Originaltitel: Chapter 1 – Introduction

1

Einführung

Willkommen beim *Betriebshandbuch zur Sicherheit von Microsoft® Exchange 2000 Server* bzw. *Security Operations Guide for Microsoft® Exchange 2000 Server* (englischsprachig). In diesem Handbuch werden die Schritte beschrieben, die Sie zur täglichen, optimalen Absicherung Ihrer Exchange Server-Umgebung ausführen sollten.

Der Inhalt dieses Handbuchs dient als Ergänzung zu *Security Operations for Microsoft® Windows® 2000 Server* (Microsoft Press, ISBN: 0-7356-1823-2; bisher nur englischsprachig veröffentlicht). Wir empfehlen Ihnen, vor der Lektüre des vorliegenden Handbuchs das oben genannte Handbuch zu lesen. Einige Abschnitte im vorliegenden Handbuch werden sich direkt auf Informationen in *Security Operations for Microsoft® Windows® 2000 Server* (englischsprachig) beziehen. Darüber hinaus empfehlen wir Ihnen die Lektüre von *Microsoft® Exchange 2000 Server Operations* (Microsoft Press, ISBN: 0-7356-1831-3; bisher nur englischsprachig veröffentlicht). In diesem Buch werden weitere allgemeine Informationen zu Exchange 2000 Server bereitgestellt.

Microsoft Operations Framework

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 Ihnen bei der Leitung Ihres Unternehmens helfen. Das Befolgen der MOF-Richtlinien soll Ihnen dabei helfen, die Sicherheit, Zuverlässigkeit, Verfügbarkeit, Unterstützungsfähigkeit und Verwaltbarkeit unternehmenswichtiger Produktionssysteme dauerhaft sicherzustellen.

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.

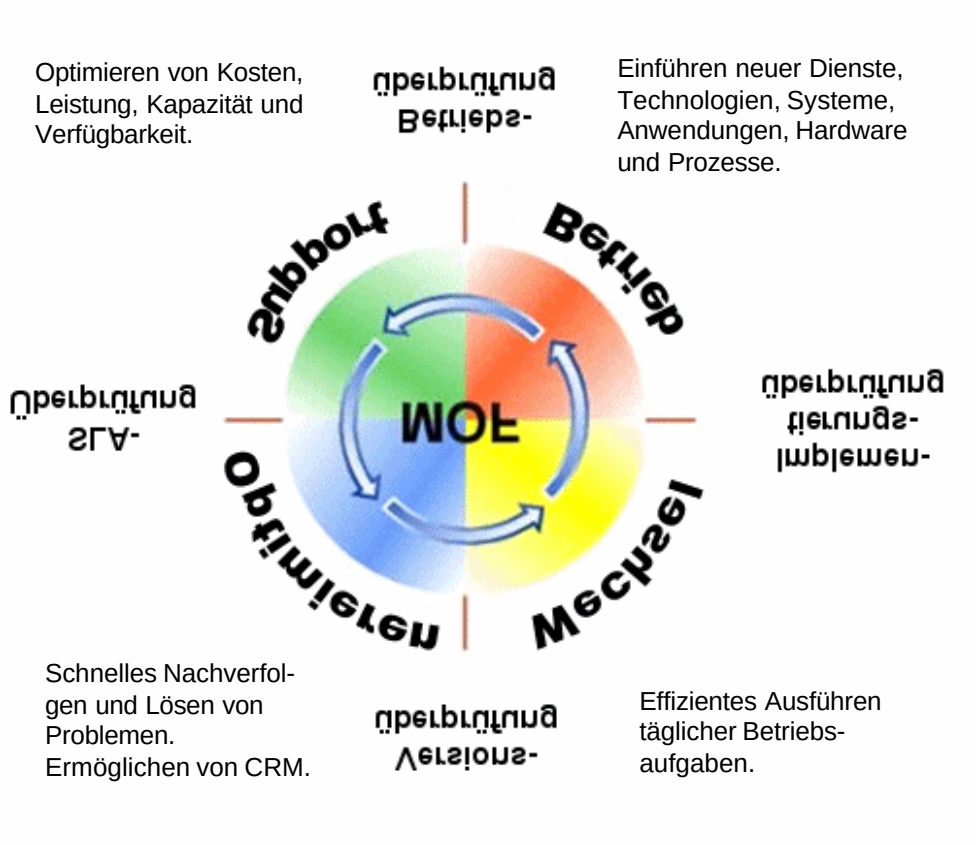

Abbildung 1.1
MOF-Lebenszyklus

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 (Operations Management; auch Überprüfungsmeilenstein genannt) unterstützt. Dabei werden die SMFs 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 erfahren möchten oder wissen wollen, wie MOF Ihnen im Unternehmen helfen kann, besuchen Sie die Microsoft Operations Framework-Website. Weitere Informationen finden Sie im Abschnitt "Weitere Informationen" am Ende dieses Kapitels.

Get Secure und Stay Secure

Im Oktober 2001 hat Microsoft eine neue Initiative gestartet: das Strategic Technology Protection Program (STPP). Mit diesem Programm sollen Produkte, Dienste und Support von Microsoft 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 zum Toolkit und zu STPP finden Sie im Abschnitt "Weitere Informationen".)

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 ausgeführt 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 ggf. effektiv reagieren zu können.

Umfang dieses Handbuchs

In diesem Handbuch werden schwerpunktmäßig die Arbeitsschritte behandelt, die zum Erstellen und Warten einer sicheren Umgebung auf Computern mit Exchange 2000 Server erforderlich sind. Dabei werden zwei bestimmte für Server definierte Rollen untersucht – OWA-Front-End- und -Back-End-Server (Outlook Web Access). Wir werden nicht darauf eingehen, wie Internet Message Access Protocol 4 (IMAP4) oder Post Office Protocol 3 (POP3) sicher ausgeführt 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. In der folgenden Abbildung ist eine Übersicht über diese Bereiche dargestellt. Das im dunkel schattierten Feld mit weißer Schrift aufgeführte Thema wird in diesem Handbuch behandelt. Die in den übrigen Feldern aufgeführten Themen werden im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* bzw. *Security Operations Guide for Windows 2000 Server* (englischsprachig) behandelt.

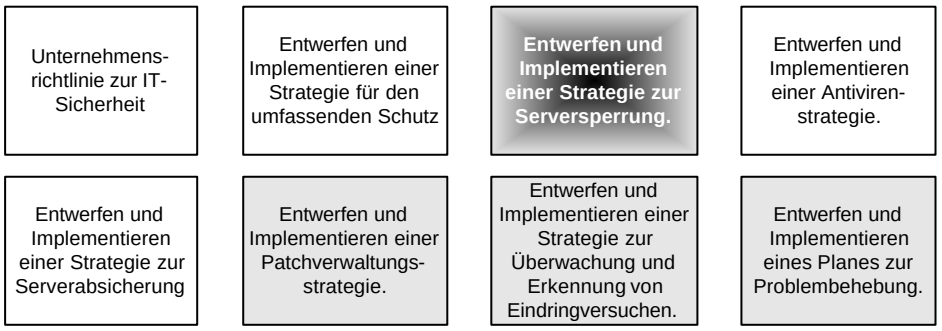

Abbildung 1.2

Umfang des vorliegenden Handbuchs hinsichtlich der umfassenden Sicherheitsstrategie für Exchange

---

Hinweis: *Das Betriebshandbuch zur Sicherheit von Microsoft® Exchange 2000 Server* bzw. *Security Operations Guide for Microsoft® Exchange 2000 Server* (englischsprachig) ist online verfügbar. Weitere Informationen finden Sie im Abschnitt "Weitere Informationen" am Ende dieses Kapitels.

In der Abbildung werden die Schritte gezeigt, die erforderlich sind, um für einen Server Sicherheit zu schaffen (Get Secure) und um die Sicherheit zu wahren (Stay Secure). Es wird auch dargestellt, wie die Kapitel dieses Handbuchs sowie die des *Betriebshandbuchs zur Sicherheit von Windows 2000 Server* bzw. *Security Operations Guide for Windows 2000 Server* (englischsprachig) Ihnen dabei helfen, diese Ziele zu erreichen.

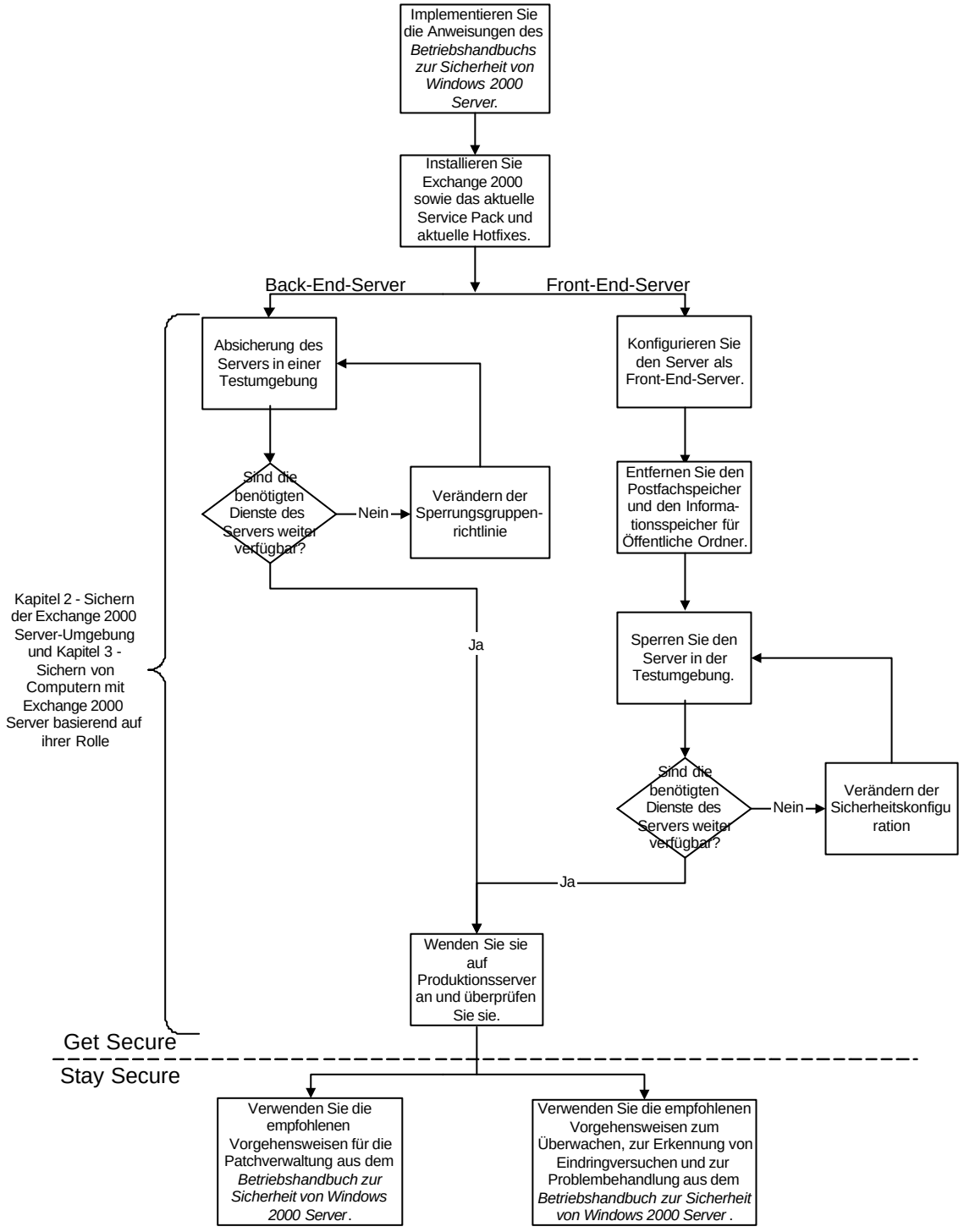

Abbildung 1.3

Prozessflussdiagramm zu den einzelnen Phasen von "Get Secure" und "Stay Secure"

Zusammenfassung der Kapitel

Dies es 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 – Absichern der Exchange 2000 Server-Umgebung

Exchange ist eine komplexe Anwendung mit vielen Komponenten, die voneinander abhängen. Zum erfolgreichen Absichern von Exchange sollten Sie diese Zusammenhänge kennen und bei Ihrem Sicherheitsentwurf berücksichtigen. In diesem Kapitel werden allgemeine Risiken für Exchange 2000 Server-Umgebungen beschrieben. Darüber hinaus werden die beiden Serverrollen vorgestellt, die in den nachfolgenden Kapiteln beschrieben werden: Back-End- und Front-End-Server. Dabei werden auch Hyperlinks zum *Betriebshandbuch zur Sicherheit von Windows 2000 Server* bzw. *Security Operations Guide for Microsoft Windows 2000 Server* (englischsprachig) bereitgestellt, in dem die Vorgehensweise beim Implementieren der Sicherheit für diese Servertypen beschrieben wird.

Kapitel 3 – Absichern von Computern mit Exchange 2000 Server basierend auf ihrer Rolle

In diesem Kapitel werden das Absichern der Back-End-Serverrolle und der OWA-Front-End-Serverrolle (Outlook Web Access) und die erforderlichen Schritte zum Erhöhen der Sicherheit beschrieben. Dabei wird untersucht, welche Änderungen Sie zum Absichern einer Windows 2000-Umgebung ausführen müssen, um einen Computer mit Exchange 2000 Server so sicher wie möglich auszuführen.

Kapitel 4 – Absichern der Exchange-Kommunikation

In diesem Kapitel wird das Absichern der Kommunikation zwischen Clients und Exchange 2000 Server beschrieben, z. B. das Absichern der Kommunikation zwischen Outlook und Exchange. Dabei werden Überlegungen zu Firewalls bei der Positionierung von OWA-Servern untersucht. Darüber hinaus wird das Absichern des Datenverkehrs vom OWA-Server zum Client und vom OWA-Server zu internen Back-End-Servern mit Exchange erläutert. Abgesehen davon wird das Absichern von SMTP-Datenverkehr beschrieben.

Zielgruppe dieses Handbuchs

Dieses Handbuch sollte von allen Personen gelesen werden, die für das Absichern von Exchange 2000 Server in ihren Unternehmen verantwortlich sind und über allgemeine Kenntnisse bezüglich Windows 2000 sowie bezüglich der Grundlagen der IT-Sicherheit verfügen.

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 ausgewählte Teile lesen möchten. Sie dürfen nicht vergessen, dass für effektive und erfolgreiche Sicherheitsvorkehrungen Anstrengungen in allen Bereichen erforderlich sind, nicht nur Verbesserungen in einem einzelnen 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 bzw. http://www.microsoft.com/mof (englischsprachig)

Informationen zu Strategic Technology Protection Program (STPP)

http://www.microsoft.com/germany/themen/security/default.htm bzw. http://www.microsoft.com/security/mstpp.asp (englischsprachig)

Microsoft -Sicherheitstoolkit bzw. Microsoft Security Toolkit (englischsprachig):

http://www.microsoft.com/germany/ms/technetdatenbank/overview.asp?siteid=543003 bzw. http://www.microsoft.com/technet/security/tools/stkintro.asp (englischsprachig)

Website für das Microsoft Strategic Technology Protection Program:

http://www.microsoft.com/germany/themen/security/default.htm bzw. http://microsoft.com/security/mstpp.asp (englischsprachig)

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

http://www.microsoft.com/germany/ms/technetdatenbank/overview.asp?siteid=430926 bzw. http://www.microsoft.com/technet/security/bulletin/notify.asp (englischsprachig)

Betriebshandbuch zur Sicherheit von Windows 2000 Server bzw. *Security Operations Guide for Windows 2000 Server* (englischsprachig)

http://www.microsoft.com/technet/security/prodtech/windows/windows2000/staysecure/default.asp bzw. http://www.microsoft.com/technet/security/prodtech/windows/windows2000/staysecure/default.asp (englischsprachig)

Exchange 2000 Server-Betriebshandbuch bzw. *Exchange 2000 Server Operations Guide* (englischsprachig)

http://www.microsoft.com/germany/ms/technetdatenbank/overview.asp?siteid=446985 bzw. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/exchange/exchange2000/maintain/operate/opsguide/default.asp (englischsprachig)

Originaltitel: Chapter 2 – Securing Your Exchange Environment

2

Absichern der Exchange 2000 Server-Umgebung

Viele Organisationen verwenden bei der Erstellung einiger ihrer wichtigen Geschäftsprozesse die Funktionalität von Microsoft Exchange. Es kann sehr problematisch sein, wenn die von Exchange bereitgestellten Dienste nicht zur Verfügung stehen (E-Mail, Kalender, Kontaktinformationen, miteinander verbundene Anwendungen usw.).

Ein Risiko für fortlaufend ausgeführte Exchange 2000 Server-Operationen sind Angriffe von innerhalb oder außerhalb der Organisation. Dieses Risiko ist für Exchange besonders groß, weil dort viele Zugriffsmöglichkeiten bestehen. Es ist möglich, dass fast alle Personen innerhalb Ihrer Organisation auf Exchange zugreifen können. Sie können sogar den Zugriff über das Internet ermöglichen.

In diesem Kapitel untersuchen wir viele Schritte, die Sie ausführen können, um das Risiko eines Angriffs auf die Exchange 2000 Server-Umgebung zu minimieren.

Hinweis: Wenn Sie Änderungen an der Exchange 2000 Server-Umgebung vornehmen, ist es wichtig, jede dieser Änderungen genau zu dokumentieren. Weitere Informationen zum Change Management und Configuration Management finden Sie im *Exchange 2000 Server-Betriebshandbuch* bzw. *Exchange 2000 Server Operations Guide* (englischsprachig). Darüber hinaus finden Sie Informationen im Abschnitt "Weitere Informationen" am Ende dieses Kapitels.

Allgemeine Überlegungen zur Sicherheit von Exchange

Bei Überlegungen bezüglich einer Erhöhung der Sicherheit von Exchange ist zu berücksichtigen, dass es sich bei Exchange um eine Reihe von Diensten handelt, die auf lokalen Computern und Remotecomputern ausgeführt werden und miteinander kommunizieren. Dabei gilt insbesondere, dass Computer mit Exchange Server mit anderen Computern mit Exchange Server, Domänencontrollern sowie einer Reihe verschiedener Clients kommunizieren müssen. IIS bildet die Grundlage für die Funktionalität von Exchange.Auf Computer mit Exchange Server kann sogar über das Dateisystem zugegriffen werden. Aufgrund dieser komplizierten Beziehungen sollten Sie beim Absichern eines Computers mit Exchange Server einige unterschiedliche Aspekte berücksichtigen. Dazu zählen folgende Aspekte:

Dienstsicherheit

Dateisicherheit

IIS-Sicherheit

Registrierungseinträge

Zugrunde liegende Windows 2000-Sicherheit

Sicherheit der Domänencontroller und des globalen Katalogs

Active Directory-Sicherheit

Sicherheit der Exchange-Datenbank

Mechanismen des Exchange-Transports

Exchange-Dienstabhängigkeiten

Dieses Handbuch soll Ihnen beim Absichern der Exchange 2000 Server-Umgebung größtmögliche Hilfestellung bieten, ohne dass dabei die Hauptfunktionalität von Exchange beeinträchtigt wird. Dabei sollten u. a. die Exchange-Dienste besonders berücksichtigt werden. Exchange wird unter Windows 2000 ausgeführt. Zur Installation des Produkts oder zu dessen fortlaufender korrekter Funktionsweise sind einige Windows 2000-Dienste erforderlich. Darüber hinaus hängen einige Exchange-Dienste auch von anderen Exchange-Diensten ab.

In der folgenden Abbildung sind die Dienste, die standardmäßig auf einem Computer mit Exchange Server ausgeführt werden, sowie deren Abhängigkeiten untereinander dargestellt.

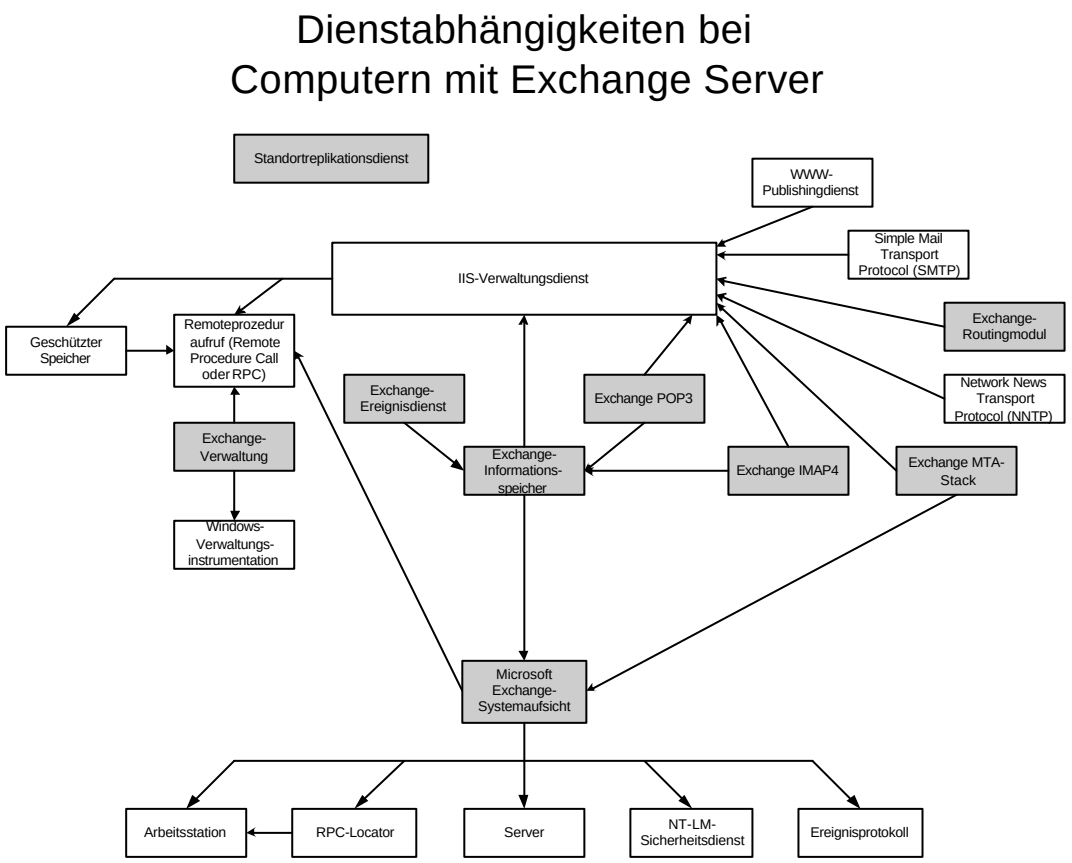

Abbildung 2.1

Dienstabhängigkeiten bei Computern mit Exchange Server

Im vorliegenden Handbuch geben wir Empfehlungen bezüglich der Einstellungen für viele dieser Dienste, die normalerweise so konfiguriert sind, dass sie standardmäßig automatisch starten. Sie können einige dieser Dienste deaktivieren. Dadurch wird allerdings die Funktionalität des Servers verringert. Sie müssen entscheiden, ob diese Funktionalitätseinbuße für Ihre Umgebung akzeptiert werden kann.

Installieren von Exchange

Exchange 2000 Server ist eine schemaverändernde Anwendung. Das bedeutet, dass der Schemacontainer von Active Directory bei der Ausführung von Setup/ForestPrep geändert wird. Dementsprechend wird der Konfigurationscontainer nach der Installation aller Computer mit Exchange 2000 Server so geändert, dass er die entsprechenden Exchange 2000 Server-Objekte enthält. Das bedeutet, dass für das Setup /ForestPrep ausführende Konto Schema-Admin-Berechtigungen benötigt werden, während für die Konten, die zur Installation von Exchange verwendet werden, die vollständigen Exchange-Administratorberechtigungen erforderlich sind. Zusätzlich werden für die Installation eines Exchange Servers auch lokale Administrationsrechte benötigt.

Hinweis: Weitere Informationen zu Exchange 2000 Server-Berechtigungen finden Sie in *Microsoft Exchange 2000 Internals: Permissions Guide* (englischsprachig). Darüber hinaus finden Sie Informationen im Abschnitt "Weitere Informationen" am Ende dieses Kapitels.

Wie bei allen Aspekten der Berechtigungsverwaltung sollten Sie sicherstellen, dass Administratoren nur über die Rechte verfügen, die zur Erledigung ihrer Aufgaben erforderlich sind. Weit reichende Berechtigungen sollten besonders gut geschützt werden, d. h. nur wenigen Personen zur Verfügung stehen. Es empfiehlt sich, dass die Gruppe der Schema-Admins standardmäßig keine Benutzer enthält und diese nur zur Ausführung von Setup /ForestPrep hinzugefügt werden. Diese Vorgehensweise ist sehr verbreitet und stellt sicher, dass Sie immer gewarnt werden, bevor eine Anwendung das Schema ändert.
Im Rahmen der Ausführung von Setup /ForestPrep erhält der Schemaadministrator die Möglichkeit, ein Exchange 2000 Server-Administratorkonto anzugeben. Diesem Konto werden die vollständigen Exchange-Administratorberechtigungen über die Exchange-Organisation erteilt, die die Ausführung späterer Exchange-Installationen ermöglichen. Eine Möglichkeit, die Sicherheitsrisiken während der Installation zu minimieren, ist die Erstellung einer bestimmten universellen Sicherheitsgruppe, die zur Installation von Exchange berechtigt ist. Anschließend können Sie der Gruppe vollständige Exchange-Administratorberechtigungen erteilen. Wenn Sie die Mitgliedschaft der Gruppe überwachen, können Sie genau kontrollieren, wer Exchange installieren kann.

Exchange 2000 Server-Patchverwaltung

Um Exchange dauerhaft abzusichern, müssen Sie immer die aktuellen Patches installieren. Dies betrifft zwei Bereiche – sowohl das Betriebssystem als auch Exchange müssen aktualisiert werden. Wenn das Betriebssystem Schwachstellen aufweist, betrifft das auch Exchange. Daher sollten Sie die Sicherheit des Betriebssystems auf Computern mit Exchange besonders ernst nehmen.

Es gibt eine Reihe von Dienstprogrammen, die Ihnen aktuelle Informationen zu Windows 2000-Service Packs, -Hotfixes und -Patches liefern. Microsoft stellt in diesem Zusammenhang zwei Dienstprogramme bereit – Hfnetchk und Microsoft Baseline Security Analyzer (MBSA).

Seit der Veröffentlichung von Windows 2000 Service Pack 2 und höher wurden mehrere Sicherheitsupdates bereitgestellt. Viele davon wurden im Security Rollup Package für Windows 2000 zusammengestellt. Weiterführende Informationen dazu finden Sie am Ende dieses Kapitels im Abschnitt "Weitere Informationen". Darüber hinaus sollten Sie sich stets über aktuelle Schwachstellen im Zusammenhang mit IIS und Internet Explorer informieren.

Exchange 2000 Server weist seltener Schwachstellen auf als Windows 2000 und diese werden nicht von den in diesem Abschnitt erwähnten Tools gemeldet. Sie sollten sicherstellen, dass Sie von Microsoft über neue Patches für Ihre Umgebung informiert werden. Wenn Sie Microsoft-Sicherheitsbulletins abonnieren, erhalten Sie diese Benachrichtigungen automatisch.

Hinweis: Informationen dazu, wie Sie Microsoft-Sicherheitsbulletins erhalten, finden Sie im Abschnitt "Weitere Informationen" am Ende dieses Kapitels.

Hinweis: Weiterführende Informationen zur Patchverwaltung in einer Windows 2000-Umgebung finden Sie im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* bzw. *Security Operations Guide for Windows 2000 Server* (englischsprachig).

Hinweis: Informationen zur empfohlenen Konfiguration und zu Aktualisierungen für Exchange 2000 Server finden Sie im Abschnitt "Weitere Informationen" am Ende dieses Kapitels.

Absichern der Clientumgebung

Exchange 2000 Server ist eine Client/Server-Anwendung. Daher ist es sehr wichtig, dass Sie bei Überlegungen zur umfassenden Sicherheit der Exchange-Umgebung auch die Clients untersuchen, die verwendet werden sollen.

Exchange unterstützt eine große Anzahl unterschiedlicher Clients. Im Zusammenhang mit Ihrer Risikomanagementstrategie sollten Sie untersuchen, welche Clients tatsächlich benötigt werden und sich auf diese beschränken. Stellen Sie sicher, dass Sie die aktuelle Version und Patchversionen der Clientsoftware verwenden. Darüber hinaus sollten Sie regelmäßig Clientsicherheitsupdates installieren, da diese genauso wichtig sein können wie der Server.

Benutzer spielen beim Absichern von Clients eine wichtige Rolle. Wenn Sie Benutzer schulen, Clients auf vernünftige Weise zu verwenden, können Sie das Angriffsrisiko verringern. Benutzer sollten beispielsweise über E-Mail-Viren, Virus-Hoaxes, Kettenbriefe und unerwünschte E-Mails informiert werden.

Hinweis: Informationen zum Absichern der Kommunikation zwischen Client und Server finden Sie in Kapitel 4, "Absichern der Exchange-Kommunikation".

Schutzmaßnahmen gegen Adressenspoofing

Eine der verbreitetsten Methoden zum Angreifen eines Mailsystems ist das Manipulieren der Absenderangabe. SMTP (Simple Mail Transfer Protocol) überprüft nicht die Identität von Benutzern, aber Sie können in Exchange einige Aktionen durchführen, um das Risiko von Nachrichtenspoofing zu minimieren.

Eines der schlimmsten Probleme beim Adressenspoofing (Adressenfälschung) ist, wenn externe Angreifer die E-Mail-Adresse eines internen Benutzers verwenden. Dies kann auf verschiedene Arten erfolgen, häufig als eine Form von Social Engineering, um andere Benutzer zu überzeugen, vertrauliche Informationen bekannt zu geben, wodurch wiederum weitere Angriffe ermöglicht werden.

Exchange 2000 Server wird standardmäßig eine E-Mail-Adresse im Adressbuch zu dem in der Globalen Adressliste verwendeten Namen auflösen. Dadurch kann es sehr schwierig zu beurteilen sein, ob eine Nachricht von außerhalb der Organisation gesendet wurde. Sie können die Standardkonfiguration ändern, so dass Mails von außerhalb der Organisation nicht aufgelöst werden. Wenn Sie die Benutzer anschließend dahin gehend schulen, dass sie nach nicht

aufgelösten E-Mail-Adressen suchen, wird es dabei helfen, sich gegen diese Form von Adressenspoofing zu schützen.

Anmerkung: Weitere Informationen dazu, wie Sie sicherstellen können, dass E-Mails von außerhalb der Exchange-Organisation nicht aufgelöst werden, finden Sie im Knowledge Base-Artikel Q288635, "XIMS: ResolveP2 Functionality in Exchange 2000 Server" (englischsprachig).

Wenn Sie Nachrichten direkt von anderen Domänen im Internet erhalten, können Sie Ihren virtuellen SMTP-Server so konfigurieren, dass ein Reverse-DNS-Lookup (Domain Name System) für eingehende E-Mail-Nachrichten durchgeführt wird. Auf diese Weise wird überprüft, ob die IP-Adresse (Internet Protocol) für den Mailserver des Absenders sowie der voll qualifizierte Domänenname dem in der Nachricht aufgeführten Domänennamen entsprechen.

Reverse-Lookup führt zu einer zusätzlichen Belastung des Computers mit Exchange Server. Darüber hinaus ist es notwendig, dass der Computer mit Exchange Server sich mit der Reverse-Lookup-Zone der sendenden Domäne in Verbindung setzen kann.

Hinweis: Weitere Informationen zur Verwendung von Reverse-DNS-Lookup finden Sie im Knowledge Base-Artikel Q319356, "HOW TO: Prevent Unsolicited Commercial E-Mail in Exchange 2000 Server" (englischsprachig).

Schutzmaßnahmen gegen Viren

Eine der größeren Bedrohungen für Ihre Umgebung sind Viren, die per E-Mail übertragen werden. E-Mail-Viren können das Computersystem oder die E-Mail-Umgebung angreifen, indem sie das System mit Nachrichten überhäufen, bis es überlastet ist. Sie können sicherstellen, dass Sie in Ihrer Umgebung über ausreichende Schutzmaßnahmen gegen Viren verfügen.

Sie sollten Schutzmaßnahmen gegen Viren an folgenden Stellen implementieren: dem Firewall, am und außerhalb des SMTP-Gateways, an jedem Computer mit Exchange Server und an jedem Client.

Hinweis: Weitere Informationen zu Anti-Virus-Software für Computer mit Exchange Server finden Sie im Knowledge Base-Artikel Q245822, "XGEN: Recommendations for Troubleshooting an Exchange Computer with Antivirus Software Installed" (englischsprachig).

Auf Clientebene blockiert Outlook 2002 viele Anlagen und verhindert dadurch, dass sie von Benutzern angezeigt werden und möglicherweise Schäden an Ihrer Umgebung verursachen. Sie sollten allerdings daran denken, dass bei der Aktivierung von Outlook Web Access (OWA) diese Anlagen nicht vom OWA-Client blockiert werden.

Hinweis: Weitere Informationen zu Schutzmaßnahmen gegen Virusangriffe und zur Vorgehensweise bei Vorfällen finden Sie im *Exchange 2000 Server-Betriebshandbuch* bzw. *Exchange 2000 Server Operations Guide* (englischsprachig)

Schutzmaßnahmen gegen unerwünschte E-Mails (Spammails)

Unerwünschte E-Mails können für viele Organisationen ein großes Problem darstellen. Sie sind in vielerlei Hinsicht sehr kostenintensiv: von der Zeit, die Benutzer durch die Beschäftigung mit solchen Mails verlieren, bis zu der Bandbreite und dem Speicherplatz, der durch die Übertragung und Speicherung dieser unwichtigen E-Mails belegt wird.

Es kann sehr schwierig sein, sich gegen Angriffe in Form unerwünschter E-Mails zu schützen. Es gibt allerdings eine Reihe von Maßnahmen, die Sie ergreifen können, um die Anzahl der eintreffenden unerwünschten E-Mails zu verringern.

Schulen von Benutzern

Die Benutzer innerhalb des Netzwerks spielen beim Schutz gegen unerwünschte E-Mails eine wichtige Rolle. Diese Art von Mail ist häufig das Ergebnis von Social Engineering innerhalb Ihres Netzwerks, und es ist wichtig, die Benutzer dahin gehend zu schulen, wie sie sich dagegen schützen können. Unerwünschte E-Mails können beispielsweise eine Verzichtserklärung enthalten, die besagt, dass Sie sich von der Adressenliste entfernen lassen können, indem Sie auf die Mail antworten und "Entfernen" in die Betreffzeile schreiben. In den meisten Fällen ist dies nur eine Methode, um zu überprüfen, ob eine E-Mail-Adresse gültig ist, so dass sie wieder angeschrieben werden kann. Benutzer sollten dahin gehend geschult werden, dass sie auf keinen Fall auf unerwünschte E-Mails antworten dürfen. Darüber hinaus sollten sie unerwünschte E-Mails nicht an Kollegen weiterleiten.

Features in Outlook 2002 gegen unerwünschte E-Mails

Outlook 2002 enthält einige Features, die Ihnen dabei helfen werden, sich gegen unerwünschte E-Mails zu schützen. Outlook kann in E-Mails nach bestimmten Sätzen suchen und entsprechende E-Mails automatisch aus dem **Posteingang** in einen von Ihnen angegebenen Ordner verschieben, einschließlich des von Outlook erstellten Ordners für Junk-E-Mails oder des Ordners **Gelöschte Objekte**. Outlook speichert die Liste der Ausdrücke, die beim Filtern nach unerwünschten E-Mails verwendet werden, für Absenderadressen in der Datei **JunkSenders.txt** und für Dateiinhalte in der Datei **AdultContentSenders.txt**. Diese Dateien enthalten eine Liste von Absendern unerwünschter E-Mails. Sie enthalten auch Sätze, bei deren Verwendung in einer E-Mail diese wie eine unerwünschte E-Mail behandelt wird.

Wenn Sie anfangen, diese Features zu verwenden, sollten Sie sicherstellen, dass die Benutzer alle Nachrichten überprüfen, die aus dem **Posteingang** entfernt wurden, damit nicht versehentlich gültige Nachrichten entfernt werden.

Hinweis: Weitere Informationen zum Schutz vor unerwünschten E-Mails in Outlook 2002 finden Sie im Artikel "Verwalten von Junk-E-Mails und nicht jugendfreiem Inhalt in Outlook 2002" bzw. "Manage Junk and Adult Content Mail in Outlook 2002" (englischsprachig) im Microsoft Office Hilfecenter (Microsoft Office Assistance Center). Darüber hinaus finden Sie weiterführende Informationen im Abschnitt "Weitere Informationen".

Features in Exchange 2000 Server gegen unerwünschte E-Mails

Einige Features von Exchange 2000 Server können Ihnen dabei helfen, sich gegen unerwünschte E-Mails zu schützen. Insbesondere können Sie verhindern, dass E-Mails übermittelt werden, wenn kein Absender angegeben ist oder wenn die E-Mail von einer der mehreren bestimmten Domänen gesendet wurde. Sie können auf allen Computern mit Exchange Server filtern oder einen bestimmten virtuellen SMTP-Server ermitteln, der das Filtern ausführt.

Hinweis: Weitere Informationen zum Filtern von unerwünschten E-Mails mithilfe von Exchange 2000 Server finden Sie in dem Knowledge Base-Artikel Q276321, "XADM, How to Filter Junk Mail in Exchange 2000" (englischsprachig).

Hinweis: Darüber hinaus können Sie sich gegen unerwartete E-Mails schützen, indem Sie die Nachrichtenüberwachung verwenden. Dieses Thema wird in Kapitel 4, "Absichern der Exchange-Kommunikation" beschrieben.

Schutzmaßnahmen gegen DoS-Angriffe

Im Allgemeinen ist es nicht einfach, sich gegen DoS-Angriffe (Denial-of-Service) zu schützen. Es gibt bei Exchange allerdings eine Reihe von Einstellungen, die diese Aufgabe erleichtern können. Die auf dem virtuellen SMTP-Server konfigurierten Parameter für die Nachrichtengröße ermöglichen Ihnen, eine maximale Anzahl von Empfängern pro Nachricht, eine maximale Nachrichtengröße, eine maximale Anzahl von Nachrichten pro Verbindung usw. anzugeben. Diese Beschränkungen werden Ihnen dabei helfen, sicherzustellen, dass ein DoS-Angriff mithilfe des Mailtransports der SMTP-Dienste sehr schwierig wird.

Hinweis: Weitere Informationen zum Festlegen von Parametern für die Nachrichtengröße finden Sie im Knowledge-Base-Artikel Q319356, "HOW TO: Prevent Unsolicited Commercial E-Mail in Exchange 2000 Server" (englischsprachig).

Eine andere Form von DoS-Angriffen könnte darin bestehen, dass eine große Anzahl von E-Mails zu einem bestimmten Server gesendet wird, bis der Speicherplatz des Servers belegt ist. Sie können das Risiko eines solchen Angriffs möglichst gering halten, indem Sie Speichergrenzwerte für Postfächer und Öffentliche Ordner festlegen.

Hinweis: Weitere Informationen zum Festlegen von Speichergrenzwerten finden Sie im Knowledge-Base-Artikel Q319583, "HOW TO: Configure Storage Limits on Mailboxes in Exchange 2000" (englischsprachig).

Steuern des Zugriffs auf Exchange 2000 Server mithilfe von Berechtigungen und administrativen Gruppen

Wie auch bei allen anderen Anwendungen in Ihrer Umgebung sollten Sie beim Definieren der Berechtigungen für Exchange die Funktionen des Exchange-Administrators innerhalb der Umgebung überprüfen und ihm nur die erforderlichen Berechtigungen erteilen. Um diesen Prozess zu vereinfachen, verwendet Exchange 2000 Server administrative Gruppen. Eine administrative Gruppe ist eine Sammlung von Exchange 2000 Server-Objekten, die zum Verwalten und Delegieren von Berechtigungen gesammelt werden. Eine administrative Gruppe kann Richtlinien, Routinggruppen, Öffentliche Ordner-Hierarchien, Server, Konferenzobjekte und Chat-Netzwerke enthalten. Wenn Ihre Organisation beispielsweise über zwei Administratorenteams verfügt, die Ihre Exchange-2000-Server-Umgebung verwalten, können Sie zwei administrative Gruppen erstellen und Ihre Exchange Server auf diese administrativen Gruppen aufteilen. Jedes Administratorenteam erhält nur die Exchangeadministrationsrechte für die eigene administrative Gruppe. Abhängig von dem Verwaltungsmodell, das Ihre Organisation verwendet, können Sie einen Verwaltungsplan entwickeln, der Ihren Ansprüchen gerecht wird.

Die einfachste Möglichkeit, administrativen Gruppen (und der Exchange-Organisation) Berechtigungen zuzuweisen, besteht in der Verwendung des Assistenten für die Zuweisung von Verwaltungsberechtigungen auf Exchange-Objekte. Sie müssen sich als Benutzer mit Vollzugriff für die Exchange-Organisation anmelden, um den Assistenten zu verwenden. Um den Assistenten für die Zuweisung von Verwaltungsberechtigungen auf Exchange-Objekte zu starten, müssen Sie mit der rechten Maustaste auf die Organisation oder die administrative Gruppe im Exchange-System-Manager und anschließend auf **Objektverwaltung zuweisen** klicken.

Es gibt drei administrative Funktionen:

Tabelle 2.1: Administrative Funktionen bei Exchange 2000 Server

Funktion	Beschreibung
Exchange-Administrator - Nur Ansicht	Erteilt Berechtigungen zum Auflisten und Lesen der Eigenschaften aller Objekte unterhalb dieses Containers. Weisen Sie immer diese Funktion zu, sofern der Administrator keine Objekteigenschaften ändern muss.
Exchange-Administrator	Erteilt alle Berechtigungen außer zum Übernehmen von Besitz und Ändern von Berechtigungen und verweigert das Öffnen von Benutzerpostfächern. Weisen Sie diese Funktion zu, sofern der Administrator keine Objekte hinzufügen oder Objekteigenschaften ändern, aber Berechtigungen für Objekte delegieren muss.
Exchange-Administrator - Vollständig	Erteilt Berechtigungen für alle Objekte unterhalb des Containers einschließlich der Möglichkeit, Berechtigungen zu ändern, verweigert jedoch das Öffnen von Benutzerpostfächern oder das Verwenden des Profils eines anderen Benutzers für dessen Postfach. Weisen Sie diese Funktion nur den Administratoren zu, die Berechtigungen für Objekte delegieren oder neue Server zur administrativen Gruppe hinzufügen müssen.

In einigen Fällen werden Sie bemerken, dass der Assistent für die Zuweisung von Verwaltungsberechtigungen auf Exchange-Objekte nicht immer das Maß an Granularität bereitstellt, das zum Absichern erforderlich ist. Sie können auf der Registerkarte **Sicherheit** die Einstellungen für jedes einzelne Objekt in Exchange ändern. Allerdings wird die Registerkarte **Sicherheit** standardmäßig nur für folgende Objekte angezeigt:

Adresslisten

Globale Adresslisten

Datenbanken (Postfachspeicher und Informationsspeicher für Öffentliche Ordner)

Oberste Öffentliche Ordner-Hierarchie

Sie müssen die Sicherheitsoptionen für andere Exchange-Objekte i .d . R. nicht ändern. Aber es ist möglich, die Registerkarte **Sicherheit** für alle Exchange-Objekte anzeigen zu lassen.

Hinweis: Seien Sie vorsichtig, wenn Sie Berechtigungen für Exchange-Objekte ändern. Wenn Berechtigungen fälschlicherweise verweigert werden, kann dies dazu führen, dass Exchange-Objekte im Exchange-System-Manager nicht angezeigt werden können.

▶ **Zum Anzeigen der Registerkarte "Sicherheit" für alle Exchange-Objekte**

1. Starten Sie **Regedt32.exe**.
2. Suchen Sie folgenden Schlüssel in der Registrierung:
   HKEY_CURRENT_USER\Software\Microsoft\Exchange\ExAdmin
3. Klicken Sie im Menü **Bearbeiten** auf **Wert hinzufügen**, und fügen Sie dann folgenden Registrierungswert hinzu.
   Wertname : ShowSecurityPage
   Datentyp : REG_DWORD
   Daten : 1
4. Schließen Sie den **Registrierungs-Editor**.

Diese Änderung wird sofort umgesetzt, ohne dass Sie den Exchange-System-Manager neu starten müssen.

Hinweis: Wenn Sie einen Schlüssel innerhalb von **HKEY_CURRENT_USER** ändern, wirkt sich die Änderung nur auf den gerade angemeldeten Benutzer des Computers aus, an dem Sie arbeiten.

Zentrale und verteilte Verwaltung

Im Allgemeinen gibt es für die Verwaltung zwei Hauptmodelle: zentrale und verteilte Verwaltung. Welches dieser Modelle Sie verwenden, hängt von den Anforderungen Ihrer Organisation ab.

Zentrales Verwaltungsmodell

Das einfachste Modell ist das zentrale Modell. Unternehmen, die dieses Modell verwenden, delegieren die Verwaltung der Computer mit Exchange Server an eine Person, Abteilung oder Gruppe. Um dieses Modell zu implementieren, müssen Sie eine einzige administrative Gruppe erstellen, die alle Exchange 2000-Objekte enthält und Berechtigungen für das Exchange 2000 Server-Organisationsobjekt zuweisen.

Verteiltes Verwaltungsmodell

Beim verteilten Modell werden mehrere administrative Gruppen erstellt, die logische Gruppierungen der Organisation darstellen. Bei diesen Gruppierungen kann es sich um geografische, politische oder andere Abteilungen der Organisation handeln. Eine Organisation kann beispielsweise über drei weit gehend autonome Geschäftsbereiche an einem Ort verfügen. Jeder Geschäftsbereich hat eine eigene IT-Abteilung und verfügt über eigenes IT-Personal, ein eigenes Budget und einen eigenen Verantwortungsbereich. Mithilfe des verteilten Verwaltungsmodells können sie ihre eigenen Exchange-Verwaltungsaufgaben verwalten.

Gemischtes Verwaltungsmodell

In der Realität gibt es selten eine rein zentrale oder eine rein verteilte Verwaltung, sondern eher eine Verwaltung mit einer stärkeren Ausrichtung zu einem der beiden Modelle. Ein sinnvolles Modell wäre, wenn bestimmte Konfigurationseinstellungen auf der Ebene der administrativen Gruppen und wichtiger Einstellungen zentral vorgenommen werden könnten. Dies ist beispielsweise der Fall, wenn Sie den Administratoren aller administrativen Gruppen die Berechtigung erteilen möchten, für die Wartung einen bestimmten Zeitrahmen festzulegen und gleichzeitig sicherstellen möchten, dass Nachrichtentracking und Speichergrenzwerte für Postfächer für die gesamte Organisation erzwungen werden.

Erstellen einer Umgebung für das gemischte Verwaltungsmodell

Zur Unterstützung des gemischten Verwaltungsmodells müssen eine Reihe von Schritten durchgeführt werden. Dazu zählen Folgende:

- Erstellen einer oder mehrerer administrativer Gruppen für die Objekte, die zentral verwaltet werden.
- Erstellen von Exchange-Systemrichtlinien zur zentralen Steuerung individueller Einstellungen.
- Zuweisen der geeigneten Sicherheitseinstellungen, um sicherzustellen, dass bestimmte Einstellungen von lokalen Administratoren nicht geändert werden können.

Erstellen administrativer Gruppen zur zentralen Steuerung

Für gewöhnlich werden administrative Gruppen zur Verwaltung von Servern verwendet. Wie bereits erwähnt, handelt es sich bei administrativen Gruppen um eine Sammlung von Objekten, die Sie für die Verwaltung zusammenstellen. Dies kann Ihnen dabei helfen, die Verwaltung der Exchange-Organisation zu steuern. Sie können sich beispielsweise entschließen, dass die routinemäßige Konfiguration von Computern mit Exchange Server von regionalen Administratoren durchgeführt werden soll. Dabei sollen allerdings Entscheidungen bezüglich des Routings sowie die Öffentliche Ordner-Hierarchie zentral gesteuert werden. Zu diesem Zweck müssten Sie eine administrative Gruppe erstellen und die Routinggruppen und die Öffentlichen Ordner zu dieser administrativen Gruppe verschieben. Wenn Sie dann die Berechtigungen für die administrative Gruppe angemessen steuern, können Sie verhindern, dass lokale Administratoren diese Elemente von Exchange ändern können.

Verwenden von Exchange-Systemrichtlinien für ein gemischtes Verwaltungsmodell

Sie können Exchange 2000 Server verwenden, um Richtlinien für die Konfiguration von Postfachspeichern, Informationsspeichern für Öffentliche Ordner sowie für die Konfiguration von Servern zu erstellen. Richtlinien können auf ein, mehrere oder alle entsprechenden Objekte in der Exchange-Organisation angewendet werden. Wenn Richtlinien gemeinsam mit den geeigneten Sicherheitseinstellungen angewendet werden, können Sie Richtlinien dazu verwenden, bestimmte Bereiche der Konfiguration zentral zu steuern und andere Eigenschaften lokal zu ändern. Zu den Einstellungen, die auf diese Weise konfiguriert werden können, zählen Nachrichtentracking und Grenzwerte für Postfächer.

Wir empfehlen Ihnen, Systemrichtlinien in Verbindung mit administrativen Gruppen zu verwenden. Wenn Sie die Richtlinien in einer eigenen Gruppe platzieren, können lokale Administratoren die Richtlinieneinstellungen nicht ändern, wenn sie nicht über Berechtigungen für diese administrative Gruppe verfügen.

In der folgenden Tabelle sind die Einstellungen für eine einfache Umgebung mit zwei administrativen Gruppen für die Serversteuerung aufgeführt. In diesem Beispiel haben jeweils Administratoren der administrativen Gruppen in London und New York die Steuerung über die Server beschränkt und können tägliche routinemäßige Änderungen vornehmen. Allerdings gelten für die Server Richtlinien, die die Administratoren nicht ändern können. Abgesehen davon haben sie keinen Einfluss auf die Verwaltung der Öffentlichen Ordner-Hierarchie oder des Routings zwischen Servern. Zusätzlich zu den in der Tabelle aufgeführten Berechtigungen erhalten die Administratoren der Gruppen A und B das Ansichtsrecht und die Administratoren der Verwaltung Vollzugriff auf die Exchange-Organisation.

Tabelle 2.2: Beispiel eines gemischten Verwaltungsmodells für Exchange 2000 Server

Name der administrativen Gruppe	Inhalt	Angewendete Richtlinien	Berechtigungen
Management	Container für Öffentliche Ordner Container für Routinggruppen Container für Systemrichtlinien	Keine	Exchange-Verwaltung – Vollzugriff erteilen Administrator der Gruppe A – Vollzugriff verweigern Administrator der Gruppe B – Vollzugriff verweigern
London	Server	Serverrichtlinie Richtlinie für Postfachspeicher Richtlinie für den Informationsspeicher für Öffentliche Ordner	Exchange-Verwaltung – Vollzugriff erteilen Administrator der Gruppe A – Vollzugriff erteilen
New York	Server	Serverrichtlinie Richtlinie für Postfachspeicher Richtlinie für den Informationsspeicher für Öffentliche Ordner	Exchange-Verwaltung – Vollzugriff erteilen Administrator der Gruppe B – Vollzugriff erteilen

Steuern der Benutzerverwaltung

Unter Exchange 2000 Server werden postfachaktivierte Benutzer sowie E-Mail-aktivierte Benutzer und Kontakte über das Snap-In **Active Directory-Benutzer und -Computer** gesteuert. Dies ermöglicht Ihnen, die Verwaltung von Benutzern und Computern auf der Ebene der Organisationseinheiten zu delegieren, getrennt von den übrigen Exchange-Bereichen, und so für die Steuerung eine höhere Granularität zu erreichen.

Hinweis: Um Exchange-Einstellungen für einen Benutzer zu ändern, muss der Administrator zumindest über die Berechtigung **Exchange-Administrator – Nur Ansicht** für die Exchange-Organisation verfügen.

Zusammenfassung

Es gibt viele Elemente zum Erhöhen der Sicherheit einer Exchange 2000 Server-Umgebung. Zunächst müssen Sie sicherstellen, dass die zugrunde liegende Windows-Umgebung möglichst sicher ist (weitere Informationen dazu finden Sie im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* bzw. *Security Operations Guide for Windows 2000 Server* [englischsprachig]). Dann müssen Sie Maßnahmen ergreifen, um die Sicherheit von Exchange 2000 Server zu erhöhen. Der Inhalt dieses Kapitels und der nachfolgenden Kapitel wird Ihnen dabei helfen.

Weitere Informationen

Exchange 2000 Server-Betriebshandbuch bzw. *Exchange 2000 Server Operations Guide*:

http://www.microsoft.com/germany/ms/technetdatenbank/overview.asp?siteid=446985 bzw. http://www.microsoft.com/technet/prodtechnol/exchange/exchange2000/maintain/operate/opsguide/default.asp (englischsprachig)

Microsoft Exchange 2000 Internals: Permissions Guide:

http://www.microsoft.com/technet/prodtechnol/exchange/exchange2000/deploy/depovg/exchperm.asp (englischsprachig)

Regelmäßig veröffentlichte Microsoft-Sicherheitsbulletins:

http://www.microsoft.com/germany/ms/technetservicedesk/Sicherheit.htm bzw. http://www.microsoft.com/technet/security/bulletin/notify.asp (englischsprachig)

Einzelheiten zum Security Rollup Package für Windows 2000 Server:

http://www.microsoft.com/technet/security/news/w2ksrp1.asp (englischsprachig)

Betriebshandbuch zur Sicherheit von Windows 2000 Server bzw. *Security Operations Guide for Windows 2000 Server* (englischsprachig):

http://www.microsoft.com/germany/ms/technetdatenbank/overview.asp?siteid=542484 bzw. http://www.microsoft.com/technet/security/prodtech/windows/windows2000/staysecure/DEFAULT.asp (englischsprachig)

Einzelheiten zur empfohlenen Konfiguration und zu empfohlenen Aktualisierungen für Exchange 2000 Server:

http://www.microsoft.com/Exchange/techinfo/deployment/2000/BestConfig.asp (englischsprachig)

Einzelheiten dazu, wie sichergestellt werden kann, dass E-Mails von außerhalb der Exchange-Organisation nicht aufgelöst werden:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q288635 (englischsprachig)

Einzelheiten zur Verwendung von Reverse-DNS-Lookup:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q319356 (englischsprachig)

Einzelheiten zum Verhindern unerwünschter E-Mails mit Outlook 2002:

http://office.microsoft.com/germany/Assistance/2002/articles/OlManageJunkAndAdultMail.aspx bzw. http://office.microsoft.com/assistance/2002/articles/OlManageJunkAndAdultMail.aspx (englischsprachig)

Einzelheiten zu Anti-Virus-Software für Computer mit Exchange Server:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q245822 (englischsprachig)

Einzelheiten zum Filtern unerwünschter E-Mails mit Exchange 2000 Server:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q276321 (englischsprachig)

Einzelheiten zum Festlegen von Speichergrenzwerten:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q319583 (englischsprachig)

Einzelheiten zu den Sicherheitsfeatures von Outlook 2002:

http://www.microsoft.com/germany/ms/officexp/security/default.htm bzw. http://www.microsoft.com/office/techinfo/administration/security.asp (englischsprachig)

Originaltitel: Chapter 3 – Securing Exchange 2000 Servers Based on Role

3

Absichern von Computern mit Exchange 2000 Server basierend auf ihrer Rolle

Im vorangegangenen Kapitel wurden einige allgemeine Empfehlungen zum Absichern der Exchange 2000 Server-Umgebung untersucht. Nun sollen die Einzelheiten hinsichtlich der Steigerung der Sicherheit der Computer mit Exchange 2000 Server basierend auf der Rolle, die sie in der IT-Umgebung ausüben, erläutert werden.

Das Gewährleisten der Sicherheit von Windows 2000 ist für die Sicherheit von Exchange 2000 Server wesentlich, da es sich bei Exchange 2000 Server um eine Anwendung handelt, die in einer Windows 2000-Umgebung ausgeführt wird. Im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* bzw. *Security Operations Guide for Windows 2000 Server* (englischsprachig) werden Empfehlungen für das Absichern bestimmter Serverrollen geboten, und dieses Kapitel erweitert die in diesem Handbuch ausgesprochenen Empfehlungen, um Exchange 2000 Server zu berücksichtigen. Insbesondere werden die OWA-Front-End-Serverrolle (Outlook Web Access) und die Serverrolle des Back-End-Servers mit Exchange untersucht.

Hinweis: Dieses Kapitel ergänzt die Empfehlungen, die in den Kapiteln 3 und 4 des *Betriebshandbuchs zur Sicherheit von Windows 2000 Server* bzw. *Security Operations Guide for Windows 2000 Server* (englischsprachig) ausgesprochen wurden. Informationen zu diesem Handbuch finden Sie im Abschnitt "Weitere Informationen" am Ende dieses Kapitels.

Testumgebung

Es ist wichtig, dass Sie alle Änderungen der Sicherheit Ihrer IT-Systeme in einer Testumgebung beurteilen, bevor Sie Änderungen 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 die Schwachstellen in der Testumgebung beurteilen.

Hinweis: Bevor die Schwachstellen in der Organisation beurteilt werden, sollten die dafür zuständigen Personen über eine entsprechende schriftliche Genehmigung verfügen.

Verwenden von OWA-Front-End- und Back-End-Servern

Jeder Computer mit Exchange 2000 Server besitzt standardmäßig OWA-Funktionen. Dadurch ist es Benutzern möglich, über HTTP (Hypertext Transfer Protocol) eine Verbindung zu ihrem Postfach auf dem Exchange 2000 Server herzustellen. Dies ist möglich, weil die Komponenten, aus denen die OWA-Lösung besteht, in einer Standardinstallation auf einem Computer mit Exchange Server installiert sind. In den meisten mittleren bis großen Umgebungen ist es jedoch besser, eine Front-End-/Back-End-Lösung zu implementieren, um den Zugriff auf OWA zu erlauben. In diesem Fall stellen Benutzer Verbindungen mit dem Front-End-Server her, der die Anforderung annimmt, die Anmeldeinformationen des Benutzers in Active Directory überprüft und die Anforderung dann an den entsprechenden Back-End-Server mit Exchange weiterleitet. Der Back-End-Server stellt den Zugriff auf Postfächer und Öffentliche Ordner zur Verfügung. Diese Vorgehensweise bietet die folgenden Vorteile:

- Benutzer müssen nicht den Namen des lokalen Computers mit Exchange Server kennen, um darauf zugreifen zu können.
- Die Namen der Server, die die Postfächer enthalten, sind verborgen.
- Für die Front-End-Server kann Lastenausgleich eingesetzt werden.
- SSL-Overhead (Secure Sockets Layer) kann an die Front-End-Server übergeben werden.
- Sie können die Back-End-Server hinter zusätzlichen Firewalls weiter absichern.

Hinweis: Front-End-Server können auch für Verbindungen über POP3 und IMAP4 verwendet werden. Dieses Handbuch geht jedoch davon aus, dass nur HTTP- und MAPI-Verbindungen aktiviert werden.

Hinweis: Eine ausführliche Darstellung von OWA-Front-End-/Back-End-Serverumgebungen in Exchange finden Sie im Abschnitt "Weitere Informationen" am Ende dieses Kapitels.

Absichern von Serverrollen für eine Exchange 2000 Server-Umgebung

Für dieses Handbuch stehen Sicherheitsvorlagen zur Verfügung, um die Sicherheit für die Serverrollen der Computer mit Exchange 2000 Server zu ändern. Sie müssen diese Vorlagen in die Gruppenrichtlinieneinstellungen importieren, damit diese auf Exchange angewendet werden können.

Die folgende Tabelle definiert die Serverrollen und die Vorlagen, die zum Steigern ihrer Sicherheit verwendet werden.

Tabelle 3.1: Serverrollen für Computer mit Exchange 2000 Server

Serverrolle	Beschreibung	Sicherheitsvorlagen
OWA-Server	Dedizierter OWA-Front-End-Server für Outlook Web Access	**Baseline.inf** und **OWA front-end Incremental.inf**
Back-End-Server mit Exchange 2000 Server	Server für Zugriff auf Postfach, Öffentliche Ordner und Routing	**Baseline.inf** und **Exchange back-end Incremental.inf**

Zusätzlich zu den oben genannten Vorlagen müssen Sie außerdem eine weitere Sicherheitsvorlage auf die Basisgruppenrichtlinie für Domänencontroller anwenden. Die im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* bzw. *Security Operations Guide for Windows 2000 Server* (englischsprachig) definierten Einstellungen gehen nicht davon aus, dass Exchange Teil Ihrer Umgebung ist, und erfordern aus diesem Grund Änderungen, um Exchange 2000 Server zu berücksichtigen.

Zum Ändern der Domänencontrollereinstellungen zur Unterstützung von Exchange-Operationen wird eine Vorlage **Exchange DC Incremental.inf** zur Verfügung gestellt. Diese sollte in ein Gruppenrichtlinienobjekt in der Organisationseinheit (Organizational Unit oder OU) **Domain Controllers** importiert werden. Tatsächlich wird nur eine Einstellung geändert – die in der Tabelle gezeigte Sicherheitsoption.

Tabelle 3.2: Sicherheitsoption auf Domänencontrollern für die Unterstützung von Exchange 2000 Server

Option	Sicherheitsoperationen für Windows 2000 Server	Sicherheitsoperationen für Exchange 2000 Server
Weitere Einschränkungen für anonyme Verbindungen	Kein Zugriff ohne ausdrückliche anonyme Verbindungen	Keine. Verwendung der Standardberechtigungen.
System sofort herunterfahren, wenn Sicherheitsüberprüfungen nicht protokolliert werden können	Aktiviert	Deaktiviert
Anmeldeversuche überwachen	Erfolg und Fehler	Fehler
Anmeldeereignisse überwachen	Erfolg und Fehler	Fehler

Die Einstellung **Weitere Einschränkungen für anonyme Verbindungen** muss geändert werden, da sich Outlook 2000- und Outlook 2002-Clients mit dem globalen Katalogserver anonym in Verbindung setzen, um Informationen abzurufen. Mit den im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* bzw. *Security Operations Guide for Windows 2000 Server* (englischsprachig) definierten Einstellungen sind Outlook-Benutzer nicht in der Lage, interne E-Mails zu senden; sie müssen in diesem Fall externe Adressen verwenden.

Hinweis: Weitere Informationen zu diesem Thema finden Sie im Knowledge Base-Artikel Q309622, "XADM: Clients Cannot Browse the Global Address List After You Apply the Q299687 Windows 2000 Security Hotfix" (englischsprachig).

Die anderen Einstellungen werden geändert, um der großen Anzahl der Ereignisse für erfolgreiche Anmeldung Rechnung zu tragen, die Exchange 2000 Server generiert. Wenn Erfolgsüberwachung für Anmeldeereignisse aktiviert ist, wächst das Sicherheitsprotokoll sehr schnell an.

Hinweis: Weitere Informationen zu diesem Thema finden Sie im Knowledge Base-Artikel Q316685, "Active Directory-Integrated Domain Name Is Not Displayed in DNS Snap-in with Event ID 4000 and 4013 Messages" (englischsprachig).

Active Directory-Struktur zur Unterstützung der Serverrollen von Computern mit Exchange 2000 Server

Betriebshandbuch zur Sicherheit von Windows 2000 Server bzw. *Security Operations Guide for Windows 2000 Server* (englischsprachig) empfiehlt eine Organisationseinheitsstruktur, die das einfache Übernehmen der zur Verfügung gestellten Sicherheitsvorlagen erlaubt. Die in diesem Handbuch empfohlene Organisationseinheitsstruktur kann auf einfache Weise erweitert werden, um die beiden hier definierten neuen Serverrollen zu berücksichtigen. Exchange 2000 Server ist eine Anwendung. Aus diesem Grund wird eine Organisationseinheit Computer mit Exchange Server unter der Organisationseinheit Anwendungsserver erstellt, und unter der Organisationseinheit Computer mit Exchange Server werden dann weitere Organisationseinheiten für diese Serverrollen hinzugefügt.

Die Abbildung unten zeigt die Organisationseinheitsstruktur, die für die Integration der beiden neuen Serverrollen empfohlen wird:

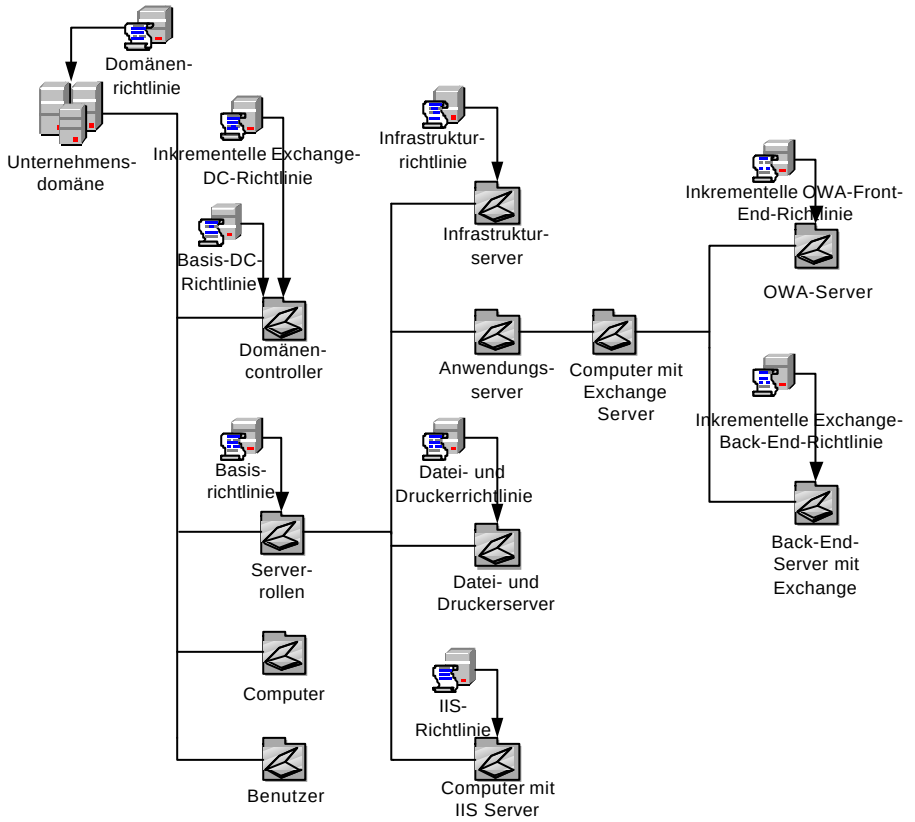

Abbildung 3.1

Organisationseinheitsstruktur mit den hinzugefügten Organisationseinheiten für Computer mit Exchange Server und für Anwendungsserver

Hinweis: Das Erstellen der Organisationseinheitsstruktur für die Unterstützung der Empfehlungen in diesem Handbuch wird ausführlich im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* bzw. *Security Operations Guide for Windows 2000 Server* (englischsprachig) behandelt.

Importieren der Sicherheitsvorlagen

Die unten beschriebenen Sicherheitsvorlagen sind in der Datei **ExSecurityOps.exe** enthalten, die dem Handbuch beigefügt ist. Sie müssen diese Datei extrahieren, bevor Sie die Sicherheitsvorlagen importieren können. Wenn Sie Windows 2000, Service Pack 2, verwenden, müssen Sie außerdem sicherstellen, dass die in den folgenden Artikeln der Knowledge Base beschriebenen Hotfixes angewendet wurden:

Q295444: "SCE Cannot Alter a Service's SACL Entry in the Registry" (englischsprachig)

Q272560: "Race Condition May Lead to Loss of Group Policy Changes" (englischsprachig)

Hinweis: Sie müssen sich mit dem Microsoft-Produktsupport in Verbindung setzen, um die in den oben genannten Artikeln der Knowledge Base beschriebenen Hotfixes zu beziehen. Weitere Informationen dazu, wie Sie sich mit dem Produktsupport in Verbindung setzen können, finden Sie unter der Adresse **http://support.microsoft.com**.

Achtung: Mit den Sicherheitsvorlagen in diesem Handbuch soll die Sicherheit in Ihrer Umgebung erhöht werden. Es ist möglich, dass durch Installieren der in diesem Handbuch enthaltenen Vorlagen Funktionen in Ihrer Umgebung verloren gehen. 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 Ihre Umgebung erforderlich ist, sollten Sie die entsprechenden Änderungen vornehmen. Absichern Sie alle Domänencontroller und Server, bevor Sie die neuen Sicherheitseinstellungen übernehmen. Der Systemstatus muss in der Absicherung enthalten sein, da im Systemstatus die Registrierungsdaten gespeichert sind. Auf Domänencontrollern enthält er außerdem alle Active Directory-Objekte.

Hinweis: Die Domänencontroller-Basisrichtlinie und die Mitgliedsserver-Basisrichtlinie, die im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* bzw. *Security Operations Guide for Windows 2000 Server* (englischsprachig) enthalten sind, legen die LAN Manager-Authentifizierungsebene nur als **NTLMv2** fest. Damit Outlook-Clients erfolgreich mit Computern mit Exchange Server und Domänencontrollern kommunizieren können, müssen diese ebenfalls für die ausschließliche Verwendung von **NTLMv2** konfiguriert werden.

Das folgende Verfahren importiert die im Handbuch enthaltenen Sicherheitsvorlagen in die in diesem Kapitel vorgeschlagene Organisationseinheitsstruktur.

▶ **So erstellen Sie das Domänencontroller-Gruppenrichtlinienobjekt und importieren die Sicherheitsvorlage:**

1. Klicken Sie in **Active Directory-Benutzer und -Computer** mit der rechten Maustaste auf **Domain Controllers**, und wählen Sie dann **Eigenschaften** aus.
2. Klicken Sie auf der Registerkarte **Gruppenrichtlinie** auf **Neu**, um ein neues Gruppenrichtlinienobjekt hinzuzufügen.
3. Geben Sie **Exchange DC Policy** ein, und drücken Sie dann die **Eingabetaste**.
4. Klicken Sie auf **Nach oben**, bis sich der Eintrag **Exchange DC Policy** ganz oben in der Liste befindet.
5. Klicken Sie auf **Bearbeiten**.
6. Erweitern Sie **Windows-Einstellungen**, klicken Sie mit der rechten Maustaste auf **Sicherheitseinstellungen**, und wählen Sie dann **Richtlinie importieren** aus.

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

7. Navigieren Sie im Dialogfeld **Richtlinie importieren von** in den Ordner **C:\SecurityOps\Templates**, und doppelklicken Sie dann auf die Datei **Exchange DC Incremental.inf**.
8. Schließen Sie das Dialogfeld **Gruppenrichtlinie**, und klicken Sie dann auf **Schließen**.
9. Erzwingen Sie die Replikation zwischen den Domänencontrollern, damit alle Domänencontroller über die Richtlinie verfügen.
10. Überprüfen Sie im Ereignisprotokoll, ob die Richtlinie angewendet 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.

▶ **So erstellen Sie das Exchange Server-Gruppenrichtlinienobjekt und importieren die Sicherheitsvorlagen:**

1. Erweitern Sie in **Active Directory-Benutzer und -Computer** das Objekt **Mitgliedsserver**, erweitern Sie **Anwendungsserver**, erweitern Sie **Exchange Server-Computer**, klicken Sie mit der rechten Maustaste auf **OWA Front-End Server**, und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie auf der Registerkarte **Gruppenrichtlinie** auf **Neu**, um ein neues Gruppenrichtlinienobjekt hinzuzufügen.
3. Geben Sie **OWA Policy** ein, und drücken Sie dann die **Eingabetaste**.
4. Klicken Sie auf **Bearbeiten**.
5. Erweitern Sie **Windows-Einstellungen**, klicken Sie mit der rechten Maustaste auf **Sicherheitseinstellungen**, und wählen Sie dann **Richtlinie importieren** aus.

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

6. Navigieren Sie im Dialogfeld **Richtlinie importieren von** in den Ordner **C:\SecurityOps\Templates**, und doppelklicken Sie dann auf die Datei **OWA front-end Incremental.inf**.
7. Schließen Sie das Dialogfeld **Gruppenrichtlinie**, und klicken Sie dann auf **Schließen**.
8. Wiederholen Sie die Schritte 1 bis 7 für die Organisationseinheit Back-End-Server mit der Datei **Exchange back-end Incremental.inf**

9. Erzwingen Sie die Replikation zwischen den Domänencontrollern, damit alle Domänencontroller über die Richtlinie verfügen.
10. Verschieben Sie einen Server für jede Rolle in die entsprechende Organisationseinheit.
11. Downloaden Sie die Richtlinie auf dem Server, indem Sie den Befehl **secedit /refreshpolicy machine_policy /enforce** verwenden.
12. Überprüfen Sie im Ereignisprotokoll, ob die Richtlinie angewendet 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.

Hinweis: Weitere Informationen zum Überprüfen des Erfolgs des Gruppenrichtliniendownloads finden Sie in Kapitel 3, "Verwalten von Sicherheit mit Windows 2000-Gruppenrichtlinien", im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* (bzw. "Managing Security with Windows 2000 Group Policy" in *Security Operations Guide for Windows 2000 Server* [englischsprachig]).

13. Starten Sie die Server neu, um sicherzustellen, dass die Server erfolgreich gestartet werden können.

Exchange Server-Richtlinien

Es ist möglich, eine große Anzahl von Sicherheitseinstellungen in Windows 2000 zu definieren, z. B. Überwachung, Sicherheitsoptionen, Registrierungseinstellungen, Dateiberechtigungen und Dienste. Im *Betriebshandbuch zur Sicherheit von Windows 2000 Server* bzw. *Security Operations Guide for Windows 2000 Server* (englischsprachig) finden Sie Vorschläge für viele dieser Einstellungen, und diese Empfehlungen müssen für Exchange 2000 Server nicht geändert werden. Der Hauptbereich, in dem zusätzliche Einstellungen angewendet werden, bezieht sich auf Dienste. Es werden jedoch auch einige Änderungen der Dateiberechtigungen vorgenommen.

Da sie sich in Organisationseinheiten unterhalb der Organisationseinheit Mitgliedsserver befinden, erben die Computer mit Exchange Server die Einstellungen, die in der Basisrichtlinie für Mitgliedsserver definiert wurden. Die Exchange-Richtlinien verändern diese Einstellungen auf zwei Arten. Zunächst werden einige Dienste, die nicht für Windows 2000-Basisfunktionen erforderlich sind, für erfolgreiche Exchange 2000 Server-Operationen benötigt. Außerdem führt Exchange 2000 Server mehrere zusätzliche Dienste ein, von denen nicht alle erforderlich sind, damit die Computer mit Exchange Server ihre individuellen Rollen ausführen können.

Hinweis: Zwar findet dies keine ausdrückliche Erwähnung in den inkrementellen Exchange-Richtlinien, NNTP (Network News Transfer Protocol) wird jedoch von der Windows 2000-Basisrichtlinie für Mitgliedsserver deaktiviert. Dieser Dienst ist für die Installation von Exchange erforderlich, wird jedoch nur dann für Exchange-Dienste benötigt, wenn Newsgroupfunktionen erforderlich sind.

Richtlinie für den Back-End-Server mit Exchange

Die Richtlinie für den Back-End-Server mit Exchange definiert Einstellungen in zwei Bereichen – Dienste und Zugriffssteuerungslisten für Dateien.

Diensterichtlinie für den Back-End-Server mit Exchange

In der Tabelle werden die Dienste dargestellt, die in der Richtlinie für den Back-End-Server mit Exchange angegeben werden.

Tabelle 3.3: Dienste, die in der Basisrichtlinie für das Exchange Server-Back-End konfiguriert werden.

Dienstname	Startmodus	Grund
Microsoft Exchange IMAP4	Deaktiviert	Server nicht für IMAP4 konfiguriert.
Microsoft Exchange-Informationsspeicher	Automatisch	Für den Zugriff auf Postfächer und Informationsspeicher für Öffentliche Ordner erforderlich.
Microsoft Exchange POP3	Deaktiviert	Server nicht für POP3 konfiguriert.
Microsoft Search	Deaktiviert	Für Kernfunktionen nicht erforderlich.
Microsoft Exchange-Ereignisdienst	Deaktiviert	Nur aus Gründen der Abwärtskompatibilität erforderlich.
Microsoft Exchange-Standortreplikationsdienst	Deaktiviert	Nur aus Gründen der Abwärtskompatibilität erforderlich.
Microsoft Exchange-Verwaltung	Automatisch	Für Nachrichtentracking erforderlich.
Windows-Verwaltungsinstrumentation	Automatisch	Für Microsoft Exchange-Verwaltung erforderlich.
Microsoft Exchange MTA-Stacks	Deaktiviert	Nur aus Gründen der Abwärtskompatibilität oder bei Vorhandensein von X.400-Connectors erforderlich.
Microsoft Exchange-Systemaufsicht	Automatisch	Für Exchange-Verwaltung und andere Aufgaben erforderlich.
Microsoft Exchange-Routingmodul	Automatisch	Für die Koordination der Nachrichtenübertragung zwischen Computern mit Exchange Server erforderlich.
IPSEC-Richtlinien-Agent	Automatisch	Für die Implementierung der IPSec-Richtlinie auf dem Server erforderlich.
RPC-Locator	Automatisch	Für die Kommunikation mit Domänencontrollern und Clients erforderlich.
IIS-Verwaltungsdienst	Automatisch	Wird vom Exchange-Routingmodul benötigt.
NT-LM-Sicherheitsdienst	Automatisch	Die Systemaufsicht hängt von diesem Dienst ab.
SMTP	Automatisch	Für den Exchange-Transport erforderlich.
WWW-Publishingdienst	Automatisch	Für die Kommunikation mit OWA-Front-End-Servern erforderlich.

Hinweis: Die Exchange-Systemaufsicht verlangt, dass die folgenden Dienste gestartet und ausgeführt werden, bevor sie gestartet wird:

- Ereignisprotokoll
- NT-LM-Sicherheitsdienst
- RPC
- RPC-Locator
- Server
- Arbeitsstation

Deaktivierte wichtige Dienste

Im Rahmen dieses Handbuchs wurden alle Dienste deaktiviert, die für die Kernfunktionen von Exchange 2000 Server nicht erforderlich sind. In einigen Fällen müssen Sie möglicherweise Dienste erneut aktivieren, um die Funktionen zur Verfügung zu stellen, die in Ihrer Umgebung erforderlich sind. Die folgende Beschreibung nennt wichtige Dienste, die von der inkrementellen Richtlinie für Back-End-Server deaktiviert werden.

Ereignisdienst

Dieser Dienst wurde mit Exchange Server 5.5 eingeführt. Der Exchange Server-Ereignisdienst unterstützt serverseitige Skripts, die durch Ordnerereignisse ausgelöst werden – entweder in Öffentlichen Ordnern oder in einzelnen Postfächern. Der Exchange-Ereignisdienst wird in Exchange 2000 Server aus Gründen der Abwärtskompatibilität mit Exchange Server 5.5-Ereignisskripts zur Verfügung gestellt. Neue Anwendungen, die eigens für Exchange 2000 Server geschrieben wurden, sollten systemeigene Webspeichersystem-Ereignisse statt des Exchange-Ereignisdienstes verwenden. Eine Beschreibung hierzu finden Sie im Exchange 2000 Server Software Development Kit (SDK), das im MSDN verfügbar ist. Nähere Einzelheiten finden Sie im Abschnitt "Weitere Informationen".

Microsoft Search

Der Informationsspeicherprozess erstellt und verwaltet Indizes für gemeinsame Schlüsselfelder, um schnellere Nachschlage- und Suchvorgänge von Dokumenten zu ermöglichen, die in einem Informationsspeicher gespeichert sind. Ein Index ermöglicht Outlook-Benutzern das einfachere Suchen nach Dokumenten. Der Index wird mit Volltextindizierung für die Clientsuche erzeugt und ermöglicht auf diese Weise schnellere Suchvorgänge. Mailanhänge werden in den Volltextindex einbezogen, wenn es sich dabei um normale Texte, Worddokumente, Excelarbeitsmappen oder PowerPoint-Präsentationen handelt.

Die Indizierung wird vom Microsoft Search-Dienst zur Verfügung gestellt. Sowohl der Informationsspeicherdienst als auch der Search-Dienst müssen ausgeführt werden, damit der Index erstellt, aktualisiert, gelöscht oder durchsucht werden kann.

Microsoft Exchange-Standortreplikationsdienst

Dieser Dienst ist für die Replikation von Exchange Server 5.x-Standort- und Konfigurationsinformationen auf die Konfigurationspartition von Active Directory verantwortlich, wenn ein Computer mit Exchange 2000 Server zu einem vorhandenen Exchange Server 5.5-Standort gehört.

Microsoft Exchange MTA-Stacks

Dies ist eine zusätzliche Komponente, die Exchange 2000 Server mit fremden Systemen verbindet. Der MTA (Message Transfer Agent) ist für die Weiterleitung von Nachrichten über X.400 und Gatewayconnectors an fremde Umgebungen verantwortlich. Dieser Dienst verwaltet

seine eigenen, spezifischen Nachrichtenwarteschlangen außerhalb des Informationsspeicherdienstes im Verzeichnis **\Programme\Exchsrvr\Mtadata**.

Datei-ACL-Richtlinie für den Back-End-Server mit Exchange

Die Richtlinie für Back-End-Server mit Exchange bearbeitet Zugriffssteuerungslisten (Access Control Lists oder ACLs) in mehreren Verzeichnissen. Die Tabelle zeigt die Einstellungen, die definiert sind.

Tabelle 3.4: Datei-ACLs, die von der Richtlinie für den Back-End-Server mit Exchange konfiguriert werden.

Verzeichnis	Alte ACL	Neue ACL	Auf Unterverzeichnisse angewendet?
%systemdrive%\Inetpub\mailroot	Jeder: Vollzugriff	Domänen-Admins: Vollzugriff Lokales System: Vollzugriff	Ja
%systemdrive%\Inetpub\nntpfile\	Jeder: Vollzugriff	Domänen-Admins: Vollzugriff Lokales System: Vollzugriff	Ja
%systemdrive%\Inetpub\nntpfile\root	Jeder: Vollzugriff	Jeder: Vollzugriff	Ja

Hinweis: Die für das Verzeichnis **nntpfile** und die Unterverzeichnisse definierten Einstellungen sind nicht zwingend erforderlich, da NNTP nicht auf dem Server ausgeführt wird. Diese Einstellung wird jedoch definiert, weil sie die Beschränkungen des Dateisystems erhöht und verwendungsbereit ist, wenn Sie zu einem späteren Zeitpunkt NNTP aktivieren möchten.

Richtlinie für den OWA-Front-End-Server

Die Richtlinie für den OWA-Front-End-Server definiert Einstellungen in zwei Bereichen – Dienste und Zugriffssteuerungslisten für Dateien.

Diensterichtlinie für den OWA-Front-End-Server

Da die Rolle dieses Servers allein in der Unterstützung webbasierter E-Mails besteht, können viele der von der Standardkonfiguration installierten Exchange-Dienste deaktiviert werden. In der Tabelle werden die Dienste dargestellt, die in der Richtlinie für den OWA-Front-End-Server konfiguriert werden.

Tabelle 3.5: Dienste, die in der Richtlinie für den OWA-Front-End-Server konfiguriert werden.

Dienstname	Startmodus	Grund
Microsoft Exchange IMAP4	Deaktiviert	OWA-Server nicht für IMAP4 konfiguriert.
Microsoft Exchange-Informationsspeicher	Deaktiviert	Nicht erforderlich, weil kein Postfachspeicher oder Informationsspeicher für Öffentliche Ordner vorhanden ist.
Microsoft Exchange POP3	Deaktiviert	OWA-Server nicht für POP3 konfiguriert.
Microsoft Search	Deaktiviert	Keine zu durchsuchenden Datenspeicher.
Microsoft Exchange-Ereignis	Deaktiviert	Nur aus Gründen der Abwärtskompatibilität erforderlich.
Microsoft Exchange-Standortreplikationsdienst	Deaktiviert	Nur aus Gründen der Abwärtskompatibilität erforderlich.
Microsoft Exchange-Verwaltung	Deaktiviert	Für Nachrichtentracking erforderlich.
Microsoft Exchange-MTA	Deaktiviert	Nur aus Gründen der Abwärtskompatibilität oder bei Vorhandensein von X.400-Connectors erforderlich.
Microsoft Exchange-Routingmodul	Automatisch	Stellt Exchange-Routingfunktionen zur Verfügung.
IPSEC-Richtlinien-Agent	Automatisch	Für die Implementierung des IPSec-Filters auf dem OWA-Server erforderlich.
RPC-Locator	Automatisch	Für die Kommunikation mit dem Domänencontroller und den Start der Systemaufsicht erforderlich.
IIS-Verwaltungsdienst	Automatisch	Wird vom MSExchange-Routingmodul benötigt.
WWW-Publishingdienst	Automatisch	Für die Clientkommunikation mit OWA-Front-End-Servern erforderlich.

Wichtige Dienste, die in der Richtlinie für den OWA-Front-End-Server deaktiviert sind

Ebenso wie bei der Back-End-Konfiguration müssen Sie möglicherweise einige Dienste erneut aktivieren, um die Funktionen zur Verfügung zu stellen, die in Ihrer Umgebung erforderlich sind. Die folgende Beschreibung nennt wichtige Dienste, die von der inkrementellen Richtlinie für den OWA-Front-End-Server deaktiviert werden.

Microsoft Exchange POP3 und Microsoft Exchange IMAP4

Wie bereits in Kapitel 2 erwähnt wurde, sollten Sie ermitteln, ob Sie die vollständigen Funktionen von Exchange in Ihrer Umgebung benötigen. In vielen Fällen sind keine POP3- oder IMAP4-Clients vorhanden, und Sie können sicherstellen, dass diese Dienste durch die Gruppenrichtlinie deaktiviert werden. Sie sollten außerdem sicherstellen, dass keine benutzerdefinierten Programme in Ihrer Umgebung ausgeführt werden, die diese Funktion benötigen, bevor Sie die Funktion deaktivieren.

Systemaufsicht

Auf einem Front-End-Server ist die Systemaufsicht nur erforderlich, wenn Sie Konfigurationsänderungen am Server vornehmen möchten. Aus diesem Grund wird die Systemaufsicht in der Vorlage deaktiviert. Dies bedeutet, dass Sie die Systemaufsicht und die zugehörigen Dienste zuerst vorübergehend starten müssen, um Änderungen an einem Server vornehmen zu können, der die Richtlinie für OWA-Front-End-Server verwendet (z. B. auch, um einen Server als OWA-Front-End-Server zu konfigurieren).

▶ **So nehmen Sie Änderungen an der Konfiguration eines Servers vor, auf den die Gruppenrichtlinie für OWA-Front-End-Server angewendet wurde:**

1. Starten Sie das Verwaltungstool **Dienste**.
2. Klicken Sie mit der rechten Maustaste auf **NT-LM-Sicherheitsdienst**, und wählen Sie dann **Eigenschaften** aus.
3. Wählen Sie im Dropdownlistenfeld **Starttyp** die Option **Automatisch** aus.
4. Klicken Sie auf **Übernehmen**.
5. Klicken Sie auf **Starten**.
6. Klicken Sie auf **OK**.
7. Wiederholen Sie die Schritte 2 bis 6 für die **Systemaufsicht**.
8. Nehmen Sie alle erforderlichen Konfigurationsänderungen vor.
9. Starten Sie das Verwaltungstool **Dienste**.
10. Klicken Sie mit der rechten Maustaste auf **Systemaufsicht**, und wählen Sie dann **Eigenschaften** aus.
11. Wählen Sie im Dropdownlistenfeld **Starttyp** die Option **Deaktiviert** aus.
12. Klicken Sie auf **Übernehmen**.
13. Klicken Sie auf **Beenden**.
14. Klicken Sie auf **OK**.
15. Wiederholen Sie die Schritte 2 bis 6 für den **NT-LM-Sicherheitsdienst**.

Informationsspeicher

Der Informationsspeicherdienst ist nicht erforderlich, weil an diesen Server keine E-Mail übermittelt wird. Ohne den Informationsspeicherdienst wird das dem Buchstaben M: zugeordnete Laufwerk, das normalerweise auf allen Computern mit Exchange 2000 Server vorhanden ist, entfernt. Das installierbare Exchange-Dateisystem (IFS) steht auf diesem OWA-Front-End-Server nicht zu Verfügung.

Microsoft Exchange-Verwaltung

Dieser Dienst wurde als Teil von Exchange 2000 Server, Service Pack 2, eingeführt. Mithilfe dieses Dienstes kann angegeben werden (über die Benutzeroberfläche), welchen Domänencontroller oder globalen Katalogserver Exchange 2000 Server beim Zugriff auf das Verzeichnis verwenden soll. Er ist außerdem für Nachrichtentracking erforderlich. Sie können diesen Dienst deaktivieren, ohne dass dies Auswirkungen auf die Kernfunktionen von Exchange besitzt. Möglicherweise benötigen Sie jedoch Nachrichtentracking als Teil der Überwachung der Exchange-Funktionen. In diesem Fall wird der OWA-Front-End-Server für den Zugriff auf E-Mail statt für das Weiterleiten von Mail verwendet, und der Microsoft Exchange-Verwaltungsdienst sollte nicht auf den OWA-Front-End-Servern ausgeführt werden müssen.

SMTP-Dienst

Der OWA-Front-End-Server benötigt SMTP in diesem Fall nicht, weil er nur als OWA-Server fungiert. Sie müssen den SMTP-Dienst aktivieren, wenn Sie den Front-End-Server für den Empfang von SMTP-Mail konfiguriert haben, um entweder als Gateway oder als Front-End-Server für IMAP4 oder POP3 zu fungieren. Wenn der Server außerdem die Funktion eines SMTP-Gateways übernimmt, sind die Informationsspeicher- und Systemaufsichtsdienste ebenfalls erforderlich.

Datei-ACL-Richtlinie für den OWA-Front-End-Server

Diese Richtlinie definiert Datei-ACLs auf genau die gleiche Weise wie die Back-End-Serverrichtlinie. Einzelheiten hierzu finden Sie unter "Datei-ACL-Richtlinie für den Back-End-Server mit Exchange" weiter oben in diesem Kapitel.

Installieren und Aktualisieren von Exchange in einer Umgebung mit erhöhter Sicherheit

Wenn Sie die in diesem Kapitel bis jetzt beschriebenen Verfahren befolgt haben, haben Sie vorhandene Computer mit Exchange Server in die entsprechenden Organisationseinheiten verschoben, um den Sicherheitsgrad in Ihrer Umgebung zu erhöhen. Um die Sicherheit zu maximieren, müssen neue Server in die entsprechende Organisationseinheit verschoben werden, bevor Exchange installiert wird. In der Umgebung können Exchange-Kerndienste ausgeführt werden, Exchange kann jedoch standardmäßig nicht installiert werden, und ein Update von Exchange auf zukünftige Service Packs ist ebenfalls nicht möglich. Um Exchange oder Exchange Service Packs auf gesperrten Servern zu installieren, verwenden Sie das folgende Verfahren.

Hinweis: Wenn Sie Exchange 2000 Server auf einem Server installieren, der bereits gesichert wurde, erhalten Sie Fehlermeldungen des Typs "Digitale Signatur nicht gefunden". Dies ist ein Ergebnis der erhöhten Sicherheit auf dem Server und kann umgangen werden.

▶ **So installieren Sie Exchange oder ein Exchange Service Pack auf einem gesperrten Server:**

1. Starten Sie das Verwaltungstool **Dienste**.
2. Klicken Sie mit der rechten Maustaste auf **Distributed Transaction Coordinator**, und wählen Sie dann **Eigenschaften** aus.
3. Wählen Sie im Dropdownlistenfeld **Starttyp** die Option **Automatisch** aus.
4. Klicken Sie auf **Übernehmen**.
5. Klicken Sie auf **Starten**.
6. Klicken Sie auf **OK**.
7. Wiederholen Sie die Schritte 2 bis 6 für **Network News Transport Protocol (NNTP)** und **Windows Installer**.

Hinweis: Wenn Sie diese Schritte auf einem Server in der Organisationseinheit für das OWA-Front-End ausführen, wiederholen Sie die Schritte 2 bis 6 außerdem für **Windows-Verwaltungsinstrumentation**.

8. Installieren Sie Exchange 2000 Server oder das aktuelle Exchange 2000 Server Service Pack.

Hinweis: Wenn Sie Exchange 2000 Server installieren, wird am Ende der Installation möglicherweise ein Dialogfeld angezeigt, das angibt, dass ein mittelschwerer Installationsfehler aufgetreten ist, weil der Microsoft Search-Dienst nicht gestartet wurde. Dieser Fehler muss bei der Installation auf einem bereits gesicherten Server erwartet werden und kann folgenlos ignoriert werden.

9. Starten Sie das Verwaltungstool **Dienste**.
10. Klicken Sie mit der rechten Maustaste auf **Distributed Transaction Coordinator**, und wählen Sie dann **Eigenschaften** aus.
11. Wählen Sie im Dropdownlistenfeld **Starttyp** die Option **Deaktiviert** aus.
12. Klicken Sie auf **Übernehmen**.
13. Klicken Sie auf **Beenden**.
14. Klicken Sie auf **OK**.
15. Wiederholen Sie die Schritte 2 bis 6 für **Network News Transport Protocol (NNTP)** und **Windows Installer**.

Hinweis: Wenn Sie diese Schritte auf einem Server in der Organisationseinheit für das OWA-Front-End ausführen, wiederholen Sie die Schritte 9 bis 14 außerdem für **Windows-Verwaltungsinstrumentation**.

Hinweis: Die inkrementellen Richtlinien für OWA-Front-End-Server und Back-End-Server mit Exchange aktivieren NTLMv2. Dadurch wird es den Computern mit Exchange Server ermöglicht, mit den gesicherten Domänencontrollern zu kommunizieren. Wenn Sie die Server vor der Installation von Exchange nicht in der entsprechenden Organisationseinheit platzieren, sind die Server nicht in der Lage, Verbindungen mit Domänencontrollern herzustellen.

Weitere Sicherheitsmaßnahmen

Zusätzlich zur erweiterten Sicherheit, die durch die Gruppenrichtlinienvorlagen zur Verfügung gestellt wird, sollten weitere Sicherheitsmaßnahmen auf Computern mit Exchange 2000 Server implementiert werden. In den folgenden Abschnitten werden diese Maßnahmen beschrieben.

IIS Lockdowntool

Nachdem die Sicherheitsvorlage auf den Computern mit Exchange 2000 Server übernommen wurde, müssen Sie weitere Sicherheitskontrollen für IIS einrichten, insbesondere auf den OWA-Front-End-Servern. Um viele der Änderungen an IIS zu automatisieren, kann das IIS Lockdowntool verwendet werden. IIS Lockdown gibt Einstellungen an, die für die Erhöhung der IIS-Sicherheit erforderlich sind, Exchange 2000 Server jedoch trotzdem erlauben, entweder als Back-End-Server oder als OWA-Front-End-Server zu fungieren.

Hinweis: Sie können das IIS Lockdowntool unter folgender Adresse beziehen: http://www.microsoft.com/technet/security/tools/tools/locktool.asp (englischsprachig).

Das IIS Lockdowntool besitzt zwei Modi: Einen Expressmodus, der sich für die meisten grundlegenden Webserver eignet, sowie einen erweiterten Modus, der Administratoren das Auswählen der Technologien ermöglicht, die der Server unterstützt. Das Tool stellt eine "Rückgängig"-Funktion zur Verfügung, mit der die Auswirkungen des letzten Lockdowns rückgängig gemacht werden können.

IIS Lockdown implementiert außerdem URLScan; dieses Programm filtert alle eingehenden Anforderungen an einen Computer mit IIS und gibt nur die Anforderungen weiter, die einer bestimmten Regelsammlung genügen. Auf diese Weise wird die Sicherheit des Servers erheblich gesteigert, weil sichergestellt wird, dass er ausschließlich auf gültige Anforderungen reagiert. URLScan ermöglicht das Filtern von Anforderungen basierend auf der Länge, dem Zeichensatz, dem Inhalt und anderen Faktoren. Es wird eine Standardregelsammlung zur Verfügung gestellt, die an die Anforderungen eines bestimmten Servers angepasst werden kann.

▶ **So sperren Sie OWA-Front-End-Server mit Exchange 2000 Server:**

1. Installieren und starten Sie **IISLockd.exe** auf dem Server.
2. Klicken Sie auf **Weiter**.
3. Lesen Sie den Lizenzvertrag, wählen Sie **I agree** aus, und klicken Sie dann auf **Weiter**.
4. Wählen Sie die Servervorlage **Exchange 2000 (OWA, PF Management, IM, SMTP, NNTP)** aus, aktivieren Sie das Kontrollkästchen **View template settings**, und klicken Sie dann auf **Weiter**.
5. Im Dialogfeld **Internet Services** werden vier Dienste angezeigt (HTTP, FTP, SMTP und NNTP). Wenn das Kontrollkästchen für einen bestimmten Dienst abgeblendet ist, ist dieser Dienst entweder nicht installiert oder bereits deaktiviert. Stellen Sie sicher, dass nur **Web service (HTTP)** aktiviert ist, und klicken Sie dann auf **Weiter**, um fortzufahren.

Hinweis: Wenn IIS Lockdown nach dem Übernehmen der Sicherheitsvorlage für OWA-Front-Ends aus dem Gruppenrichtlinienobjekt ausgeführt wird, sollte der Webdienst (HTTP) der einzige Dienst sein, der als aktiviert angezeigt wird, während alle anderen Dienste deaktiviert sind.

6. Das Dialogfeld **Script Maps** ermöglicht das Deaktivieren der Unterstützung für bestimmte ISAPI-Anwendungen, indem die zugehörige Skriptzuordnung entfernt wird. Die Tabelle zeigt die Standardeinstellungen, die in der Exchange 2000 Server-Vorlage implementiert werden. Nur Active Server Pages sind aktiviert. Alle anderen Skriptzuordnungen sind deaktiviert. Klicken Sie auf **Weiter**.

Tabelle 3.6: Einstellungen für die Standardskriptzuordnung in der Exchange 2000 Server-Vorlage für IISLockDown

Typ	Eintrag	Status
Active Server Pages	.asp	Aktiviert
Index Server Web Interface	.htw, .ide, .idq	Deaktiviert
Server side includes	.stm, .shtm, .shtml	Deaktiviert
Internet Data Connector	.idc	Deaktiviert
.HTR scripting	.htr	Deaktiviert
Internet printing	.printer	Deaktiviert

Hinweis: Wenn Sie die Unterstützung für die .htr-Skriptzuordnung deaktivieren, funktioniert das Feature für die OWA-Kennwortänderung nicht. Dieses OWA-Feature wird von IIS LockDown standardmäßig deaktiviert.

7. Die Optionen im Dialogfeld **Additional Security** ermöglichen das Entfernen der virtuellen Standardverzeichnisse, die bei der IIS-Standardinstallation erstellt werden, sowie das Übernehmen von Datei-ACLs für bestimmte Verzeichnisse und alle ausführbaren system32-Dateien. Klicken Sie auf **Weiter**, um fortzufahren.

   Die Tabelle zeigt die virtuellen Verzeichnisse, die entfernt werden.

Tabelle 3.7: Von IISLockdown entfernte virtuelle Verzeichnisse

Name	Virtuelles Verzeichnis	Standardpfad
IIS Samples	\IISSamples	c:\inetpub\iissamples
IISHelp	\IISHelp	c:\winnt\help\iishelp
MSADC	\MSADC	C:\Programme\Gemeinsame Dateien\System\msadc
Scripts	\Scripts	c:\inetpub\scripts
IISAdmin	\IISAdmin	c:\winnt\system32\inetsrv\iisadmin

Um den Zugriff auf das Dateisystem zu beschränken, erstellt IIS Lockdown zwei neue lokale Gruppen namens **Web Anonymous Users** und **Web Applications** auf dem OWA-Server. Das Tool platziert alle anonymen Benutzer oder anonymen Anwendungskonten in der entsprechenden Gruppe. Normalerweise wird **IUSR_<Computername>** in der Gruppe **Web Anonymous Users** und **IWAM_<Computername>** in der Gruppe **Web Applications** platziert. IIS Lockdown legt anschließend Berechtigungen fest und verweigert den Schreibzugriff für diese Gruppen für die Verzeichnisse

C:\inetpub\wwwroot

C:\Programme\Exchsrvr\ExchWeb.

Außerdem wird der Ausführungszugriff auf alle Systemdienstprogramme, z. B. **cmd.exe**, im Ordner **c:\winnt\system32** verweigert. Denken Sie daran, dass die Gruppenrichtlinie aus der Basisvorlage einen bestimmten Zugriffssteuerungseintrag (Access Control Entry oder ACE) auf die ausführbaren Dateien im Systemverzeichnis anwendet, der nur Administratoren Vollzugriff erlaubt. Es werden keine weiteren Benutzer oder Gruppen definiert. Diese Einstellungen überschreiben die IIS Lockdown-Einstellung, wenn die Gruppenrichtlinie erneut übernommen wird.

8. Sie werden nun aufgefordert, **URLScan** zu installieren. Standardmäßig ist das Kontrollkästchen für die Installation bereits aktiviert. Klicken Sie auf **Weiter**.
9. Lesen Sie sich die auszuführenden Aufgaben durch, und klicken Sie dann auf **Weiter**.
10. Das Dialogfeld **Installing Unknown Software Package** wird aufgrund der erhöhten Sicherheit angezeigt; klicken Sie auf **Ja**.
11. IIS Lockdown generiert einen Bericht, der die vorgenommenen Änderungen sowie ggf. aufgetretene Fehler ausführlich beschreibt. Im Bericht werden Fehler bei der Zuweisung von ACLs zu einigen NTFS-Verzeichnissen durch IIS Lockdown aufgeführt. Diese Verzeichnisse sind das Postfach und die Öffentlichen Ordner, die als Teil der OWA-Serverkonfiguration gelöscht wurden. Klicken Sie auf **Weiter**.
12. Klicken Sie auf **Fertig stellen**.

Hinweis: Um IIS Lockdown auf einem Back-End-Server mit Exchange 2000 Server auszuführen, wiederholen Sie das oben beschriebene Verfahren, und stellen Sie in Schritt 5 sicher, dass HTTP und SMTP aktiviert sind.

Ändern der IIS Lockdown- und URLScan-Einstellungen für OWA-Front-End-Server

Möglicherweise müssen Sie die IIS Lockdown- und URLScan-Standardeinstellungen für Ihre Umgebung ändern. Die URLScan-Einstellungen werden in der Datei **URLScan.ini** im Ordner **<WinDir>\System32\Inetsrv\Urlscan** gespeichert. Sollten Probleme auftreten, wenn OWA und UrlScan aktiviert sind, untersuchen Sie die Datei **Urlscan.log** im Ordner **<WinDir>\System32\Inetsrv\Urlscan**, um die Liste der Anforderungen zu überprüfen, die zurückgewiesen wurden.

Hinweis: Weitere Informationen zur Problembehandlung und Konfiguration von IIS Lockdown und URLScan finden Sie im Knowledge Base-Artikel Q309677, "XADM: Known Issues and Fine Tuning When You Use the IIS Lockdown Wizard in an Exchange 2000 Environment" (englischsprachig).

Unterstützung für Kennwortänderung in OWA

Standardmäßig deaktiviert IIS Lockdown .htr-Dateien. Wenn dieser Dateityp deaktiviert ist, funktioniert das OWA-Feature zum Ändern von Kennwörtern nicht. Wenn .htr-Dateien deaktiviert sind, sollten Sie außerdem die Schaltfläche **Kennwort ändern** in OWA ausblenden, um Benutzer nicht unnötig zu verwirren und Anrufe beim Helpdesk zu vermeiden.

Hinweis: Weitere Informationen zum Deaktivieren der Schaltfläche **Kennwort ändern** in OWA finden Sie im Knowledge Base-Artikel Q297121, "XWEB: How to Hide the "Change Password" Button on the Outlook Web Access Options Page" (englischsprachig).

Blockierte E-Mail

Der Abschnitt [DenyUrlSequences] der Datei **URLScan.ini** listet Zeichen auf, die ausdrücklich blockiert sind, und kann möglicherweise Auswirkungen auf den Zugriff auf OWA besitzen. Jeder E-Mail-Betreff oder E-Mail-Ordnername, der eine der folgenden Zeichenfolgen enthält, wird blockiert:

..
./
\
%
&

Hinweis: Die Angabe ".." in der Datei **URLScan.ini** blockiert E-Mail-Nachrichten mit einer Betreffzeile, die mit einem Punkt endet.

Aufheben der Bereitstellung des Postfachspeichers und Löschen des Informationsspeichers für Öffentliche Ordner

Da die Rolle des OWA-Front-End-Servers im Weiterleiten von Anforderungen an die Back-End-Server besteht, benötigen Sie keine Exchange Server-Postfächer oder Öffentliche Ordner auf den OWA-Front-End-Servern. Der Back-End-Server mit Exchange verwaltet diese. Sie können aus diesem Grund die Bereitstellung dieser Informationsspeicher aufheben und diese löschen.

▶ **So heben Sie die Bereitstellung der Postfachdatenbanken und Öffentlichen Ordnerdatenbanken auf:**

1. Starten Sie das Verwaltungstool **Dienste**.
2. Klicken Sie mit der rechten Maustaste auf **NT-LM-Sicherheitsdienst**, und wählen Sie dann **Eigenschaften** aus.
3. Wählen Sie im Dropdownlistenfeld **Starttyp** die Option **Automatisch** aus.
4. Klicken Sie auf **Übernehmen**.
5. Klicken Sie auf **Starten**.
6. Klicken Sie auf **OK**.
7. Wiederholen Sie die Schritte 2 bis 6 für die **Microsoft Exchange-Systemaufsicht**.
8. Starten Sie **Exchange System-Manager** auf dem OWA-Front-End-Server.
9. Erweitern Sie **Server**, erweitern Sie den OWA-Front-End-Server, und erweitern Sie dann **Erste Speichergruppe**.
10. Wenn der Postfachspeicher bereitgestellt ist, klicken Sie mit der rechten Maustaste auf **Postfachspeicher**, wählen Sie **Bereitstellung des Informationsspeichers aufheben** aus, und klicken Sie dann auf **Ja**, um die Bereitstellung des Postfachspeichers aufzuheben.
11. Klicken Sie mit der rechten Maustaste auf **Postfachspeicher**, und wählen Sie dann **Eigenschaften** aus.
12. Klicken Sie auf die Registerkarte **Datenbank**, klicken Sie auf **Diesen Informationsspeicher beim Start nicht bereitstellen**, und klicken Sie dann auf **OK**.
13. Wenn der Informationsspeicher für Öffentliche Ordner bereitgestellt ist, klicken Sie mit der rechten Maustaste auf **Informationsspeicher für Öffentliche Ordner**, wählen Sie **Bereitstellung des Informationsspeichers aufheben** aus, und klicken Sie dann auf **Ja**, um die Bereitstellung des Informationsspeichers für Öffentliche Ordner aufzuheben.
14. Klicken Sie mit der rechten Maustaste auf **Informationsspeicher für Öffentliche Ordner**, und wählen Sie dann **Löschen** aus.
15. Klicken Sie auf **Ja**, klicken Sie auf **OK**, wählen Sie einen Back-End-Server aus, und klicken Sie dann auf **OK**.
16. Klicken Sie auf **Ja**, um den Informationsspeicher für Öffentliche Ordner zu löschen, und klicken Sie dann auf **OK**, um die Meldung zu schließen.
17. Starten Sie den OWA-Server neu.

Hinweis: Sie müssen den NT-LM-Sicherheitsdienst und die Systemaufsicht nicht erneut deaktivieren, da dies automatisch beim Neustart des Servers geschieht.

Hinweis: Der private Informationsspeicher muss bereitgestellt werden, wenn SMTP auf dem Front-End-Server ausgeführt wird.

Hinweis: Nach dem Aufheben der Bereitstellung des Postfachspeichers und des Informationsspeichers für Öffentliche Ordner wird das dem Buchstaben M: zugeordnete Laufwerk, das normalerweise auf allen Computern mit Exchange 2000 Server vorhanden ist, entfernt. Das installierbare Exchange-Dateisystem (IFS) steht auf diesem OWA-Front-End-Server nicht zu Verfügung.

Sie werden im Systemprotokoll Ereignisfehler (Ereignis-ID 101) bemerken, die angeben, dass der Pfad eines bestimmten virtuellen Verzeichnisses ungültig ist. Diese virtuellen Verzeichnisse **public**, **Exchange** und **Exadmin** besitzen außerdem den Status **Beendet** in der Internetdienste-Manager-Konsole. Diese Fehler werden generiert, nachdem der Computer mit Exchange Server auf dem Computer mit IIS installiert wurde und der Server erneut gestartet wird. Nach einem Neustart startet der IIS-Dienst (W3SVC), bevor der Exchange-Informationsspeicherdienst gestartet wird. Der Informationsspeicherdienst ist für das Erstellen des zugeordneten virtuellen Laufwerks (M:) verantwortlich, dem diese drei virtuellen Verzeichnisse zugewiesen werden. Da das zugeordnete Laufwerk noch nicht erstellt wurde, generiert IIS diese Fehlermeldungen. Da der Informationsspeicherdienst deaktiviert ist, wenn die Sicherheit über die Gruppenrichtlinie übernommen wird, wird das zugeordnete virtuelle Laufwerk niemals bereitgestellt, und diese Fehler werden auch weiterhin im Ereignisprotokoll aufgezeichnet. Sie sind jedoch vollkommen harmlos.

Hinweis: Weitere Informationen zur Ereignisprotokoll-ID 101 finden Sie im Knowledge Base-Artikel Q259373, "XADM: W3SVC Logs Event ID 101 in the System Event Log (englischsprachig).

Ändern des SMTP-Banners

Je weniger Informationen Sie einem Angreifer zur Verfügung stellen, desto schwieriger werden Angriffe auf Ihr System. Eine Methode, mit der ein Angreifer versuchen kann, Informationen zu der ausgeführten Version von Exchange zu erhalten, besteht im Verwenden von Telnet zum Herstellen einer Verbindung mit dem SMTP-Dienst. Standardmäßig wird das folgende Banner angezeigt, wenn Sie eine Verbindung mit dem SMTP-Dienst auf einem Computer mit Exchange Server herstellen:

220 *hostname*.*domain*.com Microsoft ESMTP MAIL Service, Version: 5.0.2195.1600 ready at *aktuelles Datum* and *Uhrzeit*.

Sie sollten in Erwägung ziehen, diese Angabe auf allen Back-End-Servern mit Exchange zu ändern, damit die betreffende Version nicht angezeigt wird. Sie können außerdem einen rechtlichen Hinweis anbringen, dass die unberechtigte Verwendung des SMTP-Dienstes verboten ist.

▶ **So ändern Sie das SMTP-Banner von Windows 2000:**

1. Suchen Sie mit einem Metabasis-Bearbeitungstool wie z. B. MetaEdit den folgenden Eintrag:
   Lm\Smtpsvc\Nummer_des_virtuellen_Servers.
2. Klicken Sie auf **Edit**, klicken Sie auf **New**, und klicken Sie dann auf **String**.
3. Vergewissern Sie sich, dass der Eintrag im Feld **Id (Other)** lautet, und geben Sie dann **36907** (dezimal) auf der rechten Seite des Feldes **Id** ein.
4. Geben Sie im Feld **Data** das Banner ein, das angezeigt werden soll.
5. Beenden Sie den virtuellen SMTP-Server oder den SMTP-Dienst, und starten Sie diesen dann neu.

Stellen Sie mit Telnet eine Verbindung mit Port 25 des virtuellen Servers her (dies ist die Standardeinstellung), um zu bestätigen, dass das Banner geändert wurde. Das Banner "ESMTP MAIL Service, Version: 5.0.2195.1600" sollte nicht mehr angezeigt werden. Der voll qualifizierte Domänenname (wie in den Eigenschaften des SMTP-Dienstes eingegeben) sowie Datum und Uhrzeit werden hingegen auch weiterhin angezeigt.

Gruppen-Lockdown für Exchange Domain Servers

Als Teil einer Standardinstallation wird eine Gruppe **Exchange Domain Servers** für jede Domäne in der Gesamtstruktur erstellt. Diese Gruppe enthält die Computerkonten für alle Computer mit

Exchange Server in der betreffenden Domäne. Standardmäßig wird den Gruppen **Exchange Domain Servers** der Zugriff auf alle Exchange-Informationsspeicher für Öffentliche Ordner und Postfachspeicher in der Gesamtstruktur gewährt. Sie können den Zugriff auf Postfachspeicher nur auf den lokalen Server beschränken, der die Informationsspeicher ausführt, indem Sie das EDSLock-Skript ausführen.

Hinweis: Weitere Informationen zum EDSLock-Skript finden Sie im Knowledge Base-Artikel Q313807, "XADM: Enhancing the Security of Exchange 2000 for the Exchange Domain Servers Group" (englischsprachig).

Exchange-Clustererwägungen

Exchange 2000 Server in einer Clusterumgebung wird in diesem Handbuch nicht behandelt. Es versteht sich jedoch von selbst, dass Sie bestimmte Änderungen an den hier gezeigten Sicherheitseinstellungen vornehmen müssen, damit Exchange 2000 Server in einer Clusterumgebung ausgeführt werden kann. Diese Änderungen umfassen Folgendes:

Aktivieren von NTLM auf den Clusterservern und Domänencontrollern, da NTLMv2 auf Windows 2000-Clustern nicht unterstützt wird. Weitere Informationen finden Sie im Knowledge Base Artikel Q272129, "Cluster Service Does Not Start on "Joining" Node in Windows 2000" (englischsprachig).

Anpassen der Einstellung in der Sicherheitsvorlage für den NT-LM-Sicherheitsdienst (NTLMSSP) für die Back-End-Server mit Exchange. NTLMSSP muss als 0 festgelegt werden:

MACHINE\System\CurrentControlSet\Control\LSA\MSV1_0\NtlmMinServerSec=4,0

Aktivieren des Clusterdienstes in der Sicherheitsvorlage für die Back-End-Server mit Exchange.

Keine Implementierung von IPSec für OWA-Front-End-/Back-End-Kommunikation, da IPSec auf Clustern nicht unterstützt wird; weitere Informationen finden Sie im Knowledge Base-Artikel 306677, "IPSec Is Not Designed for Failover" (englischsprachig).

Zusammenfassung

Das Erhöhen der Sicherheit der Computer mit Exchange Server ist ein wichtiger Bestandteil bei der Absicherung des Unternehmens. Wenn Sie die in diesem und im vorangegangenen Kapitel genannten Empfehlungen befolgen sowie die Sicherheit Ihrer Windows 2000-Umgebung erhöhen, verringern Sie das Risiko eines erfolgreichen Angriffs auf die Exchange-Umgebung erheblich.

Weitere Informationen

Vollständiges *Betriebshandbuch zur Sicherheit von Microsoft® Exchange 2000 Server* bzw. *Security Operations Guide for Microsoft® Exchange 2000 Server* (englischsprachig):

http://www.microsoft.com/germany/ms/technetdatenbank/overview.asp?siteid=542484 bzw. http://www.microsoft.com/technet/security/prodtech/windows/windows2000/staysecure/DEFAULT.asp (englischsprachig)

Ausführliche Behandlung von OWA-Front-End-/Back-End-Serverumgebungen in Exchange:

http://www.microsoft.com/Exchange/techinfo/deployment/2000/E2KFrontBack.asp (englischsprachig)

Einzelheiten zu den Auswirkungen von Windows 2000-Sicherheitsfixes auf den globalen Katalogserver:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q309622 (englischsprachig)

Einzelheiten zum Aktivieren von Erfolgsüberwachung für Anmeldeereignisse im Sicherheitsprotokoll:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q316685 (englischsprachig)

Ausführliche Behandlung systemeigener Web Storage System-Ereignisse:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/wss/wss/_exch2k_welcome_to_exchange.asp?frame=true (englischsprachig)

Download des IIS Lockdowntools:

http://www.microsoft.com/technet/security/tools/tools/locktool.asp (englischsprachig)

Einzelheiten zur Problembehandlung und Konfiguration von IIS Lockdown und URLScan:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q309677 (englischsprachig)

Einzelheiten zum Deaktivieren der Schaltfläche **Kennwort ändern** in OWA:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q297121 (englischsprachig)

Einzelheiten zu Ereignisprotokoll-ID 101:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q259373 (englischsprachig)

Einzelheiten zum EDSLock-Skript:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q313807 (englischsprachig)

Einzelheiten zur fehlenden Unterstützung von NTLMv2 auf Windows 2000-Clustern:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q272129 (englischsprachig)

Einzelheiten zur Nichtimplementierung von IPSec für OWA-Front-End/Back-End-Kommunikation:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q306677 (englischsprachig)

Originaltitel: Chapter 4 – Securing Exchange Communications

4

Absichern der Exchange-Kommunikation

Wenn Sie die Sicherheit eines beliebigen Netzwerks erhöhen, sollten Sie nicht nur die Sicherheit der Computer selbst, sondern auch die Sicherheit der Daten untersuchen, die zwischen diesen übertragen werden. Wie bei jedem System besteht die beste Vorgehensweise im Vergleichen der verfügbaren Funktionen mit den erforderlichen Funktionen, wobei das durch jede einzelne Funktion entstehende Risiko berücksichtigt wird.

In diesem Handbuch wird davon ausgegangen, dass Sie die folgenden Funktionen benötigen: a) Senden und Empfangen von E-Mails über das Internet und b) Zugriff auf Exchange über das Internet mit Outlook Web Access. Wenn Sie diese Funktionseinheiten nicht benötigen, können Sie die Systeme weiter sperren. Wenn Sie andererseits POP3- und IMAP4-Funktionen benötigen, müssen Sie die Umgebung weiter öffnen, damit diese Funktionen ermöglicht werden.

Die in diesem Handbuch vorgeschlagene Front-End-/Back-End-Umgebung erlaubt das Senden von E-Mails in das und aus dem Internet, und sie bietet Exchange-Zugriff über das Internet. Dieses Kapitel behandelt das Absichern dieser Kommunikation und untersucht außerdem das Absichern der Kommunikation auf dem Client.

Hinweis: Es ist möglich, über das Internet auf Outlook zuzugreifen, indem ein Anwendungsfilter für Exchange-Remoteprozeduraufruf (Remote Procedure Call oder RPC) verwendet wird, der im Lieferumfang von ISA Server enthalten ist. Diese Zugriffsmethode auf Exchange wird in diesem Handbuch nicht behandelt. Weitere Informationen finden Sie im Whitepaper "Configuring and Securing Microsoft Exchange 2000 Server and Clients" (englischsprachig) sowie in der *Microsoft Exchange 2000 Server Hosting Series* (Microsoft Press, ISBN: 0-7356-1829-1 und 0-7356-1830-5); eine Liste dieser Informationsquellen finden Sie im Abschnitt "Weitere Informationen".

Absichern der Kommunikation in Outlook 2002

Es gibt eine Reihe von Maßnahmen in Outlook 2002, um die Sicherheit der Kommunikation zu erhöhen. Diese Maßnahmen umfassen Folgendes:

- Verschlüsseln der MAPI-Verbindung von Outlook 2002 zum Computer mit Exchange Server.
- Signieren und Verschlüsseln von Nachrichten unter Verwendung von S/MIME-Zertifikaten.

Verschlüsseln der MAPI-Verbindung von Outlook 2002 zu Exchange Server

Windows 2000 verfügt über ein integriertes Sicherheitsfeature, das die 128-Bit-Verschlüsselung von RPC-Kommunikation ermöglicht. MAPI-Verbindungen erfolgen über RPC. Sie können diese Funktion daher nutzen, um die Sicherheit der Verbindung vom Outlook 2002-Client zum Computer mit Exchange Server zu erhöhen.

▶ **So aktivieren Sie RPC-Verschlüsselung der MAPI-Verbindung von Outlook 2002 zum Computer mit Exchange Server:**

1. Klicken Sie in Outlook 2002 auf **Extras** und dann auf **E-Mail-Konten**.
2. Klicken Sie auf **Weiter**.
3. Stellen Sie sicher, dass der Computer mit Exchange Server ausgewählt ist, und klicken Sie dann auf **Ändern**.
4. Klicken Sie auf **Weitere Einstellungen**.
5. Klicken Sie auf die Registerkarte **Erweitert**.
6. Aktivieren Sie das Kontrollkästchen **Wenn eine Netzwerkverbindung verwendet wird**.
7. Klicken Sie auf **OK**.
8. Klicken Sie auf **Weiter**.
9. Klicken Sie auf **Fertig stellen**.

Hinweis: Sie können diese Einstellung auch angeben, wenn Sie Benutzerprofile in Outlook 2002 einrichten.

RPC-Verschlüsselung verschlüsselt nur die Daten vom MAPI-Client zum Computer mit Exchange Server. Die Nachrichten selbst werden nicht verschlüsselt.

Signieren und Verschlüsseln von Nachrichten

Outlook 2002 hat die Fähigkeit, Nachrichten für die Übermittlung an interne oder externe Empfänger zu signieren und zu verschlüsseln. Für diese Verschlüsselung benötigen Sie ein Zertifikat. Wenn Sie signierte und/oder verschlüsselte E-Mails an Internetempfänger übermitteln möchten, müssen Sie ein anerkanntes Zertifikat (das als digitale Signatur bezeichnet wird) von einem Drittanbieter verwenden.

Sobald ein Zertifikat auf dem Client installiert wurde, können Sie mit dem Senden signierter und verschlüsselter Nachrichten mit S/MIME beginnen. Sie können nur dann verschlüsselte E-Mails an andere Benutzer senden, wenn Sie Zugriff auf deren öffentlichen Schlüssel haben. Sie erreichen diesen Zugriff, indem Sie den anderen Benutzer eine signierte Nachricht an Sie senden lassen und diesen Benutzer dann zu Ihren Kontakten hinzufügen. Nun ist der öffentliche Schlüssel des betreffenden Benutzers verfügbar.

Hinweis: Weitere Informationen zum Signieren und Verschlüsseln von Nachrichten finden Sie im Knowledge Base-Artikel Q286159, "Encryption and Message Security Overview" (englischsprachig).

Schlüsselverwaltungsdienst

Wenn Sie routinemäßig signierte und verschlüsselte Nachrichten zwischen Benutzern in der Exchange-Organisation versenden möchten, sollten Sie die Verwendung des Schlüsselverwaltungsdienstes in Erwägung ziehen, der im Lieferumfang von Exchange 2000 Server enthalten ist. Dieser Dienst verwendet die Windows 2000 Certificate Services und bietet Zugriff auf öffentliche Schlüssel sowie sicheren, zentralisierten Zugriff auf private Schlüssel. Auf diese Weise erhalten Clients nahtlosen Zugriff auf signierte und verschlüsselte Nachrichten, und sie können diese Nachrichten an jeden beliebigen anderen Empfänger in der Globalen Adressliste (Global Address List oder GAL) senden, für den Sicherheit aktiviert wurde.

Hinweis: Wenn Sie den Schlüsselverwaltungsserver (Key Management Server oder KMS) mit einer Zertifizierungsstelle (Certificate Authority oder CA) verwenden, die einer Drittanbieter-Zertifizierungsstelle untergeordnet ist, können Sie Ihren Schlüsselverwaltungsdienst in andere Schlüsselverwaltungsdienste im Internet integrieren.

Absichern der OWA-Kommunikation

Auf den ersten Blick ist die Kommunikation mit OWA sehr einfach. Webbrowser kommunizieren mit OWA-Servern, um E-Mails auszutauschen. Dies geschieht über Port 80 oder Port 443, wenn die Kommunikation sicher ist. Dies ist jedoch nur ein Teil des Vorgangs. Zwar stellen Clients die Verbindung mit Front-End-Servern über Port 80 oder Port 443 her, diese Front-End-Server müssen anschließend jedoch mit Domänencontrollern in ihrer Domäne kommunizieren, um die Benutzer zu authentifizieren. Außerdem müssen sie mit Back-End-Servern mit Exchange kommunizieren, um tatsächlich auf Informationen aus dem entsprechenden Postfach oder Öffentlichen Ordner zugreifen zu können.

OWA-Front-End-Server können gesichert werden, indem sie in einem Perimeternetzwerk (auch als DMZ bezeichnet) platziert werden, wobei sich der Back-End-Server hinter dem inneren Firewall befindet. Damit diese Konfiguration funktioniert, müssen jedoch viele Ports auf dem inneren Firewall geöffnet werden.

Verwenden von ISA Server zum Absichern von OWA

Um die Anzahl der Anschlüsse möglichst gering zu halten, die auf dem inneren Firewall geöffnet werden müssen, können Sie einen Firewall auf Anwendungsebene verwenden, z. B. Microsoft Internet Security and Acceleration (ISA) Server. ISA Server ermöglicht die Positionierung sowohl des SMTP-Servers als auch des OWA-Front-End-Servers hinter dem Firewall. Unter Verwendung von Serververöffentlichungs- und Webpublishing-Regeln stellt ISA Server Dienste interner Server in der Außenwelt zur Verfügung, ohne diese Server in der DMZ platzieren zu müssen.

Hinweis: Eine Liste der für die Kommunikation zwischen Front-End- und anderen Servern verwendeten Ports finden Sie im Whitepaper "Exchange 2000 Front-end and Back-end Topology" (englischsprachig), eine Informationsquelle, die im Abschnitt "Weitere Informationen" am Ende dieses Kapitels aufgeführt wird.

Die Abbildung zeigt einen ISA-Server, der einen OWA-Server für OWA-Clients im Internet veröffentlicht:

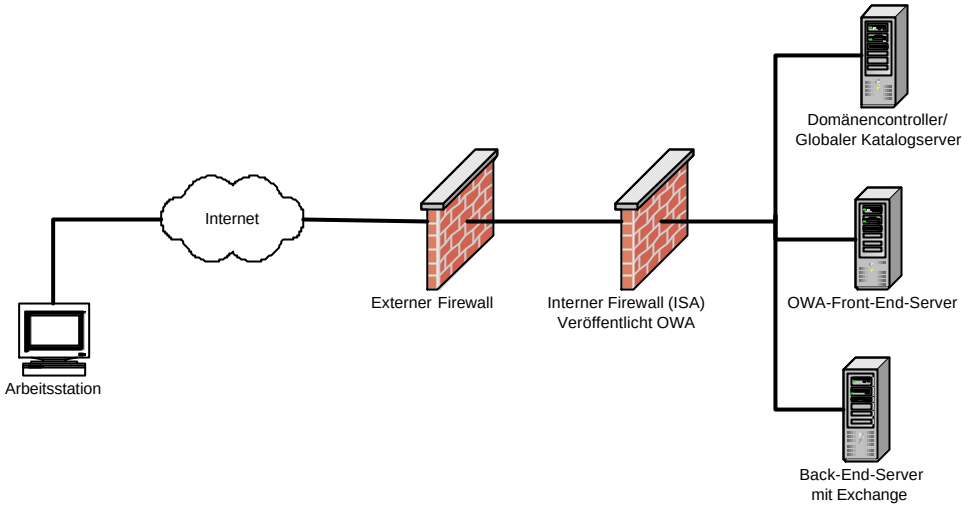

Abbildung 4.1
Sichere Firewallstruktur

Hinweis: In dieser Konfiguration müssen externe DNS-Einträge für den Front-End-OWA-Server auf die IP-Adresse verweisen, die auf dem ISA-Server veröffentlicht wird, nicht auf die Adresse des OWA-Front-End-Servers.

Hinweis: Wenn es nicht möglich ist, die vorhandene Infrastruktur mit zwei Firewalls so zu ändern, dass ISA Server integriert werden kann, können Sie ISA Server hinter dem aktuellen inneren Firewall platzieren und TCP-Port 443 an den ISA-Server übergeben.

Firewalls schützen Ihre Server vor Angriffen. Sie müssen jedoch auch die Daten schützen, die zwischen den Servern übermittelt werden. Wenn Webbrowserclients im Internet über OWA unter Verwendung von HTTP auf Exchange zugreifen, geschieht Folgendes:

Eine HTTP-Anforderung wird vom Webbrowser an den ISA-Server gesendet. Wenn die ISA-Veröffentlichungsregeln dies erlauben, werden die Anforderungen an die OWA-Front-End-Server übergeben.

ISA Server stellt eine neue HTTP-Verbindung mit dem Front-End-Server mit der eigenen IP-Adresse als IP-Quelladresse her.

Die HTTP-Anforderungen werden auf dem OWA-Front-End-Server verarbeitet. Als Teil der Verarbeitung führt der OWA-Front-End-Server die folgenden Aufgaben durch:

- Authentifizieren des Benutzers und Abfragen des globalen Katalogservers, um den Speicherort des Benutzerpostfachs zu ermitteln.
- Auflösen der IP-Adresse des Benutzerpostfachservers.

Der OWA-Front-End-Server richtet eine neue HTTP-Sitzung mit dem Back-End-Server mit Exchange ein.

Als Teil der Konfiguration von IIS für die Unterstützung von OWA müssen Sie Standardauthentifizierung aktivieren. Die integrierte Windows-Authentifizierung funktioniert nicht, weil das einzige für die Kommunikation verwendete Protokoll entweder HTTP oder HTTPS ist, und Sie dürfen keinen anonymen Zugriff verwenden, weil auf diese Weise die E-Mail-Umgebung für alle Personen im Internet zugänglich sein würde.

Standardauthentifizierung bedeutet, dass in HTTP-Verbindungen Kennwörter und E-Mail-Nachrichten im Internet in unverschlüsselter Form übermittelt werden. Wenn keine zusätzlichen Verschlüsselungsmethoden verwendet werden, werden diese Pakete auch weiterhin unverschlüsselt zwischen dem ISA-Server und dem OWA-Front-End-Server als Klartext übermittelt. Nachdem OWA die Authentifizierung durchgeführt hat, werden die gleichen unverschlüsselten Informationen einschließlich Kennwörter über HTTP zwischen dem OWA-Front-End-Server und dem Back-End-Server übertragen. Damit dies verhindert wird, müssen die Benutzeranmeldeinformationen auf dem gesamten Weg zwischen dem Webbrowser und dem Back-End-Server mit Exchange unbedingt verschlüsselt werden. Sie erreichen dies auf folgende Weise:

Absichern der Kommunikation zwischen Webbrowsern und ISA Server mit SSL-Verschlüsselung.

Absichern der Kommunikation zwischen ISA Server und den OWA-Front-End-Servern mit SSL.

Absichern der Kommunikation zwischen OWA-Front-End-Servern und Back-End-Servern mit Exchange mit IPSec-Verschlüsselung.

Jede dieser Vorgehensweisen wird im Folgenden untersucht.

Absichern der Kommunikation zwischen Webbrowsern und ISA-Servern

Um die Daten zwischen Webbrowsern und einem ISA-Server mit SSL zu verschlüsseln, müssen Sie ein SSL-Zertifikat auf dem ISA-Server sowie den entsprechenden SSL-Abhörer installieren. Das Zertifikat sollte von einer global vertrauenswürdigen Zertifizierungsstelle ausgestellt sein, weil es von externen Webclients verwendet wird, die möglicherweise nicht Teil der Infrastruktur Ihrer Organisation sind.

Konfigurieren von ISA Server für die Unterstützung von SSL-Kommunikation

ISA Server kann auf verschiedene Weise konfiguriert werden, um SSL-Anforderungen von Webbrowsern zu akzeptieren. ISA Server kann die folgenden Aufgaben durchführen:

Empfangen von SSL-Kommunikation und Übergeben der Kommunikation an Server innerhalb des Firewalls.

Entschlüsseln von SSL-Kommunikation und Übergeben der unverschlüsselten Kommunikation an den Back-End-Server.

Entschlüsseln von SSL-Kommunikation und erneutes Verschlüsseln der Kommunikation vor der Übergabe an den Back-End-Server.

Hinweis: Für das Entschlüsseln und erneute Verschlüsseln von SSL-Kommunikation ist ISA Server SP1 oder höher erforderlich. Die unten beschriebenen Verfahren funktionieren nur dann einwandfrei, wenn ISA Server SP1 oder höher installiert ist.

Das sicherste der drei genannten Verfahren besteht im Entschlüsseln der Pakete und anschließenden erneuten Verschlüsseln, weil der ISA-Server die Daten auf diese Weise auf Schwachstellen untersuchen kann. Außerdem sind die Daten so vor Angriffen im ISA-Server geschützt.

Hinweis: Die gesetzlichen Vorschriften in einigen Ländern können das Entschlüsseln von Daten und deren Untersuchung an einem Zwischenort im Netzwerk untersagen. Sie sollten die rechtlichen Folgen dieser Lösung überprüfen, bevor Sie sie implementieren.

Hinweis: Um die Leistung zu steigern und den Overhead von SSL zu verringern, sollten Sie die Verwendung von SSL-Beschleuniger-Netzwerkadaptern in Erwägung ziehen.

Damit die Daten erfolgreich verschlüsselt werden, sollten Sie Folgendes sicherstellen:

Das ISA Server-Zertifikat für OWA muss den Common Name (auch als Anzeigename bezeichnet) besitzen, der dem voll qualifizierten Domänennamen (Fully Qualified Domain Name oder FQDN) entspricht, der von den Webbrowsern für Verweise auf OWA-Ressourcen verwendet wird. Wenn der vom Client verwendete OWA-URL z. B. **https://mail.nwtraders.com/exchange** lautet, sollte der Common Name des Zertifikats **mail.nwtraders.com** lauten.

Das Zertifikat muss in den *Persönlichen* Computerspeicher des ISA-Servers oder der Server importiert werden, der oder die die OWA-Ressourcen veröffentlichen. Stellen Sie beim Importieren des Zertifikats auf den ISA-Server sicher, dass das Kontrollkästchen **Privaten Schlüssel als exportierbar markieren** aktiviert ist.

Um die unbeabsichtigte Übertragung von Kennwörtern in Klartext zu vermeiden, sollte der ISA-Server nur einen sicheren Kanal erlauben und unverschlüsselte HTTP-Verbindungen für die veröffentlichte OWA-Site zurückweisen.

ISA Server verwendet eine Webveröffentlichungsregel, um den OWA-Server Internetclients zur Verfügung zu stellen. Bevor die Webveröffentlichungsregel erstellt werden kann, muss die Webveröffentlichung selbst auf dem ISA-Server vorbereitet werden. Dies erfolgt durch Konfigurieren von **Eingehende Webanfragen** und **Ausgehende Webanfragen**.

Hinweis: Bevor Sie das folgende Verfahren anwenden können, müssen Sie das externe Zertifikat importieren.

▶ **So konfigurieren Sie eingehende Webanfragen:**

1. Starten Sie **ISA-Verwaltung**.
2. Klicken Sie mit der rechten Maustaste auf den ISA-Server, und wählen Sie dann **Eigenschaften** aus.
3. Klicken Sie auf die Registerkarte **Eingehende Webanfragen**.
4. Wählen Sie **Abhörer individuell pro IP-Adresse konfigurieren** aus, und klicken Sie dann auf **Hinzufügen**.
5. Wählen Sie Ihren ISA-Server aus, und wählen Sie dann die externe IP-Adresse Ihres ISA-Servers aus.
6. Wählen Sie **Webclients mit Serverzertifikat authentifizieren** aus.
7. Klicken Sie auf **Auswählen**, und wählen Sie dann das Zertifikat für den FQDN aus, den die Clients für den Zugriff auf die SSL-Site verwenden.
8. Klicken Sie auf **OK**.
9. Wählen Sie **SSL-Abhörung aktivieren** aus.
10. Klicken Sie auf **OK**.
11. Klicken Sie auf **OK**.
12. Klicken Sie auf **Änderungen speichern und Dienste neu starten**, und klicken Sie dann auf **OK**.

▶So konfigurieren Sie ausgehende Webanfragen:

Hinweis: Wenn Sie das folgende Verfahren durchführen, wird verhindert, dass Benutzer im internen Netzwerk den ISA-Server als Proxyserver für den Zugriff auf Websites im Internet verwenden können. Dieses Verfahren ist nicht erforderlich, um OWA über ISA zur Verfügung zu stellen, wird jedoch zum Bereitstellen zusätzlicher Sicherheit beschrieben.

---

1. Starten Sie **ISA-Verwaltung**.
2. Klicken Sie mit der rechten Maustaste auf den ISA-Server, und wählen Sie dann **Eigenschaften** aus.
3. Klicken Sie auf die Registerkarte **Ausgehende Webanfragen**.
4. Wählen Sie **Abhörer individuell pro IP-Adresse konfigurieren** aus, und klicken Sie dann auf **OK**.
5. Klicken Sie auf **Änderungen speichern und Dienste neu starten**, und klicken Sie dann auf **OK**.

Sie sind nun bereit, Webveröffentlichung zur Unterstützung von OWA zu konfigurieren.

▶So konfigurieren Sie Webveröffentlichung für OWA:

1. Erweitern Sie in **ISA-Verwaltung** den ISA-Server, und erweitern Sie dann **Veröffentlichung**.
2. Klicken Sie mit der rechten Maustaste auf **Webveröffentlichungsregeln**, wählen Sie **Neu** aus, und wählen Sie dann **Regel** aus.
3. Geben Sie einen Namen an, z. B. *OWA – <FQDN des OWA-Front-End-Servers>*, und klicken Sie dann auf **Weiter**.
4. Vergewissern Sie sich, dass **Alle Ziele** ausgewählt ist, und klicken Sie dann auf **Weiter**.
5. Vergewissern Sie sich, dass **Alle Anfragen** ausgewählt ist, und klicken Sie dann auf **Weiter**.
6. Wählen Sie **Anfrage an internen Webserver (Name oder IP-Adresse) umleiten** aus, klicken Sie auf **Durchsuchen**, und wählen Sie dann Ihren OWA-Front-End-Server aus.
7. Wählen Sie **Original Hostheader anstelle des oben angegebenen an den Veröffentlichungserver senden** aus, und klicken Sie dann auf **Weiter**.
8. Klicken Sie auf **Fertig stellen**.
9. Klicken Sie im Ordnerfenster auf **Webveröffentlichungsregeln,** und doppelklicken Sie dann auf die neue Regel.
10. Klicken Sie auf die Registerkarte **Überbrücken**.
11. Wählen Sie **Sicherer Kanal (SSL) ist erforderlich für die veröffentlichte Site** aus, wählen Sie **128-Bit-Verschlüsselung ist erforderlich** aus, und klicken Sie dann auf **OK**.

Hinweis: Sie müssen außerdem entsprechende Regeln für Port 80 und Port 443 auf den entsprechenden Routern und Firewalls in Ihrer Umgebung konfigurieren.

Hinweis: Weitere Informationen zum Veröffentlichen von SMTP und OWA mit ISA Server finden Sie in den Knowledge Base-Artikeln Q290113, "How to Publish Outlook Web Access Behind ISA Server" (englischsprachig), und Q308599, "How to Configure ISA Server to Publish Exchange for OWA" (englischsprachig).

Verschlüsselung zwischen ISA-Servern und OWA-Front-End-Servern

Um den HTTP-Datenverkehr zwischen dem ISA-Server und einem OWA-Front-End-Server zu verschlüsseln, müssen Sie ein SSL-Zertifikat auf den OWA-Front-End-Servern installieren. ISA-Server und OWA-Front-End-Server sind Teil der Infrastruktur Ihrer Organisation. Aus diesem Grund kann das OWA-Front-End-Zertifikat von der internen Stammzertifizierungsstelle Ihrer Organisation oder einer ihrer vertrauenswürdigen untergeordneten Zertifizierungsstelle ausgestellt werden.

▶ **So fordern Sie ein Zertifikat für den OWA-Front-End-Server an:**

Hinweis: Die folgenden Schritte setzen voraus, dass in Ihrer Umgebung eine Organisationszertifizierungsstelle installiert ist.

---

1. Starten Sie **Internetdienste-Manager** auf dem OWA-Front-End-Server.
2. Klicken Sie mit der rechten Maustaste auf **Standardwebsite**, und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf die Registerkarte **Verzeichnissicherheit**, und klicken Sie dann auf **Serverzertifikat**.
4. Klicken Sie auf **Weiter**, klicken Sie auf **Neues Zertifikat erstellen**, und klicken Sie dann auf **Weiter**.
5. Klicken Sie auf die Optionsschaltfläche **Anforderung sofort an eine Onlinezertifizierungsstelle senden**, und klicken Sie dann auf **Weiter**.
6. Geben Sie im Feld **Name** einen Namen ein, und klicken Sie dann auf **Weiter**.
7. Geben Sie im Feld **Organisation** den Namen Ihrer Organisation ein.
8. Geben Sie im Feld **Organisationseinheit** den Namen Ihrer Organisationseinheit ein, und klicken Sie dann auf **Weiter**.
9. Geben Sie im Feld **Common Name** den voll qualifizierten Domänennamen des OWA-Front-End-Servers ein, und klicken Sie dann auf **Weiter**.
10. Geben Sie die Bundesland- und Städteinformationen ein, und klicken Sie dann auf **Weiter**.
11. Vergewissern Sie sich im Dropdownlistenfeld **Zertifizierungsstellen**, dass Ihre Zertifizierungsstelle ausgewählt ist, und klicken Sie dann auf **Weiter**.
12. Klicken Sie auf **Weiter**, um die Anforderung zu senden, und klicken Sie dann auf **Fertig stellen**, um den Assistenten abzuschließen.
13. Klicken Sie auf der Registerkarte **Verzeichnissicherheit** im Gruppenfeld **Sichere Kommunikation** auf **Bearbeiten**.
14. Wählen Sie **Sicherer Kanal (SSL) ist erforderlich** aus, wählen Sie **128-Bit-Verschlüsselung erforderlich** aus, und klicken Sie dann auf **OK**.
15. Klicken Sie auf der Registerkarte **Verzeichnissicherheit** im Gruppenfeld **Steuerung des anonymen Zugriffs und der Authentifizierung** auf **Bearbeiten**.
16. Wählen Sie **Standardauthentifizierung (Kennwort wird als Klartext gesendet)** aus, und klicken Sie dann auf **Ja**, um die Warnung zu bestätigen.
17. Deaktivieren Sie alle anderen Optionen, und klicken Sie dann auf **OK**.
18. Klicken Sie auf **OK**.
19. Klicken Sie auf **OK**, um das Dialogfeld **Vererbungsüberschreibungen** zu schließen, und schließen Sie dann **Internetdienste-Manager**.

Hinweis: Der Common Name ist der voll qualifizierte Domänenname des OWA-Servers, weil dieser der OWA-Veröffentlichungsregeleigenschaft auf dem ISA-Server entspricht. ISA Server überprüft während des Veröffentlichungsvorgangs die Gültigkeit des OWA-Webzertifikats sowie die Zertifikatsvertrauenskettenüberprüfung und das Ablaufdatum des Zertifikats.

Verschlüsselung zwischen OWA-Front-End-Servern und Back-End-Servern mit Exchange

Zwischen OWA-Front-End-Servern und Back-End-Servern können Daten nicht mit SSL verschlüsselt werden. Da jedoch sowohl die Front-End- als auch die Back-End-Server Windows 2000 ausführen, können Sie IPSec für diese Verschlüsselung verwenden. IPSec besitzt den Vorteil, erheblich schneller als SSL zu sein.

Hinweis: Um die Leistung zu steigern und den Overhead von IPSec zu verringern, sollten Sie die Verwendung spezieller Netzwerkadapter in Erwägung ziehen, die die IPSec-Verarbeitung auf den Adapter verlagern.

IPSec ermöglicht die Steuerung, welche Protokolle vom Netzwerkadapter akzeptiert werden, das Blockieren oder Freigeben bestimmter Anschlüsse und das Verschlüsseln von Anschlüssen. Im Fall der Front-End-/Back-End-Serverkommunikation müssen Sie sicherstellen, dass Port 80 verschlüsselt ist.

IPSec wird über IPSec-Richtlinien gesteuert, die in der Windows 2000-Gruppenrichtlinie definiert werden.

Tabelle 4.1: IPSec-Richtlinieneinstellungen

Richtlinie	Einstellungen
OWA-Front-End	Port 80 Ausgehend – Verschlüsseln Port 80 Eingehend – Blockieren
Back-End	Port 80 Eingehend – Verschlüsseln

Es ist möglich, eingehende Anforderungen vom Front-End-Server zu blockieren, weil der Front-End-Server die gesamte Kommunikation mit dem Back-End-Server einleitet. Durch das Blockieren dieser Anforderungen wird die unbeabsichtigte Übertragung von Benutzeranmeldeinformationen als Klartext vermieden und das Risiko von Pufferüberlaufangriffen auf dem Front-End-Server verringert.

Erstellen der IPSec-Richtlinie für den OWA-Front-End-Server

Die erste Richtlinie, die erstellt und konfiguriert werden muss, bezieht sich auf den OWA-Front-End-Server.

▶ **So erstellen Sie den TCP-Port 80-Filter für ausgehenden Datenverkehr:**

1. Starten Sie **Active Directory-Benutzer und -Computer**.
2. Erweitern Sie **Mitgliedsserver**, erweitern Sie **Anwendungsserver**, und erweitern Sie dann **Exchange 2000**.
3. Klicken Sie mit der rechten Maustaste auf die Organisationseinheit **OWA Front-end Servers**, und klicken Sie dann auf **Eigenschaften**.
4. Klicken Sie auf die Registerkarte **Gruppenrichtlinie**.
5. Wählen Sie das Gruppenrichtlinienobjekt **OWA Front End Incremental** aus.
6. Klicken Sie auf **Bearbeiten**.
7. Erweitern Sie **Windows-Einstellungen**, **Sicherheitseinstellungen**, und klicken Sie dann mit der rechten Maustaste auf **IP-Sicherheitsrichtlinien auf Active Directory**.
8. Klicken Sie auf **IP-Filterlisten und Filteraktionen verwalten**.
9. Klicken Sie auf **Hinzufügen**.
10. Geben Sie **Ausgehend TCP 80 – OWA FE** im Feld **Name** ein.
11. Geben Sie **Der Filter gleicht ausgehenden TCP Port 80-Datenverkehr mit dem OWA Front-End-Server ab** im Feld **Beschreibung** ein.
12. Klicken Sie auf **Hinzufügen**, und klicken Sie dann auf **Weiter**.
13. Vergewissern Sie sich im Dropdownlistenfeld **Quelladresse**, dass **Eigene IP-Adresse** angezeigt wird, und klicken Sie dann auf **Weiter**.
14. Vergewissern Sie sich im Dropdownlistenfeld **Zieladresse**, dass **Beliebige IP-Adresse** angezeigt wird, und klicken Sie dann auf **Weiter**.
15. Wählen Sie im Dropdownlistenfeld **Wählen Sie einen Protokolltyp** den Typ **TCP** aus, und klicken Sie dann auf **Weiter**.
16. Vergewissern Sie sich im Feld **Legen Sie den Port des IP-Protokolls fest**, dass **Von jedem Port** ausgewählt ist, wählen Sie **Zu diesem Port** aus, und geben Sie dann **80** ein.
17. Klicken Sie auf **Weiter**, und klicken Sie dann auf **Fertig stellen**.
18. Klicken Sie auf **Schließen**, um das Fenster **IP-Filterliste** zu schließen.

▶ **So erstellen Sie den TCP-Port 80-Filter für eingehenden Datenverkehr:**

1. Klicken Sie auf **Hinzufügen**.
2. Geben Sie **Eingehend TCP 80 – OWA FE** im Feld **Name** ein.
3. Geben Sie **Der Filter gleicht eingehenden TCP Port 80-Datenverkehr mit dem OWA Front-End-Server ab** im Feld **Beschreibung** ein.
4. Klicken Sie auf **Hinzufügen**, und klicken Sie dann auf **Weiter**.
5. Vergewissern Sie sich im Dropdownlistenfeld **Quelladresse**, dass **Beliebige IP-Adresse** angezeigt wird, und klicken Sie dann auf **Weiter**.
6. Vergewissern Sie sich im Dropdownlistenfeld **Zieladresse**, dass **Eigene IP-Adresse** angezeigt wird, und klicken Sie dann auf **Weiter**.
7. Wählen Sie im Dropdownlistenfeld **Wählen Sie einen Protokolltyp** den Typ **TCP** aus, und klicken Sie dann auf **Weiter**.
8. Vergewissern Sie sich im Feld **Legen Sie den Port des IP-Protokolls fest**, dass **Von jedem Port** ausgewählt ist, wählen Sie **Zu diesem Port** aus, und geben Sie dann **80** ein.
9. Klicken Sie auf **Weiter**, und klicken Sie dann auf **Fertig stellen**.

10. Klicken Sie auf **Schließen**.
11. Klicken Sie auf **Schließen**.

▶ **So erstellen Sie die Blockieraktion, die mit dem TCP-Port 80-Filter für eingehenden Datenverkehr verwendet wird:**

1. Klicken Sie im Fenster **Gruppenrichtlinie** mit der rechten Maustaste auf **IP-Sicherheitsrichtlinien auf Active Directory,** und wählen Sie dann **IP-Filterlisten und Filteraktionen verwalten** aus.
2. Klicken Sie auf die Registerkarte **Filteraktionen verwalten**.
3. Klicken Sie auf **Hinzufügen**, und klicken Sie dann auf **Weiter**.
4. Geben Sie **Blockieren** im Feld **Name** ein, und klicken Sie dann auf **Weiter**.
5. Wählen Sie **Sperren** aus, und klicken Sie dann auf **Weiter**.
6. Klicken Sie auf **Fertig stellen**.

▶ **So erstellen Sie die Verschlüsselungsaktion, die mit dem TCP-Port 80-Filter für ausgehenden Datenverkehr verwendet wird:**

1. Klicken Sie auf die Registerkarte **Filteraktionen verwalten**.
2. Klicken Sie auf **Hinzufügen**, und klicken Sie dann auf **Weiter**.
3. Geben Sie **Verschlüsseln** im Feld **Name** ein, und klicken Sie dann auf **Weiter**.
4. Wählen Sie **Sicherheit aushandeln** aus, und klicken Sie dann auf **Weiter**.
5. Wählen Sie **Keine Kommunikation mit Computern zulassen, die IPSec nicht unterstützen** aus, und klicken Sie dann auf **Weiter**.
6. Vergewissern Sie sich, dass **Hoch (Encapsulated Secure Payload)** ausgewählt ist, und klicken Sie dann auf **Weiter**.
7. Klicken Sie auf **Eigenschaften bearbeiten**, und klicken Sie dann auf **Fertig stellen**.
8. Klicken Sie auf **Hinzufügen**.
9. Wählen Sie **Benutzerdefiniert (nur für erfahrene Benutzer)** aus, und klicken Sie dann auf **Einstellungen**.
10. Vergewissern Sie sich, dass nur **Datenintegrität und Verschlüsselung (ESP)** ausgewählt ist.
11. Wählen Sie **3DES** als **Verschlüsselungsalgorithmus** aus.
12. Klicken Sie auf **OK**.
13. Klicken Sie auf **OK**.
14. Wählen Sie **Benutzerdefiniert** aus, und klicken Sie dann auf **Nach oben**.
15. Klicken Sie auf **OK**.
16. Klicken Sie auf **Schließen**.

▶ **So erstellen Sie die IP-Sicherheitsrichtlinie, wenden die Filter an und geben die Aktionen an:**

1. Klicken Sie mit der rechten Maustaste auf **IP-Sicherheitsrichtlinien auf Active Directory**, wählen Sie **IP-Sicherheitsrichtlinie erstellen** aus, und klicken Sie dann auf **Weiter**.
2. Geben Sie **Blockieren-Verschlüsseln TCP 80 Datenverkehr – OWA FE** im Feld **Name** ein, und klicken Sie dann auf **Weiter**.
3. Vergewissern Sie sich, dass **Die Standardantwortregel aktivieren** ausgewählt ist, und klicken Sie dann auf **Weiter**.
4. Vergewissern Sie sich, dass **Windows 2000-Standard (Kerberos V5-Protokoll)** ausgewählt ist, und klicken Sie dann auf **Weiter**.

5. Vergewissern Sie sich, dass **Eigenschaften bearbeiten** ausgewählt ist, und klicken Sie dann auf **Fertig stellen**.
6. Klicken Sie auf der Registerkarte **Regeln** auf **Hinzufügen**, und klicken Sie dann auf **Weiter**.
7. Vergewissern Sie sich, dass **Diese Regel spezifiziert keinen Tunnel** ausgewählt ist, und klicken Sie dann auf **Weiter**.
8. Vergewissern Sie sich, dass **Alle Netzwerkverbindungen** ausgewählt ist, und klicken Sie dann auf **Weiter**.
9. Vergewissern Sie sich, dass **Windows 2000-Standard (Kerberos V5-Protokoll)** ausgewählt ist, und klicken Sie dann auf **Weiter**.
10. Wählen Sie **Eingehend TCP 80 – OWA FE** in den **IP-Filterlisten** aus, und klicken Sie dann auf **Weiter**.
11. Klicken Sie im Feld **Filteraktionen** auf **Blockieren**, und klicken Sie dann auf **Weiter**.
12. Vergewissern Sie sich, dass das Kontrollkästchen **Eigenschaften bearbeiten** deaktiviert ist, und klicken Sie dann auf **Fertig stellen**.
13. Klicken Sie auf der Registerkarte **Regeln** auf **Hinzufügen**, und klicken Sie dann auf **Weiter**.
14. Vergewissern Sie sich, dass **Diese Regel spezifiziert keinen Tunnel** ausgewählt ist, und klicken Sie dann auf **Weiter**.
15. Vergewissern Sie sich, dass **Alle Netzwerkverbindungen** ausgewählt ist, und klicken Sie dann auf **Weiter**.
16. Vergewissern Sie sich, dass **Windows 2000-Standard (Kerberos V5-Protokoll)** ausgewählt ist, und klicken Sie dann auf **Weiter**.
17. Wählen Sie **Ausgehend TCP 80 – OWA FE** in den **IP-Filterlisten** aus, und klicken Sie dann auf **Weiter**.
18. Klicken Sie im Feld **Filteraktionen** auf **Verschlüsseln**, und klicken Sie dann auf **Weiter**.
19. Vergewissern Sie sich, dass das Kontrollkästchen **Eigenschaften bearbeiten** deaktiviert ist, und klicken Sie dann auf **Fertig stellen**.
20. Klicken Sie auf **Schließen**.

▶ **So wenden Sie den Filter für ausgehenden Datenverkehr auf die Gruppenrichtlinie an:**

1. Klicken Sie im Inhaltsfenster der Gruppenrichtlinie mit der rechten Maustaste auf **Blockieren-Verschlüsseln TCP 80 Datenverkehr – OWA FE**, und klicken Sie dann auf **Zuweisen**.
2. Schließen Sie das Dialogfeld **Gruppenrichtlinie**, und klicken Sie dann auf **OK**.

▶ **So wenden Sie die Gruppenrichtlinie auf den OWA-Front-End-Server an:**

1. Starten Sie auf dem OWA-Front-End-Server eine Eingabeaufforderung.
2. Geben Sie **secedit /refreshpolicy machine_policy /enforce** ein, und drücken Sie dann die EINGABETASTE.
3. Starten Sie den Server neu.

Erstellen der IPSec-Richtlinie für den Back-End-Server

Die Richtlinie auf dem Back-End-Server verschlüsselt eingehenden Datenverkehr an Port 80.

▶ **So erstellen Sie den TCP-Port 80-Filter für eingehenden Datenverkehr:**

1. Starten Sie **Active Directory-Benutzer und -Computer**.
2. Erweitern Sie **Mitgliedsserver**, erweitern Sie **Anwendungsserver**, und erweitern Sie dann **Exchange 2000**.
3. Klicken Sie mit der rechten Maustaste auf die Organisationseinheit **Back-End-Server**, und klicken Sie dann auf **Eigenschaften**.

4. Klicken Sie auf die Registerkarte **Gruppenrichtlinie**.
5. Wählen Sie das Gruppenrichtlinienobjekt **Back End Incremental** aus.
6. Klicken Sie auf **Bearbeiten**.
7. Erweitern Sie **Windows-Einstellungen**, **Sicherheitseinstellungen**, und klicken Sie dann mit der rechten Maustaste auf **IP-Sicherheitsrichtlinien auf Active Directory**.
8. Klicken Sie auf **IP-Filterlisten und Filteraktionen verwalten**.
9. Klicken Sie auf **Hinzufügen**.
10. Geben Sie **Eingehend TCP 80 – BE** im Feld **Name** ein.
11. Geben Sie **Der Filter gleicht eingehenden TCP Port 80-Datenverkehr mit dem Back-End-Server ab** im Feld **Beschreibung** ein.
12. Klicken Sie auf **Hinzufügen**, und klicken Sie dann auf **Weiter**.
13. Vergewissern Sie sich im Dropdownlistenfeld **Quelladresse**, dass **Eigene IP-Adresse** angezeigt wird, und klicken Sie dann auf **Weiter**.
14. Vergewissern Sie sich im Dropdownlistenfeld **Zieladresse**, dass **Beliebige IP-Adresse** angezeigt wird, und klicken Sie dann auf **Weiter**.
15. Wählen Sie im Dropdownlistenfeld **Wählen Sie einen Protokolltyp** den Typ **TCP** aus, und klicken Sie dann auf **Weiter**.
16. Vergewissern Sie sich im Feld **Legen Sie den Port des IP-Protokolls fest**, dass **Von jedem Port** ausgewählt ist, wählen Sie **Zu diesem Port** aus, und geben Sie dann **80** ein.
17. Klicken Sie auf **Weiter**, und klicken Sie dann auf **Fertig stellen**.
18. Klicken Sie auf **Schließen**, um das Fenster **IP-Filterliste** zu schließen.

▶ **So erstellen Sie die IP-Sicherheitsrichtlinie, wenden die Filter an und geben die Aktionen an:**

1. Erweitern Sie **IP-Sicherheitsrichtlinien auf Active Directory**, wählen Sie **IP-Sicherheitsrichtlinie erstellen** aus, und klicken Sie dann auf **Weiter**.
2. Geben Sie **Verschlüsseln TCP 80 Datenverkehr – BE** im Feld **Name** ein, und klicken Sie dann auf **Weiter**.
3. Vergewissern Sie sich, dass **Die Standardantwortregel aktivieren** ausgewählt ist, und klicken Sie dann auf **Weiter**.
4. Vergewissern Sie sich, dass **Windows 2000-Standard (Kerberos V5-Protokoll)** ausgewählt ist, und klicken Sie dann auf **Weiter**.
5. Vergewissern Sie sich, dass **Eigenschaften bearbeiten** ausgewählt ist, und klicken Sie dann auf **Fertig stellen**.
6. Klicken Sie auf der Registerkarte **Regeln** auf **Hinzufügen**, und klicken Sie dann auf **Weiter**.
7. Vergewissern Sie sich, dass **Diese Regel spezifiziert keinen Tunnel** ausgewählt ist, und klicken Sie dann auf **Weiter**.
8. Vergewissern Sie sich, dass **Alle Netzwerkverbindungen** ausgewählt ist, und klicken Sie dann auf **Weiter**.
9. Vergewissern Sie sich, dass **Windows 2000-Standard (Kerberos V5-Protokoll)** ausgewählt ist, und klicken Sie dann auf **Weiter**.
10. Wählen Sie **Eingehend TCP 80 – BE** in den **IP-Filterlisten** aus, und klicken Sie dann auf **Weiter**.
11. Klicken Sie im Feld **Filteraktionen** auf **Verschlüsseln**, und klicken Sie dann auf **Weiter**.
12. Vergewissern Sie sich, dass das Kontrollkästchen **Eigenschaften bearbeiten** deaktiviert ist, und klicken Sie dann auf **Fertig stellen**.
13. Klicken Sie auf **Schließen**.

▶ So wenden Sie den Filter für eingehenden Datenverkehr auf die Gruppenrichtlinie an:

1. Klicken Sie im Inhaltsfenster der Gruppenrichtlinie mit der rechten Maustaste auf **Verschlüsseln TCP 80 Datenverkehr – BE**, und klicken Sie dann auf **Zuweisen**.
2. Schließen Sie das Dialogfeld **Gruppenrichtlinie**, und klicken Sie dann auf **OK**.

▶ **So wenden Sie die Gruppenrichtlinie auf den Back-End-Server an:**

1. Starten Sie auf dem OWA-Front-End-Server eine Eingabeaufforderung.
2. Geben Sie **secedit /refreshpolicy machine_policy /enforce** ein, und drücken Sie dann die EINGABETASTE.
3. Starten Sie den Server neu.

Hinweis: Sie können die IPSec-Einstellungen auch auf jedem lokalen Computer anwenden. Dies stellt sicher, dass IPSec auch dann verwendet wird, wenn ein Problem beim Zugreifen auf die Gruppenrichtlinie vom Domänencontroller aus auftritt.

Überwachen von IP-Sicherheitsverbindungen

Nachdem Sie IPSec konfiguriert haben, ist es sinnvoll, die Funktionalität zu überprüfen, indem auf IPSec bezogene Ereignisse überwacht werden und das IP-Sicherheitsüberwachungstool verwendet wird.

▶ **So starten und konfigurieren Sie die IP-Sicherheitsüberwachung:**

1. Klicken Sie auf dem OWA-Front-End- oder dem Back-End-Server zum Starten des IP-Sicherheitsüberwachungstools auf **Start**, klicken Sie auf **Ausführen**, und geben Sie dann **ipsecmon** im Feld **Öffnen** ein.
2. Klicken Sie auf **Optionen**, und ändern Sie den standardmäßigen Wert für **Aktualisierung (Sek.)** von **15** in **1**.
3. Klicken Sie auf **OK**.

▶ **So überprüfen Sie die erfolgreiche Konfiguration von IPSec:**

1. Generieren Sie Datenverkehr zwischen den OWA-Front-End- und Back-End-Servern, indem Sie einen Benutzer E-Mails mit OWA senden lassen.
2. Wechseln Sie zur IP-Sicherheitsüberwachung, die anzeigen sollte, dass der Datenverkehr zwischen dem OWA-Front-End-Server und dem Back-End-Server verschlüsselt ist.

Hinweis: Weitere Informationen zu IPSec finden Sie in "Step-by-Step Guide to Internet Protocol Security (IPSec)" (englischsprachig). Einzelheiten hierzu finden Sie im Abschnitt "Weitere Informationen".

Absichern der SMTP-Kommunikation

Jeder Back-End-Server mit Exchange führt SMTP aus, da dieses Protokoll für den Mailtransport zwischen Computern mit Exchange Server und dem Mailtransport im Internet verantwortlich ist. Dieser Abschnitt erläutert, wie bei möglichst geringem Risiko von Angriffen auf Ihre Organisation im Netzwerk SMTP-Verbindungen zur Verfügung gestellt werden können.

Verwenden von ISA Server zum Absichern von SMTP

Ebenso wie beim OWA-Front-End-Server können Sie auch auf dem inneren Firewall die Anzahl der geöffneten Ports so gering wie möglich halten, indem Sie die Funktionen von ISA Server verwenden. In diesem Fall können Sie die Veröffentlichungsfunktion von ISA Server verwenden, um den SMTP-Server zu veröffentlichen und den Computer mit Exchange Server selbst hinter dem Firewall zu positionieren. ISA Server verkörpert den internen SMTP-Server, ohne dass Sie Exchange im Perimeternetzwerk platzieren müssen.

Hinweis: In dieser Konfiguration müssen externe DNS-Einträge für SMTP auf die IP-Adresse verweisen, die auf dem ISA-Server veröffentlicht wird, nicht auf die Adresse des SMTP-Servers.

Hinweis: Wenn es nicht möglich ist, die vorhandenen Infrastrukturen mit zwei Firewalls so zu ändern, dass ISA Server integriert werden kann, können Sie den ISA-Server hinter dem aktuellen inneren Firewall platzieren und TCP-Port 25 an den ISA-Server übergeben.

Hinweis: Wenn Sie eine Form von Authentifizierung über Port 25 implementieren möchten, sollten Sie SSL-Authentifizierung für SMTP aktivieren.

Hinweis: Sie können ausgehendes SMTP nicht auf einem ISA-Server veröffentlichen, wenn der Server ein aktives Mitglied eines ISA-Arrays ist.

Verwenden von Inhaltsfiltern mit der Nachrichtenüberwachung

Inhaltsfilter aktivieren den SMTP-Filter, der eingehenden Datenverkehr an Port 25 akzeptiert, diesen untersucht und nur dann weiterleitet, wenn die Regeln dies erlauben. Der Filter kann Nachrichten basierend auf dem Benutzernamen oder Domänennamen des Senders, Anlagen oder Schlüsselwörter akzeptieren oder zurückweisen und sogar einen gewissen Schutz vor Pufferüberlaufangriffen bieten. Damit der SMTP-Filter umfassende Funktionalität besitzt, sollten Sie jedoch außerdem die Nachrichtenüberwachung installieren.

Nachrichtenüberwachung ist ein separates Dienstprogramm, das im Lieferumfang von ISA Server enthalten ist. Es kann in verschiedenen Konfigurationen installiert werden; die sicherste Implementierung der Nachrichtenüberwachung ist jedoch auf einem Server, der IIS mit einem virtuellen SMTP-Server ausführt. Dieser virtuelle Server kommuniziert dann mit Exchange, um E-Mails zu senden und zu empfangen. Dieses Vorgehen besitzt den Vorteil, dass der Computer mit Exchange Server noch weiter vor Zugriffen aus externen Netzwerken geschützt ist.

Hinweis: Weitere Informationen zum Bereitstellen von Nachrichtenüberwachung finden Sie im Knowledge Base-Artikel Q315132, "HOW TO: Configure SMTP Message Screener in ISA Server 2000" (englischsprachig). Weitere Informationen finden Sie im Abschnitt "Weitere Informationen" am Ende dieses Kapitels.

Weitere Maßnahmen zum Absichern von SMTP

Das Veröffentlichen von SMTP über ISA Server und das Verwenden des SMTP-Filters mit Nachrichtenüberwachung unterstützen Sie beim Schützen der Exchange SMTP-Server. Sie können jedoch auch noch weitere Maßnahmen in Betracht ziehen.

Verwenden eines separaten SMTP-Gateways

Als Teil Ihrer Strategie der umfassenden Verteidigung können Sie die Back-End-Server mit Exchange vor SMTP-Angriffen schützen, indem Sie ein separates SMTP-Gateway in Ihrem

Netzwerk verwenden. Die eingehenden E-Mails aus dem Internet durchlaufen dann diesen Server, bevor sie an einen Computer mit Exchange Server weitergeleitet werden. Dieser Server ist nicht Teil einer Windows 2000-Domäne und führt aus diesem Grund Exchange nicht aus. Der Vorteil dieser Vorgehensweise besteht darin, dass ein externer Angreifer, der SMTP für seinen Angriffsversuch auf Computer mit Exchange Server verwendet, zuerst mit dem separaten SMTP-Server konfrontiert ist. Das Ausschalten des SMTP-Servers bedeutet möglicherweise, dass Sie nicht mehr in der Lage sind, E-Mails über das Internet zu senden, Sie können jedoch auch weiterhin interne E-Mails senden. Auf diesem Server können Sie auch Antivirensoftware ausführen.

Hinweis: Weitere Informationen zum Einrichten und Konfigurieren eines virtuellen SMTP-Servers finden Sie im Knowledge Base-Artikel Q308161, "HOW TO: Set Up and Configure an SMTP Virtual Server in Windows 2000" (englischsprachig).

Verhindern von Mailweiterleitung

Mailweiterleitung ist das Verwenden eines Zwischenservers zum Annehmen und anschließenden erneuten Senden von E-Mail an Empfänger auf einem anderen Server. Sie kann berechtigte Gründe haben. Benutzer, die reisen, können z. B. wünschen, Verbindungen mit Ihrem SMTP-Server herstellen zu können, um E-Mail senden zu können, wenn sie sich außerhalb des Netzwerks befinden.

Wenn Sie eingeschränkte Weiterleitung von außerhalb des Netzwerks zulassen möchten, sollten Sie die verwendeten Verfahren sehr streng regulieren und sicherstellen, dass Authentifizierung der Benutzer durchgeführt wird, die die Weiterleitung nutzen müssen (Authentifizierung ist standardmäßig aktiviert). Wenn Sie die SMTP-Weiterleitung zu weit öffnen, werden bald sehr große Mengen von E-Mails Ihren SMTP-Server durchlaufen, die Leistung der Umgebung beeinträchtigen und die Menge unerwünschter Nachrichten im Internet vergrößern. Außerdem ist es möglich, dass Sie in Spammail-Blockierlisten aufgenommen werden. Dies verhindert möglicherweise, dass Ihre ordnungsgemäßen E-Mails ihr Ziel erreichen.

Selbst eine autorisierte Mailweiterleitung kann Probleme auf Ihrem Mailserver verursachen. Angreifer verwenden die Tatsache, dass Ihr Mailserver authentifizierte Anforderungen akzeptiert, um einen Wörterbuchangriff auf den Server zu versuchen.

Eine empfehlenswerte Vorgehensweise zum Schutz des Servers besteht im größtmöglichen Deaktivieren von Weiterleitung. Externe Benutzer benötigen keine direkten Verbindungen mit Ihrem SMTP-Server, um E-Mails senden zu können, da sie OWA verwenden können.

Um die Computer mit Exchange Server vor Mailweiterleitung zu schützen, ziehen Sie die folgenden Maßnahmen auf den internen virtuellen SMTP-Servern in Betracht:

- Zulassen ausschließlich anonymer Verbindungen mit den SMTP-Servern.
- Verhindern, dass Computer, die erfolgreich authentifiziert werden, Nachrichten weiterleiten können.
- Zulassen ausschließlich von SMTP-Verbindungen von bestimmten IP-Adressen.

Sie müssen diese Konfiguration auf SMTP-Servern am Gateway ein wenig öffnen. Die genauen Einstellungen hängen vom Nachrichtenfluss und der Konfiguration des Mailservers Ihres Internetdienstanbieters ab. Die beste Methode zum Erhöhen der Sicherheit besteht jedoch im vollkommenen Sperren der Systeme, um die Weiterleitung zu verhindern, und dem anschließenden Ermitteln der minimalen Einstellungen, die für den erfolgreichen Fluss von E-Mails erforderlich sind.

Hinweis: SMTP für authentifizierte Computer ist erforderlich, wenn Sie IMAP und POP3 unterstützen. Wenn Sie diese Protokolle aktivieren möchten, sollten Sie das Erstellen eines separaten virtuellen Servers für diesen Datenverkehr in Betracht ziehen und SSL verwenden, um den virtuellen Server zu schützen.

Hinweis: Weitere Informationen zum Verhindern unerwünschter SMTP-Weiterleitung in Exchange finden Sie im TechNet-Artikel "Steuern von SMTP-Relaying mit Microsoft Exchange" bzw. "Controlling SMTP Relaying in Microsoft Exchange" (englischsprachig) und im Knowledge Base-Artikel Q319356, "HOW TO: Prevent Unsolicited Commercial E-Mail in Exchange 2000" (englischsprachig).

Zusammenfassung

Sie können nur dann davon ausgehen, dass Exchange die größtmögliche Sicherheit aufweist, wenn Sie Maßnahmen durchführen, die den Datenfluss absichern. Wenn Sie OWA über das Internet erlauben, ist dieses Vorgehen besonders wichtig – ohne Sicherheitsmaßnahmen werden Kennwörter unverschlüsselt über das Internet und im internen Netzwerk übermittelt. Verwenden Sie die Richtlinien in diesem Kapitel, um die Sicherheit der Exchange-Kommunikation zu erhöhen.

Weitere Informationen

Konfigurieren und Absichern von Computern mit Microsoft Exchange 2000 Server und Microsoft Exchange 2000 Server-Clients:

http://www.microsoft.com/isaserver/techinfo/deployment/ISAandExchange.asp (englischsprachig)

Microsoft Exchange 2000 Server Hosting Series:

http://www.microsoft.com/technet/prodtechnol/exchange/plan/hostedexch/aspintro.asp (englischsprachig)

oder

von Microsoft Press

Microsoft Exchange 2000 Server Hosting Series Volume 1: Planning (ISBN:0-7356-1829-1; englischsprachig) and *Microsoft Exchange 2000 Server Hosting Series Volume 2: Deployment* (ISBN: 0-7356-1830-5; englischsprachig)

Einzelheiten zum Signieren und Verschlüsseln von Nachrichten:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q286159 (englischsprachig)

Ausführliche Behandlung der Front-End-/Back-End-Serverumgebungen in Exchange:

http://www.microsoft.com/Exchange/techinfo/deployment/2000/E2KFrontBack.asp (englischsprachig)

Einzelheiten zum Veröffentlichen von SMTP und OWA mit ISA Server:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q290113 (englischsprachig)

und

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q308599 (englischsprachig)

"Step-by-Step Guide to Internet Protocol Security (IPSec)":
http://www.microsoft.com/technet/prodtechnol/windows2000serv/howto/ipsptep.asp (englischsprachig)

Einzelheiten zum Konfigurieren von Nachrichtenüberwachung aus Microsoft ISA Server:

http://www.microsoft.com/serviceproviders/webhosting/HowTo/P116785.asp (englischsprachig)

und

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q315132 (englischsprachig)

Informationen zum Steuern von SMTP-Weiterleitung (Relaying) mit Microsoft Exchange:

http://www.microsoft.com/germany/ms/technetdatenbank/overview.asp?siteid=531635 bzw. http://www.microsoft.com/technet/security/prodtech/mailexch/excrelay.asp (englischsprachig)

Einzelheiten zum Einrichten und Konfigurieren eines virtuellen SMTP-Servers:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q308161 (englischsprachig)

Einzelheiten zum Verhindern unerwünschter E-Mails mit Outlook 2002:

http://office.microsoft.com/germany/Assistance/2002/articles/OlManageJunkAndAdultMail.aspx bzw. http://office.microsoft.com/assistance/2002/articles/OlManageJunkAndAdultMail.aspx (englischsprachig)

Einzelheiten zum Verhindern unerwünschter kommerzieller E-Mails:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q319356 (englischsprachig)