall zu übersehen. Ihre erste Beurteilung sollte daher so kurz wie möglich sein, wobei offensichtlich falsche Meldungen ausgeschlossen werden sollten.

Melden des Vorfalls

Sobald Sie einen Sicherheitsvorfall vermuten, sollten Sie die Sicherheitsverletzung schnell den übrigen Mitgliedern des Kernteams melden. Die Vorfallleitung und die übrigen Mitglieder des Teams sollten schnell ermitteln, welche Person außerhalb des Kernteams zu kontaktieren ist. Dadurch kann eine geeignete Kontrolle und Koordination für den Vorfall beibehalten und gleichzeitig das Ausmaß des Schadens begrenzt werden. Es gibt verschiedene Arten von Schaden, und eine Schlagzeile in der Zeitung, in der auf eine Sicherheitsverletzung hingewiesen wird, kann größeren Schaden anrichten als viele Eindringversuche bei Systemen. Daher und auch um zu verhindern, dass ein Angreifer einen Hinweis erhält, sollten nur an der Vorgehensweise bei Vorfällen beteiligte Personen informiert werden, bis der Vorfall unter Kontrolle ist. Der Teamleiter wird später bestimmen, wer über den Vorfall informiert werden muss. Dabei kann es sich um eine bestimmte Person oder um das gesamte Unternehmen und externe Kunden handeln.

Begrenzen des Schadens und des Risikos

Wenn Sie schnell handeln, um die tatsächlichen und potenziellen Auswirkungen eines Angriffs zu verringern, können Sie eine Verschlimmerung des Ereignisses verhindern. In RFC 2196 ist eine Reihe von Prioritäten zum Begrenzen des Schadens

in der Umgebung definiert. Die genaue Vorgehensweise hängt von der Organisation und der Art des Angriffs ab. Allerdings sollen Ihnen die folgenden Prioritäten eine erste Hilfestellung bieten.

1. **Schutz von Leben und Sicherheit**. Dieser Aspekt sollte selbstverständlich immer oberste Priorität haben.
2. **Schutz klassifizierter und/oder privater Daten**. Während Sie die Vorgehensweise bei Vorfällen planen, sollten Sie die klassifizierten und privaten Daten klar definieren. Dadurch wird das Festlegen von Prioritäten für die Vorgehensweise zum Schutz der Daten vereinfacht.
3. **Schutz anderer Daten, einschließlich proprietärer und wissenschaftlicher Daten sowie Daten der Geschäftsführung**. Auch andere Daten in der Umgebung können wichtig sein. Sie sollten zunächst die wertvollsten Daten schützen, bevor Sie sich um die anderen, weniger wichtigen Daten kümmern.
4. **Schutz der Hard- und Software gegen Angriffe**. Dazu zählt auch der Schutz vor dem Verlust oder der Änderung von Systemdateien und vor der physischen Beschädigung der Hardware. Schäden an Systemen können kostspielige Downtime zur Folge haben.
5. **Minimierte Unterbrechung von Computerressourcen (einschließlich Prozesse)**. Obwohl die Betriebszeit in den meisten Umgebungen sehr wichtig ist, kann das Inbetriebhalten eines Systems während eines Angriffs später zu weit größeren Problemen führen. Daher sollte das Minimieren der Unterbrechungen von Computerressourcen im Allgemeinen eine relativ niedrige Priorität haben.

Es gibt eine Reihe von Maßnahmen zur Begrenzung des Schadens und des Risikos für die Umgebung. Sie sollten zumindest Folgendes beachten:

Sie sollten die Angreifer nicht merken lassen, dass Sie ihre Aktivitäten entdeckt haben. Das kann schwierig sein, denn durch einige wichtige Vorgehensweisen könnten Angreifer gewarnt werden. Wenn beispielsweise eine Notfallbesprechung des CSIRT angesetzt wird und alle Kennwörter sofort geändert werden sollen, werden interne Angreifer vermuten, dass Sie den Vorfall bemerkt haben.

Wägen Sie die Kosten, die durch die gefährdeten und damit verbundenen Systeme entstehen und das mit der Aufrechterhaltung des Betriebs verbundene Risiko gegeneinander ab. In den meisten Fällen sollten Sie das System sofort vom Netz nehmen. Es ist allerdings möglich, dass Vereinbarungen auf Dienstebene vorliegen, die eine Aufrechterhaltung der Systeme vorsehen, selbst wenn die Möglichkeit weiterer Schäden besteht. Unter diesen Umständen werden Sie sich möglicherweise dafür entscheiden, ein System mit beschränkter Verbindung online zu halten, um während des laufenden Angriffs weitere Beweise zu sammeln.

In manchen Fällen können der Schaden und der Umfang eines Vorfalls so weitreichend sein, dass Sie Maßnahmen ergreifen müssen, die die in den Vereinbarungen auf Dienstebene enthaltenen Paragraphen zur strafrechtlichen Verfolgung betreffen. Es ist auf jeden Fall wichtig, dass die von Ihnen bei einem Vorfall ergriffenen Maßnahmen vorher diskutiert und in dem Plan zur Vorgehensweise bei Vorfällen dargelegt werden, damit bei einem Angriff sofort entsprechende Maßnahmen ergriffen werden können.

Ermitteln Sie den oder die vom Angreifer verwendeten Zugriffspunkt(e) und implementieren Sie Maßnahmen, um solchen Zugriff in Zukunft zu verhindern. Diese Maßnahmen können Folgendes beinhalten: das Deaktivieren eines Modems, das Hinzufügen von Einträgen für die Zugriffssteuerung (Access Control Entry oder ACE) zu einem Router oder einer Firewall oder das Implementieren weiterer physischer Sicherheitsmaßnahmen.

Sie sollten ein neues System mit neuen Festplatten installieren (die vorhandenen Festplatten sollten entfernt und verwahrt werden, da sie im Fall einer strafrechtlichen Verfolgung der Angreifer als Beweis verwendet werden können). Stellen Sie sicher, dass alle lokalen Kennwörter nach dem Angriff geändert wurden. Sie sollten auch die Kennwörter für Administrator- und Dienstkonten in anderen Teilen der Umgebung ändern.

Identifizieren des Schweregrads der Gefährdung

Um das System nach einem Angriff wiederherstellen zu können, müssen Sie das Ausmaß der Gefährdung für die Systeme ermitteln. Davon hängt ab, wie das Risiko weiter begrenzt und das System wiederhergestellt werden kann, wie schnell und wem der Vorfall gemeldet werden soll, und ob rechtliche Schritte ergriffen werden sollen.

Sie sollten Folgendes versuchen:

Bestimmen Sie die Art des Angriffs (das Ergebnis kann sich von dem der ersten Beurteilung unterscheiden).

Ermitteln Sie, wo der Angriff begonnen wurde.

Ermitteln Sie den Zweck des Angriffs. War der Angriff speziell dazu bestimmt, Informationen über Ihre Organisation zu sammeln, oder handelte es sich um einen zufälligen Angriff.

Identifizieren Sie die gefährdeten Systeme.

Identifizieren Sie die Dateien, auf die zugegriffen wurde, und ermitteln Sie den Umfang der in diesen Dateien enthaltenen privaten Informationen.

Mithilfe dieser Schritte können Sie die geeignete Vorgehensweise für Ihre Umgebung ermitteln. Ein guter Plan zur Vorgehensweise bei Vorfällen enthält bestimmte Verfahren, die anzuwenden sind, sobald Sie mehr über den Angriff wissen. Im Allgemeinen hängt die Reihenfolge der im Plan festgelegten Verfahren von den Anzeichen des Angriffs ab. Zeit spielt eine große Rolle. Deshalb sollten vor den zeitaufwändigen Verfahren im Allgemeinen zunächst weniger aufwändige Verfahren angewendet werden. Sie sollten Folgendes tun, um den Schweregrad der Gefährdung besser bestimmen zu können:

Kontaktieren Sie andere Mitglieder des CSIRT, informieren Sie diese über Ihre Beobachtungen, und lassen Sie Ihre Ergebnisse von ihnen überprüfen. Ermitteln Sie, ob die anderen Mitglieder damit verbundene Vorkommnisse oder andere mögliche Angriffshandlungen bemerkt haben und helfen Sie dabei zu untersuchen, ob es sich um einen echten Vorfall oder eine falsche Meldung handelt. In einigen Fällen kann sich ein bei erster Beurteilung für echt gehaltener Vorfall als falscher Alarm darstellen.

Ermitteln Sie, ob nicht autorisierte Hardware an das Netzwerk angeschlossen wurde oder ob es Anzeichen für nicht autorisierten Zugriff durch die Umgehung physischer Sicherheitskontrollen gibt.

Überprüfen Sie wichtige Gruppen (**Domänen-Administratoren**, **Administratoren** usw.) auf nicht autorisierte Einträge.

Suchen Sie nach Software, die zur Beurteilung der Sicherheit oder zur Ausnutzung des Systems verwendet werden kann. Häufig werden beim Sammeln von Beweisen Dienstprogramme zur unerlaubten Entschlüsselung auf den gefährdeten Systemen gefunden.

Suchen Sie nicht autorisierte Prozesse oder Anwendungen, die mithilfe der Ordner **Autostart** oder der Registrierungseinträge bereits ausgeführt werden bzw. ausgeführt werden sollen.

Suchen Sie nach Lücken in bzw. nach fehlenden Systemprotokollen.

Überprüfen Sie die Protokolle für das System zur Erkennung von Eindringversuchen auf Anzeichen von Eindringversuchen. Überprüfen Sie, welche Systeme betroffen sind, welche Angriffsmethoden eingesetzt wurden, wann der Angriff stattgefunden und wie lange er gedauert hat, und versuchen Sie, das gesamte Ausmaß des Schadens zu ermitteln.

Überprüfen Sie andere Protokolldateien auf ungewöhnliche Verbindungen, fehlgeschlagene Sicherheitsüberprüfungen, ungewöhnliche erfolgreiche Sicherheitsüberprüfungen, fehlgeschlagene Anmeldeversuche, versuchte Anmeldungen bei Standardkonten, Aktivitäten außerhalb der Arbeitszeiten, Änderungen hinsichtlich Datei-, Verzeichnis- und Freigabeberechtigungen und erhöhte oder geänderte Benutzerberechtigungen.

Vergleichen Sie Systeme mit den Ergebnissen vorher durchgeführter Überprüfungen der Datei-/Systemintegrität. Dadurch können Sie hinzugefügte und entfernte Komponenten sowie Änderungen und Berechtigungen identifizieren und Änderungen am Dateisystem und an der Dateiregistrierung steuern. Sie können bei der Vorgehensweise bei Vorfällen viel Zeit sparen, indem Sie genau identifizieren, welche Bereiche gefährdet wurden und welche Bereiche wiederhergestellt werden müssen.

Suchen Sie nach privaten Daten wie Kreditkartennummern und die Mitarbeiter oder Kunden betreffenden Daten, die möglicherweise zwecks späteren Zugriffs/späterer Änderungen verschoben oder ausgeblendet wurden. Systeme müssen möglicherweise auf unternehmensfremde Daten geprüft werden, wie beispielsweise pornografische Inhalte, illegale Kopien von Software sowie E-Mails und andere Einträge, die Ihnen bei den Nachforschungen von Nutzen sein könnten. Wenn Sie bei den Nachforschungen auf einem System möglicherweise die Privatsphäre anderer verletzen oder gegen andere Gesetze verstoßen könnten, sollten Sie sich zuvor an die Rechtsabteilung wenden.

Stimmen Sie die Leistung der für gefährdet gehaltenen Systeme auf die geplante Systemleistung ab. Das setzt natürlich voraus, dass die vorgesehenen Ausgangswerte erstellt und korrekt aktualisiert wurden. Weitere Informationen zum Erstellen von Ausgangswerten finden Sie in Kapitel 27 in *Windows 2000 Professional – Die technische Referenz* (Microsoft Press, ISBN: 3-86063-274-4).

Bei der Ermittlung der gefährdeten Systeme und der Art der Gefährdung werden Sie Ihre Systeme mit den Ausgangswerten vergleichen, die vor dem Angriff für die gleichen Systeme aufgezeichnet wurden. Wenn Sie davon ausgehen, dass ein kürzlich erstellter Snapshot für den Vergleich ausreicht, könnte sich das Problem ergeben, dass der vorherige Snapshot von einem bereits angegriffenen System stammt.

Anmerkung: Tools wie EventCombMT, DumpEL und Microsoft Operations Manager können dabei helfen, das Ausmaß eines Systemangriffs zu ermitteln. Systeme von Drittanbietern zur Erkennung von Eindringversuchen zeigen vor dem Auftreten von Angriffen Warnmeldungen an, andere Tools verweisen auf Dateiänderungen im System. Weitere Informationen zur Überwachung und Erkennung von Eindringversuchen finden Sie in Kapitel 6, "Überwachung und Erkennung von Eindringversuchen".

Schützen von Beweisen

Bei einem absichtlichen Angriff auf die Umgebung werden Sie vermutlich rechtliche Schritte gegen den Täter einleiten. In diesem Fall müssen Sie Beweise sammeln, die gegen den oder die Täter verwendet werden können. Es ist sehr wichtig, die gefährdeten Systeme so früh wie möglich zu sichern; das heißt, vor dem Ergreifen von Maßnahmen, die die Datenintegrität auf den Originalmedien beeinträchtigen

könnten. Sie sollten von einem Experten für Computerforensik mindestens zwei vollständige, bitgenaue Sicherungen des gesamten Systems auf bisher noch nicht verwendeten Medien erstellen lassen. Mindestens eine Sicherung sollte auf einem einmal beschreibbaren, mehrfach lesbaren Medium wie einer CD-R oder einer DVD-R erstellt werden. Diese Sicherung sollte nur bei einer strafrechtlichen Verfolgung des Täters verwendet und bis dahin sicher verwahrt werden. Die andere Sicherung kann zur Datenwiederherstellung verwendet werden. Auf diese Sicherungen sollte nur im Zusammenhang mit rechtlichen Schritten zugegriffen werden. Daher sollten Sie sie an einem sicheren Ort aufbewahren. Sie müssen auch Informationen über die Sicherungen dokumentieren, beispielsweise Folgendes: Wer hat die Systeme gesichert, wann wurden sie gesichert, wo wurden die Sicherungen verwahrt, und wer konnte darauf zugreifen?

Nach dem Durchführen der Sicherungen sollten Sie die ursprünglichen Festplatten entfernen und an einem physisch sicheren Ort aufbewahren. Diese können bei einer strafrechtlichen Verfolgung als rechtsgültige Beweise verwendet werden. Zum Wiederherstellen des Systems sollten neue Festplatten verwendet werden.

Manchmal ist der durch die Erhaltung von Daten erzielte Nutzen angesichts der durch verspätete Vorgehensweise und Wiederherstellung des Systems entstandenen Kosten sehr gering. Kosten und Nutzen der Erhaltung von Daten sollten mit denen einer schnelleren Wiederherstellung für jeden Vorfall verglichen werden.

Für sehr große Systeme können möglicherweise keine umfassenden Sicherungen aller gefährdeten Systeme erstellt werden. Stattdessen sollten Sie alle Protokolle und ausgewählte Teile des Systems sichern, bei denen Sicherheitsverletzungen beobachtet wurden.

Falls möglich, sollten Sie auch den Systemstatus sichern. Bis zu einer strafrechtlichen Verfolgung können Monate oder Jahre vergehen. Deshalb sollten möglichst viele Informationen zu jedem Vorfall archiviert werden.

Bei der strafrechtlichen Verfolgung eines *Cyber Crimes* ist es besonders schwierig, Beweise zu sammeln, die nach Maßgabe der geltenden Gesetze zur Beweisvorlage von der Gerichtsbarkeit anerkannt werden. Deshalb ist eine detaillierte und vollständige Dokumentation für das forensische Verfahren besonders wichtig. Diese sollte Informationen zur Art der Verwendung der Systeme beinhalten und darüber, wer sie zu welchem Zeitpunkt verwendet hat, damit zuverlässige Beweise vorliegen. Unterzeichnen und datieren Sie jede Seite der Dokumentation.

Sobald Sie über funktionsfähige, überprüfte Sicherungen verfügen, können Sie die betroffenen Systeme löschen und neu installieren. Dies führt zu einer schnellen Sicherung und Ausführung. Die Sicherungen liefern die für eine strafrechtliche Verfolgung relevanten, verwertbaren Beweise. Zusätzlich zu der Sicherung für das Gericht sollte eine Sicherung für die Datenwiederherstellung erstellt werden.

Benachrichtigen externer Stellen

Nach dem Begrenzen des Vorfalls und der Datensicherung für eine eventuelle strafrechtliche Verfolgung müssen Sie mit der Benachrichtigung der betreffenden externen Personen beginnen. Dazu zählen möglicherweise Behörden zur Wahrung des regionalen oder nationalen Rechts, externe Sicherheitsdienstleister und Virusexperten. Externe Stellen können technische Hilfe und eine schnellere Lösung anbieten und bei ähnlichen Vorfällen gesammelte Informationen bereitstellen, damit Sie das System nach dem Vorfall vollständig wiederherstellen und derartige Vorfälle in Zukunft verhindern können.

In bestimmten Industriezweigen und Branchen kann ein Benachrichtigen der Kunden und/oder der Öffentlichkeit erforderlich sein, insbesondere wenn Kunden durch den Vorfall möglicherweise direkt betroffen sind.

Verursacht der Vorfall hohe Kosten, müssen Sie den Vorfall möglicherweise einer Behörde zur Wahrung des Rechts melden.

Bei bekannteren Unternehmen und schwerwiegenderen Vorfällen können auch die Medien eingeschaltet werden. Obwohl die Einbeziehung der Medien bei einem Sicherheitsvorfall nicht wünschenswert ist, ist es für das Unternehmen häufig unvermeidbar und sinnvoll, den Medien zuvorzukommen und ihnen den Vorfall zu melden. Für die Vorgehensweise bei Vorfällen sollte auch genau definiert sein, welche Personen mit Medienvertretern sprechen dürfen. Dabei wird es sich i. d. R. um Mitglieder der PR-Abteilung Ihres Unternehmens handeln. Sie sollten nicht versuchen, den Vorfall gegenüber den Medien abzustreiten, da derartiges Verhalten Ihren Ruf vermutlich mehr schädigt als eine vorherige Bekanntgabe des Vorfalls und eine erkennbare Vorgehensweise. Das bedeutet allerdings nicht, dass die Medien über jeden Vorfall, unabhängig von dessen Ausmaß, informiert werden sollen. Sie sollten von Fall zu Fall entscheiden, wie diesbezüglich zu verfahren ist.

Wiederherstellen von Systemen

Die Vorgehensweise bei der Wiederherstellung des Systems hängt im Allgemeinen vom Ausmaß der Sicherheitsverletzung ab. Sie müssen ermitteln, ob Sie das vorhandene System größtenteils wiederherstellen können oder das gesamte System neu installieren müssen.

Das Wiederherstellen der Daten setzt natürlich voraus, dass Sie über fehlerfreie Sicherungen verfügen, d. h. Sicherungen, die *vor* dem Vorfall erstellt wurden. Mithilfe von Software zur Ermittlung der Dateiintegrität können Sie erkennen, wann der erste Schaden festgestellt wurde. Wenn die Software Warnhinweise für eine geänderte Datei generiert, wissen Sie, dass die kurz vor der Warnung erstellte Sicherung fehlerfrei ist und für die Neuerstellung des gefährdeten Systems aufbewahrt werden sollte.

Ein Vorfall kann Daten über Monate hinweg beschädigen, bevor er entdeckt wird. Daher sollten Sie, während Sie gegen den Vorfall vorgehen, auch die Dauer des Vorfalls ermitteln. (Software zur Ermittlung der Datei-/Systemintegrität und Systeme zur Ermittlung von Eindringversuchen können Sie dabei unterstützen.) In einigen Fällen reichen möglicherweise die letzte oder sogar die letzten sieben Sicherungen nicht aus, damit ein fehlerfreier Status vorliegt. Daher sollten Sie Datensicherungen regelmäßig an einem sicheren Standort außerhalb des Unternehmens archivieren.

Zusammenstellen und Gliedern der Dokumentation zum Vorfall

Das CSIRT sollte bei Vorfällen alle Prozesse sorgfältig dokumentieren. Dazu zählen auch eine Beschreibung der Sicherheitsverletzung und detaillierte Informationen zu den ergriffenen Maßnahmen (von wem wurden die Maßnahmen wann und warum ergriffen). Alle beteiligten Personen und alle zum Zugriff berechtigten Personen müssen vermerkt werden. Die Dokumentation sollte chronologisch geordnet, auf Vollständigkeit geprüft und von Mitgliedern des Managements und der Rechtsabteilung unterschrieben und überprüft werden. Sie müssen auch die gesammelten Beweise sichern. Zwei Personen mit Entscheidungsbefugnis sollten während aller Phasen erreichbar sein. Dadurch sinkt die Wahrscheinlichkeit, dass Beweise nach dem Vorfall nicht mehr zugänglich sind oder geändert werden.

Sie dürfen nicht vergessen, dass es sich bei dem Täter um einen Mitarbeiter, einen Vertragsnehmer, einen befristet beschäftigten Mitarbeiter oder andere Beteiligte der Organisation handeln kann. Ohne eine genaue und detaillierte Dokumentation ist die Identifizierung eines internen Täters sehr schwierig. Eine sorgfältige Dokumentation verbessert auch Ihre Chancen hinsichtlich einer strafrechtlichen Verfolgung der Täter.

Beurteilen der durch den Vorfall entstandenen Schäden und Kosten

Beim Ermitteln der für die Organisation entstandenen Schäden sollten Sie sowohl direkte als auch indirekte Kosten berücksichtigen. Dazu zählen die folgenden:

Kosten im Zusammenhang mit dem durch die Veröffentlichung proprietärer oder privater Daten entstandenen Verlust eines Wettbewerbsvorteils

Gerichtskosten

Für die Analyse der Sicherheitsverletzung, für die Neuinstallation von Software und zur Wiederherstellung von Daten anfallende Personalkosten

Durch Downtime entstandene Kosten (beispielsweise durch verringerte Produktivität, entgangene Gewinne und durch Ersetzen von Hardware, Software oder anderem Eigentum)

Durch Reparaturen und eventuelle Verbesserungen beschädigter oder ineffizienter physischer Sicherheitsmaßnahmen entstandene Kosten (Schlösser, Wände, spezielle Vorrichtungen usw.)

Folgeschäden wie ein Verlust der Reputation und des Kundenvertrauens

Überprüfen der Richtlinien zur Vorgehensweise und Aktualisierung

Sobald die Dokumentierungs- und die Wiederherstellungsphase abgeschlossen sind, sollten Sie den Prozess sorgfältig untersuchen. Ermitteln Sie gemeinsam mit Ihrem Team, welche Schritte erfolgreich ausgeführt und welche Fehler gemacht wurden. In manchen Fällen werden Sie feststellen, dass die Prozesse modifiziert werden müssen, damit Vorfälle in Zukunft effizienter behandelt werden können.

Fallstudie – Behandlung von Vorfällen bei Northwind Traders

Zur Verdeutlichung der Schritte während der verschiedenen Stufen der Reaktion bei Angriffen haben wir eine Fallstudie entworfen, in der wir die Vorgehensweise des CSIRT bei Northwind Traders gegen den Wurm Code Red II beschreiben. Diese Fallstudie ist zwar fiktiv, aber die beschriebenen Maßnahmen ähneln denen, die echte Organisationen bei Angriffen ergreifen.

Tabelle 7.3: Fallstudie zu Northwind Traders

Vorgehensweise (Schritt)	Ergriffene Maßnahmen
Durchführen einer ersten Beurteilung	Susanne Schmidt, die auf Abruf für das CSIRT arbeitet, wird kontaktiert und erhält dabei die kurze Beschreibung eines Ereignisses, das vom System zur Erkennung von Eindringversuchen protokolliert

Vorgehensweise (Schritt)	Ergriffene Maßnahmen
	wurde. Das System gibt an, dass beim Webserver, WEB2, möglicherweise ein Code Red II-Vorfall vorliegt. Sie überprüft die Signaturzeichenfolgen in der Protokolldatei der Internet-Informationsdienste (Internet Information Services oder IIS) von WEB2 und überprüft, ob die Datei **Root.exe** in **c:\inetpub\scripts** gespeichert ist. Die Ergebnisse dieser Nachforschungen lassen darauf schließen, dass es sich nicht um eine falsche Meldung handelt.
Melden des Vorfalls	Susanne informiert die anderen Mitglieder des CSIRT per Telefon über die ersten Ergebnisse und erklärt sich bereit, genauere Informationen sofort weiterzugeben.
Begrenzen des Schadens und des Risikos	In der Richtlinie zur Vorgehensweise bei Vorfällen von Northwind Traders ist festgelegt, dass das System vor der Suche eines potenziellen Wurms aus dem Netzwerk entfernt werden muss. Susanne entfernt das Netzwerkkabel. Glücklicherweise gehört WEB2 zu einer Reihe von Servern mit Lastenausgleich, so dass durch das Unterbrechen der Verbindung für die Kunden keine Downtime verursacht wird.
Identifizieren des Schweregrads der Gefährdung	Susanne scannt die Protokolldateien anderer Server, um zu entscheiden, ob sich ein Wurm verbreitet hat. Sie entdeckt, dass dies nicht der Fall ist.
Melden des Vorfalls	Susanne meldet diese Ergebnisse den anderen Mitgliedern des CSIRT per E-Mail und nimmt direkten Kontakt zum Teamleiter des CSIRT auf. Der Leiter des CSIRT bestimmt Michael Meier, einen Manager für Informationssichereit, zur Vorfallleitung. Michael wird alle Maßnahmen und die gesamte Kommunikation vom bzw. zum Kernteam des CSIRT koordinieren. Michael benachrichtigt den Leiter für Technologie und das auf Abruf gehaltene IT-Team darüber, dass der Webserver aus dem Netzwerk entfernt wurde, dass der Wurm zunächst entfernt und der Server erst anschließend wieder angeschlossen wird. Michael benachrichtigt auch die Geschäftsleitung, den Kommunikationsmitarbeiter und den Rechtsvertreter. Der Rechtsvertreter informiert Michael darüber, dass er Beweise sammeln soll, obwohl eventuell keine strafrechtliche Verfolgung möglich ist.
Begrenzen des Schadens und des Risikos	Robert Braun, ein anderes Mitglied des CSIRT, führt **Hfnetchk** aus, um zu ermitteln, ob auf anderen Servern Patches gegen Code Red II installiert wurden. Er findet heraus, dass zwei Server nicht aktualisiert wurden und wendet den Patch sofort an.
Identifizieren des Schweregrads der Gefährdung	Robert scannt erneut die Protokolldateien aller IIS-Server und ermittelt, dass zum derzeitigen Zeitpunkt keine weiteren Vorfälle eines Code Red II vorliegen.

Vorgehensweise (Schritt)	Ergriffene Maßnahmen
Schützen von Beweisen	Alles lässt darauf schließen, dass der Schaden auf WEB2 begrenzt wurde. Da der Schaden inzwischen begrenzt wurde und der rechtliche Vertreter ihn angewiesen hat, Beweise zu sammeln, entscheidet sich Michael, dies zu tun, bevor er eine intensivere Analyse des Systems vornimmt, durch die die Beweise beeinträchtigt oder zerstört werden könnten. Andere Mitglieder des Teams überwachen weiterhin die anderen Webserver und protokollieren verdächtige Aktivitäten. Ein auf das Sammeln rechtsgültiger Beweise geschultes Mitglied des CSIRT erstellt zwei Snapshots des gefährdeten Systems. Ein Snapshot wird für eine spätere computerforensische Untersuchung sorgfältig aufbewahrt. Der andere Snapshot wird möglicherweise bei der Wiederherstellung zusammen mit fehlerfreien, sicheren Sicherungen verwendet, die vor dem Vorfall erstellt wurden. Die Sicherung für das Gericht wird gemäß der Sicherheitsrichtlinie auf einem noch nicht verwendeten, einmal beschreibbaren Medium gespeichert, genau dokumentiert, versiegelt und zusammen mit den Festplatten des Servers gesichert.
Identifizieren der Art und des Schweregrads der Gefährdung	Das Laptop der Organisation mit dem Sicherheitstoolkit, das eine Reihe von Tools zum Sammeln rechtsgültiger Beweise enthält, wird zum Überprüfen der Wiederherstellungssicherung auf Vorfälle und zusätzliche Gefährdung verwendet. Bei Registrierungseinträgen und Ordnern wird überprüft, ob Komponenten zu Bereichen hinzugefügt wurden, die beim Start Software ausführen, beispielsweise die Profilverzeichnisse und **Autostart** ebenso wie die Registrierungsschlüssel **Run** und **RunOnce**. Benutzer- und Gruppenkonten sowie Benutzerrechte und Sicherheitsrichtlinien werden auf Änderungen überprüft.
Benachrichtigen externer Stellen	Michael meldet den Vorfall dem National Infrastructure Protection Center des FBI, da Northwind Traders an vielen Großprojekten der US-Regierung beteiligt ist. Da weder die Kundeninformationen noch der Zugriff auf Systeme gefährdet war, werden die Kunden nicht benachrichtigt.
Wiederherstellen der Systeme	Obwohl Tools zum Beseitigen von Code Red II von WEB2 verfügbar sind, entscheiden sich das CSIRT und das WEB2-Supportteam für eine Neuinstallation des Betriebssystems auf neuen Medien. Durch die Neuinstallation des Betriebssystems von der ursprünglichen CD und auf neue Medien, können sie sicherstellen, dass das System fehlerfrei ist und keine "Hintertürchen" für Hacker oder beschädigte Dateien enthält. Nach der Neuinstallation von Windows 2000 werden zur Erhöhung der Sicherheit des Systems die im letzten Kapitel dieses Handbuchs angegebenen Richtlinien befolgt. Eine nicht durch den Vorfall beeinträchtigte Sicherung wird gesucht, und die Daten werden wiederhergestellt. Wenn nur Daten von einer gefährdeten Sicherung verfügbar sind, werden diese zunächst auf einem separaten offline geschalteten System wiederhergestellt und erst auf WEB2 gespeichert, wenn eine Gefährdung ausgeschlossen werden kann. Das CSIRT führt eine Beurteilung aller Schwachstellen des Systems durch und dokumentiert alle dabei gesammelten Informationen. WEB2 wird wieder angeschlossen und gut überwacht.

Vorgehensweise (Schritt)	Ergriffene Maßnahmen
Zusammenstellen und Gliedern der Dokumentation zum Vorfall	Michael und das CSIRT untersuchen die Ursache der Schwachstelle und ermitteln, dass das System kürzlich neu installiert wurde, ohne dass Patches angewendet wurden. Dadurch wurde gegen eine klar definierte und bereits geltende Richtlinie verstoßen. Die Fehler, die zu diesem Ereignis führten, wurden an drei Stellen begangen: Das Supportteam hat die Patches nicht wieder angewendet, die Abteilung für Informationssicherheit hat die angewendeten Patches nicht rechtzeitig überwacht und die Gruppe des Konfigurationsmanagments (Configuration Management) hat nicht erkannt, dass Patches angewendet werden müssen und dass die für die Informationssicherheit zuständigen Mitarbeiter das System vor der erneuten Inbetriebnahme überprüfen müssen. Durch eine dieser Maßnahmen hätte der Vorfall verhindert werden können. Das Team entschließt sich, ein neues Verfahren zu implementieren, um derartige Vorfälle in Zukunft auszuschließen. Eine Prüfliste wird erstellt, die vom Änderungsmanagement, vom Webserver-Support und von den für die Informationssicherheit zuständigen Mitarbeiter ausgefüllt werden muss, bevor Letztere das System (wieder) mit dem internen Netzwerk verbinden. Die Prüfliste muss ausgefüllt werden, bevor die für die Informationssicherheit zuständigen Mitarbeiter den Firewall neu konfigurieren, damit externer Zugriff vom und zum System zugelassen werden kann. Die Überwachungsabteilung sollte regelmäßig überprüfen, ob die Prüflisten genau und vollständig ausgefüllt werden. Michael und das CSIRT stellen die gesamte Dokumentation zusammen, um zu ermitteln, welche speziell diesen Vorfall betreffenden Aufgaben erledigt wurden, wie viel Zeit für jede Aufgabe benötigt wurde und wer sie erledigt hat. Diese Informationen werden an den Vertreter der Finanzabteilung geschickt, damit dieser die Kosten gemäß der geltenden Rechnungslegungsgrundsätze (Generally Accepted Accounting Principles oder GAAP) für Computerschäden berechnen kann. Der Teamleiter des CSIRT stellt sicher, dass das Management die Gesamtkosten und die Ursachen des Ereignisses sowie die zu dessen zukünftiger Vermeidung geplante Vorgehensweise nachvollziehen kann. Es ist sehr wichtig, dass das Management erkennt, welche Auswirkungen das Befolgen bzw. Fehlen von Vorgehensweisen und das Fehlen von Ressourcen wie dem CSIRT hat. Folgende Aspekte werden von geeigneten Mitgliedern des Teams überprüft: die gesamte Dokumentation zum Vorfall, die für die Zukunft gewonnenen Erkenntnisse und welche Richtlinien befolgt bzw. nicht befolgt wurden. Die Dokumentation und die Verfahren, die sich für die Einleitung rechtlicher Schritte eignen, werden vom Rechtsvertreter, dem Teamleiter und der Vorfallleitung des CSIRT und von der Geschäftsleitung überprüft.

Zusammenfassung

In vielen Abschnitten dieses Handbuchs wurden Maßnahmen behandelt, durch die Sie das Risiko eines Angriffs verringern können. Im Zusammenhang mit der Sicherheit Ihres Unternehmens ist es allerdings besonders empfehlenswert, das Risiko von Angriffen weitestgehend zu senken und anschließend trotzdem mit einem Angriff zu rechnen. Zu diesem Prozess zählt auch die in Kapitel 6 behandelte Überwachung zum Schutz vor Angriffen. Darüber hinaus sollten Sie für den Fall eines erfolgreichen Angriffs unbedingt über eine Reihe definierter und umfassend getesteter Vorgehensweisen verfügen.

Verwandte Themen

Hacking Exposed Windows 2000 von Joel Scambray und Stuart McClure (McGraw-Hill Professional Publishing, ISBN: 0072192623)

Das Computer Security Institute (http://www.gocsi.com/) – veröffentlicht jährlich eine Studie mit dem Titel "Computer Crime and Security Survey"

Weitere Informationen

Handbook for Computer Security Incident Response Teams, Http://interactive.sei.cmu.edu/Recent_Publications/1999/March/98hb001.htm (englischsprachig).

Das Forum of Incident Response and Security Teams (FIRST), http://www.first.org (englischsprachig).

Incident Response: Investigating Computer Crime von Chris Prosise und Kevin Mandia (McGraw-Hill Professional Publishing, ISBN: 0072131829) (englischsprachig)

The Internet Security Guidebook: From Planning to Deployment von Juanita Ellis, Tim Speed und William P. Crowell (Academic Pr, ISBN: 0122374711) (englischsprachig)

RFC 2196

http://www.ietf.org/rfc/rfc2196.txt?number=2196 (englischsprachig)

Kapitel 27 in *Windows 2000 Professional – Die technische Referenz*

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/nimda.asp (englischsprachig)

Das Cert Coordination Center (CERT/CC):

http://www.cert.org (englischsprachig)

Originaltitel: Appendix A – File Permissions

Anhang A

Dateien, die durch die Basisrichtlinie für Mitgliedsserver gesichert werden, zusätzlich zu den Zugriffssteuerungslisten der Vorlage **hisecws.inf**.

Datei	Basisberechtigungen
%SystemDrive%\Boot.ini	Administratoren: Vollzugriff System: Vollzugriff
%SystemDrive%\Ntdetect.com	Administratoren: Vollzugriff System: Vollzugriff
%SystemDrive%\Ntldr	Administratoren: Vollzugriff System: Vollzugriff
%SystemDrive%\Io.sys	Administratoren: Vollzugriff System: Vollzugriff
%SystemDrive%\Autoexec.bat	Administratoren: Vollzugriff System: Vollzugriff Authentifizierte Benutzer: Lesen und Ausführen, Ordnerinhalt auflisten und Lesen
%SystemDrive%\Config.sys	Administratoren: Vollzugriff System: Vollzugriff Authentifizierte Benutzer: Lesen und Ausführen, Ordnerinhalt auflisten und Lesen
%SystemRoot%\system32\Append.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Arp.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\At.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Attrib.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Cacls.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Change.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Chcp.com	Administratoren: Vollzugriff
%SystemRoot%\system32\Chglogon.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Chgport.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Chguser.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Chkdsk.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Chkntfs.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Cipher.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Cluster.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Cmd.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Compact.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Command.com	Administratoren: Vollzugriff
%SystemRoot%\system32\Convert.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Cscript.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Debug.exe	Administratoren: Vollzugriff

Datei	Basisberechtigungen
%SystemRoot%\system32\Dfscmd.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Diskcomp.com	Administratoren: Vollzugriff
%SystemRoot%\system32\Diskcopy.com	Administratoren: Vollzugriff
%SystemRoot%\system32\Doskey.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Edlin.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Exe2bin.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Expand.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Fc.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Find.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Findstr.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Finger.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Forcedos.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Format.com	Administratoren: Vollzugriff
%SystemRoot%\system32\Ftp.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Hostname.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Iisreset.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Ipconfig.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Ipxroute.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Label.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Logoff.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Lpq.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Lpr.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Makecab.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Mem.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Mmc.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Mode.com	Administratoren: Vollzugriff
%SystemRoot%\system32\More.com	Administratoren: Vollzugriff
%SystemRoot%\system32\Mountvol.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Msg.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Nbtstat.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Net.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Net.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Netsh.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Netstat.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Nslookup.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Ntbackup.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Ntsd.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Pathping.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Ping.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Print.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Query.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Rasdial.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Rcp.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Recover.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Regedit.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Regedt32.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Regini.exe	Administratoren: Vollzugriff

Datei	Basisberechtigungen
%SystemRoot%\system32\Register.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Regsvr32.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Replace.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Reset.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Rexec.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Route.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Routemon.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Router.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Rsh.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Runas.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Runonce.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Secedit.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Setpwd.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Shadow.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Share.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Snmp.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Snmptrap.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Subst.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Telnet.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Termsrv.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Tftp.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Tlntadmin.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Tlntsess.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Tlntsvr.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Tracert.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Tree.com	Administratoren: Vollzugriff
%SystemRoot%\system32\Tsadmin.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Tscon.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Tsdiscon.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Tskill.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Tsprof.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Tsshutdn.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Usrmgr.com	Administratoren: Vollzugriff
%SystemRoot%\system32\Wscript.exe	Administratoren: Vollzugriff
%SystemRoot%\system32\Xcopy.exe	Administratoren: Vollzugriff

Originaltitel: Appendix B – Default Windows 2000 Services

Anhang B – Standardmäßige Windows 2000-Dienste

In der Spalte **Standard** ist angegeben, wie der Dienst auf einem Windows 2000-basierten Server gestartet wird. In der Spalte **Ausgangswert** ist angegeben, wie der Start der Dienste konfiguriert ist, nachdem die Basisrichtlinie für Mitgliedsserver angewendet wurde.

Dienst	Vollständiger Name	Standard	Ausgangswert
Alerter	Warndienst	Automatisch	Deaktiviert
AppMgmt	Anwendungsmanagement (Application Management)	Manuell	Deaktiviert
ClipSrv	Ablagemappe	Manuell	Deaktiviert
EventSystem	COM+-Ereignissystem	Manuell	Manuell
Browser	Computerbrowser	Automatisch	Deaktiviert
DHCP	DHCP-Client	Automatisch	Automatisch
Dfs	Verteiltes Dateisystem (DFS)	Automatisch	Nur auf Domänen-controllern aktiviert
TrkWks	Überwachung verteilter Verknüpfungen (Client)	Automatisch	Automatisch
TrkSrv	Überwachung verteilter Verknüpfungen (Server)	Manuell	Deaktiviert
MSDTC	Distributed Trans action Coordinator	Automatisch	Deaktiviert
DNSCache	DNS-Client	Automatisch	Automatisch
EventLog	Ereignisprotokoll	Automatisch	Automatisch
Fax	Faxdienst	Manuell	Deaktiviert
NtFrs	Dateireplikation	Manuell	Deaktiviert
IISADMIN	IIS-Verwaltungsdienst	Automatisch	Deaktiviert
Cisvc	Indexdienst	Manuell	Deaktiviert
SharedAccess	Gemeinsame Nutzung der Internetverbindung	Manuell	Deaktiviert
IsmServ	Standortübergreifender Meldungsdienst	Deaktiviert	Deaktiviert
PolicyAgent	IPSEC-Richtlinienagent (IPSEC-Dienst)	Automatisch	Deaktiviert
Kdc	Kerberos-Schlüsselverteilungscenter	Deaktiviert	Nur auf Domänen-controllern aktiviert
LicenseService	Lizenzprotokollierdienst	Automatisch	Deaktiviert
Dmserver	Verwaltung logischer Datenträger	Automatisch	Automatisch
Dmadmin	Verwaltungsdienst für die Verwaltung logischer Datenträger	Manuell	Manuell
Messenger	Nachrichtendienst	Automatisch	Deaktiviert
Netlogon	Anmeldedienst	Automatisch*	Automatisch
Mnmsrvc	NetMeeting-Remotedesktop-Freigabe	Manuell	Deaktiviert
Netman	Netzwerkverbindungen	Manuell	Manuell
NetDDE	Netzwerk-DDE-Dienst	Manuell	Deaktiviert
NetDDEdsdm	Netzwerk-DDE-Serverdienst	Manuell	Deaktiviert
NtLmSsp	NT-LM-Sicherheitsdienst	Manuell	Deaktiviert
SysmonLog	Leistungsdatenprotokolle und Warnungen	Manuell	Manuell
PlugPlay	Plug & Play	Automatisch	Automatisch
Spooler	Druckwarteschlange	Automatisch	Nur auf Datei- und Druckservern aktiviert
ProtectedStorage	Geschützter Speicher	Automatisch	Automatisch

Dienst	Vollständiger Name	Standard	Ausgangswert
RSVP	QoS-Zugangssteuerungsdienst (RSVP)	Manuell	Deaktiviert
RasAuto	Verwaltung für automatische RAS-Verbindung	Manuell	Deaktiviert
RasMan	RAS-Verbindungsverwaltung	Manuell	Deaktiviert
RpcSs	Remoteprozeduraufruf (RPC)	Automatisch	Automatisch
Rpclocator	RPC-Locator	Manuell	Nur auf Domänen-controllern aktiviert
RemoteRegistry	Remote-Registrierungsdienst	Automatisch	Automatisch
NtmsSvc	Wechselmedienverwaltung	Automatisch	Deaktiviert
RemoteAccess	Routing und RAS	Deaktiviert	Deaktiviert
Seclogon	Dienst "Ausführen als"	Automatisch	Deaktiviert
SamSs	Sicherheitskontenverwaltung	Automatisch	Automatisch
Lanmanserver	Server	Automatisch	Automatisch
SMTPSVC	SMTP-Server (Simple Mail Transport Protocol)	Automatisch	Deaktiviert
ScardSvr	Smartcard	Manuell	Deaktiviert
ScardDrv	Smartcard-Hilfsprogramm	Manuell	Deaktiviert
SENS	Systemereignisbenachrichtigung	Automatisch	Automatisch
Schedule	Taskplaner	Automatisch	Deaktiviert
LmHosts	TCP/IP-NetBIOS-Hilfsprogramm	Automatisch	Automatisch
TapiSrv	Telefonie	Manuell	Deaktiviert
TlntSvr	Telnet	Manuell	Deaktiviert
TermService	Terminaldienste	Deaktiviert	Deaktiviert
UPS	Unterbrechungsfreie Spannungsversorgung	Manuell	Deaktiviert
UtilMan	Hilfsprogramm-Manager	Manuell	Deaktiviert
MSIServer	Windows Installer	Manuell	Deaktiviert
WinMgmt	Windows-Verwaltungsinstrumentation	Manuell	Deaktiviert
WMI	Windows-Verwaltungsinstrumentations-Treibererweiterungen	Manuell	Manuell
W32Time	Windows-Zeitgeber	Automatisch*	Automatisch
LanmanWorkstation	Arbeitsstation	Automatisch	Automatisch
W3svc	WWW-Publishingdienst	Automatisch	Nur auf IIS-Servern aktiviert

* Automatisch auf einem Server in einer Domäne. Manuell, wenn der Server zu einer Arbeitsgruppe gehört.

Originaltitel: Appendix C – Additional Services

Anhang C – Zusätzliche Dienste

In der folgenden Tabelle sind zusätzliche Dienste von Windows 2000 Server und Windows 2000 Advanced Server aufgeführt, die zu einer Standardinstallation hinzugefügt werden können.

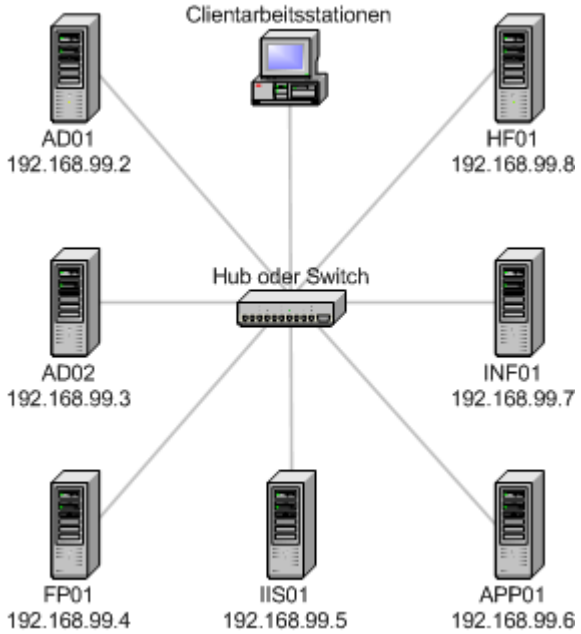
Dienst	Vollständiger Name	Ausgangswert
BINLSVC	Verhandlungsschicht für Startinformationen	Deaktiviert
CertSvc	Zertifikatsdienste	Deaktiviert
ClusSvc	Clusterdienst	Deaktiviert
DHCPServer	DHCP-Server	Nur in der Infrastrukturfunktion aktiviert
DNS	DNS-Server	Nur in der Infrastrukturfunktion und auf Domänencontrollern aktiviert
MacFile	Dateiserver für Macintosh	Deaktiviert
MSFTPSVC	FTP-Dienst	Deaktiviert
NWCWorkstation	Gateway Service für NetWare	Deaktiviert
IAS	Internetauthentifizierungsdienst	Deaktiviert
MSMQ	Message Queuing	Deaktiviert
NntpSvc	NNTP-Server (Network News Transport Protocol)	Deaktiviert
NSLService	Onlinepräsentationsübertragung	Deaktiviert
MacPrint	SFM-Druck-Server	Deaktiviert
RSVP	QoS-RSVP-Dienst	Deaktiviert
Remote_Storage_Engine	Remotespeichermodul	Deaktiviert
Remote_Storage_File_System_Agent	Dateidienst des Remotespeichers	Deaktiviert
Remote_Storage_Subsystem	Remotespeichermedium	Deaktiviert
Remote_Storage_User_Link	Remotespeicherbenachrichtigung	Deaktiviert
NwSapAgent	SAP-Agent	Deaktiviert
SimpTcp	Einfache TCP/IP-Dienste	Deaktiviert
Groveler	Einzelinstanz-Speicherung (Groveler)	Deaktiviert
LDAPSVCX	Site Server-ILS-Dienst	Deaktiviert
SNMP	SNMP-Dienst	Deaktiviert
SNMPTRAP	SNMP-Trap-Dienst	Deaktiviert
LPDSVC	TCP/IP-Druckserver	Deaktiviert
TermServLicensing	Terminaldienstelizenzierung	Deaktiviert
TFTPD	Daemon für "Trivial FTP"	Deaktiviert
WINS	WINS (Windows Internet Name Service)	Nur in der Infrastrukturfunktion aktiviert
nsmonitor	Windows Media-Überwachungsdienst	Deaktiviert
nsprogram	Windows Media-Sendungsdienst	Deaktiviert
nsstation	Windows Media-Stationsdienst	Deaktiviert
nsunicast	Windows Media-Unicastdienst	Deaktiviert

Anhang D

In diesem Anhang wird dargestellt, wie eine einfache Infrastruktur, die im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* beschrieben wird, bereitgestellt werden kann. Es wird Schritt für Schritt erläutert, wie eine Testumgebung erstellt wird und welche relevanten Betriebssysteme, Dienste, Patches usw. installiert werden müssen. Außerdem wird angegeben, wie Active Directory mithilfe von **dcpromo** konfiguriert wird und welche Prüfungen vor der eigentlichen Testphase durchgeführt werden sollten.

Erstellen der Testumgebung

1. Installieren Sie ein Netzwerk oder einen Switch, um eine einfache Netzwerktopologie bereitzustellen, die bis zu 10 Computer unterstützen kann.



2. Installieren Sie Windows 2000 Server auf einer NTFS-Partition auf allen Testservern. Verwenden Sie dabei die Namenskonventionen und IP-Adressen, die in der Abbildung angegeben sind.
3. Weisen Sie dem Administratorkonto ein sicheres Kennwort zu.
4. Konfigurieren Sie die Computer so, dass **192.168.99.7** als primärer DNS-Server verwendet wird.
5. Konfigurieren Sie die Computer so, dass **192.168.99.7** als primärer WINS-Server verwendet wird.
6. Legen Sie für jeden Computer fest, dass er Mitglied einer Arbeitsgruppe mit dem Namen **Arbeitsgruppe** ist.
7. Installieren Sie DNS, DHCP und WINS auf dem Infrastrukturserver.

8. Installieren Sie Windows 2000 Service Pack 2 auf allen Computern.
9. Installieren Sie den im englischsprachigen Knowledge Base-Artikel Q295444 "SCE Cannot Alter a Service's SACL Entry in the Service's Registry Key" erläuterten Hotfix auf allen Computern.
10. Stufen Sie AD01 zum Domänencontroller der Testdomäne herauf.
11. Nehmen Sie AD02 in die Active Directory-Domäne auf.
12. Nehmen Sie die Mitgliedsserver in die Active Directory-Domäne auf.
13. Erstellen Sie anhand der Schritte in Kapitel 3 des Leitfadens die Organisationseinheitsstruktur.
14. Installieren Sie Hfnetchk anhand der Schritte in Kapitel 5 dieses Leitfadens, und führen Sie Hfnetchk aus.

Testfälle

Test-fall	Priorität	Zu testende Bedingung	Einzelheiten zur Ausführung	Erforderliche Daten	Erwartetes Ergebnis:
1.1	Niedrig	Keine	Sichern Sie den Systemstatus aller Server auf einem Datenträger.	Keine	Erfolgreiche Sicherung
1.2	Hoch	Importieren der Basisgruppenrichtlinie für Domänencontroller und Überprüfen der im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* beschriebenen Schritte	1. Importieren Sie die Basisrichtlinie, wie in Kapitel 3, "Importieren der Basisrichtlinie für Domänencontroller", beschrieben. 2. Benennen Sie das Domänenadministratorkonto um (Kapitel 4). 3. Benennen Sie das lokale Administratorkonto um (Kapitel 4). 4. Starten Sie den Domänencontroller neu.	**Baselinedc.inf**	Der Domänen-controller ist gesperrt.
1.3	Hoch	Verwenden von Dienstprogrammen wie GpoTool und Gpresult, um die Gruppenrichtlinieneinstellungen des Domänencontrollers zu überprüfen	1. Überprüfen Sie, ob die Richtlinie erfolgreich auf jeden Domänencontroller gedownloadet wurde, indem Sie die Ereigniskennung 1704 auf jedem Domänencontroller suchen. 2. Überprüfen Sie mithilfe der Admin MMC **Lokale Richtlinie**, ob die Richtlinie auf jeden Domänencontroller angewendet wurde. 3. Überprüfen Sie mithilfe des Befehls **secedit /analyze /db secedit.sdb /cfg *Vorlagenname***, ob die Richtlinie auf jeden Domänencontroller angewendet wurde. 4. Überprüfen Sie mithilfe des Befehls **gpresult /c**, ob die Richtlinie angewendet wurde. 5. Überprüfen Sie mithilfe des Befehls **gptool /gpo *Vorlagenname***, ob die Richtlinie angewendet wurde.		Es wird überprüft, ob das Gruppenrichtlinien objekt des Domänencontrollers angewendet wurde.

Test-fall	Priorität	Zu testende Bedingung	Einzelheiten zur Ausführung	Erforderliche Daten	Erwartetes Ergebnis:
1.4	Hoch	Testen der Basisgruppenrichtlinie für Domänencontroller und Überprüfen der im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* beschriebenen Schritte	1. Überprüfen Sie, ob die Einstellungen der Überwachungsrichtlinien für Domänencontroller festgelegt wurden (Kapitel 4). 2. Überprüfen Sie, ob die Einstellungen der Sicherheitsrichtlinien für Domänencontroller festgelegt wurden (Kapitel 4). 3. Überprüfen Sie, ob die Einstellungen der Diensterichtlinien für Domänencontroller festgelegt wurden (Kapitel 4). 4. Überprüfen Sie, ob eine Reihe von Basisdiensten und Basisdiensten des Domänencontrollers gestartet werden.		Die Gruppenrichtlinieneinstellungen des Domänencontrollers stimmen mit denen im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* überein. Es wird überprüft, ob die richtigen Dienste gestartet werden und reagieren.
1.5	Hoch	Importieren der Basisrichtlinie für die Mitgliedsserver, Verschieben von AP01 in die Organisationseinheit und anschließendes Überprüfen der im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* beschriebenen Schritte	1. Konfigurieren Sie den Server AP01 mit allen verfügbaren Diensten. 2. Deaktivieren Sie die Datei- und Druckdienste auf AP01. 3. Importieren Sie die Basisrichtlinie, wie in Kapitel 3, "Importieren von Richtlinien für Mitgliedsserver", beschrieben. 4. Verschieben Sie Anwendungsserver AP01 in die Organisationseinheit **Anwendungsserver**. 5. Erzwingen Sie die Replikation des Domänencontrollers. 6. Starten Sie den Server neu.	**Baseline.inf** RepAdmin oder ReplMon	Der Mitgliedsserver AP01 ist gesperrt.
1.6	Hoch	Verwenden von Dienstprogrammen wie GpoTool und Gpresult, um die Gruppenrichtlinieneinstellungen des Mitgliedsservers AP01 zu überprüfen	1. Überprüfen Sie, ob die Richtlinie erfolgreich auf den Mitgliedsserver AP01 gedownloadet wurde, indem Sie die Ereigniskennung 1704 suchen. 2. Überprüfen Sie mithilfe der Admin MMC **Lokale Richtlinie**, ob die Richtlinie auf den Mitgliedsserver angewendet wurde. 3. Überprüfen Sie mithilfe des Befehls **secedit /analyze /db secedit.sdb /cfg *Vorlagenname***, ob die Richtlinie auf den Mitgliedsserver angewendet wurde.		Zeigt, dass das Gruppenrichtlinienobjekt auf den Mitgliedsserver AP01 angewendet wurde

Test-fall	Priorität	Zu testende Bedingung	Einzelheiten zur Ausführung	Erforderliche Daten	Erwartetes Ergebnis:
			4. Überprüfen Sie mithilfe des Befehls **gpresult /c**, ob die Richtlinie angewendet wurde. 5. Überprüfen Sie mithilfe des Befehls **gptool /gpo *Vorlagenname***, ob die Richtlinie angewendet wurde.		
1.7	Hoch	Testen der Basisgruppenrichtlinie für den Mitgliedsserver und Überprüfen der im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* beschriebenen Schritte	1. Überprüfen Sie, ob die Einstellungen der Überwachungsrichtlinien für AP01 festgelegt wurden (Kapitel 4). 2. Überprüfen Sie, ob die Einstellungen der Sicherheitsrichtlinien für AP01 festgelegt wurden (Kapitel 4). 3. Überprüfen Sie, ob die Dienste, wie in Anhang B und Anhang C beschrieben, konfiguriert wurden. 4. Überprüfen Sie, ob die Basisdienste gestartet werden (vergleichen Sie dies mit den Anhängen). 5. Überprüfen Sie, ob die Registrierungseinträge für Denial-of-Service angewendet wurden (Kapitel 4). 6. Überprüfen Sie, ob die Registrierungseinträge für 8.3-Dateinamen angewendet wurden (Kapitel 4). 7. Überprüfen Sie, ob die LMHash-Registrierungseinträge angewendet wurden (Kapitel 4). 8. Überprüfen Sie, ob die NTLMSSP-Registrierungseinträge angewendet wurden (Kapitel 4). 9. Überprüfen Sie, ob die AutoRun-Registrierungseinträge angewendet wurden (Kapitel 4). 10. Überprüfen Sie, ob die Basiszugriffssteuerungslisten des Dateisystems angewendet wurden (Anhang A und Kapitel 4). 11. Überprüfen Sie die Authentifizierung von AP01 mit dem Domänencontroller.		Die Gruppenrichtlinieneinstellungen des Mitgliedsservers AP01 stimmen mit denen im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* überein. Zusätzliche Registrierungseinstellungen wurden auf AP01 angewendet. Alle Dienste auf AP01 wurden deaktiviert.

Test-fall	Priorität	Zu testende Bedingung	Einzelheiten zur Ausführung	Erforderliche Daten	Erwartetes Ergebnis:
Ver-schie-denes	Niedrig	Replikation zwischen Standorten mit SMTP	1. Erstellen Sie einen neuen Standort. 2. Verschieben Sie AD02 zu dem neuen Standort. 3. Aktivieren Sie SMTP. 4. Überprüfen Sie, ob die Replikation funktioniert.		Die Replikation sollte mit den angewendeten Richtlinien funktionieren.

Testfall	Priorität	Zu testende Bedingung	Einzelheiten zur Ausführung	Erforderliche Daten	Erwartete Ergebnisse
2.1	Hoch	Ausführen von HfNetChk für alle Server	**Genauere Angaben zur Vorgehensweise finden Sie im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* in Kapitel 5.** 1. Bereitstellung • Auf dem Server mit dem Namen HF01 befindet sich **SecurityOps.exe.** • Führen Sie die EXE -Datei aus, um die Ordnerstruktur zu erstellen. • Auf HF01 befindet sich **Hfnetchk.exe** im Ordner **C:\SecurityOps\PatchMgmt\Hfnetchk.** • Downloaden Sie **mssecure.xml**, und platzieren Sie diese Datei im gleichen Ordner wie HfNetChk. 2. Erstellen Sie die Serverliste mit den Namen aller Server, und platzieren Sie die Liste im Ordner **C:\SecurityOps\PatchMgmt\ServerLists.** 3. Führen Sie an der Eingabeaufforderung HfNetChk mit der Serverliste aus **HfNetChk.cmd Server.txt**. 4. Führen Sie **Qfecheck.exe /v** aus, und überprüfen Sie die installierten Service Packs und Hot Fixes.	Für die Ausführung von HfNetChk: • **SecurityOps.exe** • **nshc33.exe** • **Qfecheck.exe**	• Die Ausgabe von HfNetChk sollte in einer Protokolldatei in einem Ordner gespeichert werden, der mit dem aktuellen Datum benannt wird. • Der Patch Q259444 sollte nicht in der Liste aufgeführt sein. • Überprüfen Sie die Ergebnisse von **Qfecheck.exe**.

Testfall	Priorität	Zu testende Bedingung	Einzelheiten zur Ausführung	Erforderliche Daten	Erwartete Ergebnisse
2.2	Hoch	Erneutes Ausführen von HfNetChk nach der Installation einiger Patches der Liste	1. Einige Patches sollten installiert sein. 2. Führen Sie das Tool wie oben beschrieben aus.	• Wie oben	• In der Ausgabe sollten die installierten Patches nicht aufgeführt sein. • Überprüfen Sie das Ereignisprotokoll auf Fehler.
2.3	Mittel	Ausführen von HfNetChk mit mehreren Serverlisten und einem Testzeitplan	1. Erstellen Sie mehrere Serverlisten. 2. Führen Sie das Tool wie oben beschrieben aus. 3. Verwenden Sie den Taskplaner, um eine Befehlszeile für 15 Min. zu planen.	• Wie oben	• Die Ausgabe unterschiedlicher Server sollte überprüft werden können. • Überprüfen Sie nach 20 Min. den Zeitstempel. (Möglicherweise muss dazu der Taskplaner aktiviert werden.)

Testfall	Priorität	Zu testende Bedingung	Einzelheiten zur Ausführung	Erforderliche Daten	Erwartetes Ergebnis
1.1 DTP 1	Hoch	Importieren der einzelnen Serverrichtlinien für Datei- und Druckserver und Überprüfen der im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* beschriebenen Schritte	**Genauere Angaben zur Vorgehensweise finden Sie im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* in Kapitel 4.** 5. Importieren Sie die Richtlinie 6. Importieren Sie **File&print Incremental.**inf. 7. Verschieben Sie den Datei- und Druckserver in die Organisationseinheit **F&B.** 8. Erzwingen Sie die Replikation des Domänencontrollers. 9. Starten Sie den Server FP01 neu.	Vorlage **File&print Incremen-tal.inf**	• Ereigniskennung 1704 sollte auf jedem Domänencontroller vorhanden sein. • Der Spoolerdienst wurde gestartet.
2.	Hoch	Verwenden von Dienstprogrammen wie GpoTool und Gpresult, um die Richtlinieneinstellungen zu überprüfen	1. Überprüfen Sie, ob die Richtlinie erfolgreich auf jeden Domänencontroller gedownloadet wurde, indem Sie die Ereigniskennung 1704 auf jedem Domänencontroller suchen. 2. Überprüfen Sie mithilfe der Admin MMC **Lokale Richtlinie**, ob die Richtlinie auf jeden Domänencontroller angewendet wurde. 3. Überprüfen Sie, ob die Richtlinie auf den Datei- und Druckserver angewendet wurde.	GpoTool und Gpresult	• Überprüfen Sie, ob die Richtlinie angewendet wurde.
3	Hoch	Testen der zusätzlichen Einstellungen einzelner Richtlinien, wie im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* beschrieben, und Überprüfen der Konfiguration	1. Nehmen Sie die zusätzlichen Einstellungen vor, die im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* beschrieben sind. 2. Stellen Sie eine Verbindung mit einem Drucker her und führen Sie einen Druckauftrag aus. 3. Erstellen Sie eine Dateifreigabe, und überprüfen Sie, ob ein Client eine Verbindung herstellen kann.		• Der Server sollte drucken können. • Die Dateifreigabe sollte funktionieren.

Testfall	Priorität	Zu testende Bedingung	Einzelheiten zur Ausführung	Erforderliche Daten	Erwartetes Ergebnis
1.2 DTP 4	Hoch	Importieren der einzelnen Serverrichtlinien für Infrastrukturserver und Überprüfen der *Betriebshandbuch zur Sicherheit von Windows 2000 Server* beschriebenen Schritte	**Genauere Angaben zur Vorgehensweise finden Sie im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* in Kapitel 4.** 1. Importieren Sie die Richtlini 2. Importieren Sie **Infrastructure.inf.** 3. Verschieben Sie den Infrastrukturserver in die Organisationseinheit **Infrastruktur.** 4. Erzwingen Sie die Replikation des Domänencontrollers. 5. Starten Sie den Server INF01 neu. 6. Deaktivieren Sie die Datei- und Druckerfreigabe.	Vorlage **Infrastructure .inf**	• Ereigniskennung 1704 sollte auf jedem Domänencontroller vorhanden sein. • Der DHCP-Server, der DNS-Server, NTLMssp und der WINS-Dienst wurden gestartet.
5.	Hoch	Verwenden von Dienstprogrammen wie GpoTool und Gpresult, um die Richtlinieneinstellungen zu überprüfen	1. Überprüfen Sie, ob die Richtlinie erfolgreich auf jeden Domänencontroller gedownloadet wurde, indem Sie die Ereigniskennung 1704 auf jedem Domänencontroller suchen. 2. Überprüfen Sie mithilfe der Admin MMC **Lokale Richtlinie**, ob die Richtlinie auf jeden Domänencontroller angewendet wurde. 3. Überprüfen Sie, ob die Richtlinie auf den Infrastrukturserver angewendet wurde.	GpoTool und Gpresult	• Überprüfen Sie, ob die Richtlinie angewendet wurde.
6	Hoch	Testen der zusätzlichen Einstellungen einzelner Richtlinien, wie im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* beschrieben, und Überprüfen der Konfiguration	1. Nehmen Sie die zusätzlichen Einstellungen vor, die im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* beschrieben sind. 2. Verbinden Sie einen Client mit dem Netzwerk, und stellen Sie fest, ob der Client die Adresse abrufen kann. 3. Überprüfen Sie, ob sichere dynamische Aktualisierungen aktiviert wurden. 4. Überprüfen Sie, ob die WINS-Auflösung und die NetBIOS-Namensauflösung funktionieren.		• Der Server sollte die grundlegenden DHCP-, DNS- und WINS-Funktionen ausführen können.

Testfall	Priorität	Zu testende Bedingung	Einzelheiten zur Ausführung	Erforderliche Daten	Erwartetes Ergebnis
1.3 DTP 7	Hoch	Importieren der einzelnen Serverrichtlinien für IIS-Server und Überprüfen der im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* beschriebenen Schritte	**Genauere Angaben zur Vorgehensweise finden Sie im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* in Kapitel 4.** 1. Importieren Sie die Richtlinie • Importieren Sie **IISIncremental.inf.** 2. Verschieben Sie den IIS-Server in die Organisationseinheit **IIS.** 3. Erzwingen Sie die Replikation des Domänencontrollers. 4. Starten Sie den Server IIS01 neu. 5. Deaktivieren Sie die Datei- und Druckerfreigabe.	• **IISIncremental. inf** • **IISLock.exe**	• Ereigniskennung 1704 sollte auf jedem Domänencontroller vorhanden sein. • Die IISAdmin- und W3SVC-Dienste sollten gestartet worden sein.
8.	Hoch	Verwenden von Dienstprogrammen wie GpoTool und Gpresult, um die Richtlinieneinstellungen zu überprüfen	1. Überprüfen Sie, ob die Richtlinie erfolgreich auf jeden Domänencontroller gedownloadet wurde, indem Sie die Ereigniskennung 1704 auf jedem Domänencontroller suchen. 2. Überprüfen Sie mithilfe der Admin MMC **Lokale Richtlinie**, ob die Richtlinie auf jeden Domänencontroller angewendet wurde. 3. Überprüfen Sie, ob die Richtlinie auf den IIS-Server angewendet wurde.	GpoTool und Gpresult	• Überprüfen Sie, ob die Richtlinie angewendet wurde.
1.4 DTP 9	Hoch	Testen der zusätzlichen Einstellungen einzelner Richtlinien, wie im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* beschrieben, und Überprüfen der Konfiguration	1. Führen Sie **IISLockd.exe** aus, dadurch wird auch **URLscan.exe** installiert. • Überprüfen Sie die Einstellungen für URLScan, wie in Kapitel 6 beschrieben. 2. Richten Sie statische Seiten ein, und überprüfen Sie, ob ein Client eine Verbindung mit dem Server herstellen kann.		• Überprüfen Sie die auf der statischen Webseite vorgenommenen Änderungen. • Nachdem die zusätzlichen Einstellungen festgelegt wurden, sollte IIS funktionieren.

Testfall	Priorität	Zu testende Bedingung	Einzelheiten zur Ausführung	Erforderliche Daten	Erwartetes Ergebnis
1.5 DTP 10	Hoch	Änderungen an der empfohlenen Umgebung für Remoteverwaltung	**Genauere Angaben zur Vorgehensweise finden Sie im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* in Kapitel 4.** 1. Aktivieren Sie den WMI-Dienst für APP01. 2. Aktivieren Sie den Wechselmediendienst für APP01. 3. Für die Remoteverwaltung bestimmter Server: • Aktivieren Sie den Serverdienst für APP01. • Aktivieren Sie die Remoteregistrierung für den Infrastrukturserver. 4. Verwenden Sie unter **Arbeitsplatz** die Option **Verwalten**, um eine Verbindung mit APP01 herzustellen und die oben angegebenen Einstellungen zu überprüfen. 5. Ein Client sollte eine Verbindung mit dem Datei- und Druckserver herstellen und drucken können.		• Die Remoteverwaltung folgender Bereiche sollte möglich sein: Freigegebene Ordner, lokale Benutzer und Gruppen, alles unter **Datenspeicher**, außer Logische Laufwerke, Dienste, Geräte-Manager, die Ereignisanzeige, Leistungsprotokolle und Warnungen. • Die Datenträgerverwaltung, die Defragmentierung und die Wechselmedienverwaltung funktionieren. • Remoteverwaltung sollte für Mitgliedsserver möglich sein.

Originaltitel: Job Aid 1 – Threat and Vulnerability Analysis Table

Aufgabenhilfe 1: Tabelle zur Analyse möglicher Bedrohungen und Schwachstellen

Da in Ihrer Umgebung ständig neue Bedrohungen und Schwachstellen entstehen, müssen Sie das Risiko für die Umgebung einschätzen. Dadurch können Sie sicherstellen, dass auf besonders große Bedrohungen schneller reagiert wird. Verwenden Sie die unten stehende Tabelle, um Informationen über Bedrohungen und Schwachstellen aufzulisten, die Ihre Computerumgebung betreffen.

Bedrohung <Benennen Sie hier die Bedrohung>

Bedrohung	<Bezeichnung für die Bedrohung>
Bedrohungsart	Um welche Art oder Arten von Bedrohung(en) handelt es sich?
Schwachstelle	Wo besteht eine Schwachstellen?
Ausnutzung	Inwiefern könnte eine Bedrohung diese Schwachstelle ausnutzen?
Gegenmaßnahmen	Welche Maßnahmen ergreifen Sie gegen die Bedrohung der Umgebung?
Schweregrad	Als wie kritisch würden Sie die Bedrohung auf einer Skala von 1-10 einschätzen?
Erforderlicher Aufwand	Wie leicht ist diese Schwachstelle auszunutzen? Bitte bewerten Sie auch hier auf einer Skala von 1-10.
Ausmaß des Risikos	Schweregrad/erforderlicher Aufwand
Wahrscheinlichkeit	Wie hoch schätzen Sie die Wahrscheinlichkeit einer Bedrohung ein (in Prozent).
Gesamtes Ausmaß der Bedrohung	Risiko x Wahrscheinlichkeit
Konsequenzen einer Gefährdung	Was passiert, wenn eine Schwachstelle in Ihrer Umgebung ausgenutzt wird?
Verluste (geschätzte Verluste)	Geschätzte finanzielle Verluste
Verlustrisiko	Verluste x Wahrscheinlichkeit
Ausgleich/Zuweisung	Welche Schutzmaßnahmen ergreifen Sie hinsichtlich der Schwachstelle, sofern Sie diese offen halten müssen?
Reaktion	Was tun Sie im Fall einer Gefährdung?
Besitzer	Wer ist verantwortlich?
Status	Welchen Status hat die Schwachstelle zum jetzigen Zeitpunkt: **Geschlossen**, **Offen** oder **Ausgeglichen**?
Softwareversion	Welche Version ist betroffen?

Originaltitel: Job Aid 2 – Top Security Blunders

Aufgabenhilfe 2: Die häufigsten Fehler in Bezug auf die Sicherheit

Selbst die neueste Technologie und gutes IT-Sicherheitspersonal helfen Ihnen nicht weiter, wenn die Benutzer unvorsichtig oder nicht informiert sind. Die Liste der unten aufgeführten Fehler ist folgendermaßen aufgeteilt: in Ereignisse, die am Clientcomputer auftreten (oder durch den Benutzer hervorgerufen werden) und in Ereignisse, die am Server auftreten (oder durch das IT-Personal hervorgerufen werden).

Die 11 häufigsten clientseitigen Fehler in Bezug auf die Sicherheit

1. **Kennwortfehler**
   a. **Unsichere Kennwörter.** Benutzer tendieren dazu, leicht zu merkende (und daher leicht zu entschlüsselnde) Kennwörter auszuwählen. Komplexe Kennwörter können zwar über Windows 2000-Sicherheitsrichtlinien erzwungen werden, aber letztendlich hängt die Kennwortsicherheit vom jeweiligen Benutzer ab. Als Kennwörter dienen häufig die Namen der Kinder oder Haustiere, Geburtsdaten oder Wörter im Zusammenhang mit dem Arbeitsumfeld. Noch gravierender ist es, wenn sich die Quelle für das Kennwort in Sichtweite befindet!

   b. **Gemeinsame Nutzung von Kennwörtern durch mehrere Benutzer.** Insbesondere in Umgebungen, in denen sich Benutzer Computer teilen, teilen sich Benutzer häufig auch die Kennwörter. Diese Vorgehensweise ist nicht sicher und sollte nicht zugelassen werden.

   c. **Verwenden des internen Organisationskennworts auf externen Websites.** Wenn die Benutzer ihr Kennwort außerhalb der Organisation verwenden, erhöht sich für Sie das Risiko von Angriffen. Benutzerkennwörter werden häufig zusammen mit E-Mail-Adressen gespeichert. Allein dadurch, dass ein Hacker diese Kombination verwendet, kann er sowohl die Organisation ermitteln, für die der Benutzer arbeitet, als auch den Netzwerknamen des Benutzers (wenn es sich um das Präfix der SMTP-Adresse handelt) und dessen Kennwort.

2. **Nicht ordnungsgemäßes Sichern und/oder Speichern wichtiger Informationen (lokal statt zentral).** In vielen Organisationen werden Clientcomputer (insbesondere Laptops) nicht gesichert. Das lokale Speichern von Informationen auf Clientcomputern anstelle des Speicherns auf verwalteten Servern kann dazu führen, dass die Wiederherstellung der Daten nach einem Angriff so gut wie unmöglich ist.
3. **Ungesperrte, nicht beaufsichtigte Arbeitsstationen.** Gibt es in Ihrer Organisation eine Richtlinie, die besagt, dass Benutzer ihre Arbeitsstationen beim Verlassen sperren? Andernfalls können andere Personen problemlos Wege finden, um nach Dienstschluss auf die Arbeitsstation zuzugreifen (beispielsweise durch das Installieren von Terminalserver, PC Anywhere oder durch das Ausweiten lokaler Berechtigungen).

4. **Ignorieren von Updates und Patches der Anbieter.** Jede Soft- und Hardware hat Schwachstellen und unterliegt einem ständigen Entwicklungsprozess. Featureverbesserungen, Entwurfsverbesserungen und Fixes zu Programmfehlern werden im Allgemeinen veröffentlicht, bis die Software nicht mehr verwendet wird. Da Software und (in geringerem Umfang) Hardware ständig verändert wird, muss das IT-Personal immer die aktuellen Patches, Updates und Fixes auf dem System installieren. Bei unterlassenen Aktualisierungen ist der Angreifer im Vorteil.
5. **Nicht physisches Sichern der Computerausstattung.** Ausstattung, insbesondere Laptops, wird häufig gestohlen. Ein Laptop, den ein Angreifer in seinen Besitz gebracht hat, kann ein ernst zu nehmendes Sicherheitsrisiko darstellen. Dies gilt vor allem, wenn er einem Benutzer mit signifikanten Systemrechten gehört.
6. **Deaktivieren oder Vermindern vorhandener Sicherheitskontrollen.** Benutzer versuchen häufig, durch die Deaktivierung von Antivirenprogrammen die Verarbeitungsgeschwindigkeit zu erhöhen. Darüber hinaus senken oder entfernen Sie aus Bequemlichkeit die Makrosicherheit bei Produktivitätsanwendungen wie Microsoft Word, Microsoft Excel usw. Es ist wichtig, Benutzer über die Notwendigkeit und das Beibehalten von Sicherheitskontrollen zu informieren.
7. **Installieren nicht erforderlicher und/oder nicht genehmigter Software.** Benutzer installieren häufig nicht genehmigte Software und gefährden dadurch die Organisation, denn sie führen möglicherweise Anwendungen aus, die trojanische Pferde oder andere Sicherheitsrisiken beinhalten.
8. **Veröffentlichen nicht erforderlicher persönlicher Informationen.** Durch die Bekanntgabe der Namen von Kindern, vollständiger Geburtsdaten usw. können Angreifer Kennwörter erraten oder sich durch Social Engineering nicht autorisierten Zugriff verschaffen. Informationen können direkt mitgeteilt werden, z. B. können sie dem Angreifer per Telefon oder per E-Mail mitgeteilt werden oder passiv, durch Hinweise innerhalb der Arbeitsumgebung (Fotos der Kinder, Informationen, die ihre Sozialversicherungsnummer beinhalten, Krankenversicherungskarten usw.).
9. **Verbreiten von Viren- und anderen Hoaxes.** Falsche Viren und Warnungen, die per E-Mail in großen Mengen verbreitet werden, sind kosten- und zeitaufwändig. Sie sollten sicherstellen, dass Benutzer diese Informationen direkt an die IT-Abteilung weitergeben und nicht innerhalb der Organisation verteilen.
10. **Öffnen nicht erwarteter E-Mail-Anlagen.** Eine eher "konservative" und vorsichtige Einstellung beim Empfangen und Öffnen von Anlagen trägt erheblich zur Vermeidung von Sicherheitsvorfällen bei.
11. **Fehlende Schulungen von Benutzern auf das Erkennen von Sicherheitsvorfällen und die anschließende geeignete Vorgehensweise.** Viele Vorfälle könnten ausgeglichen oder vermieden werden, wenn Benutzer auf das Erkennen der Anzeichen für Angriffe, Konfigurationsfehler, Viren oder andere Vorfälle geschult wären. Sie müssen ebenfalls auf eine geeignete Vorgehensweise bei Vorfällen geschult werden.

Die 8 häufigsten serverseitigen Fehler in Bezug auf die Sicherheit

1. **Kennwortfehler**
   a. **Unsichere Kennwörter.** Das IT-Personal sichert sich häufig gegen Sperrungen ab, indem es "Hintertüren" einbaut. Kennwörter für diese "Hintertüren" sind im Allgemeinen leichter zu merken und daher weniger sicher. Diese Situation kann zwar durch das Implementieren und Erzwingen von Windows 2000-Sicherheitsrichtlinien zum größten Teil ausgeglichen werden, aber Sie müssen sicherstellen, dass Benutzer mit weitreichenden Zugriffsrechten an eine Gruppenrichtlinie gebunden sind.
   b. **Gemeinsame Nutzung von Kennwörtern durch das IT-Personal.** Wenn Sie beispielsweise mehr als einem Benutzer Zugriff auf das Administratorkonto gestatten, wird dadurch das Überwachen und Verwalten des Kontos erschwert oder unmöglich gemacht, wenn im Zusammenhang mit diesem Konto ein Sicherheitsereignis auftritt. Benutzer, insbesondere Mitarbeiter der IT-Abteilung, haben eine individuelle Verantwortlichkeit für ihr Konto, die überwacht werden kann. Die Benutzer und das IT-Personal sollten eine Richtlinie unterzeichnen, die das Teilen von Kennwörtern untersagt.
   c. **Verwenden des internen Organisationskennworts auf externen Websites.** Wenn die Benutzer ihr Kennwort außerhalb der Organisation verwenden, erhöht sich für Sie das Risiko von Angriffen. Benutzerkennwörter werden häufig zusammen mit E-Mail-Adressen gespeichert. Allein dadurch, dass ein Hacker diese Kombination verwendet, kann er sowohl ermitteln, wo der Benutzer beschäftigt ist, als auch dessen Benutzernamen (wenn es sich um das Präfix der SMTP-Adresse handelt) und dessen Kennwort.

2. **Nicht erfolgtes Implementieren aller Ebenen der umfassenden Abwehrstrategie.** Es ist zwar wichtig, einen Firewall und ein System zur Erkennung von Eindringversuchen zu implementieren und richtig zu konfigurieren, allerdings müssen die Gegenmaßnahmen zum Schutz der Sicherheit noch darüber hinausgehen. Ihre umfassende Abwehrstrategie sollte Kontrollen auf Verwaltungs- und Personalebene beinhalten. Bei vielen Unternehmen werden Mitarbeiter mit Kundenkontakt, wie beispielsweise Empfangsangestellte und Telefonist(inn)en, nicht auf das Erkennen und Schützen sensibler Informationen geschult. Unzureichender Schutz gegen alle potenziellen Angriffe ist ein verbreiteter Fehler, der zu einem falschen Sicherheitsverständnis führt. Weitere Informationen zu umfassenden Schutzmaßnahmen finden Sie in Kapitel 2 dieses Handbuchs.
3. **Unzureichendes Ausführen und Überprüfen von Systemsicherungen.** Viele Organisationen, darunter auch große, sichern die wichtigen Systemdaten nicht angemessen. Von den wenigen Organisationen, die Sicherungen durchführen, nehmen sich viele nicht die Zeit, eine Datei wieder herzustellen oder den Erfolg eines Sicherungsvorgangs zu überprüfen. Dies kann zu Situationen führen, bei denen ganze Sätze von Sicherungsmedien unbrauchbar geworden sind. Diese Medien können dann nicht zum Wiederherstellen von Daten verwendet werden, die durch einen Angriff oder einen schwerwiegenden Fehler verlorenen gegangen sind.
4. **Ausführen nicht erforderlicher Dienste.** Standardinstallationen umfassen häufig eine größere Anzahl von Diensten als für den Betrieb erforderlich sind. Durch diese zusätzlichen Dienste wird eine größere Angriffsfläche geschaffen. Dies sollte verhindert werden. Es sollten nur erforderliche Dienste ausgeführt werden. Überprüfen Sie regelmäßig, ob Dienste noch benötigt werden.

5. **Nicht Erkennen von internen Sicherheitsbedrohungen.** In vielen Organisationen stehen die Sicherheitsmaßnahmen und -ressourcen gegen Angriffe von außen im Mittelpunkt. Dies führt manchmal dazu, dass die potenziell größere Bedrohung nicht ausreichend beachtet wird: Personen innerhalb der Organisation. Sie haben besonders weitreichenden Zugriff und stellen daher absichtlich oder unabsichtlich die größte potenzielle Bedrohung in Bezug auf Schäden dar.
6. **Nicht konsequentes Anwenden von Sicherheitsrichtlinien.** Eine hervorragende Sicherheitsrichtlinie, die nicht konsequent angewendet wird, bietet für die Organisation keinen großen Nutzen. Die nachlässige Anwendung einer Sicherheitsrichtlinie kann auch den gefährlichen Nebeneffekt haben, dass die Mitarbeiter Gleichgültigkeit gegenüber dem Sicherheitsaspekt entwickeln.
7. **Gewähren einer zu großen Anzahl von Berechtigungen für Dienste.** Dienste benötigen eine bestimmte Zugriffsebene, um ihre Aufgaben innerhalb des Systems ausführen zu können. Beim Installieren oder bei der Problembehandlung dieser Dienste wird möglicherweise weitreichenderer Zugriff gewährt als erforderlich, um die Funktionalität möglichst schnell zu erreichen. Dienste dürfen nur über das geringstmögliche Maß an Berechtigungen verfügen, damit die Sicherheit des Systems beibehalten werden kann. Sie sollten sicherstellen, dass dies sowohl von den Systemadministratoren durchgesetzt wird, die die Dienstberechtigungen konfigurieren, als auch von den Anwendungsentwicklern, die die Dienstabhängigkeiten erstellen.
8. **Unzureichendes Sichern in-house entwickelter Anwendungen.** In-house entwickelte Anwendungen sollten genauso intensiv oder sogar intensiver geprüft werden, wie Anwendungen von Drittanbietern.

Originaltitel: Job Aid 3 – Attacks and Countermeasures
Aufgabenhilfe 3 – Angriffe und Gegenmaßnahmen

Ausnutzung technischer Schwachstellen	Konkrete Gegenmaßnahmen	Standardmäßige Gegenmaßnahmen											
		Erzwingen komplexer Kennwörter	Aktivieren der Protokollierung/ Überwachung	Prüfen der Systemkonfiguration	Deaktivieren von Diensten	Erkennungssystem für Eindringversuche	Datenverschlüsselung	Digitale Signaturen	Implementieren eines Firewalls	Anwendungs-absicherung	Verwenden der aktuellsten Anbieterpatches	Richtlinien und Verfahren	Implementieren von Hindernissen
Unerlaubtes Entschlüsseln von Kennwörtern	Verwenden Sie das höchstmögliche Maß an Verschlüsselung.	✓	✓	✓		✓	✓					✓	
Pufferüberlauf	Zwingen Sie das Betriebssystem und die Anwendungen, die Größe und den bevorzugten Typ angenommener Daten zu überprüfen. Verwenden Sie einen Firewall auf Anwendungsebene.			✓	✓	✓			✓*	✓	✓		
Netzwerksniffing	Beschränken Sie lokale Netzwerkverbindungen und Hardwarebedienelemente. Verwenden Sie Tools zur Sniffererkennung.			✓	✓	✓	✓					✓	

Ausnutzung technischer Schwachstellen	Konkrete Gegenmaßnahmen	Standardmäßige Gegenmaßnahmen											
		Erzwingen komplexer Kennwörter	Aktivieren der Protokollierung/ Überwachung	Prüfen der Systemkonfiguration	Deaktivieren von Diensten	Erkennungssystem für Eindringversuche	Datenverschlüsselung	Digitale Signaturen	Implementieren eines Firewalls	Anwendungs-absicherung	Verwenden der aktuellsten Anbieterpatches	Richtlinien und Verfahren	Implementieren von Hindernissen
Wiederholungs-angriff	Richten Sie Kennwörter ein, die nur ein Mal verwendet werden können, und verhindern Sie Paketsniffing.			✓	✓			✓					
Sitzungsübernahme	Verhindern Sie vorhersagbare TCP-Sequenznummern, implementieren Sie SSL, erzwingen Sie Cookies und verhindern Sie lokale Netzwerkverbindungen.					✓	✓	✓	✓				
Sammeln von Informationen	Beschränken Sie den direkten Zugriff mithilfe eines proxybasierten Firewalls, und implementieren Sie ein intelligentes System zur Erkennung von Eindringversuchen, das Filtergeräte aktualisieren kann. Verlangen Sie Authentifizierung für den Zugriff auf Anwendungen,		✓	✓	✓	✓			✓		✓		

Ausnutzung technischer Schwachstellen	Konkrete Gegenmaßnahmen	Standardmäßige Gegenmaßnahmen											
		Erzwingen komplexer Kennwörter	Aktivieren der Protokollierung/ Überwachung	Prüfen der Systemkonfiguration	Deaktivieren von Diensten	Erkennungssystem für Eindringversuche	Datenverschlüsselung	Digitale Signaturen	Implementieren eines Firewalls	Anwendungs-absicherung	Verwenden der aktuellsten Anbieterpatches	Richtlinien und Verfahren	Implementieren von Hindernissen
	und trennen Sie Sicherheitsdomänen mithilfe von Firewalls ab.												

Ausnutzung technischer Schwachstellen	Konkrete Gegenmaßnahmen	Standardmäßige Gegenmaßnahmen											
		Erzwingen komplexer Kennwörter	Aktivieren der Protokollierung/ Überwachung	Prüfen der Systemkonfiguration	Deaktivieren von Diensten	Erkennungssystem für Eindringversuche	Datenverschlüsselung	Digitale Signaturen	Implementieren eines Firewalls	Anwendungs-absicherung	Verwenden der aktuellsten Anbieterpatches	Richtlinien und Verfahren	Implementieren von Hindernissen
Auswerten von Dokumenten	Überprüfen Sie alle öffentlich zugänglichen Informationen auf das Einhalten von Sicherheitsrichtlinien Wie viele E-Mail-Adressen können beispielsweise von der öffentlichen Website ermittelt werden? Können diese E-Mail-Adressen direkt Benutzerkonten zugeordnet werden?											✓	
Sicherheitslücken bei drahtlosen Verbindungen	Verkleinern Sie die Zone für drahtlose Verbindungen, implementieren Sie Hardwarebeschränkungen, und verwenden Sie multifaktorielle Authentifizierung.			✓		✓	✓						
Social Engineering	Implementieren Sie strenge Richtlinien sowie ein Schulungsprogramm.											✓	

Ausnutzung technischer Schwachstellen	Konkrete Gegenmaßnahmen	Standardmäßige Gegenmaßnahmen											
		Erzwingen komplexer Kennwörter	Aktivieren der Protokollierung/ Überwachung	Prüfen der Systemkonfiguration	Deaktivieren von Diensten	Erkennungssystem für Eindringversuche	Datenverschlüsselung	Digitale Signaturen	Implementieren eines Firewalls	Anwendungs-absicherung	Verwenden der aktuellsten Anbieterpatches	Richtlinien und Verfahren	Implementieren von Hindernissen
Denial-of-Service & Distributed Denial-of-Service-Angriffe	Sammeln Sie Grundlagen zum Definieren normaler Dienstebenen. Bei jedem Zugriff sollten nur minimale Berechtigungen gewährt werden. Wenden Sie Netzwerkeintrittsfilterung an, um die Anzahl von IP-Spoofing-Paketen zu reduzieren. (Weitere Informationen dazu finden Sie in RFC 2267.) Implementieren Sie Routerfilter, aktivieren Sie Quota-Systeme, überwachen Sie die Systemleistung, überwachen Sie Signaturen für Distributed Denial-of-Service-Angriffe mithilfe eines Systems zur Erkennung von Eindringversuchen, und implementieren Sie Fehlertoleranz und			✓		✓			✓		✓		

Ausnutzung technischer Schwachstellen	Konkrete Gegenmaßnahmen	Standardmäßige Gegenmaßnahmen											
		Erzwingen komplexer Kennwörter	Aktivieren der Protokollierung/ Überwachung	Prüfen der Systemkonfiguration	Deaktivieren von Diensten	Erkennungssystem für Eindringversuche	Datenverschlüsselung	Digitale Signaturen	Implementieren eines Firewalls	Anwendungs-absicherung	Verwenden der aktuellsten Anbieterpatches	Richtlinien und Verfahren	Implementieren von Hindernissen
	Lastenausgleichslösungen. Implementieren Sie, je nach Anbieter, Verbesserungen für den TCP/IP-Stack.												

Ausnutzung technischer Schwachstellen	Konkrete Gegenmaßnahmen	Standardmäßige Gegenmaßnahmen												
		Erzwingen komplexer Kennwörter	Aktivieren der Protokollierung/ Überwachung	Prüfen der Systemkonfiguration	Deaktivieren von Diensten	Erkennungssystem für Eindringversuche	Datenverschlüsselung	Digitale Signaturen	Implementieren eines Firewalls	Anwendungs-absicherung	Verwenden der aktuellsten Anbieterpatches	Richtlinien und Verfahren	Implementieren von Hindernissen
Missbrauch von Cookies	Für Personen, die Cookies implementieren, gilt Folgendes: Fügen Sie möglichst wenig Informationen ein, verwenden Sie NIE Klartext zum Speichern von Informationen in Cookies, verwenden Sie, sofern möglich, spezielle Pfade.			✓		✓					✓		
CGI-Angriffe	Stellen Sie sicher, dass Ihre CGI-Skripts unterschiedliche Mengen von Benutzereingaben dynamisch verarbeiten, und geben Sie nie ungeprüfte Eingaben von Remotebenutzern an einen Shellbefehl weiter. Sie sollten einen CGI-Wrapper verwenden.									✓	✓		✓

Ausnutzung technischer Schwachstellen	Konkrete Gegenmaßnahmen	Standardmäßige Gegenmaßnahmen											
		Erzwingen komplexer Kennwörter	Aktivieren der Protokollierung/ Überwachung	Prüfen der Systemkonfiguration	Deaktivieren von Diensten	Erkennungssystem für Eindringversuche	Datenverschlüsselung	Digitale Signaturen	Implementieren eines Firewalls	Anwendungs-absicherung	Verwenden der aktuellsten Anbieterpatches	Richtlinien und Verfahren	Implementieren von Hindernissen
DNS Poisoning	Verwenden Sie Secure DNS (sicheres DNS oder SDNS), und implementieren Sie ein aufgeteiltes DNS, das ein vertrauenswürdiges internes und ein nicht vertrauenswürdiges externes DNS verwendet. Beide können sich auf demselben Firewall befinden. Beschränken und authentifizieren Sie Zonenübertragungen.			✓		✓			✓	✓	✓		✓
E-Mail-Spoofing	Verwenden Sie digitale Signaturen oder Zertifikate. Verhindern Sie Mailweiterleitungen und -Spoofing auf den SMTP-Servern.			✓		✓		✓		✓	✓		
IP-Spoofing	Wenden Sie Netzwerkeintrittsfilterung an (weitere Informationen dazu			✓		✓			✓				

Ausnutzung technischer Schwachstellen	Konkrete Gegenmaßnahmen	Standardmäßige Gegenmaßnahmen											
		Erzwingen komplexer Kennwörter	Aktivieren der Protokollierung/ Überwachung	Prüfen der Systemkonfiguration	Deaktivieren von Diensten	Erkennungssystem für Eindringversuche	Datenverschlüsselung	Digitale Signaturen	Implementieren eines Firewalls	Anwendungs-absicherung	Verwenden der aktuellsten Anbieterpatches	Richtlinien und Verfahren	Implementieren von Hindernissen
	finden Sie in RFC 2821).												

Ausnutzung technischer Schwachstellen	Konkrete Gegenmaßnahmen	Standardmäßige Gegenmaßnahmen											
		Erzwingen komplexer Kennwörter	Aktivieren der Protokollierung/ Überwachung	Prüfen der Systemkonfiguration	Deaktivieren von Diensten	Erkennungssystem für Eindringversuche	Datenverschlüsselung	Digitale Signaturen	Implementieren eines Firewalls	Anwendungs-absicherung	Verwenden der aktuellsten Anbieterpatches	Richtlinien und Verfahren	Implementieren von Hindernissen
Viren	Zeigen Sie den Benutzern, wie sie das Verhalten von Viren und die geeignete Reaktion darauf ermitteln können, vermeiden Sie das Deaktivieren der Software für die Viruserkennung, erzwingen Sie rechtzeitige Aktualisierungen von Virussignaturen. Verwenden Sie nur vertrauenswürdige Software.		✓	✓				✓			✓	✓	✓
Würmer	Zeigen Sie den Benutzern, wie sie das Verhalten von Viren und die geeignete Reaktion darauf ermitteln können, vermeiden Sie das Deaktivieren der Software für die Viruserkennung, erzwingen Sie rechtzeitige Aktualisierungen von Virussignaturen.		✓	✓	✓	✓			✓	✓	✓	✓	✓

Ausnutzung technischer Schwachstellen	Konkrete Gegenmaßnahmen	Standardmäßige Gegenmaßnahmen											
		Erzwingen komplexer Kennwörter	Aktivieren der Protokollierung/ Überwachung	Prüfen der Systemkonfiguration	Deaktivieren von Diensten	Erkennungssystem für Eindringversuche	Datenverschlüsselung	Digitale Signaturen	Implementieren eines Firewalls	Anwendungs-absicherung	Verwenden der aktuellsten Anbieterpatches	Richtlinien und Verfahren	Implementieren von Hindernissen
Trojanische Pferde	Zeigen Sie den Benutzern, wie sie das Verhalten von Viren und die geeignete Reaktion darauf ermitteln können, vermeiden Sie das Deaktivieren der Software für die Viruserkennung, erzwingen Sie rechtzeitige Aktualisierungen von Virussignaturen. Verwenden Sie nur vertrauenswürdige Software.		✓	✓				✓			✓	✓	✓
Missbrauch durch Insider	Es ist besonders schwierig, die Bedrohung durch Insider zu verringern oder ganz auszuschließen. Implementieren Sie strenge Richtlinien, teilen Sie Pflichten auf, beschränken Sie Rechte, und implementieren Sie Peerprüfungen, Jobrotationen sowie Systeme zur	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Ausnutzung technischer Schwachstellen	Konkrete Gegenmaßnahmen	Standardmäßige Gegenmaßnahmen											
		Erzwingen komplexer Kennwörter	Aktivieren der Protokollierung/ Überwachung	Prüfen der Systemkonfiguration	Deaktivieren von Diensten	Erkennungssystem für Eindringversuche	Datenverschlüsselung	Digitale Signaturen	Implementieren eines Firewalls	Anwendungs-absicherung	Verwenden der aktuellsten Anbieterpatches	Richtlinien und Verfahren	Implementieren von Hindernissen
	Erkennung von Eindringversuchen.												

Ausnutzung technischer Schwachstellen	Konkrete Gegenmaßnahmen	Standardmäßige Gegenmaßnahmen											
		Erzwingen komplexer Kennwörter	Aktivieren der Protokollierung/ Überwachung	Prüfen der Systemkonfiguration	Deaktivieren von Diensten	Erkennungssystem für Eindringversuche	Datenverschlüsselung	Digitale Signaturen	Implementieren eines Firewalls	Anwendungs-absicherung	Verwenden der aktuellsten Anbieterpatches	Richtlinien und Verfahren	Implementieren von Hindernissen
Versehentliches Löschen oder falsches Konfigurieren von Diensten	Begrenzen Sie den Umfang von Berechtigungen (melden Sie sich nur als Organisationsadministrator oder Domänenadministrator an, wenn dies unbedingt erforderlich ist). Mithilfe direkt verfügbarer, aktueller Sicherungen können grobe Fehler ausgeglichen werden. Implementieren Sie ein verlässliches Schulungsprogramm und, falls erforderlich, auch ein Peerprüfungsprogramm.		✓									✓	✓

Originaltitel: Job Aid 4 – Incident Response Quick Reference Card

Aufgabenhilfe 4 – Referenzliste zur Vorgehensweise bei Vorfällen

Mithilfe der folgenden Prüfliste können Sie sicherstellen, dass Sie die erforderlichen Schritte ausführen, um angemessen auf Vorfälle zu reagieren. Die genaue Reihenfolge der Schritte wird allerdings vom Organisationstyp und von der Art des Vorfalls abhängen. Weitere Informationen zur Vorgehensweise bei Vorfällen finden Sie in Kapitel 7, "Vorgehensweise bei Vorfällen".

Allgemeine Richtlinien zur Vorgehensweise bei Vorfällen	
Dokumentieren Sie alles. Sie sollten Ihre Kommentare auf Band aufnehmen. Vermerken Sie, wer was wann und warum getan hat.	
Bleiben Sie ruhig. Vermeiden Sie Überreaktionen oder Panik. Befolgen Sie systematisch die Sicherheitsrichtlinien.	
Verwenden Sie Out-Of-Band-Kommunikationsmittel, wie z. B. Telefon und Fax, oder sprechen Sie persönlich mit den betreffenden Personen. Angreifer können sonst möglicherweise mithören.	
Neben der Kommunikation der Mitglieder eines Teams untereinander sollte auch der Kontakt zu anderen involvierten Personen gesichert sein.	
Vermeiden Sie das Neustarten des Computers, das An- und Abmelden oder andere Handlungen, durch die schädlicher Code versehentlich gestartet werden könnte.	
Ziel 1 – Führen Sie eine anfängliche Beurteilung durch	
1.1	Wenden Sie sich an das technische Team, um sicherzustellen, dass es sich tatsächlich um einen problematischen Vorfall handelt.
1.2	Untersuchen Sie Überwachungsprotokolle nach ungewöhnlicher Aktivität, fehlenden Protokollen und Lücken in Protokollen.
1.3	Suchen Sie Hackertools (Tools zum unerlaubten Entschlüsseln von Kennwörtern, Trojanische Pferde usw.).
1.4	Suchen Sie nicht autorisierte Anwendungen, die so konfiguriert sind, dass sie automatisch starten.
1.5	Untersuchen Sie Konten nach erweiterten Berechtigungen und nicht autorisierten Gruppenmitgliedern.
1.6	Suchen Sie nach nicht autorisierten Prozessen.
1.7	Legen Sie fest, ob Beweise erhalten bleiben.
1.8	Vergleichen Sie die Systemleistung des kompromittierten Systems mit der geplanten Systemleistung.
1.9	Legen Sie eine anfängliche Prioritätsebene fest, und bestimmen Sie für Vorfälle einen Verantwortlichen.
Ziel 2 – Geben Sie die Informationen zum Vorfall weiter	
2.1	Geben Sie die Informationen zum Vorfall an die zuständigen Ansprechpartner und an das für die Computersicherheit verantwortliche Team (Computer Security Incident Response Team oder CSIRT) weiter.
Ziel 3 – Begrenzen Sie den Schaden und minimieren Sie das Risiko	
3.1	Isolieren Sie, je nach Schweregrad und Sicherheitsrichtlinie, die betroffenen Systeme, indem Sie sie vom Netzwerk trennen.
3.2	Ändern Sie die Kennwörter auf den betroffenen Systemen.
3.3	Sichern Sie die Systeme für die Wiederherstellung, und sammeln Sie gegebenenfalls Beweise.

Ziel 4 – Identifizieren Sie die Art und den Schweregrad der Gefährdung(en)	
4.1	Ermitteln Sie die Art des Angriffs.
4.2	Ermitteln Sie den Zweck des Angriffs (besonders Ihr Unternehmen betreffend, automatisierter Angriff, Sammeln von Informationen)
4.3	Identifizieren Sie alle von dem Angriff betroffenen Systeme. Beachten Sie erneut die Schritte zur Schadensbegrenzung, wenn weitere betroffene Systeme identifiziert werden.
4.4	Führen Sie erneut eine Überprüfung durch, und legen Sie gegebenenfalls erneut eine Prioritätsebene für das Ereignis fest.
Ziel 5 – Sichern Sie Beweise	
5.1	Sichern Sie die Systeme innerhalb der Reaktions- und Wiederherstellungsphase so schnell wie möglich mit bisher noch nicht verwendeten Sicherungsmedien.
5.2	Wenn möglich, sollten Sie die Systeme vollständig sichern, einschließlich der Protokolle und Systemstatusdaten.
5.3	Behalten Sie die nachweisbare Reihenfolge der gesammelten Beweise bei.
5.4	Sichern Sie die Beweise, und dokumentieren Sie, wer Sie wie und wann gesammelt hat und wer darauf zugreifen konnte.
Ziel 6 – Benachrichtigen Sie externe Stellen	
6.1	Benachrichtigen Sie gemäß den Anweisungen eines Rechtsberaters die entsprechende(n) Behörde(n) zur Wahrung des regionalen und/oder bundesstaatlichen Rechts.
6.2	Informieren Sie die PR-Abteilung des für die Computersicherheit verantwortlichen Teams (CSIRT) über das Ergebnis, und bieten Sie gegebenenfalls Ihre Hilfe an.
6.3	Benachrichtigen Sie andere Stellen, wie beispielsweise DFN-CERT in Hamburg (http://www.cert.dfn.de/). DFN-CERT und andere Stellen können nützliche Informationen zur Wiederherstellung liefern.
Ziel 7 – Stellen Sie das System wieder her	
7.1	Suchen und überprüfen Sie aktuelle, nicht beschädigte Sicherungen.
7.2	Stellen Sie das System wieder her.
7.3	Überprüfen Sie die Funktionen und stimmen Sie die Systemleistung auf die ursprünglich als Basis geplante Systemleistung ab.
7.4	Überprüfen Sie, ob im Zusammenhang mit der Schadensbegrenzung Angriffe und falsche Konfigurationen wiederholt werden.
Ziel 8 – Stellen Sie die gesamte Dokumentation zu den Vorfällen geordnet zusammen	
8.1	Stellen Sie alle Aufzeichnungen und Aufnahmen in einem umfassenden Aktivitätsprotokoll über den Sicherheitsvorfall zusammen.
8.2	Verteilen Sie dieses Protokoll zur Überprüfung und Zustimmung an die vom Vorfall Betroffenen. (Einschließlich rechtlicher Überprüfung zur Eignung als Beweismittel).
8.3	Untersuchen Sie die Ursachen für die Sicherheitsverletzung, und verbessern Sie die Schutzmaßnahmen, um erneute Eindringversuche und damit verbundene Angriffe in Zukunft zu verhindern.
8.4	Helfen Sie der Finanzabteilung bei der Berechnung der Kosten für die Sicherheitsverletzung.
8.5	Bereiten Sie einen Bericht für die Geschäftsleitung und andere Ansprechpartner vor, in dem Sie die Ursachen des Ereignisses, die Kosten der Sicherheitsverletzung und die für die Zukunft geplanten Schutzmaßnahmen erläutern.