

## Kapitel 19

# Grundlagen zur Sicherheit von Exchange Server

**In diesem Kapitel:**

Der Umfang der Sicherheitsvorkehrungen	470
Motive krimineller Hacker	471
Die Arbeitsweise von Hackern	472
Physische Sicherheit	476
Administrative Sicherheit	476
Sicherheitsmaßnahmen für SMTP	482
Computerviren	486
Was sind Viren?	486
Spam	488
Sicherheitstools von Microsoft	489
Zusammenfassung	490

Verletzungen der Sicherheit, wie z.B. durch Hacker, Viren, Spyware und Vorgabe falscher Identitäten, sind zu einer ständigen Bedrohung der IT-Welt geworden. Da E-Mail-Server auf den Zugriff auf externe Netzwerke angewiesen sind, hat sich E-Mail vielerorts zum Angriffsziel Krimineller entwickelt, die über dieses Medium versuchen, Zugriff auf eine Organisation zu erlangen. Die Sicherheit ist daher für Administratoren so wichtig geworden, dass ein großer Teil des Buchs diesem Thema gewidmet ist.

Dieses Kapitel bietet Ihnen Ratschläge dafür, wie Sie das Eindringen in Ihr Netzwerk über Port 25 kompliziert gestalten und erheblich erschweren. Es gibt keine idiotensicheren Verfahrensweisen, je mehr Sie jedoch in die Sicherheit investieren, desto besser wird Ihr E-Mail-Server geschützt sein. Wenn Sie jedoch mit guten Strategien aufwarten können und die Unterstützung durch ausgeklügelte Werkzeuge haben, können Sie den meisten Angriffen zuvorkommen und sie verhindern.

### Globales Denken bei der Diagnose von Sicherheitsproblemen

Neulich wurde ein bekanntes US-amerikanisches Unternehmen von einer außerhalb der Vereinigten Staaten beheimateten Gruppe angegriffen. Diese Gruppe verwendete den Exchange Server-Computer des Unternehmens, um Spam-Mails (in ihrer eigenen Sprache) an Empfänger überall auf der Welt zu versenden. Zunächst sah dieses Problem nach einem Virus aus, doch dann stellte die Firma fest, dass Hacker auf dem Exchange Server-Computer ein Programm eingerichtet hatten, das ausgehende E-Mails erstellte.

Als die US-Firma das Problem erkannt hatte, befanden sich in den ausgehenden SMTP-Warteschlangen fast 100.000 sendebereite Nachrichten. Neben den offensichtlichen Bedenken, dass die Empfänger der Spam-Mails verärgert sein würden, gab es weitere mögliche negative Konsequenzen, die das Resultat dieses Angriffs sein könnten:

- **Rufschädigung** Dadurch, dass der Missbrauch des Exchange Server-Computers zum Versand von Spam möglich war, zeigte das Unternehmen, dass seine Sicherheitsvorkehrungen unzureichend waren. Unabhängig davon, ob diese Interpretation korrekt war oder nicht, änderte sie auf jeden Fall die Wahrnehmung der Firma in der Öffentlichkeit.
- **Gerichtsverfahren** Durch das Versenden von Spam setzte sich die Firma potenziellen Klagen aus, die nicht nur kostenintensiv sein, sondern auch zu einer weiteren Rufschädigung führen können.

## Der Umfang der Sicherheitsvorkehrungen

Wir alle kennen den alten Grundsatz: »Eine Kette ist nur so stark wie ihr schwächstes Glied.« Sie können diese Denkweise sehr einfach auf die Sicherheit anwenden: »Ein Netzwerk ist nur so sicher wie sein unsicherstes Glied.« Sie sollten E-Mail immer als eines der »unsichersten Glieder« Ihres Netzwerks betrachten, da sie einen offensichtlichen Angriffspunkt darstellt. Angreifer verwenden E-Mails, um Schaden anzurichten, weil es so einfach ist: Ungeachtet wie sicher Ihr Netzwerk ist, bleibt die Wahrscheinlichkeit groß, dass Port 25 in Ihrer Firewall geöffnet ist und ein SMTP-Server darauf wartet, eingehende E-Mails zu verarbeiten.

Wenn Sie über Sicherheitsstrategien nachdenken, sollten Sie immer die folgende Frage beantworten: »Gegen was sichere ich Exchange Server 2007?« Die Antworten auf diese Frage sind unterschiedlich und können in vier Bereiche eingeteilt werden:

1. Ausspähen von Daten durch Social Engineering
2. Physische Sicherheit
3. Administrative Sicherheit
4. SMTP-Sicherheit

Informationen über Social Engineering haben Sie bereits ausführlich in Kapitel 18, »Sicherheitsrichtlinien in Exchange Server 2007«, erhalten. In diesem Kapitel werden wir die anderen drei Sicherheitskategorien untersuchen.

## Motive krimineller Hacker

Obwohl es große Mengen von Literatur über die technischen Aspekte zur Absicherung eines Netzwerks gibt, findet man nicht viel darüber, wer Ihre Feinde sind und welche Motivation sie für einen Angriff haben. Bevor Sie entscheiden können, wie Sie Ihre Organisation schützen, müssen Sie lernen, wie ein Hacker zu denken, herausfinden, wo Sie verwundbar sind, und dann ein Planspiel dafür aufstellen, wie Sie Ihr Risiko verringern. Wenn Sie verstehen, wer Ihnen Schaden zufügen mag und was diese Personen von dem Schaden haben, können Sie Ihre Firma und Ihre Daten besser schützen. Gehen Sie von folgenden Voraussetzungen aus:

- Sie haben professionelle Gegner.
- Sie stehen auf deren Zielliste.
- Sie werden eines Tages angegriffen werden.
- Sie können es sich nicht leisten, selbstzufrieden zu sein.

Eine der für eine Organisation am schwierigsten zu akzeptierenden Tatsachen ist das Vorhandensein von Feinden, die mithilfe der Technik versuchen könnten, ihr zu schaden. Es ist ebenfalls möglich, dass Sie keine Gegner im herkömmlichen Sinne haben. Heutzutage suchen Angreifer nach Systemen mit Sicherheitslücken, die sie zu ihrem Vorteil modifizieren und missbrauchen können. Häufig werden solche schlecht gesicherten Systeme als Basis für ausgefeiltere Angriffe eingesetzt.

Die Motive von Hackern können vielfältig und komplex sein. Sie werden oftmals teilweise durch ihre Unsichtbarkeit angetrieben. Die modernen, gut ausgebildeten Hacker werden oft durch die Aussicht auf hohe Gewinne getrieben. Im Internet kann ein Hacker in die private Welt einer Firma – ihr Netzwerk – hineinschauen und eine Menge lernen, während er anonym bleibt.

Einige Personen sind nur neugierig zu sehen, was sie über Ihre Firma oder die Mitarbeiter in Ihrer Firma herausfinden können. Diese Hacker haben oftmals keine bösen Absichten und sind sich nicht im Klaren darüber, dass ihre Tätigkeiten Sicherheitsrichtlinien oder Gesetze verletzen. Das bedeutet jedoch nicht, dass diese sorglos vorgehenden Hacker weniger gefährlich sind.

Andere Hacker versuchen nur zu helfen. Vielleicht gehörten Sie selbst bereits ein oder zweimal dieser Kategorie an. In Ihrem Eifer, hilfsbereit zu sein, umgehen Sie Sicherheitsrichtlinien, um Probleme zu beheben oder Aufgaben im Notfall zu erledigen. Sie glauben möglicherweise sogar, dass Ihre Bemühungen effizienter sind als das Befolgen vorhandener Leit- und Richtlinien. Trotzdem fällt das Umgehen bekannter Sicherheitsrichtlinien unter den Begriff »Hacken«.

Einige Personen handeln mit böser Absicht, beteiligen sich an Sabotageakten, Spionage oder anderen kriminellen Aktivitäten. Sie können zu Maulwürfen werden und entwenden Informationen, um sie Mitbewerbern oder fremden Gruppen zu verkaufen. Manche haben einfach Freude daran, die Arbeit anderer wie auch ihre eigene zu zerstören. Andere handeln aus Rache für ein ihnen widerfahrenes tat-

sächliches oder empfundenes Unrecht oder glauben, sie handeln in Einklang mit ihrer festen inneren Überzeugung. Wieder andere gehen methodisch und berechnend vor und machen aus dem Hacken einen Beruf und könnten einfach nur aus dem Grund, ihrer Firma Schaden zuzufügen, eine Anstellung suchen.

## Die Arbeitsweise von Hackern

Hacker beginnen damit, dass sie mithilfe von Scanprogrammen die Existenz eines E-Mail-Servers feststellen. In Verbindung mit den öffentlichen Informationen über Ihre DNS-Einträge können sie in kurzer Zeit eine Menge über Ihr Netzwerk lernen.

Informationen über eine Firma zu finden, ist für jedermann einfach. Auch Sie können es tun. Öffnen Sie einfach eine Eingabeaufforderung und geben Sie **nslookup** ein. Setzen Sie die Art des Eintrags, nach dem Sie suchen, auf MX (Mail Exchanger), indem Sie **set type=mx** eingeben. Fügen Sie dann einen Domännennamen hinzu. In diesem Beispiel verwenden wir **Microsoft.com**. In Abbildung 19.1 sehen Sie das Ergebnis.

Abbildg. 19.1 Öffentliche MX-Einträge für Microsoft.com mithilfe von NSLookup finden

```
C:\WINDOWS\system32\cmd.exe - nslookup

C:\>nslookup
Standardserver:  DD-WRT
Address:  192.168.0.1

> set type=mx
> microsoft.com
Server:  DD-WRT
Address:  192.168.0.1

Nicht-autorisierende Antwort:
microsoft.com  MX preference = 10, mail exchanger = mailb.microsoft.com
microsoft.com  MX preference = 10, mail exchanger = mailc.microsoft.com
microsoft.com  MX preference = 10, mail exchanger = maila.microsoft.com

microsoft.com  nameserver = ns3.msft.net
microsoft.com  nameserver = ns4.msft.net
microsoft.com  nameserver = ns5.msft.net
microsoft.com  nameserver = ns1.msft.net
microsoft.com  nameserver = ns2.msft.net
maila.microsoft.com  internet address = 205.248.106.64
maila.microsoft.com  internet address = 131.107.115.212
mailb.microsoft.com  internet address = 131.107.115.215
mailb.microsoft.com  internet address = 205.248.106.30
mailc.microsoft.com  internet address = 131.107.115.214
mailc.microsoft.com  internet address = 205.248.106.32
ns1.msft.net  internet address = 207.68.160.190
ns2.msft.net  internet address = 65.54.240.126
ns3.msft.net  internet address = 213.199.144.151
ns4.msft.net  internet address = 207.46.66.126
ns5.msft.net  internet address = 65.55.238.126
>
```

Als Nächstes bestimmt der Hacker auf eine oder zwei Arten die Plattform Ihres SMTP-Servers. Beim ersten Ansatz verwendet der Hacker Telnet, um eine Sitzung auf Ihrem Server über Port 25 zu öffnen und die erste Meldung zu lesen. Bei Exchange Server 2007 lässt die erste Meldung keine Rückschlüsse mehr auf die installierte Version zu, allerdings schon darauf, dass der Microsoft ESMTP-Dienst läuft. Durch Weglassen der Versionsnummer macht Microsoft es für Hacker schwerer herauszufinden, welche Version von Exchange Server Sie einsetzen. Beachten Sie jedoch, dass Exchange Server 2007 die einzige Version ist, die per Vorgabe die Versionsinformation verschweigt. Es gibt Vorgehensweisen, dies auch in älteren Versionen zu erreichen. Ein Hacker kann also immer noch herausfinden, was er erfahren möchte. Es wird noch einige Service Packs und eine weitere neue Version von Exchange dauern, bis diese Vorgabeeinstellung Früchte trägt. In Abbildung 19.2 sehen Sie eine ESMTP-Meldung, die von Exchange Server 2007 ausgegeben wird.

Abbildg. 19.2 Eine Telnet-Sitzung zu einem Exchange Server 2003-Computer

```

GA Telnet e2007-4
220 E2007-4.contoso.com Microsoft ESMTP MAIL Service ready at Thu, 15 Mar 2007 2
2:17:37 -0600
ehlo
250-E2007-4.contoso.com Hello [192.168.0.114]
250-SIZE
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-X-ANONYMOUSTLS
250-AUTH GSSAPI NTLM
250-X-EXPS GSSAPI NTLM
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 XEXCH50

```

Die älteren Versionen von Exchange Server geben die genaue Versionsnummer des laufenden Servers an (siehe Abbildung 19.3). Die Hauptversion 6.0 bedeutet Exchange Server 2003, Exchange 2000 Server ist mit der Hauptversion 5.0 registriert. Ein Sendmail-Server gibt in der Meldung seinen Namen und die verwendete Version der Sendmail-Software sowie das Betriebssystem an. Mittels solcher Informationen kann ein Hacker seine Angriffe gezielt auf Schwachstellen einer bestimmten Version konzentrieren.

Abbildg. 19.3 Eine Telnet-Sitzung zu einem Exchange Server 2007-Computer

```

GA Telnet jmail.westminster-mo.edu
220 E2007-4.contoso.com Microsoft ESMTP MAIL Service, Version: 6.0.3790.1830
ready at Thu, 15 Mar 2007 23:20:49 -0500
ehlo
250-E2007-4.contoso.com Hello [68.187.13.8]
250-TURN
250-SIZE
250-ETRN
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-8bitmime
250-BINARYMIME
250-CHUNKING
250-URFV
250-X-EXPS GSSAPI NTLM LOGIN
250-X-EXPS=LOGIN
250-AUTH GSSAPI NTLM LOGIN
250-AUTH=LOGIN
250-X-LINK2STATE
250-XEXCH50
250 OK

```

### Weitere Informationen

Auch wenn Exchange Server 2007 die erste Version ist, die standardmäßig keine Versionsinformationen per Telnet mehr anzeigt, können Sie ältere Versionen von Exchange entsprechend konfigurieren. Lesen Sie nach unter <http://support.microsoft.com/kb/281224/en-us>, um weitere Informationen zu erhalten.

Die zweite Möglichkeit zum Bestimmen der Plattform Ihres E-Mail-Servers besteht darin, ihm eine gefälschte E-Mail zu schicken. Dies wird erreicht, indem eine E-Mail an eine wahrscheinlich nicht existierende E-Mail-Adresse wie z.B. pfannkuchen@contoso.com gesendet wird. Der Unzustellbarkeitsbericht (Non-Delivery Report, NDR), der zurück an den Absender geschickt wird, enthält genauere Angaben über den E-Mail-Server. Das folgende Beispiel zeigt die Nachrichtenkopfzeile, die an den

Exchange Server-Computer im Labor von **contoso.com** gesendet wurde. Beachten Sie die Versionsangabe in der Zeile **Sent by**.

```
Delivery has failed to these recipients or distribution lists:

pfannkuchen@contoso.com
This recipient e-mail address was not found in the recipient e-mail system. Microsoft Exchange will not try to redeliver this message for you. Please check the recipient e-mail address and try resending this message, or provide the following diagnostic text to your system administrator.
-----
Sent by Microsoft Exchange Server 2007
Diagnostic information for administrators:
Generating server: E2007-4.contoso.com
pancake@contoso.com
#550 5.1.1 RESOLVER.ADR.RecipNotFound; not found ##
Original message headers:
Received: from E2007-4.contoso.com ([192.168.0.22]) by E2007-4.contoso.com ([192.168.0.22]) with mapi; Thu, 15 Mar 2007 22:31:42 -0600
Content-Type: application/ms-tnef; name="winmail.dat"
Content-Transfer-Encoding: binary
From: Francis Cat <cat.francis@contoso.com>
To: "pfannkuchen@contoso.com" <pfannkuchen@contoso.com>
Date: Thu, 15 Mar 2007 22:31:37 -0600
Subject: Test message
Thread-Topic: Test message
Thread-Index: AQHHZ4P8FQkU6/4hJka20Y89GG0rfg==
Message-ID: <48B260B970217342AAFBCD9BD19B2E5D20A39D1C1B@E2007-4.contoso.com>
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach:
X-MS-TNEF-Correlator: <48B260B970217342AAFBCD9BD19B2E5D20A39D1C1B@E2007-4.contoso.com>
MIME-Version: 1.0
```

Da der Hacker nun weiß, welche E-Mail-Serversoftware Sie verwenden, überprüft er einschlägige Datenbanken, um nach Sicherheitslücken zu suchen, die er ausnutzen kann. Die bekannten Schwachstellen für Exchange Server 2007 werden in den Microsoft Security Bulletins veröffentlicht und können unter [www.microsoft.com/security/default.msp](http://www.microsoft.com/security/default.msp) abgerufen werden. Bei älteren Versionen von Exchange können diese Schwachstellen auch die Internetinformationsdienste (IIS) betreffen, da IIS den SMTP-Server für Exchange verwaltet. In Exchange Server 2007 ist SMTP Kernbestandteil von Exchange selbst, was die Angriffsmöglichkeiten auf den Server reduziert. Andere Schwachstellen können Microsoft Outlook Web Access (OWA) betreffen, da auch hier IIS zur Verwaltung der HTTP-Verbindungen zu Exchange Server beteiligt ist. Sie sollten zumindest über die Schwachstellen von Exchange Server 2007 informiert sein, diese testen und die bereitgestellten Patches installieren.

Allgemein gesagt kann ein E-Mail-Administrator mit den folgenden Arten von Angriffen rechnen:

- **Pufferüberlauf (Buffer Overflows)** Dabei sendet der Angreifer eine größere Datenmenge an den Server als erwartet. Je nachdem, wie diese Attacke ausgeführt wird, kann sie den Server veranlassen, die Verarbeitung komplett einzustellen oder böartigen Code des Angreifers ausführen.
- **Datenverarbeitungsfehler** Sie sind momentan nicht üblich, doch das Prinzip besteht darin, ein kleines Programm direkt an den Server zu senden, das der Server dann ausführt. Heutzutage ist es üblicher, diese Programme als E-Mail-Anhänge an ein Netzwerk zu schicken. Je nach ihrer Funktion und ihrem Zweck können diese Programme Viren, Trojanische Pferde oder Würmer sein (wie weiter hinten in diesem Kapitel ausführlich erörtert wird).
- **HTML-Viren** Sie erfordern keine Benutzeraktivitäten, um Skripts unbeaufsichtigt auszuführen.
- **Maßgeschneiderte Programm für Angriffe auf Port 25 (SMTP)** Die bekannten Varianten von Angriffsprogrammen für Port 25 sind z.B. Mail-Flooding-Programme oder Programme mit einer eigenen SMTP-Engine, die den Port für schädliche Zwecke in Beschlag nehmen.
- **Denial of Service (DoS)** Ein Denial-of-Service-Angriff ist ein Angriff über das Netzwerk, mit dem versucht wird, die vom Server bereitgestellten Dienste zu blockieren.
- **Siteübergreifendes Scripting (Cross-Site Scripting)** Dies ist der Versuch eines Angreifers, schädlichen Programmcode über einen Link einzubinden, der aus einer vertrauenswürdigen Quelle zu stammen scheint.
- **Spam und Phishing** Spam oder Junk-E-Mail ist ein bekanntes Übel und trifft jeden, der dieses Kommunikationsmedium nutzt. Eine besondere Art von Spam, genannt Phishing-E-Mails, versucht, leichtgläubige Benutzer dazu zu verleiten, auf unsichere Weblinks zu klicken. Diese Links führen zu Webformularen, mit denen versucht wird, persönliche Daten zu erschleichen.

Die folgenden allgemeine Maßnahmen können Sie zum Schutz vor den soeben beschriebenen und anderen Angriffen unternehmen:

- **Physischer Zugang zum Server** Verschießen Sie die Türen und nutzen Sie ein biometrisches Identifizierungsverfahren.
- **Viren, Trojaner und Würmer** Nutzen Sie Antivirussoftware und scannen Sie Ihre Server und Arbeitsplatzrechner regelmäßig. Verwenden Sie die Exchange Server 2007-Funktion des Edge Transport-Servers auf mindestens einem Computer.
- **Datenverlust** Führen Sie regelmäßig Datensicherungen durch.
- **Unautorisierte Verwendung von Benutzerkonten** Schulen Sie Ihre Benutzer zum Thema Datensicherheitsrichtlinien und erzwingen Sie sichere Passwörter.
- **Denial-of-Service-Angriffe** Schützen Sie den TCP/IP-Stack und den Router.
- **Schwachstellen der Plattform** Installieren Sie alle Patches und aktivieren Sie nur die wirklich notwendigen Dienste. Microsoft stellt hervorragende, kostenfreie Software bereit, die Ihre Server auf dem neuesten Stand hält. Diese Software heißt Windows Server Update Services (WSUS).

#### Weitere Informationen

Eine Behandlung von WSUS übersteigt den Rahmen dieses Kapitels, doch Sie können mehr darüber auf der Website von Microsoft unter dem URL <http://www.microsoft.com/windows-serversystem/updateservices/default.mspx> lernen.

Der Rest dieses Kapitels soll Sie bei dem Schützen von Exchange Server 2007 gegen diese Arten von Angriffen unterstützen. Eine kurze Abhandlung über die physische Sicherheit Ihres Exchange Server-Computers kann jedoch nicht schaden.

# Physische Sicherheit

Der physische Schutz ist ein Thema, das nicht in vielen Büchern über Sicherheit erwähnt wird, insbesondere nicht in Büchern über Exchange, doch es ist erwähnenswert. Server können sich auf dem Schreibtisch um die Ecke oder in einem unverschlossenen Serverraum befinden. Es ist immer sinnvoll, Ihre Server an einem sicheren Ort mit verschließbaren Türen aufzustellen. In manchen Fällen empfehlen sich Bewegungsmelder oder andere technische Sicherheitsmaßnahmen.

Wenn Sie den Zugang zu einem Server beschränken, grenzen Sie den Kreis derer ein, die sich lokal auf dem Server anmelden, mobilen Speicher zum Einbringen eines neuen Virus oder bösartigen Programms in Ihr Netzwerk nutzen und Informationen direkt vom Server abrufen können. Die Beschränkung des physischen Zugangs ist eines der leichtesten und grundlegendsten Verfahren zur Absicherung Ihres Servers gegen interne Angreifer.

Die meisten Administratoren, die dieses Buch lesen, werden bereits technische Sicherheitsmaßnahmen umgesetzt haben. Diejenigen, die ihre Server noch nicht abgesichert haben, möchten das bitte bei der nächsten Gelegenheit tun. Die Beschränkung des physischen Zugangs zu einem Server kann ein großer Schritt zum Schutz Ihrer Informationen vor möglichen Angreifern sein.

# Administrative Sicherheit

In früheren Ausgaben dieses Buchs handelte dieser Abschnitt intensiv von administrativen Gruppen als einer Möglichkeit, um administrative Sicherheit für Ihren Exchange Server-Computer durchzusetzen. In Exchange Server 2007 hat Microsoft viele der administrativen Gruppen abgeschafft und nur eine einzelne namens **Exchange Administrator** (FYDIBOHF23SPDLT) übrig behalten, in der nur Exchange Server 2007-Computer enthalten sind. Diese administrative Gruppe existiert nur, um die Kompatibilität zu älteren Exchange Server-Computern zu gewährleisten.

## Hinweis

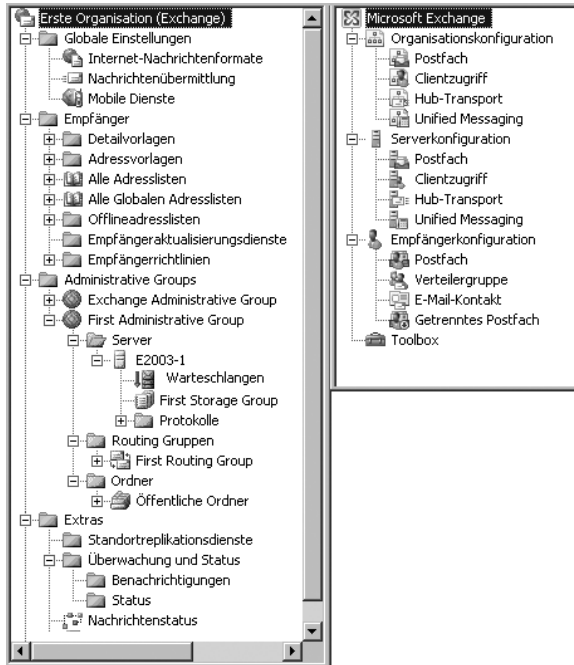
Der Name der administrativen Exchange-Gruppe, FYDIBOHF23SPDLT, klingt etwas komisch. Genau wie die alte Routinggruppe in Exchange Server 2007, DWBGZMFD01QNBJR. Haben Sie sich jemals gefragt, warum Microsoft gerade diese Namen gewählt hat? Zuerst ging es darum, keinen Namen zu verwenden, der bereits durch eigene Gruppenbezeichnungen eines Kunden belegt ist. Dann zeigte das Exchange-Team etwas Kreativität. Sehen Sie sich die beiden Namen etwas genauer an. Beide haben die gleiche Anzahl von Zeichen und die Zahlen und Buchstaben befinden sich jeweils an der gleichen Stelle. Um es kurz zu machen: Wenn Sie im Namen der administrativen Gruppe jeden Buchstaben (bzw. jede Zahl) durch den im Alphabet vorangehenden ersetzen, ergibt sich der Name »EXCHANGE12ROCKS«. Genauso finden Sie bei der Routinggruppe die Bezeichnung »EXCHANGE12ROCKS«, wenn Sie die Zeichen durch den im Alphabet jeweils nachfolgenden Buchstaben ersetzen. Es ist doch toll zu sehen, dass das Entwicklerteam so viel Spaß mit einem Produkt hat, das eigentlich aus der Business-Ecke kommt.

Warum hat das Exchange-Team jedoch die administrativen Gruppen aus Exchange entfernt? Durch die vollständige Neugestaltung der Management-Schnittstelle und den neuen Zuständigkeitsbereich sind administrative Gruppen einfach nicht mehr notwendig und blähen die Komplexität der Exchange-Verwaltung einfach nur auf. Abbildung 19.4 bietet eine Gegenüberstellung des alten Exchange System-Managers und der Exchange Server 2007-Verwaltungskonsole. Da es in Exchange 2007 keine administrativen Gruppen mehr gibt, benötigen Sie eine Alternative, um die administra-



tive Sicherheit zu gewährleisten. In diesem Abschnitt lernen Sie zwei Verfahren kennen, mit denen Sie Benutzer für die Verwaltung verschiedener Exchange-Funktionen hinzufügen können.

**Abbildung 19.4** Der System-Manager von Exchange Server 2003 befindet sich links und die Exchange Server 2007-Verwaltungskonsolle rechts



## Die integrierten Administratorgruppen von Exchange

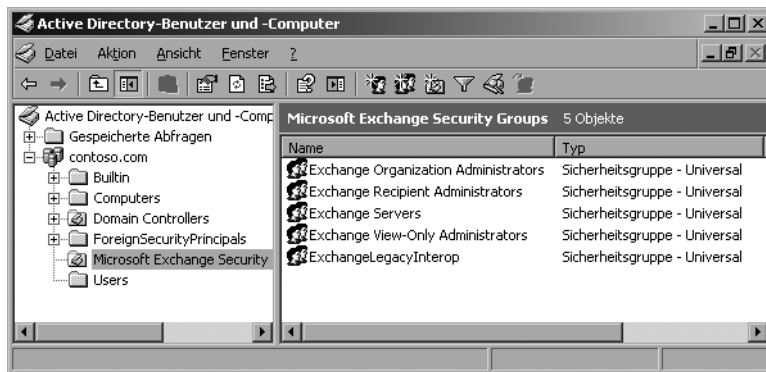
Wenn Sie die Erstinstallation von Exchange Server 2007 durchführen, werden in Active Directory fünf universelle Sicherheitsgruppen erstellt, von denen jede in verschiedenen Teilen der Exchange-Organisation besondere Rechte hat. Die folgenden vier dieser fünf Gruppen, die in Abbildung 19.5 in Active Directory-Benutzer und -Computer gezeigt werden, dienen direkt zur Verwaltung der Exchange-Organisation:

- **Exchange-Administrator mit Leserechten** Diese Rolle erlaubt Ihnen, die Konfigurationen aller Exchange-Objekte zu sehen, aber nicht, daran Änderungen vorzunehmen.
- **Exchange-Server** Diese Rolle enthält die folgenden Rechte:
  - Mitglieder dieser Gruppe haben alle Rechte der Exchange-Administratoren mit Leserechten
  - Mitglieder dieser Gruppe haben Zugang zu serverbasierten Exchange-Konfigurationsinformationen und zu serverbezogenen Active Directory-Objekten.
  - Mitglieder dieser Gruppe können serverbasierte Verwaltungsaufgaben erledigen, jedoch keine Aktionen auf der Ebene der Exchange-Organisation durchführen.
  - Mitglieder dieser Gruppe sind außerdem Mitglieder der lokalen Administratorgruppe auf dem Computer, auf dem Exchange Server 2007 installiert ist.

- **Exchange-Empfängeradministrator** Diese Rolle hat die folgenden Rechte:
  - Mitglieder dieser Gruppe haben alle Rechte der Exchange-Administratoren mit Leserechten
  - Mitglieder dieser Gruppe dürfen alle objektbezogenen Empfänger und öffentlichen Ordner konfigurieren, darunter Kontakte, Gruppen, Öffentliche Ordner-Objekte, Unified Messaging-Postfacheinstellungen, Clientzugriffs-Postfacheinstellungen und andere Empfänger-eigenschaften von Exchange in Active Directory.
- **Exchange-Organisationsadministrator** Diese Rolle hat die folgenden Rechte:
  - Mitglieder dieser Gruppe haben alle Rechte der Exchange-Empfängeradministratoren und weitere.
  - Benutzer in dieser Gruppe dürfen alle Aspekte der Exchange-Organisation lesen und verwalten, einschließlich der Server und der Konfiguration der Organisation.
  - Mitglieder dieser Rolle werden als Besitzer aller Exchange-bezogenen Active Directory-Objekte betrachtet.
  - Während der Exchange 2007-Installation wird diese Gruppe in die Gruppe der lokalen Serveradministratoren aufgenommen. Wenn Sie Exchange Server 2007 auf einem Domänencontroller installieren, was nicht empfohlen wird, haben Exchange-Organisationsadministratoren zusätzliche Rechte, je nachdem, ob die lokale Administratorengruppe über zusätzliche Rechte auf dem Domänencontroller verfügt.

Wenn Sie Ihrer Organisation einen vollständigen Exchange-Administrator hinzufügen wollen, müssen Sie das betreffende Benutzerkonto nur in die Gruppe der Exchange-Organisationsadministratoren aufnehmen. Dasselbe gilt für die anderen Sicherheitsgruppen.

Abbildg. 19.5 Die in Exchange Server 2007 integrierte Sicherheitsgruppe

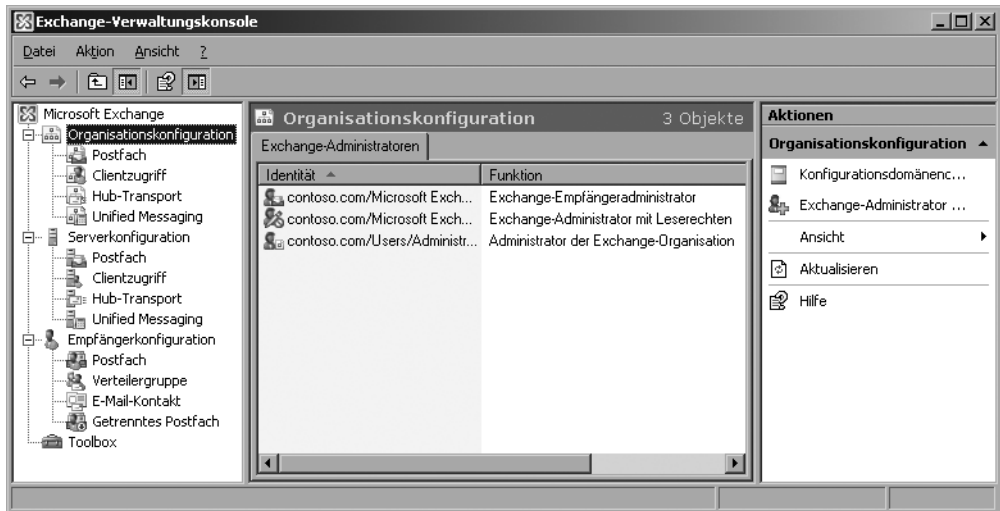


## Der Assistent zum Hinzufügen von Exchange-Administratoren

Exchange Server 2007 bietet außerdem eine einfache Möglichkeit, Exchange-Administratoren hinzuzufügen, die nur die Verantwortung für einen bestimmten Bereich der Exchange-Organisation haben, wie einen einzelnen Server oder eine Servergruppe, oder die nur Empfänger verwalten können. Sie werden sehen, dass die Delegierungsmethode für Administratorrechte viel flexibler und effizienter ist als die Administratorgruppen der Vergangenheit.

Der einfachste Weg, das Hinzufügen von Exchange-Administratoren zu erklären, besteht, es in der Praxis zu zeigen. Um den Vorgang zu beginnen, öffnen Sie die Exchange-Verwaltungskonsolle und wählen die Option **Organisationskonfiguration**, wie in Abbildung 19.6 gezeigt.

Abbildg. 19.6 Das Fenster **Organisationskonfiguration**



Beachten Sie den Arbeitsbereich in Abbildung 19.6. Die Gruppen haben hier schon bestimmte Berechtigungen für die Exchange-Organisation erlangt. Um Exchange-Administratoren hinzuzufügen, wählen Sie **Exchange-Administrator hinzufügen**. Es erscheint ein einseitiger Assistent, der in Abbildung 19.7 gezeigt wird. Sie müssen dreimal eine Auswahl treffen, um den Assistenten abzuschließen.

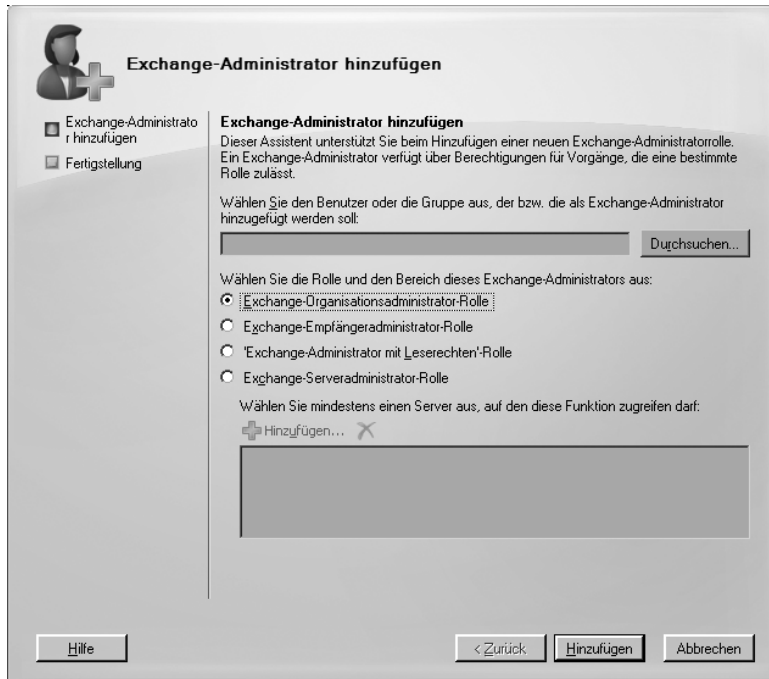
Zuerst wählen Sie die Benutzergruppe, die Exchange-Administratorrechte erhalten soll. Dann wählen Sie die Rolle und den Einflussbereich des neuen Exchange-Administrators. Schließlich, wenn Sie die Exchange Server-Administratorrolle ausgewählt haben, wählen Sie zumindest einen Server, auf den die neue Benutzergruppe Zugriff haben soll. Klicken Sie auf **Hinzufügen** und wählen Sie die gewünschten Server im Fenster **Exchange-Server auswählen**. Abbildung 19.8 zeigt, wie der Bildschirm aussieht, nachdem Sie die Exchange Server-Administratorrolle und den zu verwaltenden Server ausgewählt haben.

#### Hinweis

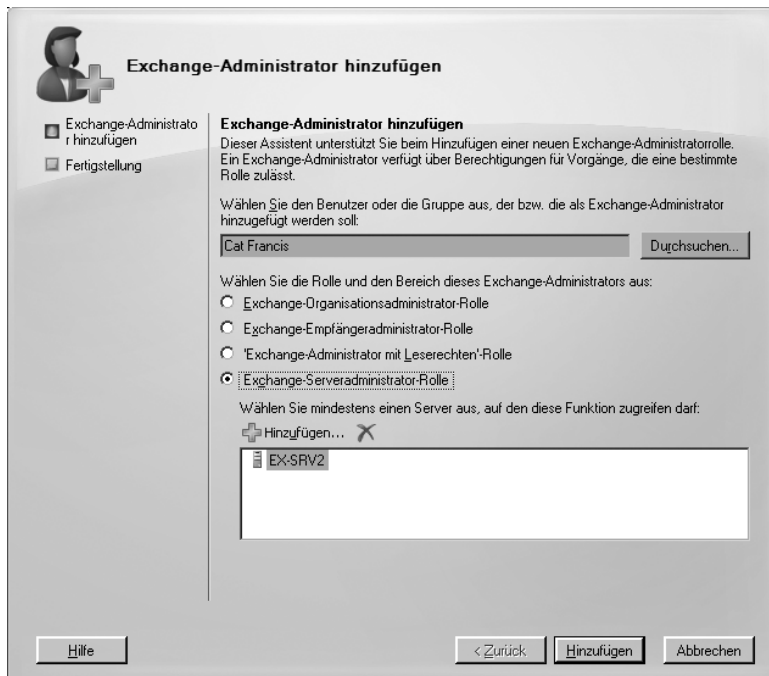
Wenn Sie jemanden zur Exchange Server-Administratorrolle hinzufügen, müssen Sie diesen Benutzer oder diese Gruppe manuell in die lokale Administratorgruppe auf jedem zu verwaltenden Server aufnehmen.

Wenn Sie in der Praxis diesen Assistenten benutzen, fügt der daraus resultierende Befehl einfach die ausgewählten Benutzer einer der vorher beschriebenen Gruppen hinzu. Die einzige Rolle, auf die das nicht zutrifft, ist die des Exchange Server-Administrators. Wenn Benutzer oder Gruppen dieser Rolle zugewiesen werden, erhalten sie Vollzugriff auf die angegebenen Server und deren untergeordnete Objekte.

Abbildg. 19.7 Der Assistent zum Hinzufügen von Exchange-Administratoren



Abbildg. 19.8 Auswählen der Exchange Server-Administratorrolle



**Verwaltungsshell**

Sie können die Administratorrollen auch mit der Exchange-Verwaltungsshell vergeben.

Der folgende Befehl fügt ein Benutzerkonto hinzu, das den Exchange Server-Computer E2007-4 verwalten darf.

```
Add-ExchangeAdministrator -Identity 'contoso.com/Users/David So'
  -Role 'ServerAdmin' -Scope 'E2007-4'
```

Wenn Sie jemanden mit der Exchange Server-Administratorrolle hinzufügen, müssen Sie den Benutzer oder die Gruppe in die integrierten lokale Administratorgruppe des Zielservers aufnehmen.

Der folgende Befehl fügt einen Benutzer zur Rolle Exchange-Empfängeradministrator hinzu.

```
Add-ExchangeAdministrator -Identity 'contoso.com/Users/David So'
  -Role 'RecipientAdmin'
```

Der nächste Befehl fügt einen Benutzer zur Rolle Exchange-Administrator mit Leserechten hinzu.

```
Add-ExchangeAdministrator -Identity 'contoso.com/Users/David So'
  -Role 'ViewOnlyAdmin'
```

Der folgende Befehl fügt einen Benutzer zur Rolle Exchange-Organisationsadministrator hinzu.

```
Add-ExchangeAdministrator -Identity 'contoso.com/Users/David So'
  -Role 'OrgAdmin'
```

Tabelle 19.1 stammt aus der Microsoft-Dokumentation über Rollen in Exchange Server 2007 und bietet eine genaue Übersicht darüber, welche Funktion eine Administratorrolle erfüllt.

**Tabelle 19.1** Exchange-Administratorrollen

Rolle	Mitglieder	Mitglied von	Exchange-Berechtigungen
Exchange-Organisationsadministrator	Administrator oder das Konto, das bei der ersten Installation von Exchange Server 2007 verwendet wurde.	Exchange-Empfängeradministrator lokale Administratorengruppe von <Server>	Vollzugriff auf den Microsoft Exchange-Container in Active Directory
Exchange-Empfängeradministrator	Exchange-Organisationsadministratoren	Exchange-Administrator mit Leserechten	Vollzugriff auf die Exchange-Eigenschaften im Active Directory-Benutzerobjekt
Exchange Server-Administratoren	Exchange-Organisationsadministratoren	Exchange-Administratoren mit Leserechten Lokale Administratorengruppe von <Server>	Vollzugriff auf <Servername>
Exchange-Administrator mit Leserechten	Exchange-Empfängeradministrator Exchange-Serveradministrator <Name>	Exchange-Empfängeradministrator Exchange Server-Administratoren	Lesezugriff auf den Microsoft Exchange-Container in Active Directory Lesezugriff auf alle Windows-Domänen mit Exchange-Empfängern

# Sicherheitsmaßnahmen für SMTP

Standardmäßig versucht ein SMTP-Server, über Port 25 eine anonyme TCP-Verbindung zu Ihrem Exchange Server-Computer aufzubauen. Anonym bedeutet nicht, dass ein in Active Directory eingerichtetes Benutzerkonto die Anfrage stellvertretend entgegennimmt, wie es beim anonymen Benutzerkonto von IIS, `IUSR_<Computername>`, der Fall ist. Im Rahmen von SMTP bedeutet anonym, dass der SMTP-Remotedienst weder einen Benutzernamen noch ein Kennwort benötigt, um eine Verbindung über Port 25 herzustellen. Somit kann standardmäßig jeder SMTP-Server im Internet über Port 25 eine Verbindung zu Ihrem Exchange-Server eingehen.

Um SMTP sicherer zu machen, können Sie entweder die Standard- oder die integrierte Windows-Authentifizierung (IWA) verlangen, bevor der virtuelle SMTP-Server eine eingehende Verbindung zulässt. Diese Konfiguration ist jedoch im Internet nicht möglich, da Sie nicht voraussagen können, wer sich zukünftig mit Ihrem Exchange Server-Computer verbinden wird, und daher nicht annehmen können, dass der Benutzer einen geeigneten Benutzernamen und ein Kennwort zur Aufnahme der Verbindung hat. Darüber hinaus sind nicht viele Messagingadministratoren daran interessiert, solche Sicherheitsvorkehrungen bei sich vorzunehmen. Obwohl also eine anonyme Verbindung zu Port 25 Ihres Exchange Server-Computers eine Verwundbarkeit darstellt, muss sie mit einem anderen Ansatz als über das Verbot anonymer Verbindungen bewältigt werden.

Wie schützen wir uns vor derartigen Angriffen? Mit Exchange Server 2007 können Sie einen Edge-Transport-Server einsetzen, der Ihrem primären Exchange Server-Computer die Verwaltung der Sicherheit abnimmt. Sie erfahren mehr über Edge-Transport-Server in Kapitel 20, »Antispam- und Antivirusfunktionen«. Dieses Kapitel beschreibt ebenfalls, wie Edge-Transport-Server dabei helfen, die Gesamtsicherheit einer Exchange-Infrastruktur zu verbessern. Allerdings sollte die herkömmliche Vorgehensweise, Exchange zu schützen, auch dann Anwendung finden, wenn Edge-Transport-Server zum Einsatz kommen.

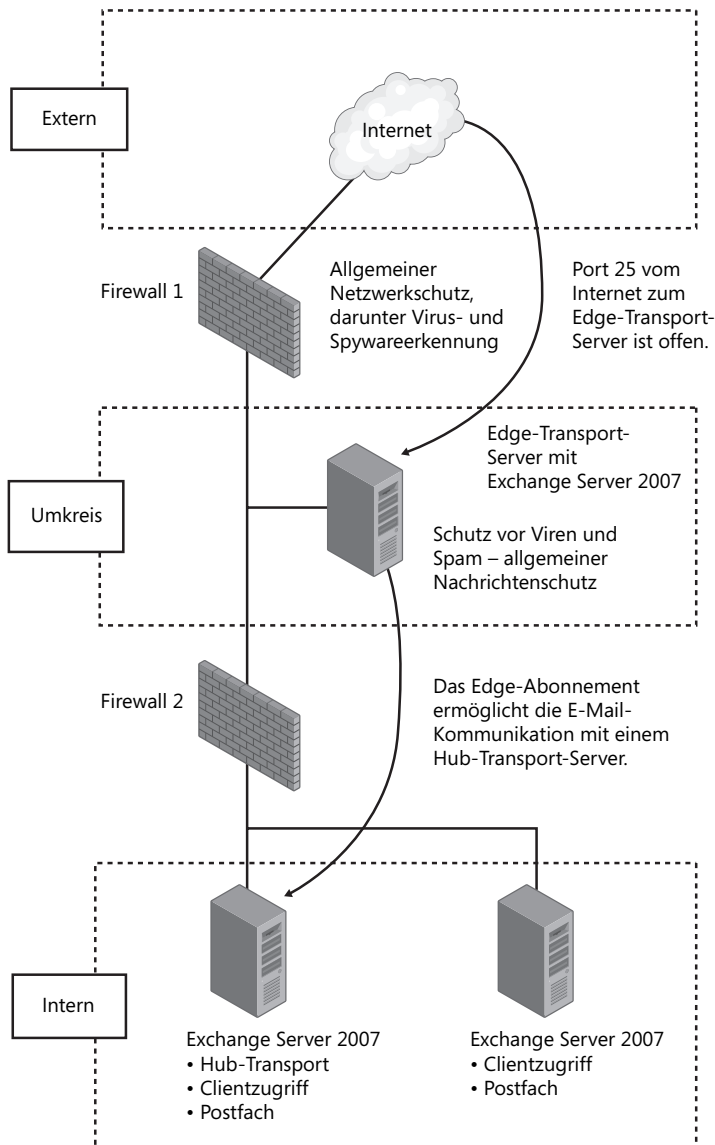
Der vermutlich am häufigsten beschrittene Weg, um eine Exchange-Infrastruktur zu schützen, ist der Einsatz zweier Firewalls. Eine duale Firewalltopologie ermöglicht es, Ihre internen Exchange Server-Computer zu schützen und auch eingehende E-Mails als Maßnahme gegen mögliche Angriffe zu filtern. Der Bereich zwischen den beiden Firewalls wird *Umkreisnetzwerk* genannt (auch bekannt als DMZ oder demilitarisierte Zone). Die Grundidee besteht darin, eine Verteidigungslinie gegen mögliche Angriffe aufzubauen. Dabei sind wir bereit, unsere Exchange Server-Computer im Umkreisnetzwerk zu opfern, jedoch nicht die Server im internen Netzwerk. Da die Exchange Server-Computer im Umkreisnetzwerk keine wichtigen Informationen beherbergen – keine Postfächer oder öffentlichen Ordner –, können Sie sowohl bei einem Angriff geopfert als auch einfach wiederhergestellt werden. Da sie nur als Übertragungsserver dienen, können wir sie zum Säubern eingehender E-Mails über Port 25 nutzen.

Werfen Sie einen Blick auf Abbildung 19.9. Achten Sie auf die drei Netzwerkschichten. Von oben nach unten wird jedem Netzwerk mehr vertraut, wobei die externe Zone (also das Internet) kein Vertrauen genießt. Dem Umkreisnetzwerk wird mehr vertraut, da es sich hinter zumindest einer Firewall der Organisation befindet und generell nur Server enthält, die als »entbehrlich« betrachtet werden. In diesem Diagramm hat die externe Firewall Port 25 geöffnet, damit eingehender SMTP-Verkehr bearbeitet werden kann. E-Mails werden an den Edge-Transport-Server mit Exchange Server 2007 geleitet, wo sie nach Viren gescannt, mit diversen Spamfiltern bearbeitet und mit verschiedenen Regeln für eingehende Nachrichten gefiltert werden. Ihr externer MX-Eintrag muss auf diesen Edge-Transport-Server zeigen. Es gibt eine weitere wichtige Information in diesem Diagramm. Bitte beachten Sie, dass die externe Firewall auch die Fähigkeit hat, eingehende Inhalte auf Viren und Spyware zu überprüfen. Wenn es möglich ist, sollten Sie Ihre E-Mails immer durch eine ähnlich konfigurierte

Firewall laufen lassen, möglichst schon, bevor sie den Edge-Transport-Server und seine Filtermechanismen erreicht. Viele der heute erhältlichen Sicherheitslösungen, wie z.B. Cisco ASA oder Sonicwall, bieten diese zusätzliche Sicherheit.

Was die Software angeht, sollten Sie auch darüber nachdenken, Microsoft Forefront Security für Exchange einzusetzen. Forefront kann jede eingehende Nachricht mit bis zu fünf vollständig unabhängigen Virusscannern bearbeiten. Durch Einführung dieser mehrschichtigen Sicherheitsinfrastruktur können alle eingehenden Mails von vielen verschiedenen Scan-Module bearbeitet werden, von denen einige hardware- und andere softwarebasiert sind. Dadurch steigt die Wahrscheinlichkeit, dass Sie gegen die neuesten Viren geschützt sind.

Abbildg. 19.9 Ein Weg, die Exchange-Infrastruktur abzusichern



Allerdings wird Sie auch die weltbeste Sicherheitsinfrastruktur nicht immer schützen können. Erinnern Sie sich bitte an einige der bekanntesten Viren der letzten Jahre, die sich sehr schnell weltweit verbreiten konnten, normalerweise innerhalb von Stunden. Es ist für die Hersteller von Antivirensoftware praktisch unmöglich, den Virus zu erhalten, ihn zu analysieren, eine entsprechende Definition zu schreiben und die Definition für diesen Virus zu verteilen, bevor er sich weltweit verbreitet. Sie können einen Edge-Transport-Server für die Inhaltsprüfung jedoch anweisen, alle Nachrichten unter Quarantäne zu stellen oder zu löschen, die gewisse Arten von Anhängen enthalten, und somit die meisten Viren aufgrund Ihres Inhaltstyps abzuweisen, anstatt einen Vergleich mit einer Virendefinitionsdatei vorzunehmen.

### Hinweis

Bei traditionellen Antivirus-Servern sollten Sie folgendes beachten: Erstens nehmen viele der bekannten Antivirus-Suites das Scannen nach Viren und das Scannen nach Inhalten gleichzeitig vor. Zwar muss dieser Ansatz beim Scannen von E-Mails kein Problem darstellen, doch sollten Sie den Unterschied zwischen Virus- und Inhaltsscan im Auge behalten, der unterstreicht, dass beide Scans im Umkreisnetzwerk notwendig sind. Dies wird durch einen Edge-Transport-Server mit Exchange Server 2007 ermöglicht. Außerdem können es die finanziellen Mittel nicht zulassen, alle im Kapitel beschriebenen notwendigen Komponenten anzuschaffen, insbesondere einen separaten Exchange Server-Computer als Edge-Transport-Server und die Firewalls bzw. Sicherheitsgeräte, die das Scannen übernehmen. Diese Vorschläge dienen dazu, die zugrunde liegenden Konzepte zu illustrieren. Daneben gibt es u.a. folgende weniger kostspielige (und weniger sichere) Möglichkeiten:

- Einsatz einer einzelnen Firewall mit mehreren Schnittstellen und Aufbau eines Umkreisnetzwerks mittels Firewallregeln.
- Einsatz einer einzelnen Firewall und Betrieb des Edge-Transport-Servers an der internen Schnittstelle neben Ihren anderen Exchange Server-Computern.
- Weglassen des Edge-Transport-Servers und Auslieferung der E-Mails direkt an einen Hub-Transport-Server.

Nach dem Scannen und der Freigabe werden die E-Mails an den internen Hub-Transport-Server gesendet. Dieser interne Hub-Transport-Server muss so konfiguriert sein, dass er eingehende E-Mails nur aus dem Umkreisnetzwerk des Edge-Transport-Servers annimmt. Eingehende E-Mails, die vom Edge-Transport-Server freigegeben sind, werden über den üblichen SMTP-TCP-Port 25 übertragen, sodass Sie diesen Port auch in Ihrer internen Firewall öffnen müssen. Um dies auf die sicherste Weise zu tun, erstellen Sie eine Firewallregel, die Verkehr auf Port 25 nur zwischen dem Edge-Transport-Server und einem der internen Hub-Transport-Server zulässt. Dann sichern Sie den Tunnel mittels IPsec, was in Kapitel 21 näher erklärt wird. Der interne Exchange Server-Computer sollte außerdem eigene Antivirussoftware besitzen, vorzugsweise von einem anderen Anbieter als auf einem der Server im Umkreisnetzwerk. Der Zweck dieses Modells besteht darin, sicherzustellen, dass der Verkehr über Port 25 so gut wie möglich gesichert ist.

Um einen Edge-Transport-Server einzusetzen, erstellen Sie ein Abonnement für den Server in der Active Directory-Domäne. Das Abonnement richtet eine Einwegreplikation der Empfänger- und Konfigurationsinformationen von Ihrem Active Directory zur einer ADAM-Instanz (Active Directory Application Mode) ein, die auf Ihrem Edge-Transport-Server ausgeführt wird. Zusätzlich erstellt das Abonnement einen SMTP-Sendeconnector, der notwendig ist, um den E-Mail-Fluss von Ihren Exchange Server-Computern über einen Edge-Transport-Server ins Internet zu ermöglichen. Wenn



Sie Funktionen für die Empfängersuche oder die Aggregation von Listen sicherer Adressen auf dem Edge-Transport-Server einsetzen, erstellen Sie ein Abonnement für den Edge-Transport-Server innerhalb der Organisation.

#### Weitere Informationen

Der vollständige Vorgang, einen Edge-Transport-Server zu installieren, zu konfigurieren und ein Abonnement zu erstellen, wird in Kapitel 20, »Antispam- und Antivirusfunktionen«, beschrieben.

Kein System ist narrensicher, doch die duale Firewalltopologie hat mehrere Vorteile:

- Durch das Weiterleiten eingehender E-Mails durch die Inhaltsfilter der Edge-Transport-Servers können Sie nach Programmcode suchen, den Antivirusscanner nicht finden können.
- Indem Sie Ihre E-Mails durch einen Virens Scanner zwingen, tun Sie Ihr Bestes, um sicherzustellen, dass alle bekannten Viren herausgefiltert werden. Es wäre unvernünftig, die E-Mails nach Passieren des Inhaltsscanners nicht durch einen aktualisierten Virens Scanner zu leiten, da ältere Viren von der Inhaltsprüfung möglicherweise nicht erkannt werden.
- Indem Sie alle ausgehenden E-Mails durch einen Edge-Transport-Server mit Exchange Server 2007 senden, wird die IP-Adresse (privat oder öffentlich) des internen Exchange Server 2007-Computers nicht in den öffentlichen DNS-Einträgen aufgeführt. Das bedeutet, dass ein Angreifer, der eine Telnet-Verbindung zu Ihrem Server versucht, ihn niemals direkt erreichen kann. Wenn Sie außerdem den internen Exchange-Server 2007-Computer so einrichten, dass er E-Mails nur von Exchange Server-Computern aus der DMZ annimmt, schlagen alle Versuche fehl, über Port 25 und eine fremde IP-Adresse eine Verbindung mit ihm aufzunehmen.

Wenn ein Hacker sich dazu entscheidet, Ihre Exchange Server-Computer im Umkreisnetzwerk zu zerstören, haben Sie tatsächlich keine Werte verloren, außer der Zeit, um sie wieder funktionsfähig zu machen.

Ihr Unternehmen könnte dadurch etwas Geld verlieren, dass zeitweise eine Kommunikation mittels E-Mail nicht möglich ist, aber es verliert keine wichtigen Daten. Das ist ein wichtiger Punkt. Der Server, auf dem Ihre Daten gespeichert sind, ist der am besten geschützte. Die anderen, die weniger gut geschützt sind, enthalten keine wichtigen Daten. Gehen diese Server verloren, sind zumindest alle geschäftskritischen Daten auf dem internen Exchange Server 2007-Computer gespeichert. Für viele Firmen ist das ein annehmbares Risiko. Dies ist der Anfang einer Verteidigungsstrategie, die mehrere Schutzschichten bietet, angefangen bei verzichtbaren Diensten bis hin zu den unentbehrlichen, die auf vielfältige Weise gesichert sind.

Wie wir in diesem Kapitel immer wieder erläutert haben, ist keine Lösung perfekt, sodass auch dieses Sicherheitsmodell einige große Lücken hat, wenn Sie z.B. nichts zum Schutz vor Nachrichten unternehmen, die über Outlook Web Access an den Exchange Server-Computer geschickt werden. Port 25 ist gut geschützt, aber der Zugang über Port 80 ist weit geöffnet. Wenn Sie wissen möchten, wie OWA abgesichert wird, verweisen wir auf [Kapitel 24, »Outlook Web Access«](#).

Die zweite große Sicherheitslücke in diesem Modell kann nicht geschlossen werden: Nachrichten erreichen Ihren internen Exchange Server-Computer. Solange ein Datenpaket diesen Server erreichen kann, ist ein Bedrohungspotenzial vorhanden. Vergessen Sie also nicht die 80%-Regel: Sie können Ihre Daten nur zu ungefähr 80% sicher machen. Doch lassen Sie sich davon nicht entmutigen, Ihre Strategien umzusetzen.

# Computerviren

In diesem Abschnitt führen wir das Thema Computerviren etwas weiter aus und erörtern einige Auswirkungen auf Exchange Server 2007.

## Was sind Viren?

Ein *Virus* ist Code, der sich an andere Programme oder Dateien anhängt. Wenn diese Dateien ausgeführt werden, wird der Code aufgerufen und beginnt, sich selbst zu vervielfältigen. Die Vervielfältigung geschieht über das Netzwerk. Viren können mittlerweile die Sicherheitslücken fast jeder Plattform ausnutzen.

Einige Viren verbleiben im Speicher, wenn das ursprüngliche Programm beendet wird. Wenn andere Programme ausgeführt werden, hängt das Virus sich daran an, bis der Computer heruntergefahren oder ausgeschaltet wird. Einige Viren haben eine »Schlafphase« und treten nur zu bestimmten Zeiten auf oder wenn bestimmte Aktionen durchgeführt werden.

Es gibt viele Arten von Viren. Einige überschreiben vorhandenen Code oder Daten. Andere können feststellen, ob eine ausführbare Datei bereits infiziert ist. Eine solche *Selbsterkennung* ist erforderlich, wenn das Virus mehrfache Infektionen einer einzelnen ausführbaren Datei verhindern will, die zu einem übermäßigem Größenwachstum solcher infizierten Dateien mit einer entsprechenden Speichernutzung und somit zur Entdeckung des Virus führen können.

*Residente Viren* installieren sich bei der Ausführung eines infizierten Wirtsprogramms selbst als Bestandteil des Betriebssystems. Ein solches Virus bleibt resident, bis das System heruntergefahren wird. Wenn es einmal im Speicher vorhanden ist, kann es alle passenden Rechner infizieren, auf die zugegriffen wird.

Ein *Tarnkappen-Virus* (Stealth-Virus) ist ein residentes Virus, das seiner Entdeckung entgehen will, indem es sich in einer infizierten Datei versteckt. Es kann z.B. den Viruscode aus einer ausführbaren Datei entfernen, wenn sie gelesen (anstatt ausgeführt) wird, sodass Antivirensoftware nur eine nicht infizierte Form der Datei sieht.

Computerviren verbreiten sich hauptsächlich durch den Gebrauch von E-Mail und treten in der Regel in E-Mail-Anhängen auf. Wenn das Virus seinen Weg in den Nachrichtenstrom findet, nutzt es die Fähigkeit des Clients, E-Mails zu senden und zu empfangen, um sich selbst schnell zu vermehren und so bald wie möglich Schaden anzurichten.

Ein notwendiger Aspekt zum Schutz Ihres Nachrichtensystems vor Viren ist die Schulung der Benutzer. Sie sollten lernen, welche Anhänge sie öffnen dürfen. Ihre Richtlinien zur Datensicherheit sollten die Arten von E-Mails und Anhängen beschreiben, die die Benutzer öffnen dürfen. Zum Beispiel sollte Benutzern in zwei Fällen das Öffnen von Anhängen verboten werden: wenn Sie sie nicht erwartet haben und wenn sie von unerkannten Aliasnamen stammen.

Wenn immer es möglich ist, sollten Sie einen zentralisierten Antivirusdienst nutzen, der die Clients im Netz über einen zentralen Server aktualisiert. Die meisten dieser Lösungen ermöglichen es Ihnen, Clients detailliert und vorausschauend zu betreuen und Probleme zu beheben, bevor sie auftreten.

## Trojanische Pferde

Ein *Trojanisches Pferd* (auch bekannt als Trojaner) ist ein bösartiges Programm innerhalb eines normalen, sicher erscheinenden Programms. Der Unterschied zwischen einem Virus und einem Trojanischen Pferd besteht darin, dass Letzteres eingebettet und das Virus an die (ausführbare) Datei angehängt ist.

Wenn das normale Programm ausgeführt wird, ist auch der bösartige Code aktiv und kann Schaden anrichten oder wichtige Informationen entwenden oder beschädigen. Ein Beispiel für ein Trojanisches Pferd ist ein Textverarbeitungsprogramm, das dem Benutzer ermöglicht, ein Dokument zu erstellen, während im Hintergrund bösartiger Code ausgeführt wird, der Dateien löscht oder andere Programme zerstört.

Trojanische Pferde werden im Allgemeinen durch E-Mail oder *Würmer* verbreitet; Letzteres sind Programme, die sich selbst ausführen. Der von einem Trojanischen Pferd angerichtete Schaden ist mit dem eines Virus vergleichbar: von gering bis geschäftskritisch. Sie sind vor allem deswegen Furcht erregend, weil die Benutzer in den meisten Fällen den verursachten Schaden nicht bemerken. Die bösartige Funktion wird durch den scheinbar nützlichen Effekt des Programms getarnt.

## Würmer

Wie bereits erwähnt, sind Würmer Programme, die sich selbst ausführen. Weder betten Sie sich in andere Programme ein oder hängen sich daran an, noch müssen sie das tun, um sich zu vermehren. Sie können über Netzwerkverbindungen von Computer zu Computer wandern und sind selbstvermehrend. Es können Teile von Würmern auf vielen verschiedenen Rechnern ausgeführt werden oder das ganze Programm auf einem einzelnen. Normalerweise verändern Würmer keine anderen Programme, obwohl sie anderen Code mitführen können, der das tut.

Die ersten Netzwerkwürmer waren dazu gedacht, sinnvolle Verwaltungsaufgaben wahrzunehmen, indem sie Eigenschaften des Betriebssystems zu ihrem Vorteil verwendeten. Bösartige Würmer nutzen Sicherheitslücken des Systems für ihre eigenen Zwecke aus. Das Freisetzen eines Wurms führt in der Regel zu kurzen Ausbrüchen und fährt ganze Netzwerke herunter.

Der Schaden, den Würmer anrichten können, reicht wie bei Trojanischen Pferden und Viren von unbedeutend bis kritisch. Die Art und das Ausmaß des Schadens müssen für jeden Wurm individuell bewertet werden. Würmer können jedoch Trojanische Pferde und Viren installieren, die dann ihren eigenen Code ausführen.

Es kann sehr schwierig sein, einem Angriff durch eine Kombination aus einem Wurm und einem Trojanischen Pferd oder einem Virus, unbeschadet zu entgehen. Die Auswirkungen von Viren, Trojanischen Pferden und Würmern auf Ihr Nachrichtensystem und Ihr Netzwerk sollten Sie nicht unterschätzen. Da sie E-Mail verwenden, um Sicherheitslücken im System auszunutzen, reicht die Installation von Antivirensoftware alleine nicht aus. Sie müssen darüber hinaus sicherstellen, dass bekannte Sicherheitslücken in allen Ihren Betriebssystemen geschlossen werden. Konzentrieren Sie sich nicht nur auf Server. Jedes Gerät sollte so schnell wie möglich mit den aktuellsten Softwarekorrekturen eines jeden Herstellers aktualisiert werden. In den meisten Umgebungen müssen diese Korrekturen vor der Installation getestet werden. Aber installieren Sie sie, nachdem sie getestet wurden.

# Spam

Spam (Junk-E-Mail) ist ein großes Problem. Ein Kunde, für den der Autor kürzlich arbeitete, führte seine erste Software zur E-Mail-Filterung ein und stellte fest, dass er 46% weniger eingehende E-Mail hatte.

Die neue Funktion des Edge-Transport-Servers in Exchange Server 2007 bietet neue Möglichkeiten, die Ihnen dabei helfen können, das Aufkommen von Spam, der Ihr Unternehmen erreicht, erheblich zu reduzieren. Die Edge-Transport-Serverfunktion verfügt über folgende Agents, die dabei helfen. Ihre E-Mail-Infrastruktur zu schützen. Die Angaben in Tabelle 19.2 stammen direkt aus der Micro-soft-Dokumentation für den Edge-Transport-Server.

**Tabelle 19.2** Edge-Transport-Server-Agents

Name des Agents	Beschreibung
Verbindungsfilter-Agent	Führt eine Filterung von Host-IP-Adressen auf der Grundlage von Anbietern von Positivlisten und IP-Sperrlisten durch.
Adressumschreibungs-Agent	Verändert SMTP-Adressen von Empfängern in eingehenden Nachrichten auf der Grundlage von vordefinierten Adress-Aliassen. Adressumschreibung kann in Situationen nützlich sein, in denen eine Organisation interne Domänen verbergen möchte.
Edge-Transport-Server-Agent	Verarbeitet alle mittels SMTP empfangenen Nachrichten, um die Transportregeln eines Edge-Transport-Servers durchzusetzen.
Sender ID-Agent	Entscheidet, ob der sendende SMTP-Host berechtigt ist, Nachrichten an die SMTP-Domäne des Absenders zu schicken.
Empfängerfilter-Agent	Prüft, ob die während der SMTP-Sitzung über den RCPT TO:-Befehl angegebenen Empfänger gültig und nicht in der Liste der blockierten SMTP-Adressen und Domänen enthalten sind.
Absenderfilter-Agent	Prüft, ob der Absender im MAIL FROM-Feld gültig und nicht in der Liste der blockierten SMTP-Adressen und Domänen enthalten ist.
Inhaltsfilter-Agent	Verwendet die Microsoft SmartScreen-Technologie, um auf den Inhalt eingehender Nachrichten zuzugreifen, und erstellt eine SCL-Bewertung für Spam auf der Grundlage der Transport- und Speicherschwel-lenwerte.
Protokollanalyse-Agent	Arbeitet mit Inhaltsfilter-, Absenderfilter-, Empfängerfilter- und Sender ID-Agents zusammen, um die Vertrauenswürdigkeit eines Absenders (SRL-Bewertung) zu ermitteln und auf dieser Grundlage Maßnahmen einzuleiten.
Anlagenfilter-Agent	Filtert Nachrichten auf der Grundlage des Namens der Anlage, der Dateierweiterung oder des MIME-Typs, um potenziell schädliche Nachrichten zu blockieren oder Anhänge zu entfernen.
Adressumschreibungs-Agent für ausgehende Nachrichten	Verändert SMTP-Adressen von Absendern in ausgehenden Nachrichten auf der Grundlage vordefinierter Adress-Aliase. Adressumschreibung kann in Situationen nützlich sein, in denen eine Organisation interne Domänen verbergen möchte.
Forefront Security für Exchange-Routing-Agent	Verantwortlich für die Verbindung mit dem Transport-Stack ,um sicherzustellen, dass der Scanvorgang Nachrichten vor der Auslieferung an den Hub-Transport-Server prüft.

Viele dieser Funktionen werden in Kapitel 20, »Antispam- und Antivirusfunktionen«, und Kapitel 21, »Exchange Server 2007-Nachrichten schützen«, beschrieben.

# Sicherheitstools von Microsoft

Um Sie dabei zu unterstützen, eine Exchange-Infrastruktur bereitzustellen und zu warten, die so sicher wie möglich ist, bietet Microsoft eine Reihe von Werkzeugen an, um Schadsoftware zu entfernen, die Konfiguration Ihrer Installationen zu prüfen und um Ihnen bei zahlreichen Servereinstellungen zu helfen.

- **Tool zum Entfernen bösartiger Software** Das Microsoft-Tool zum Entfernen bösartiger Software prüft Computer unter Windows XP, Windows 2000 und Windows Server 2003 auf Infektionen mit bestimmter gängiger Schadsoftware, z.B. Blaster, Sasser und MyDoom, und hilft dabei, diese Infektionen zu entfernen. Wenn der Erkennungs- und Entfernungsprozess abgeschlossen ist, zeigt das Tool einen Ergebnisbericht an, in dem steht, welche Schadsoftware gefunden und entfernt wurde. Microsoft gibt immer am zweiten Dienstag des Monats sowie bei Bedarf zum Schließen einer Sicherheitslücke eine aktualisierte Fassung dieses Werkzeugs heraus. Lassen Sie das Microsoft-Tool zum Entfernen bösartiger Software regelmäßig auf Ihren Exchange Server-Computer laufen, um sicherzustellen, dass Ihr System ungefährdet ist.

## Weitere Informationen

Weitere Informationen zum Download des Tools finden Sie unter <http://www.microsoft.com/security/malwareremove/default.mspx>.

- **Microsoft Baseline Security Analyser** Der Microsoft Baseline Security Analyser (MBSA) ist ein Werkzeug, das Ihre bestehende Umgebung analysiert und im Besonderen prüft, wie eine Reihe von Microsoft-Produkten konfiguriert sind, z.B. Windows 2000 SP3, Windows XP und Windows Server 2003, Office XP, Office 2003 und Office 2007, Exchange 2000, Exchange 2003 und Exchange 2007, SQL Server 2000 SP4 und SQL Server 2005. Diese Informationen vergleicht Microsoft mit einer Liste empfohlener Einstellungen und erstellt für Sie einen Bericht mit vorgeschlagenen Maßnahmen, mit denen Sie die Sicherheit Ihrer Infrastruktur verbessern können.

## Weitere Informationen

Weitere Informationen zum Download des Microsoft Baseline Security Analyzers finden Sie unter <http://www.microsoft.com/technet/security/tools/mbsa2/default.mspx>.

- **Security Configuration Wizard** Windows Server 2003 Service Pack 1 enthält den Security Configuration Wizard (SCW), ein Werkzeug, mit dem Sie die Angriffsfläche Ihrer Windows Server-Computer reduzieren können. SCW hilft Administratoren dabei, Sicherheitsrichtlinien nach dem Prinzip der geringsten Berechtigungen zu erstellen. Dies bedeutet, die auf einem Server laufenden Dienste auf ein Minimum zu reduzieren, sodass sie nicht für Angriffe auf das System genutzt werden können.

# Zusammenfassung

In diesem Kapitel haben wir ausgeführt, wie Hacker denken und wie Sie eingehende SMTP-E-Mail sowie den administrativen Zugriff auf Ihren Exchange Server-Computer absichern. Wir haben die Unterschiede zwischen einem Virus, einem Trojanischen Pferd und einem Wurm beschrieben und ein Verfahren zur Sicherung des eingehenden SMTP-Verkehrs dargestellt. Außerdem sind Sie auf zwei weitere Bereiche in diesem Buch verwiesen worden, die sich mit der Absenderfilterung und der Sicherung von OWA befassen. Im nächsten Kapitel legen wir dar, wie Sie E-Mail-Nachrichten mithilfe von Verschlüsselung und Zertifikaten schützen.