Zentrale Virenbekämpfung für firmenweite E-Mail-Systeme

Gefühlte Sicherheit

Lukas Grunwald

Kosten in Millionenhöhe und ein angeschlagenes Image drohen, wenn Schädlinge wie der Loveletter-Virus zuschlagen. Virenschutzprogramme sollen Unternehmen vor dem Schlimmsten bewahren. *iX* nahm 13 Produkte für E-Mail-Server unter die Lupe.

Die Gefahren beim Austausch von Daten haben in jüngster Zeit drastisch zugenommen. Neben der steigenden Bedrohung durch Viren, die mehr oder weniger blind Daten zerstören, besteht die Gefahr, dass böswillige Cracker und Industriespione Geschäftsgeheimnisse ausspähen, Ressourcen missbrauchen oder gezielt Angebotsparameter manipulieren. Da sich Viren, trojanische Pferde oder Würmer hauptsächlich durch E-Mail-Anhänge verbreiten, bieten sich für Firmenrechner und -daten zentrale Virenschutzlösungen an. *iX* testete 13 dieser Produkte.

Es gibt zwei Konzepte der zentralen Virenbekämpfung (siehe Kasten 'Zentraler Virenschutz'). Im ersten Fall installiert der Administrator einen Virenscanner direkt auf dem Mailserver, zum Beispiel auf einem Exchange-2000-Server oder einem Linux-System (Abb. 1). Die zweite zentrale Lösung besteht in der Installation eines SMTP-Gateways, das die Mails empfängt, auf Viren scannt und anschließend an den eigentlichen Mailserver durchreicht (Abb. 1).

Beide Varianten wurden getestet. Im Mittelpunkt stand jedoch nicht die Frage, ob die Virenscanner alle Variationen von Viren und Trojanern erkennen. Hier sei auf die regelmäßig stattfindenden Untersuchungen der Virentestlabore an den Universitäten Hamburg und Magdeburg verwiesen.

Kodierte und komprimierte Anhänge

Vielmehr war die zentrale Fragestellung, in welchen Varianten von Kodierungen – unkomprimiert oder mit verschiedenen Formaten komprimiert – diese Scanner Viren erkennen. Als Testvirus genügte daher der EICAR-Testvirus, den alle Produkte erkennen. EICAR ist ein frei verfügbarer, eigens für Testzwecke entwickelter Virus, der keinen Schaden anrichtet.

Historisch bedingt existieren verschiedene Verfahren, Binärdaten per E-Mail zu verschicken. Das ältere Verfahren kodiert die Daten mit dem aus der Unix-Umgebung stammenden *uuencode* und schickt sie im Mailbody (inline).

MIME ermöglicht ebenfalls das Verschicken im Mailbody, benutzt jedoch eine andere Kodierung (Base64). Alternativ erlaubt es das Anhängen von Binärdaten an die eigentliche Mail (Attachments).

Beim Test kamen für das Versenden des ausführbaren Virusprogramms alle drei Verfahren zum Einsatz: Versand als MIME-Attachment oder direkt im Mailbody (Inline), Base64- oder uu-kodiert. Alle drei Formate lassen sich automatisch von Netscape Messenger, Outlook, Outlook Express dekodieren und manuell per Doppelklick öffnen.

Zum Pflichtprogramm gehörte ebenfalls das Versenden des Virus in einem komprimierten Attachment, gepackt mit *arc*, *cab*, *lha*, *zip*, *rar*, *gzip*,

bzip2 und *tar* mit *gzip*; für die Linux-Plattform als unkomprimiertes *cpio*-Archiv (hier sollte der Virus im Klartext enthalten und lediglich mit einem *cpio*-Header versehen sein) sowie als *cpio.gz*, *cpio.tar.gz* und *cpio.bz2*.

In einer weiteren Teststufe wurden diese Formate untereinander permutiert, sodass jeder Scanner mit genau 1245 unterschiedlichen virusverseuchten Testmails beschickt wurde. Da sich diese Viren jedoch nicht mehr mit einem Doppelklick ausführen lassen, fällt das Nichterkennen bei der Bewertung des Produkts weniger ins Gewicht.

Der Testsender lieferte die Mail per SMTP an den Mailserver oder das SMTP-Gate. Ein Auswertungsrechner rief via IMAP die Mail vom Server ab und wertete aus, welche Mails entseucht beziehungsweise bereinigt wurden, welche mit dem Virus bis zum Client gelangt wären und welche verloren gingen, ohne dass das Verschwinden nachvollziehbar gewesen wäre.

Neben diesen zentralen Kriterien flossen in die Bewertung der Produkte Faktoren wie die Qualität der Log- und Auswertungsinstanzen, die Benutzerfreundlichkeit und Übersichtlichkeit der grafischen Oberfläche (GUI) sowie ihre Administrierbarkeit ein. Von Bedeutung für den Unternehmenseinsatz ist ebenfalls die Installation und Integration in bestehende Systeme. Und schließlich galt es zu überprüfen, ob die Produkte selbst Sicherheitsprobleme verursachen oder – etwa durch Inkompatibilität mit anderen Programmen – anderweitig Schwierigkeiten bereiten.

Heterogene Testumgebung

Als E-Mail-Server kam ein 600 MHz schneller Pentium III mit 512 MByte RAM zum Einsatz, als Gateway ein 1-GHz-Pentium-III mit 256 MByte Hauptspeicher. Folgende Plattformen dienten als Testumgebung:

– Microsoft Windows 2000 Advanced Server Service Pack 2 (SP2) mit dem Exchange-2000-Server Service Pack 1 (SP1)
– Debian Linux 2.2r4 mit Exim als Mail Transfer Agent (MTA) und dem Cyrus IMAP-Server

Als SMTP-Gateway ohne eigenen Virenscanner fungierte Baltimores MIMEsweeper 4.2.6, unter ihm wurden F-SECURE für MIMEsweeper und Sophos ANTI-Virus getestet. Unter Linux mussten sich RAV Anti-Virus, F-Prot von F-Secure und RAV von der GeCAD Software GmbH beweisen. Zum Zeitpunkt des Tests waren mehrere Produkte noch nicht verfügbar, so Norman Datadefense für Exchange 2000 und Antivirus für Linux von Kaspersky Labs, ebenso wenig der Gateway-Scanner von Computer Associates.

Produkte für Exchange-Server

Ohne Schwierigkeiten verlief die Installation von perComps **Command Antivirus 4.62 für Exchange** unter W2k. Die Administration erfolgt über eine kleine Konsole, das Produkt benutzt sowohl beim Monitoring als auch beim Login Windows-eigene Bordmittel. Von der Administrationskonsole aus lässt sich der Eventviewer zum Anzeigen der Logs benutzen oder der Performance-Monitor starten.

Der Scanner erkannte das Attachment *.cab* nicht. Weiterhin gab es Schwierigkeiten mit den Base64-Inline-Mails: Der EICAR-Virus im Klartext durfte passieren. Mit *uuencode* gepackte Attachments hingegen siebte das Produkt mühelos aus.

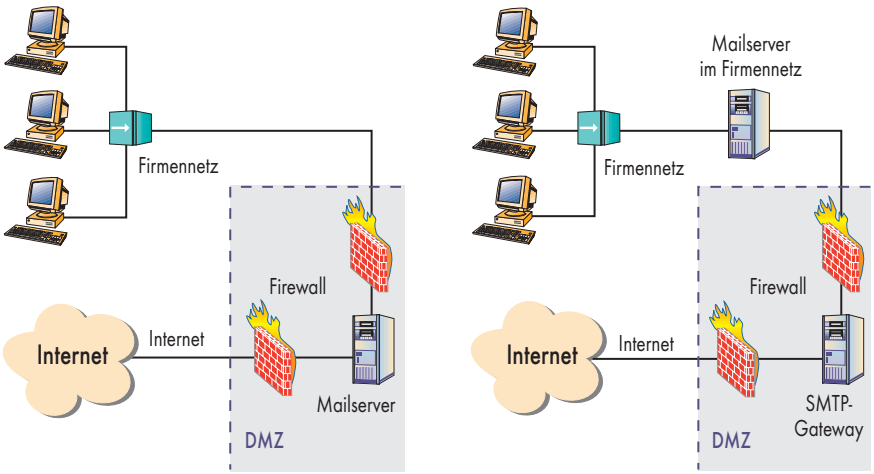
Bei **eTrust InoculateIT 6.0** von Computer Associates ist der Exchange Support als Plug-in in den eigentlichen Virenscanner für Windows 2000 zu installieren. Nachdem InoculateIT bei zwei Testläufen keinen Virus gefunden hatte, war Telefonsupport beim Hersteller gefragt. Des Rätsels Lösung: Damit der Scanner Mails überprüft, muss er über eine Checkbox im Echtzeitmonitor aktiviert werden – was man leicht übersehen kann.

InoculateIT fand die Viren in folgenden Kodier- und Pack-Kombinationen: MIME/lha, MIME/rar, MIME/zip sowie den Virus als direktes MIME-Attachment, alle anderen Mails ließ es durch. Was die Dekodierung der E-Mails anbelangt, besteht hier noch Verbesserungsbedarf. Ausreichender Schutz ist in dieser Version nicht gegeben.

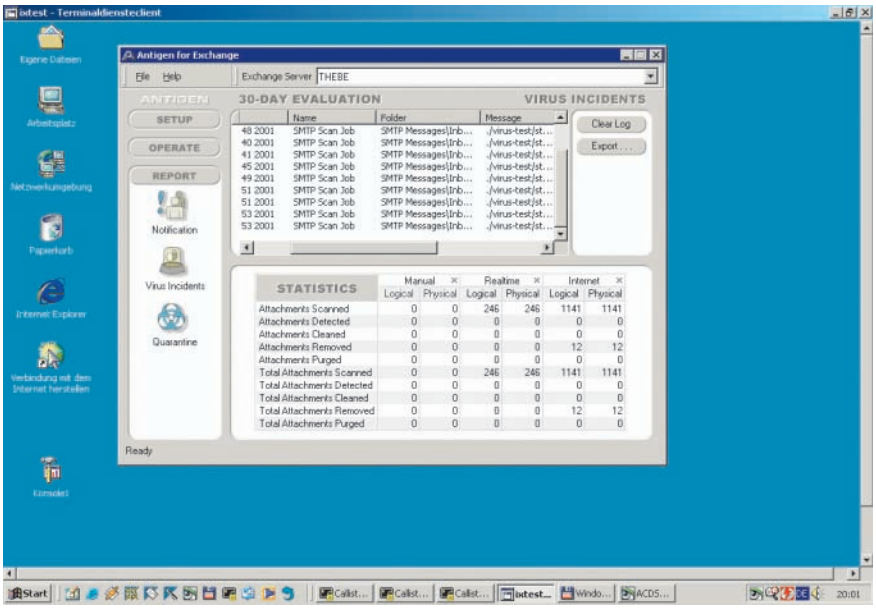
Die Installation von Trend Micros **ScanMail für Exchange 6.0** auf einem neuen System ist nicht ohne weiteres durchzuführen, da die Setup-Dateien auf der Software-CD gezippt vorhanden sind und ein Entpacker fehlt. Ein Download aus dem Internet

iX-TRACT

- Für die zentrale Bekämpfung von Viren existieren zwei Varianten: Der Virenscanner lässt sich entweder direkt auf dem Mailserver oder auf einem vorgeschalteten SMTP-Gateway installieren.
- Die getesteten Anwendungen weisen gravierende Qualitätsunterschiede bei der Implementierung und dem Erkennen der Formate auf; ein Zusammenhang zwischen Preis und Leistung ist nicht immer ersichtlich.
- Selbst die besseren Produkte sollten nicht als alleinige Lösung eingesetzt werden. Virenschutzkonzepte ohne Einbeziehen der Mail-Benutzer gaukeln Sicherheit allenfalls vor.



In der ersten Variante (links) ist der Virenscanner direkt auf dem Mailserver innerhalb des Firmennetzes installiert. Die zweite Variante (rechts) setzt auf ein SMTP-Gateway außerhalb des Firmennetzes, das die Mails erst nach dem Scannen an den Firmen-Mailserver weiterreicht (Abb. 1).



Scrollbar-Tango: Bei der ansprechenden, doch unpraktischen Benutzeroberfläche verschafft Fingerfertigkeit dem Administrator zwar keinen Über-, aber wenigstens einen Einblick (Abb. 2).

schafft kurzerhand Abhilfe. Das Gleiche gilt für die Dokumentation, ein Acrobat Reader für die erläuternden PDF-Dateien fehlt ebenfalls auf der CD. Positiv fiel auf, dass das Installationsprogramm eine ganze Serverfarm gleichzeitig installieren kann.

Was die Erkennung betrifft, fand der Scanner nur mit korrektem MIME-Attachment verschickte Viren, hier fehlte lediglich die *arc*-Erkennung. Uuencode- oder Inline-Base64-Attachments hingegen konnten ohne weiteres passieren. Auch die Option, mit der sich alle Attachments entfernen lassen sollen, zeigte sich wirkungslos. Da dem Hersteller diesbezüglich keine Schwierigkeiten bekannt sind, mutmaßt er einen Konfigurationsfehler.

Supportbedürftige Installation

In zwei Stufen erfolgt die Installation von Pandas **Global Virus Insurance**. Zuerst ist auf einer Managementstation der Panda-Administrator zu installieren, der das Netz nach Servern durchsucht. Diese lassen sich anschließend zentral von der Managementstation aus aktualisieren. Soweit die Theorie. Nachdem der Panda-Administrator den Exchange-2000-Testserver gefunden hatte, brach die Installation erst einmal ab und der Server funktionierte nicht mehr ordnungsgemäß.

Bei einem Telefonat mit der Hotline erkundigte sich der Techniker sofort, ob ein Backup des Exchange-Servers vorhanden sei, das Problem war bei Panda wohl schon bekannt. Nach der Neuinstallation von Windows 2000 und Exchange 2000 sowie einem 16 MByte großen Download ließ sich der Panda-Virenschutz schließlich installieren. Nach Angaben des Herstellers ist der Fehler in der aktuellen Download-Version bereits behoben, ebenso in der in Kürze fertig gestellten CD-Version M01-A02.

Damit der Scanner über Exchange Viruswarnungen verschicken kann, ist ein MAPI-E-Mail-Client auf dem Exchange-Server zu installieren. Falls ein Administrator Microsofts Outlook installiert, muss er allerdings die für diesen Mail-Client typischen Sicherheitsrisiken in Kauf nehmen.

Das Erkennen von uuencode-Attachments bereitet dem Panda-Scanner keine Schwierigkeiten, im Gegensatz zur Verpackung als Base64 Inline oder einem falschen MIME-Typ. Ebenso lässt die Archiv-Unterstützung zu wünschen übrig, es fehlt unter anderem der Support für *lha* in einer uukodierten Mail und *arc*.

In **Antigen**, dem Exchange-Schutz von Sybari, lassen sich bis zu fünf Scan-Engines integrieren: Sophos, Norman, NAI, CA VET und CA InoculateIT. Die Oberfläche ist zwar nett gestaltet. Leider ist es nicht vorgesehen, die Log-Fenster so zu vergrößern, dass

EICAR-TESTVIRUS IM BASE64-INLINE FORMAT

```
From root  Sun Dec  2 22:39:55 2001
Received: from ixtest. [193.108.131.11]
        by localhost with IMAP (fetchmail-5.9.5)
        for root@localhost (single-drop); Sun, 02 Dec 2001 22:39:55 +0100 (CET)
Received: from leda. ([193.108.131.14]) by thebe.ixtest with Microsoft SMTPSVC(5.0.2195.2966);
         Sun, 2 Dec 2001 21:36:41 +0100
Received: from metis ([193.108.131.21])
 by leda. (NAVGW 2.5.1.13) with SMTP id M2001120220390106927
 for <wolfgang@ixtest>; Sun, 02 Dec 2001 20:39:01 +0100
Received: from root by metis with local (Exim 2.05 #1 (Debian))
        id 16Aelf-0000Dl-00; Sun, 2 Dec 2001 22:37:25 +0100
Date: Sun, 2 Dec 2001 22:37:25 +0100
From: root <root@metis>
To: wolfgang@ixtest
Subject: ./virus-test/stufe1/eicar.com
Message-ID: <20011202223725.A849@callisto>
Mime-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Disposition: inline
User-Agent: Mutt/1.2.5i
Return-Path: root@metis
X-OriginalArrivalTime: 02 Dec 2001 20:36:41.0093 (UTC) FILETIME=[0C4C4350:01C17B71]
Status: RO
Content-Length: 150
Lines: 4
begin-base64 744 ./virus-test/stufe1/eicar.com
WDVPIVAlQEFQWzRcUFpYNTQoUF4pN0NDKTd9JEVJQ0FSLVNUQU5EQVJELUFO
VElWSVJVUy1URVNULUZJTEUhJEgrSCoNCg==
====
```

VIRENSCANNER FÜR EXCHANGE SERVER UND SMTP-GATEWAYS

Produkt	Antigen 6.2 for Exchange	F-Secure Anti-Virus for MIMEsweeper	F-Secure Anti-Virus for Linux	Sophos Anti-Virus	Sophos Anti-Virus
Hersteller	Sybari Software	F-Secure	F-Secure	Sophos	Sophos
Kontakt	www.sybari.com, +34 91/296 26 00	www.F-Secure.com, 089/78 74 67 00	www.F-Secure.com, 089/78 74 67 00	www.sophos.de, 061 36/911 93	www.sophos.de, 061 36/911 93
Preis für 1 Mailserver/50 User	1525 €	787 €	787 €	700 €	1071 €
Preis für 3 Mailserver/500 User	11 250 €	3625 €	3625 €	3750 €	5683 €
getestetes Betriebssystem	Windows 2000 SP2	Windows 2000 SP2	Debian GNU/ Linux 2.2r4	Debian GNU/ Linux 2.2r4	Windows 2000 SP2
Mailserver	Exchange 2000 SP1	MIMEsweeper / SMTP-Gate	Exim / Cyrus IMAP / Amavis	Exim / Cyrus IMAP / Amavis	MIMEsweeper / SMTP-Gate
erkannte Formate		(siehe MIMEsweeper)			(siehe MIMEsweeper)
arc	–		✓	✓	
cab	–		✓	✓	
rar	–		✓	✓	
lha	–		✓	✓	
zip	✓		✓	✓	
gzip	–		✓	✓	
bzip2	–		✓	✓	
tar	–		✓	✓	
inline/base64	–		✓	✓	
mime/base64	✓		✓	✓	
inline/uuencode	✓		✓	✓	
Installation	⊕	⊕	⊕	⊕	○
Administrierbarkeit / Handhabung	⊖⊖	⊕	⊕	⊕	⊕
Besonderheiten	große Schwierigkeiten bei Archiven				

* Open-Mail-Relay nach Installation ** Virenschutz muss explizit aktiviert werden

sich ein Administrator ohne viel Geschiebe einen Überblick über die Logs verschaffen kann (Abb. 2).

Sechs Mails für den Admin

Auch täuschen die vielen Scan-Engines nicht darüber hinweg, dass Sybaris' Produkt große Schwierigkeiten hat, den Inhalt der Mails festzustellen. Im Test konnte Antigen lediglich die EICAR-Testdatei als MIME-Attachment und uu-kodiert sowie das ZIP-Archiv ebenfalls als MIME erkennen. Das allerdings gleich von drei Engines, sodass sechs E-Mails produziert wurden. Eine so niedrige Erkennungsrate ist für ein Virenschutzprogramm indiskutabel, hinzu kommt das unbrauchbare Interface. Sybrian arbeitet bereits mit Hochdruck an den beanstandeten Schwächen und verspricht bessere Erkennungsraten in der nächsten Version.

Dass es auch anders geht, zeigt McAfees **Groupshield** Exchange. Die Anwendung ist von allen getesteten Produkten die einzige, die es in einer deutschen Version für das deutsche Exchange gibt. Die Installation verlief vorbildlich und reibungslos.

Der Manager ist übersichtlich, sodass sich der Administrator schnell einen Überblick verschaffen kann. Besonders positiv fällt der 'Outbreak Manager' auf. Bei einem massiven Virenbefall oder Angriff von außen kann er automatisch Maßnahmen einleiten. Diese reichen vom Versenden einer SMS an den Administrator über das 'Härten' des Setups bis hin zum Herunterfahren des Mailsystems.

McAfees GroupShield hat eine sehr hohe Erkennungsrate, überdies ist es das einzige Produkt für Exchange, das alle 'Pflicht'-Archivtypen unterstützt. Selbst bei exotischen Kombinationen zeigte es keine Schwächen. Einzig bei den Inline-Base64-Archiven versagte der Groupshield ebenso wie seine Konkurrenten. Wenn überhaupt ein Scanner für Exchange 2000 empfehlenswert ist, so McAfees GroupShield.

Aladdins **eSafe** wurde in zwei Versionen getestet, zum einen als Virenscanner für den Exchange-2k-Server, zum anderen als SMTP-Gateway. Nach der Installation des Produkts auf dem Exchange-Server kann man sich bei der Administratorkonsole von Aladdin anmelden. Eine Kurve soll auf der grafischen Oberfläche den Betrieb der Anwendung anzeigen. Nur zeigte sich trotz regen E-Mail-Verkehrs mit diesem Exchange-Server immer eine Flatline: eSafe untersuchte die E-Mails nicht auf Viren, erkannte sie demnach auch nicht. Mehrere Telefonate und Mails mit dem Hersteller ergaben nur, dass es sich eventuell um ein Problem mit den Rechten handeln könnte. Nachdem das Programm schließlich unter Administratorrechten lief, interagierte der Scanner nicht mit dem Exchange-Server.

Produkte für SMTP-Gateways

Das **SMTP-Gateway**, Aladdins zweites Produkt, ließ sich ebenso problemlos installieren wie der Scanner für den Exchange-Server. Bedauerlicherweise fehlt ihm die Funktion, wichtige Transaktionen zu protokollieren. So ist

Command AntiVirus	eSafe for SMTP	eTrust InoculateIT 6.0 Microsoft Exchange Option	Global Virus Insurance	InterScan Messaging Security Suite for SMTP _	McAfee Groupshield
perComp Verlag	Aladdin Knowledge Systems GmbH & Co KG	Computer Associates Int. (CA)	Panda Software	TREND MICRO Deutschld. GmbH	Network Asscociates/ McAfee
www.percomp.de, 040/696 281 60	www.aladdin.de, 089/89 42 21 0	www.ca.com, 061 51/949 0	www.pandasoftware.de, 020 65/98 76 54	www.trendmicro.de, 089/37 47 97 00	www.mcafeeb2b.com, 089/37 07 0
720 €	2400 € (mit Updates und Support für 1 Jahr)	2381,50 $	819,06 €	1390 €	auf Anfrage
3610 €	10 080 € (mit Updates und Support für 1 Jahr)	12 854,70 $	6126, 54 €	10 450 €	auf Anfrage
Windows 2000 SP2	Windows 2000 SP2	Windows 2000 SP2	Windows 2000 SP2	Windows 2000 SP2	
Exchange 2000 SP1	SMTP-Gate, alle Mailserver	Exchange 2000 SP1	Exchange 2000 SP1	SMTP-Gate, alle Mailserver	Exchange 2000 SP1
✓	–	–	–	–	✓
–	✓	–	✓	✓	✓
✓	✓	✓	✓	✓	✓
✓	✓	✓	✓	✓	✓
✓	✓	✓	✓	✓	✓
✓	–	✓	–	✓	✓
–	–	–	–	–	–
✓	✓	–	–	✓	✓
–	–	–	–	–	–
✓	✓	✓	✓	✓	✓
✓	✓	✓	✓	✓	✓
⊕	⊖*	⊖	○	⊕	⊕⊕
○	⊕	○	⊕⊕	⊕	⊕⊕
			durch PandaAdministrator zentral zu managen	parallel auf mehreren Servern installierbar	Produkt auch in Deutsch, Outbreak Manager für automatische Eskalation

das SMTP-Gate – in der Default-Einstellung – nicht in der Lage, Angriffe auf Protokollebene zu erkennen oder zu dokumentieren. Ein Expand- oder Verify-Angriff könnte unbemerkt stattfinden. Laut Hersteller lässt sich die Konfiguration jedoch ändern.

Ebenso wenig findet eine Überprüfung der E-Mail-Adressen nach RFC 2822 oder 822 statt, sodass binärer Shell-Code in der 'From'-Zeile munter mittransportiert werden kann – ohne auch nur eine Zeile im Log zu hinterlassen.

In der Default-Installation fungiert das eSafe-SMTP-Gateway zudem noch als Open-Mail-Relay: Über dieses System kann jeder im Internet seinen Spam verschicken – natürlich auf Kosten des Aladdin-Kunden. Nach einer Überarbeitung der Konfiguration ist dieses Loch aber schnell zu stopfen.

Eine Denial-of-Service-Attacke (DoS) auf SMTP-Ebene mit einer SYN-Rate von unter 400 pro Minute hat des Weiteren dazu geführt, dass der eigentliche Mailserverdienst abstürzte und sich nicht mehr starten ließ. Die Administrationskonsole verzeichnete lediglich die schon vom Exchange-Produkt bekannte Flatline. Ein Reboot war notwendig.

Wegen der Anfälligkeit der Software für Attacken unterschiedlicher Art ist von einem Betrieb in der DMZ mit offenen Port 25 nach außen nur abzuraten. Der Hersteller sieht den Einsatzbereich dieses Produkts ausdrücklich nur hinter einem weiteren SMTP-Gateway sowie einer Firewall.

Symantecs **Norton AntiVirus** für E-Mail-Gateways ließ sich ohne Schwierigkeiten installieren. Die Administration ist nur über einen Webbrowser möglich, die Verwaltung erfolgt mit einem integrierten Webserver. Die Authentifikation für die Administratoroberfläche geht allerdings im Klartext über die Lei-

tung, sodass ein Angreifer jederzeit das Administratorpasswort mitlesen kann. Auch bei Norton AntiVirus fungiert das Gate in der Default-Konfiguration als Open-Mail-Relay; mit entsprechenden Konfigurationsänderungen lässt sich das jedoch abschalten.

Probes und falsche SMTP-Kommandos werden vorbildlich erkannt und protokolliert. Die SMTP-Implementierung ist stabiler gegen DoS-Attacken als diejenige bei Aladdins Gateway. Bei den Formaten fehlt der Support für *arc*, *rar*, *tgz* und *zip*, ebenso die Fähigkeit, Inline-Base64-Attachments zu erkennen.

Spammen unerwünscht

Neben ScanMail, das auf dem Exchange-Server läuft, bietet Trend Micro eine zweite zentrale Lösung an: die **Trend Micro Viruswall**, die als SMTP-Relay läuft. Diese überrascht zunächst, indem sie bei der Installation nach den Domänen und Adressen der Forwarding-Mailserver fragt. Auf diese Weise vermeidet der Hersteller, dass sein Produkt als Open-Relay missbraucht werden kann.

Leider wird die Administration mit einem Internet Information Server (IIS) als Common Gateway Interface (CGI) durchgeführt. Spätestens nach Nimda und Code Red sollten sich Administratoren und Hersteller über das Gefahrenpotenzial des IIS im Klaren sein. Ein kleiner integrierter Webserver wie bei Norton wäre hier wünschenswert, allerdings mit SSL-Verschlüsselung. Negativ anzumerken ist ebenfalls, dass auch dieses Produkt das Administratorpasswort im Klartext über die Leitung schickt.

Positiv fällt hingegen auf, dass Trend Micro die Option bietet, einfache Richtlinien auf dem Gate abzubilden. Auch das Scannen nach Schlüsselwörtern ist vorgesehen, etwa damit Kollegen sich nicht gegenseitig beleidigen oder 'unhöfliche' Mails an Geschäftspartner verschicken. Es existieren Regeln, die die Zustellung von E-Mails mit rassistischen oder sexistischen Inhalten verhindern sollen.

Zentraler Virenschutz

Es existieren zwei verschiedene Konzepte der zentralen Virenbekämpfung, die sich auf die Sicherheitsanforderungen der Systemumgebung auswirken. Beim Aufspielen des Virenscanners direkt auf den Mailserver muss Letzterer in der demilitarisierten Zone (DMZ) installiert werden (s. Abb. 1). Versteht sich, dass dieses System durch eine Firewall zusätzlich zu schützen ist. Der Mailserver muss außerdem öffentliche IP-Adressen besitzen; mit einer privaten Adresse fungiert er als Firmen-Mailserver.

Der Vorteil dieser Installation ist, dass sie nur einen Rechner erfordert. Allerdings ist dieser mit dem Internet verbunden. Wenn Schwachstellen vorhanden sind, hat ein Angreifer Zugriff auf Firmen-Mails oder -netze. Die Clients müssen durch die Firewall auf die DMZ zugreifen.

In der zweiten Variante (s. Abb. 1) wird in der DMZ nur ein SMTP-Gateway installiert. Dieses System hat die Aufgabe, Viren zu erkennen und nur 'saubere' Mails durch eine Firewall auf den eigentlichen Mailserver der Firma zuzustellen. Bei einer solchen Installation ist der Mailserver von außen nicht sichtbar. Da sich in der DMZ nur das Gateway befindet, hat der Mailserver private IP-Adressen. Eine Firewall schützt den Zugang zum eigentlichen Mailserver.

Das Sicherheitsniveau ist im Vergleich zur ersten Lösung höher, da nur eine Kommunikationsbeziehung durch die Firewall besteht. Clients brauchen nicht durch die Firewall zuzugreifen, der Mailserver bleibt im Firmennetz. Durch den zusätzlich benötigten Rechner mit SMTP-Gateway-Software ist die zweite allerdings auch die teurere Variante.

VIRENSCANNER FÜR EXCHANGE SERVER UND SMTP-GATEWAYS

Produkt	MIMEsweeper 4.2.6	Norton AntiVirus 2.5 for Gateways	RAV AntiVirus	ScanMail for MS Exchange 2000 Server 6.0
Hersteller	Baltimore Technologies	Symantec	GeCAD Software GmbH	TREND MICRO Deutschld. GmbH
Kontakt	www.mimesweeper.com, 040/239 99 0	www.symantec.de, 021 02/74 53 0	www.rav-antivirus.de, 0421/17 888 0	www.trendmicro.de, 089/37 47 97 00
Preis für 1 Mailserver/50 User	1595 €	733,38 €	4441 € pro Server; 38 €) pro Domain (bel. Anzahl User	1250 €
Preis für 3 Mailserver/500 User	9990 €	6025,94 €	4441 € pro Server; 38 € pro Domain (bel. Anzahl User)	10 450 €
getestetes Betriebssystem	Windows 2000 SP2	Windows 2000 SP2	Debian GNU/Linux 2.2r4	Windows 2000 SP2
Mailserver	SMTP-Gate, alle Mailserver	SMTP-Gate, alle Mailserver	Exim / Cyrus IMAP / Amavis	Exchange 2000 SP1
Erkannte Formate				
arc	✓	–	✓	–
cab	✓	✓	✓	✓
rar	✓	–	✓	✓
lha	✓	–	✓	✓
zip	✓	✓	✓	✓
gzip	✓	–	✓	✓
bzip2	✓	–	✓	–
tar	✓	–	✓	✓
inline/base64	teilweise	–	✓	–
mime/base64	✓	✓	✓	✓
inline/uuencode	✓	✓	✓	✓
Installation	⊕	⊖*	⊕	⊕
Administrierbarkeit/Handhabung	⊕⊕	⊕	⊕	⊕
Besonderheiten	Komplette Integration in Microsofts Management-Konsole	Passwort für Administrator wird im Klartext übertragen		parallel auf mehreren Servern installierbar

* Open-Mail-Relay nach Installation

Die Unterstützung von Archiven ist besser als bei der Exchange-Version, nur fehlt das *arc*-Format und die Inline Base64-Unterstützung.

Die Installation von Baltimores **MIMEsweeper** mit Virenscanner als Plug-in erwies sich als ausgesprochen schwierig, da das Installationsprogramm die Minimalanforderungen pingelig überprüft. So muss eine aktuelle *mapi32.dll* installiert und das Windows-spezifische Domänenpräfix genau definiert sein. Anschließend fragt der MIMEsweeper nach einem Inbound- und Outbound-SMTP-Server, also den Maschinen, von denen er Post akzeptieren beziehungsweise weiterleiten soll. Somit wird das Open-Mail-Relay-Problem schon durch die Konzeption der Installation vermieden.

Als einziges Programm im Test benutzt der MIMEsweeper Microsofts Managementkonsole, sodass ein Administrator auf seiner gewohnten Oberfläche auch die Parameter des MIMEsweepers anpassen und die einzelnen Mail-Warteschlangen verwalten kann.

MIMEsweeper bietet weit reichende Funktionen, um komplette Richtlinien abzubilden, und hat die komplexesten Setup-Möglichkeiten von allen getesteten Windows-Produkten. Die Vielschichtigkeit des Produkts führte allerdings dazu, dass die Anpassung des Setups im Test nicht auf Anhieb gelang. Nach zwei Supportanrufen bei Baltimore ließ sich jedoch ein für das Testszenario adäquates Setup durchführen.

Als Virenscanner wurden für den Test sowohl F-Secures Anti-Virus für MIMEsweeper als auch Anti-Virus von Sophos eingebunden. Für beide bietet Baltimore auf seiner Homepage die entsprechenden Szenarien, das heißt Anpassungen an den MIMEsweeper an. Die Virenscanner funktionierten ohne Schwierigkeiten, da das Entpacken der Attachments in den Aufgabenbereich des MIMEsweeper fällt.

Mit Inline Base64 hatte der MIMEsweeper seine Schwierigkeiten, er bietet jedoch die Möglichkeit, jedes unbekannte Attachment einzufrieren, bis ein Administrator es freigibt.

Von 1245 infizierten Testmails ließ der MIMEsweeper nur 463 durch, das ist keine schlechte Rate. Für Windows ist er ein starkes Instrument, um ein SMTP-Gate aufzubauen. Er zeigt sich resistent gegen DoS-Angriffe und schreibt jedes SMTP-Sondieren (Probe) oder Angriffe auf Protokollbasis im Event-Log mit. Die Integration in ein W2k-Serverumfeld ist Baltimore von

allen getesteten Windows-Produkten am besten gelungen.

Produkte für Unix/IMAP

Alternativ wurde für den Test ein Mailserver auf der Basis der freien Linux-Distribution Debian GNU/Linux Version 2.2r4 aufgebaut. Debian benutzt als MTA Exim von Philip Hazel (www.exim.org). In diesen wurde ein Amavis-Virenscanner integriert. Bei **Amavis** in der Stable-Release-Version handelt es sich um ein Perl-Skript, das ebenfalls freie Software ist und auf eine Vielzahl von Funktionen aus dem für die Allgemeinheit verfügbaren CPAN-Archiv zugreifen kann. Als einziger Scanner war Amavis in der Lage, alle Attachments im Test korrekt zu erkennen und zu entpacken. Da Amavis keine Scan-Engine besitzt, sind externe Scanner nötig, zum Einsatz kamen folgende Produkte:

– H+BEDV AntiVir/X
– McAfee Virusscan
– DataFellows F-Secure AntiVirus
– Trend Micro FileScanner
– RAV AntiVirus
– Command AntiVirus for Linux

Mit allen Scannern ließen sich die gleichen hervorragenden Ergebnisse erzielen. Wer auf Nummer sicher gehen will, kann auch zwei oder mehr Scanner einbinden. Der einzige Nachteil bei Amavis ist die ausgesprochen hohe Systemlast, wenn sich viele Mails in der Warteschlange befinden, die parallel abgearbeitet werden. Im Stresstest zeigte *uptime* zeitweise eine Last von 96 an. Das System bewältigte zwar letztendlich die verschärfte Testsituation, hier besteht jedoch durchaus Verbesserungsbedarf.

Als einziger Viren- und Attachment-Scanner lieferte das Amavis-Skript einen falsch-positiven Alarm: Beim Inline-Transport der Sequenz eines menschlichen Genoms glaubte das Programm, es handele sich um ein unbekanntes Inline uuencode-Attachment.

Ebenso wie MIMEsweeper bietet der Mail-Transferagent Exim weit reichende Funktionen an, die das System gegen Spam oder andere Angriffe schützen. Exim hat eine eigene Skriptsprache, genauso einfach lässt sich aber auch Perl integrieren. Von allen getesteten MTAs ist Exim der funktionstüchtigste, aber auch komplexeste. Richtlinien über ‘Transports’ lassen sich ebenso abbilden wie mit dem MIMEsweeper, bei Exim fehlt allerdings die grafische Oberfläche.

Als Mail-Server kam der IMAP-Daemon von Cyrus zum Einsatz. Die Integration von Server und Skript in Exim verlief ohne Schwierigkeiten. Es bleibt noch anzumerken, dass das Gespann Exim, Amavis und IMAP ebenso auf anderen Plattformen wie FreeBSD, OpenBSD oder Solaris verfügbar ist.

Fazit

Im Gegensatz zu vielen Desktop-Scannern, die sich in die ‘File-Open’-Funktion des Betriebssystems einklinken, kommt es bei der zentralen Virenbekämpfung auf andere Qualitäten an.

Wer einen brauchbaren und unkomplizierten Schutz für seinen Exchange-Server braucht, ist mit McAfees Groupshield zwar noch nicht auf der sicheren Seite, ein besserer Schutz ist jedoch zurzeit nicht verfügbar.

Als Gateway vor dem Mailserver ist auf jeden Fall Baltimores MIMEsweeper zu empfehlen. Er erfordert zwar eine beträchtliche Einarbeitungszeit, bietet dafür ein mächtiges Werkzeug, um ein Windows-2000-Mail-System halbwegs sicher zu machen. Alle anderen getesteten Gateway-Produkte haben den einen oder anderen nicht akzeptablen Pferdefuß.

Wenn ein höheres Sicherheitsniveau angestrebt wird, kommt man um eine Linux- oder FreeBSD-Lösung kaum herum. Amavis hatte die höchste Erkennungsrate von allen Entpackern.

Im Wesentlichen unterscheiden sich die heutigen Scan-Engines kaum voneinander. Bei der Implementierung und dem Support der verschiedenen Mail-Formate sind allerdings deutliche Qualitätsunterschiede sichtbar.

Über eines sollten sich Administratoren und Entscheidungsträger in Unternehmen immer im Klaren sein: Einen hundertprozentigen Schutz, wie

Glossar

Base64: Kodierung im MIME-Standard, um Binärdaten (RFC 1421) in ASCII umzuwandeln. Dabei werden lediglich die 64 Zeichen A–Z, a–z, 0–9 und +/ benutzt.

DMZ (Demilitarisierte Zone): Dieses Netz ist Teil einer Firewall-Umgebung, für die die Zugriffsregelungen nicht so streng sind wie in einem privaten LAN hinter einer zweiten Firewall. In der DMZ stehen gewöhnlich Webserver, Mailserver, Proxy und dergleichen, die übers Internet zu erreichen sind.

Expand: SMTP-Kommando zum Auflösen von Mail-Aliassen

Falsch negativ: Ein bedenkliches Ereignis wird nicht erkannt.

Falsch positiv: Ein unbedenkliches Ereignis wird irrtümlich als Gefahr erkannt (Falschalarm).

IMAP (Internet Message Access Protocol): Mail-Protokoll (RFC 1730), das dem Client die Bearbeitung der Mails auf dem Server ermöglicht.

MAPI (Messaging Application Programming Interface): Bei MAPI handelt es sich um eine von Microsoft entwickelte Schnittstelle für E-Mail.

MIME (Multipurpose Internet Mail Extensions): Die MIME-Spezifikation (RFC 2045) erlaubt es, eine Mail in mehrere Teile aufzuteilen. Nicht-ASCII-Daten lassen sich auf diese Weise kodieren und in ein oder mehreren Anhängen übertragen.

MTA (Mail Transfer Agent): Der Dienst, der für die Weiterleitung und Zustellung von E-Mails zuständig ist. Der im Internet am häufigsten benutzte MTA ist Sendmail.

MUA (Mail User Agent): Programm zum Lesen und Verschicken von Nachrichten.

Scan-Engine: Ein Virenscanner besteht aus zwei verschiedenen Teilen: dem eigentlichen Scanner, der die Mails entpackt, und der Scan-Engine, die die entpackten Mails auf viralen Code untersucht.

SMTP (Simple Mail Transfer Protokoll): SMTP ist das Transportprotokoll für E-Mail über TCP/IP-Verbindungen.

SMTP-Gateway: Rechner, der auf Protokollebene als Brücke zwischen zwei Sicherheitslevels dient.

SYN-Rate: SYN-Pakete sind Teile des TCP-Protokolls, die dazu dienen, eine neue Verbindung aufzubauen. Die SYN-Rate gibt in diesem Zusammenhang an, wie viele neue TCP-Verbindungen (Mailzustellungen) von verschiedenen Hosts gleichzeitig abgearbeitet werden können.

Uuencode: Kodierung von Binärdaten, bei der drei 8-Bit-Zeichen einer Datei in vier nur aus 6 Bit bestehende Zeichen umgewandelt werden und zu jedem Ergebnis eine 32 addiert wird.

Verify: Überprüfen, ob es einen Account auf dem Rechner gibt

Ressourcen im Web

Virentestcenter der Universität Hamburg: agn-www.informatik.uni-hamburg.de/vtc/dt.htm

Virentestcenter der Universität Magdeburg: www.av-test.de

European Institute for Comuter Anti-Virus Research: www.eicar.org

EICAR-Testvirus: www.eicar.org/anti_virus_test_file.htm

Debian GNU/Linux: www.debian.de

Freier Amavis-Virenscanner: www.amavis.org

EXIM MTA: www.exim.org

Project Cyrus: asg.web.cmu.edu/cyrus

er auf vielen Verpackungen oder Werbeprospekten angepriesen wird, kann es nicht geben. Wer etwas anderes behauptet, sorgt bei Anwendern lediglich für ein trügerisches Gefühl der Sicherheit. Das Erwachen im Fall des Versagens von Schutzmaßnahmen trifft den Geschädigten umso härter. Nichts ist schlimmer, als wenn eine Sicherheitslösung neue Sicherheitslücken in eine bestehende Installation reißt.

Zudem ergibt der alleinige Einsatz eines Virusscanners oder SMTP-Gateways wenig Sinn. Ohne Firewall-Architektur und eine überwachte DMZ sind alle diese Produkte in einem professionellen Umfeld nutzlos. Im Unternehmen ist eine genau definierte Richtlinie für die Kommunikationsbeziehungen nach außen unumgänglich. Überdies müssen Notfallszenarien definiert sein, die ohne technisches Verständnis der Zusammenhänge eines Systems kaum zu erstellen sind.

Unumgänglich in allen Fällen ist die Förderung des Sicherheitsbewusstseins bei den Mitarbeitern eines Unternehmens. Zu sorglos wird noch immer mit dem Medium E-Mail umgegangen. Ein Viren-Scanner ist nur eine von vielen unterstützenden Maßnahmen. Solange viele E-Mail-Clients in ihrer Default-Einstellung untragbare Sicherheitsmängel aufweisen, gibt es Mittel und Wege, den Virenschutz auszuhebeln. Der beste Schutz ist immer noch Know-how im eigenem Haus und fähige Administratoren. (ur)

LUKAS GRUNWALD

studiert Informatik an der TU Braunschweig und arbeitet als Consultant bei DN Systems, Hildesheim.