Zentraler Virenschutz

Der Einsatz von Virenscannern ist der erste Schritt in Richtung Netzwerk-Sicherheit. Im Betrieb müssen sich die Programme zudem einfach zentral administrieren lassen. Das versprechen alle getesteten Pakete.

Jürgen Heyer

Jeden Monat erscheinen 500 neue Viren, über 80 000 sind weltweit registriert. Seit Ende Januar 2004 kommen fast täglich neue Varianten der Würmer Mydoom, Netsky und Bagle oder Sasser in Umlauf (siehe auch *PC Professionell* 5/2004, Seite 14). Dabei tauchen immer mehr Versionen der genannten Viren auf, und die Verbreitungsmethoden werden immer trickreicher. Angesichts dieser akuten Bedrohung ist es entscheidend, dass der Virenscanner im Netzwerk den Administrator durch eine komfortable Verwaltung entlastet. *PC Professionell* testet neun Netzwerk-Virenscanner auf Schutzfunktionen, einfache Installation und komfortable Administration. Bei der Virensuchleistung ist das Testergebnis beruhigend: Sowohl der Testsieger von McAfee als auch die Produkte von Gdata, F-Secure, Kaspersky, Sophos, Softwin sowie Trend Micro leisten eine nahezu 100-prozentige Virenerkennung. Lediglich Makroviren bleiben ein Problem, nur Trend Micro kommt über 90 Prozent Erkennung hinaus. Bei gezippten Laufwerken bieten nur Gdata und Kaspersky 100-prozentigen Schutz, besonders schwach sind hier Computer Associates und Symantec (je 64,5 Prozent Erkennung).

Voraussetzung für den Betrieb der hier vorgestellten Virenscanner ist ein Windows-Server im Netzwerk. Eine Verwaltungskonsole dient bei den Testkandidaten dazu, die Vorgaben für alle Rechner im Netzwerk festzulegen. Das Verwaltungsprogramm muss auf einem Windows Server (Windows NT/2000/2003) installiert sein und kann von einem beliebigen PC im Netzwerk aus kontrolliert werden.

Verteilungs-Varianten

Für die zentral gesteuerte Installation der Client-Software auf den Arbeitsplätzen stehen meist mehrere Varian-

»Beruhigend: Auf die aktuell getesteten Netzwerk-Virenscanner ist Verlass.«

Hardware-Leiter **Markus Bauer**

ten zur Verfügung. Wenn die Workstations unter Windows NT, 2000 oder XP Professional laufen und überall ein Administrator-Account eingerichtet ist, nimmt die Konsole darüber die Installation und Konfiguration vor. Dieses Feature bieten alle Testkandidaten. Der Admin-Account ist allerdings aufgrund seiner Netzwerk-weiten Rechte oft nicht erlaubt.

Besser ist die Installation per Log-in-Skript, das sich zentral vorgeben lässt. Die Konfiguration über Log-in-Skript erlauben die Produkte von Trend Micro, Kaspersky, Network Associates, Sophos und Symantec. In der Client Server Suite von Trend Micro hilft sogar ein Assistent bei der Anpassung.

Die beste Methode: Alle außer Gdata Antiviren Kit 2004 Client/Server verfügen über einen Packager zur Erstellung von Installationspaketen. Damit erzeugt der Administrator das Setup-Programm nach seinen Vorstellungen. Entweder enthalten die Pakete die gesamte Client-Installation oder einen Agenten, mit dem man weitere Module über die Konsole einrichtet.

Clients zentral verwalten

Nach der Client-Installation lassen sich die Arbeitsplätze bei allen Testprodukten von der Konsole des Virenscanners verwalten. Diese zeigt den aktuellen Status der Clients an, sammelt Meldungen über Virenfunde und ermöglicht die Änderung der Client-Einstellungen.

Gut: Alle Testkandidaten kennen Client-Gruppen, mit denen der Administrator die Workstations nach unterschiedlichen Einstellungen sortiert. Sinnvoll ist dies beispielsweise, wenn ausgewählte Anwender lokale Drives selbst auf Viren scannen dürfen.

Alle Hersteller veröffentlichen täglich aktualisierte Signaturen, bei akuten Gefährdungsmeldungen sogar mehrmals am Tag. Dabei holt sich die Konsole die Signatur von der Webseite des Herstellers und legt sie auf dem Server ab. Von dort aktualisieren sich die Clients. Außer bei Gdata und Network Associates können sich Clients auch direkt aus dem Internet updaten. Fällt der Intranet-Server für die Aktualisierung aus, erlauben die Scanner von Computer Associates, F-Secure und Gdata die Nutzung eines Clients als zentrale Update-Quelle.

Gefahr durch E-Mails

Eine weitere zentrale Funktion der Virenscanner ist die Kontrolle der E-Mails. Für Exchange, Lotus Notes oder Postfix sind entsprechende Plug-ins optional verfügbar. Ein SMTP-Gateway-Filter überwacht auf dem Server den gesamten Datenverkehr und prüft die E-Mail-Pakete (POP3- und SMTP-Protokoll). F-Secure und Bit Defender verlagern die Mail-Überprüfung auf die Client-Seite. Bei McAfee blockiert der Virenwächter das Öffnen infizierter E-Mails. Das verhindert eine Infektion, blockiert aber das Postfach. Ein Plug-in für Outlook bieten McAfee, Antiviren Kit, Kaspersky, Symantec und Trend Micro. MBA/NIE

Empfehlungen der Redaktion

McAfee Security Active Virusscan Suite SBE
Die McAfee-Suite ist wegen der umfangreichen Managementmöglichkeiten perfekt für den Einsatz in großen Netzwerken geeignet. Die Verwaltung ist sehr übersichtlich, besonders die Reportfunktion. Die Virensuchleistung markiert im Testfeld die Spitze.

Kaspersky Anti-Virus Business Optimal
Kaspersky Anti-Virus zeichnet sich vor allem durch einen gut ausgestatteten Client aus. Die Konsole bietet etwas weniger Funktionen als bei McAfee, für kleinere Netzwerke aber genügend. Die Virensuchleistung liegt auf dem gleichen Niveau wie bei McAfee.

	Produkt	Hersteller	(maximal 100 Punkte)
1	**McAfee Security**	Network Associates	84,7
2	**Kaspersky Anti-Virus**	Kaspersky	83,7
3	**F-Secure Anti-Virus**	F-Secure	83,1
4	**Trend Micro Client Server**	Trend Micro	80,2
5	**Symantec Antivirus**	Symantec	78,1

Produkte im Detail

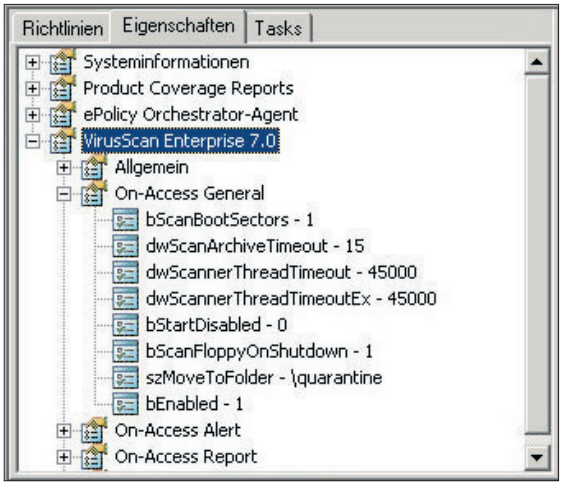
McAfee Security Active Virusscan Suite SBE

Network Associates

Gut 84,7

■ Weitgehend automatisch läuft die Installation von McAfees Virenscanner ab. Nur die Agenten sind auf den Clients einzurichten, anschließend lassen sich die Dateien automatisch verteilen. Die Bedienung der Konsole erfordert wegen des hohen Funktionsumfangs etwas Einarbeitung, erweist sich dann aber als übersichtlich. Besonders hervorzuheben ist die gute Reportfunktion mit druckfertiger Aufbereitung der gesammelten Ergebnisse.

Bei der Virensuchleistung steht die Suite auf dem zweiten Platz. Nur zwei Trojaner werden im Test nicht gefunden. Sehr gute Arbeit leistet auch der Virenwächter, nur aus passwortgeschützten Dokumenten lassen sich Makroviren nicht entfernen.



Umfangreiche Policy-Einstellungen von McAfee erfordern Einarbeitung, sind aber ein mächtiges Steuerinstrument.

Die E-Mail-Prüfung übernimmt ein Outlook-Plug-in, das zudem POP3-Accounts filtert. Kommt ein anderes E-Mail-Programm zum Einsatz, übernimmt der Virenwächter für ein- und ausgehende Dateien die Prüfung. Einziges Manko: Der Wächter sperrt nicht nur den Zugriff auf die jeweils infizierte Mail, sondern blockt den gesamten Postfachordner.

Der Testsieger von McAfee (für 1200 Euro) glänzt mit sehr guter Virensuchleistung, einfacher Installation und guter Client-Software.

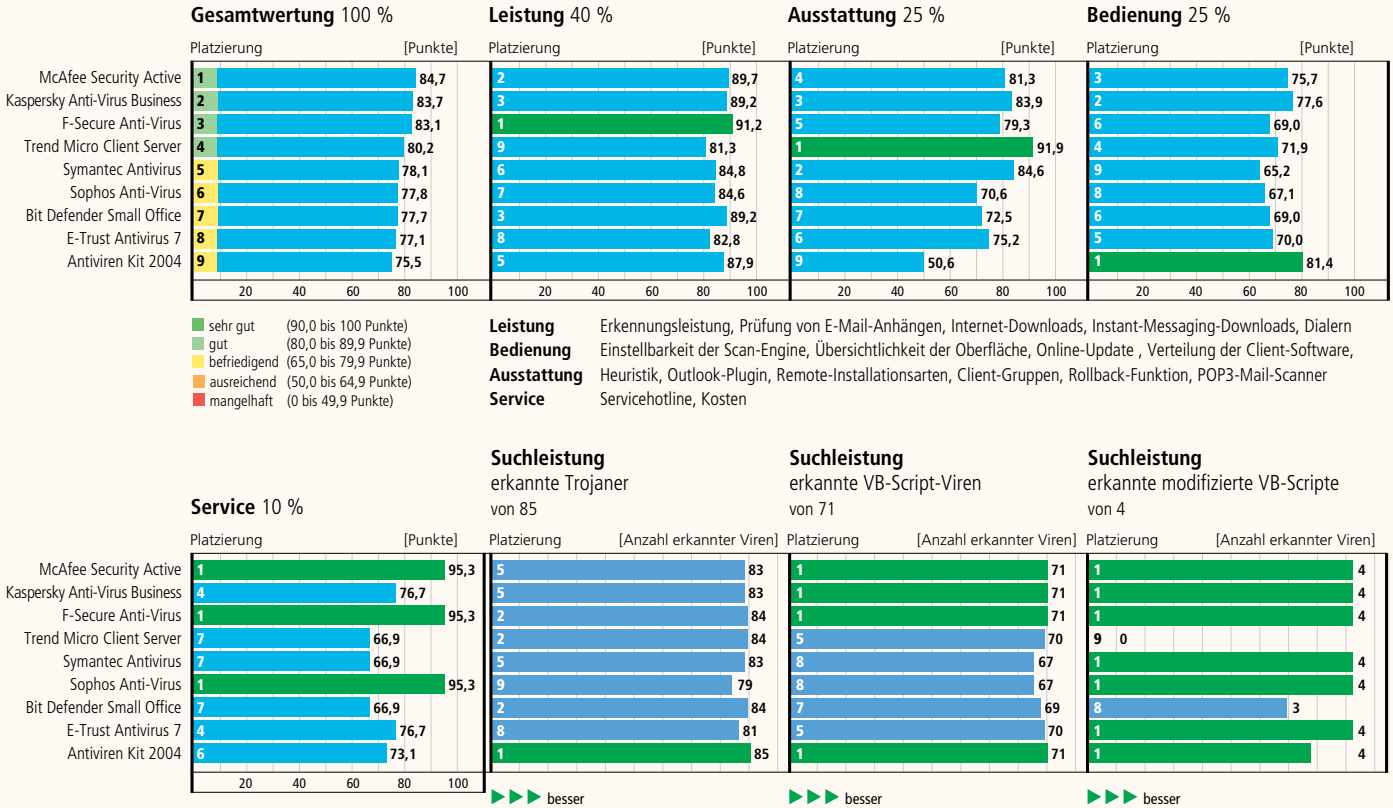
Kaspersky Anti-Virus Business Optimal

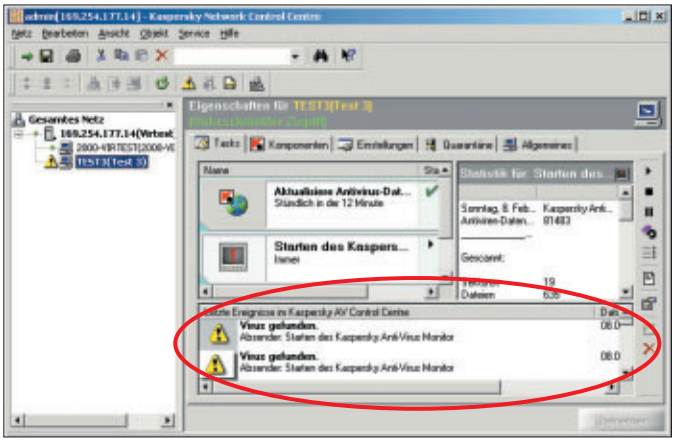
Kaspersky

Gut 83,7

■ Nach der Installation des Network Control Centre und der einzelnen Client-Pakete werden die Clients über eine Netzwerk-weite Suche in die Verwaltungsstruktur aufgenommen. Die Updates der Rechner erfolgen wahlweise über den zentralen Server oder über das Internet. So ist auch bei einem Serverausfall noch

Wertungen & Messwerte





Das Kaspersky Network Control Centre zeigt Virenfunde zwar an, verrät aber nicht den Virustyp.

eine Aktualisierung der Arbeitsplätze mit Virensignaturen möglich. Positiv fällt das übersichtliche Handbuch auf.

Als weniger gut erweist sich die Reportfunktion, die zwar meldet, dass Viren gefunden wurden, aber nicht deren Typ. Außerdem könnte die Anzeige übersichtlicher sein.

Die Virensuchleistung ist sehr gut und markiert in fast allen Bereichen die Spitzenwerte. Nur zwei Trojaner werden nicht gefunden. Schwach ist dagegen die Mail-Abwehr: Im Test lässt Kaspersky mehrere infizierte Mails passieren. Zudem fehlt die E-Mail-Prüfung von POP3-Accounts.

Das Kaspersky-Programm bietet einfache Installation, ein hochwertiges Handbuch und exzellente Trefferraten bei der Virensuche. Wegen des günstigen Preises von 820 Euro erhält die Software die »Budget-Empfehlung«.

F-Secure Anti-Virus Client Security

F-Secure

Gut 83,1

■ Im Webbrowser-Design ist die übersichtliche Verwaltungskonsole des F-Secure Policy Manager gestaltet. Problemlos läuft die Einrichtung der Clients ab, da die Konsole selbstständig das Netz nach PC-Arbeitsplätzen durchsucht und diese dann in der Zusammenfassung anzeigt. Eine Übersicht zeigt die Daten zum markierten Objekt auf: Aktualität der Virensignatur, Virenalarme und -funde.

Die Virensuchleistung von Anti-Virus ist die beste im Test. F-Secure setzt zwei Engines ein. Neben einer eigenen haben die Finnen die Engine von Kaspersky lizenziert.

Eine umfassende Ausstattung besitzt die Client-Software. Neben dem Virenscanner und -wächter sowie einem Zeitplaner ist eine komplette E-Mail-Prüfung auf IP-Basis enthalten. Ohne dass eine weitere Konfiguration erforderlich ist, filtert das Tool den POP3-Datenverkehr und prüft ein- und ausgehende E-Mails. Eine Firewall ist ebenfalls im Lieferumfang.

Die mit 1400 Euro für 15 Clients teuerste Software im Test überzeugt durch einfache Installation und die beste Gesamt-Virenschutzfunktion im Testfeld.

Trend Micro Client Server Suite for Small and Medium Businesses 2.0

Trend Micro

Gut 80,2

■ Die Verwaltung erfolgt über einen Webbrowser, so dass auf dem Server entweder IIS oder Apache 2.0 installiert sein muss. Sehr übersichtlich präsentiert sich die Bedienoberfläche. Auf der Client-Seite beschränkt sich die Unterstützung auf Windows-Betriebssysteme, beim Server können daneben auch Linux- und Netware-Server verwendet werden.

Falls die Software einen infizierten Client findet, kann die Managementkonsole Officescan freigegebene Laufwerke und TCP-Ports gezielt blockieren sowie den Schreibzugriff auf die Clients unterbinden. Funktionell gut ausgestattet ist die Client-Software. Ein Schwachpunkt ist allerdings der Scanner für POP3-E-Mail-Accounts, dieser unterstützt nur Outlook und Eudora Pro. Die Virensuchleistung ist befriedigend, die Engine lässt drei Bootviren, einen Makrovirus und einen Trojaner durch. Bei den Dialern reagiert Officescan mit neun anstelle von 16 Alarmen nur ungenügend.

Insgesamt erweist sich die 840 Euro teure Suite als durchdachtes und stabiles Produkt. Ausbaufähig ist die E-Mail-Prüfung für POP3-Accounts.

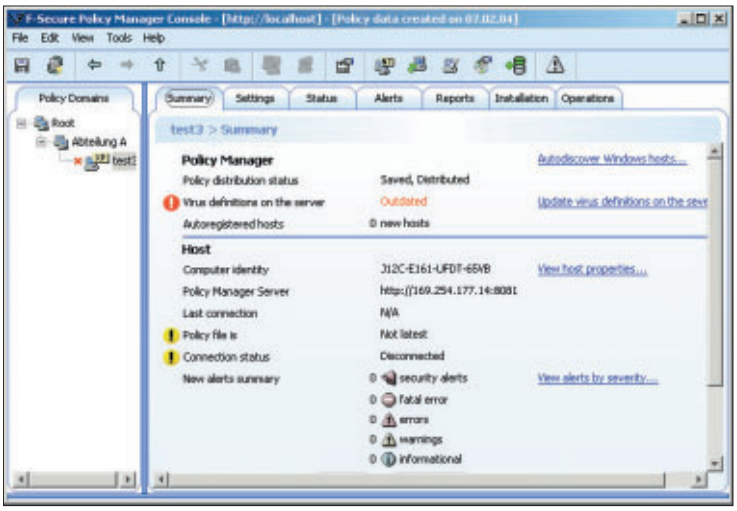
Symantec Antivirus for Small Business

Symantec

Befriedigend 78,1

■ Antivirus eignet sich für heterogene Betriebssystem-Umgebungen mit Mac-OS, Solaris und OS/2, unterstützt jedoch kein Linux. Die Installation gestaltet sich recht komplex. Die einzelnen Module sind getrennt zu installieren und deren jeweiliger Zweck ist nicht auf den ersten Blick ersichtlich. Auch das englischsprachige Handbuch hilft hier nicht weiter.

Das Symantec System Center zur Verwaltung läuft nur unter Windows NT, 2000 und XP, da es sich in die MMC (Microsoft Management Console) einklinkt. Die Konfiguration der Client-Software vom Server aus bereitet keine Probleme. Allerdings fehlt eine Überwachung für POP3-E-Mail-Accounts, und das mitgelieferte Out-



F-Secure Policy Manager Console ähnelt einem Webbrowser, ist aber ein eigenständiges Tool.

look-Plug-in funktioniert ausschließlich in Verbindung mit Exchange oder einem IMAP-Server. Positiv: Neben Exchange wird Lotus Domino unterstützt.

Die Erkennungsleistung ist gut, bis auf zwei Trojaner und vier VB-Script-Viren, die die Software übersieht. Schwach ist dagegen die Online-Abwehr, da es infizierte Anhänge erst beim Öffnen oder Speichern findet. Das 1400 Euro teure Antivirus enthält eine Lizenzierung für 20 Clients statt für 15 wie bei den anderen Produkten.

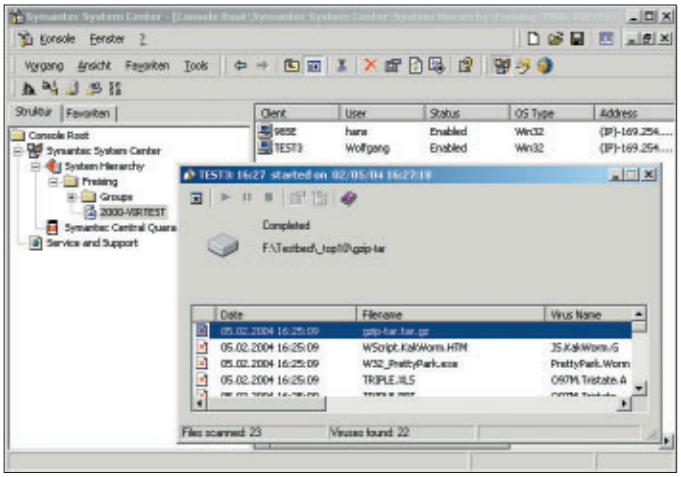
Die Symantec-Software wartet mit umfangreichen Features auf. Der Einsatz ist aber wegen der Einschränkungen beim Client und der komplexen Installation nur in Verbindung mit Exchange oder Lotus Domino sinnvoll.

Sophos Anti-Virus

Sophos

Befriedigend 77,8

■ Sophos bietet keine Einzelplatz-, sondern nur eine Netzwerk-Version an. Diese arbeitet dann aber auch mit allen gängigen Netzwerk-Betriebssystemen. Weitgehend



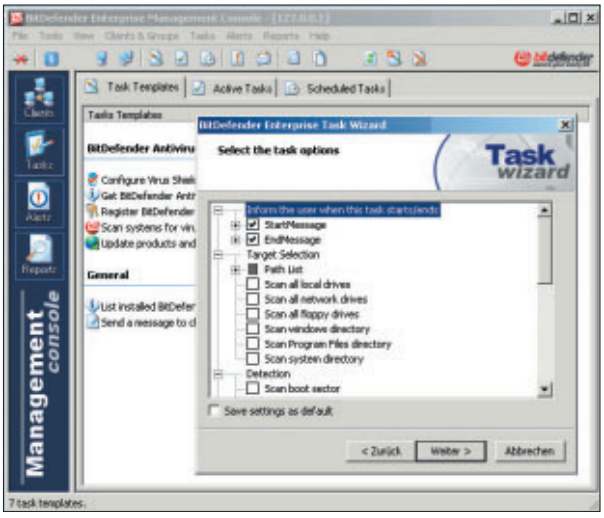
Symantec System Center nutzt die Microsoft Management Console, das schränkt den Betriebssystem-Support ein.

problemlos verläuft die Installation des zentralen Servers und der Konsole. Zuerst sind die Agenten auf den Clients zu installieren, dann wird die eigentliche Viren-Software von der Konsole aus verteilt. Für den Überblick in größeren Netzen sorgt ein spezieller Reportgenerator.

Die Client-Software ist trotz sehr umfangreicher Konfigurationsmöglichkeiten ausgesprochen übersichtlich gestaltet. Bemerkenswert ist auch die Vielzahl der unterstützten Client-Betriebssysteme.

Zur Beschleunigung der Dateiprüfung verwendet Sophos Anti-Virus eine zentrale Prüfsummenfunktion: Hierzu ermittelt der Virenwächter zu jeder Datei eine Prüfsumme und gibt diese an den zentralen Server weiter. Bei einem neuen Datei-Check wird im ersten Schritt nur die Prüfsumme verglichen. Erst bei einem Unterschied wird die Datei erneut auf Virenbefall untersucht.

Im Vergleichstest schwächelt Anti-Virus bei der Virenerkennung. Bei der Suche nach Trojanern und VB-Script-



Bei Bit Defender sind sämtliche Aufträge über den Task Wizard einzustellen, ein umständlicher Weg.

Viren ist es sogar das Schlusslicht. Sophos Anti-Virus (975 Euro) ist ein solides Werkzeug mit großem Funktionsumfang. Die Virensuchleistung ist vergleichsweise schlecht.

Bit Defender Small Office Suite
Softwin
Befriedigend 77,7

■ Wegen der eingeschränkten Steuermöglichkeit der Clients eignet sich Bit Defender von Softwin vor allem für kleinere Netzwerke. Eine Besonderheit ist der leistungsfähige, integrierte E-Mail-Scanner für Clients.

Weniger Komfort findet der Administrator bei der Verwaltung vor. Alle Aufgaben wie beispielsweise ein Scan-Vorgang auf Clients sind als eigene Tasks zu konfigurieren. Neue Einstellungen lassen sich an die Clients senden, die bestehenden jedoch nicht abfragen. Keine Probleme bereitet die Verteilung von Updates. Bit Defender nutzt auf den Clients die normale Antiviren-Software für Einzelplatzrechner inklusive aller Funktionen wie einem E-Mail-Scanner und der Überwachung der Registry. Bei den Tests schneidet Bit Defender schlecht ab, das Programm findet als Einziges den sircam.c nicht.

Bit Defender (1030 Euro) ist eine gute Wahl für den Administrator, der wenig Aufwand in die Konfiguration stecken möchte. Dafür muss er eingeschränkte Abfrage-Möglichkeiten der Clients in Kauf nehmen.

E-Trust Antivirus 7
Computer Associates
Befriedigend 77,1

■ Die Administration von E-Trust erfolgt über einen Webbrowser, sämtliche Verwaltungsfunktionen sind in die Oberfläche des Scanners integriert. Anfänglich verwirrend ist die Vielzahl an Zweigen in der Baumstruktur. Nach einer gewissen Einarbeitung wird die Systematik jedoch durchschaubar: Zuerst sind die Einstellungen zu definieren und anschließend einem oder mehreren Clients zuzuweisen. Ein Vorteil ist, dass jeder Client sich als Administratorkonsole nutzen lässt.

In E-Trust arbeiten wie bei F-Secure zwei Virensuchmaschinen, hier Iris und Vet. Zwei unabhängige Teams von CA haben sie entwickelt. Iris schneidet mit der Einstellung *Genau* deutlich besser ab. Die Vet-Engine liefert schlechtere Ergebnisse. Anders als bei F-Secure kann der Scanner nicht beide Engines gleichzeitig einsetzen, was sich in der Platzierung niederschlägt. Vier Trojaner, drei Makroviren und ein VB-Script-Virus bleiben unerkannt.

E-Trust kostet nur 555 Euro und überzeugt durch einfache Bedienbarkeit. Für 300 Euro mehr erhält man aber bei Kaspersky wesentlich bessere Virensuchleistungen.

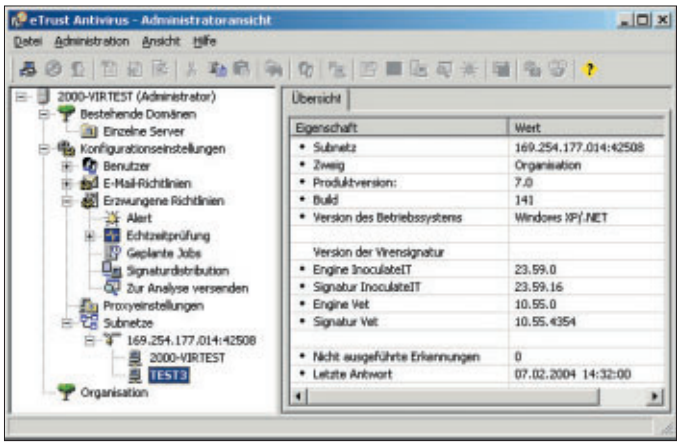
Antiviren Kit 2004 Client/Server
Gdata
Befriedigend 75,5

■ Die Verwaltung von Antiviren Kit 2004 Client/Server ist recht übersichtlich. Die Installation des Management-Servers muss auf einem System mit Windows NT/2000/XP Professional erfolgen, für die Administrationskonsole reicht Windows 98.

Der Anwender am Client kann die Tätigkeit des Virenscanners nicht beeinflussen, da alles im Hintergrund abläuft. Auch Client-Updates direkt aus dem Internet erlaubt die Software nicht. Allerdings lassen sich dediziert Datenträger in lokalen Laufwerken scannen. Die E-Mail-Überwachung ist auf Outlook beschränkt.

Die Virensuchleistung ist gut, da Gdata die leistungsstarken Engines von Kaspersky und Bit Defender lizenziert hat. Als Einziger im Test erkennt Antiviren Kit alle Trojaner. Deutliche Schwächen zeigen sich bei der Beseitigung von Makroviren in Office-Dokumenten. Im Testlabor kann AVK viele nur Viren komplett löschen, aber infizierte Dateien nicht säubern – das verhindert eine bessere Platzierung.

Wer nur Windows-Clients im Einsatz hat, ausschließlich Outlook für E-Mails verwendet und wenig Verwaltungsaufwand betreibt, ist mit Antiviren Kit 2004 Client/Server gut bedient. Mit 1340 Euro ist der Virenscanner allerdings zu teuer. MBA



Die Konsole von E-Trust Antivirus nutzt eine umfangreiche Baumstruktur für die Anzeige aller Informationen.

Weitere Infos

■ **www.sophos.de/sophos/docs/deu/comviru/viru_bde.pdf**
Leicht verständliche Einführung zum Thema Viren, Würmer und Trojaner

■ **securityresponse.symantec.com/avcenter/vinfodb.html**
Englischsprachige Informationen über nahezu alle bekannten Viren

■ **www.networkassociates.com/us/security/home.asp**
Aktuelle Virenaktivitäten

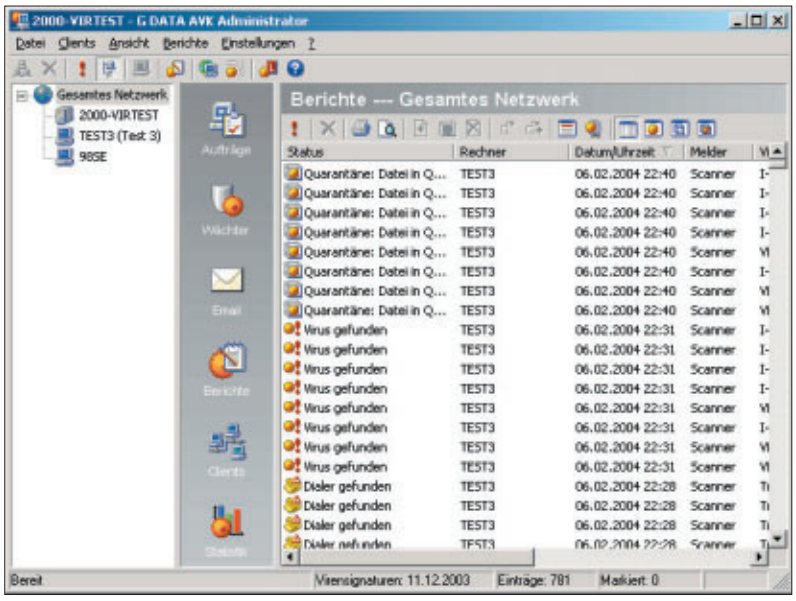
So testet PC Professionell

Für den Test müssen die Virenscanner rund 450 der am weitesten verbreiteten Schädlinge entdecken. Der Virencocktail enthält 28 aktuelle Viren, 88 Makroviren, darunter auch Junk- und Nasty-Makroviren, 119 Bootviren, 85 Trojaner, 71 VB-Script-Viren, 21 Viren vom Typ JS/HTML und 20 Dialer. Außerdem erzeugen die Tester im Labor mit einem Construction Kit insgesamt 16 VB-Script-Würmer und betten in ein Word-Dokument sowie in eine Powerpoint-Präsentation eine verseuchte Excel-Tabelle ein. Auch harmlose Word- und Excel-Makros werden durch die Virenprüfung geschickt, bei denen die Scanner nicht alarmieren sollen. Weiterhin werden die Viren in passwortgeschützte ZIP-Dateien eingepackt.

Zur Prüfung der E-Mail-Tauglichkeit werden Viren als E-Mail-Anhang versandt und per Outlook, Pegasus (jeweils POP3 und IMAP) sowie T-Online empfangen.

Geprüft wird, ob die Viren erkannt und ob sie entfernt werden. Sämtliche Tests laufen in einer abgeschotteten Laborumgebung, damit kein Virus die Testumgebung verlassen kann.

Im Testlabor werden die zu prüfenden Kandidaten in einem 100-MBit-Ethernet-Netzwerk auf einem Windows-2000-Server und zwei Clients unter Windows XP und Windows 98 SE installiert. MBA



Viel zu tun: Die Virenscanner werden im PC-Professionell-Testlabor auf Herz und Nieren geprüft.

Testaufbau

Prozessor: AMD Athlon XP 1800+ • Arbeitsspeicher: 384 MByte RAM • Mainboard: Gigabyte GA7VAXFS • Netzwerkadapter: Realtek RTL8139/810x • Betriebssystem: Windows 2000 Server mit SP 4 • LAN-Verbindung über 8-Port-Hub Fiberline FL-2008DS

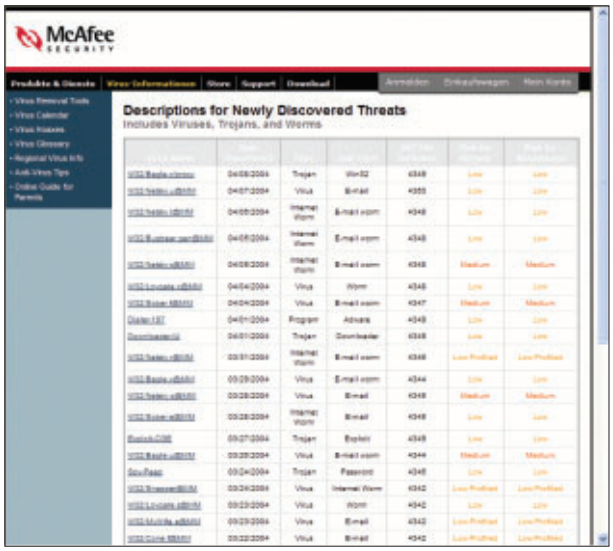
WETTLAUF DER VIREN

Immer schneller folgen die Virenvarianten aufeinander, sogar Kettenreaktionen kommen immer häufiger vor. Jürgen Heyer

Nur 26 Tage nach dem Bekanntwerden der DCOM-RPC-Schwachstelle im Juli 2003 versucht der Wurm W32.Blaster diese zu nutzen, um in PCs unter Windows NT/2000/XP/2003 einzudringen. Befallene Systeme stürzen unkontrolliert ab, außerdem führen sie eine DDoS-Attacke auf Microsoft-Server durch. Fakt ist, dass aktuelle Viren vor allem erst seit kurzem bekannte Schwachstellen nutzen. 64 Prozent aller angegriffenen Schwachstellen sind weniger als ein Jahr bekannt und 66 Prozent der angegriffenen Schwachstellen beinhalten ein hohes Risiko (Quelle Symantec). Es ist auch nicht auszuschließen, dass die Virenprogrammierer Hand in Hand arbeiten.

Chronologie der Attacken

Die Brisanz zeigt die aktuelle Entwicklung, beginnend am 26. Januar 2004 mit dem Erscheinen des Wurmes Mydoom.a. Am 2. Februar 2004 startet dann der Nachfolger Mydoom.b eine allerdings erfolglose DDoS-Attacke gegen www.microsoft.com, und Mydoom.e attackiert am 16. Februar einen Server von SCO. Als Nutznießer von Mydoom versuchen wenige Tage später die Würmer Doomjuice.a und Doomjuice.b, die von Mydoom geöffneten Hintertüren für sich zu nutzen. Die Würmer Doomhunter, Nachi.b, Bagle.b und Netsky.b von konkurrierenden Malware-Autoren wiederum versuchen, Mydoom.a/b auf infizierten Systemen zu beseitigen. Die Reaktion der Mydoom-Viren-Coder ist Mydoom.f, worauf prompt die Variante Nachi.d erscheint. Die Würmer Bagle.d/e/f wiederum versuchen, Mydoom und Netsky den Garaus zu machen. So wogt der Kampf hin und her. Am 16. April ist



Und täglich grüßt der Virus: Nur ständig aktualisierte Engines helfen gegen die häufigen Attacken.

Vergleichsweise sicher: Derzeit gibt es Länder mit noch größeren Virenproblemen als Deutschland.

Netsky bei der Variante w angelangt, Bagle existiert in der Variante x. Ein Ende der Schlacht ist noch nicht abzusehen. Wer als Administrator gegen diese Flut antreten will, braucht nicht nur eine verlässliche Antiviren-Software, sondern auch verlässliche Mitarbeiter.

Goldene Regeln

Wichtig ist vor allem, die Neugierde bei E-Mails im Zaum zu halten. Unaufgefordert zugesandte Mails von unbekannten Quellen und sogar Mails von Bekannten mit untypischen Texten sind Anzeichen dafür, dass etwas nicht stimmt. Allerdings verwenden viele Würmer wie Sober auch deutsche Anschreibentexte, die dann allerdings im Zusammenhang mit dem Versender keinen Sinn machen. Besondere Vorsicht ist geboten, wenn ein Attachment beigefügt ist. Beim Versand von Dateien sind das DOC- und XLS-Format aufgrund der Makrounterstützung besonders kritisch, da sie sich gut als Wirt für Makroviren eignen. Weniger gefährlich sind die Formate RTF und CSV, die unterstützen keine Makros. Für Dokumente, die nur zum Lesen gedacht sind, ist das PDF-Format ideal geeignet. Dieses ist weitgehend immun gegen Viren – bisher gab es nur den Virus Peachy, der zur Verbreitung eine installierte Acrobat-Vollversion voraussetzt – und sorgt gleichzeitig dafür, dass der Empfänger ein ordentlich formatiertes Dokument erhält. Verpönt ist grundsätzlich der Versand von EXE-Dateien, die von Outlook XP und neueren Outlook-Versionen standardmäßig blockiert werden.

Am besten ist es, wenn der Administrator am E-Mail-Gateway der Firma grundsätzlich all jene Dateitypen abblockt, die häufig als Virenträger fungieren. Dies sind EXE-, COM-, SCR-, VBS-, SHS-, CHM- und BAT-Dateien. Die E-Mail-Software sollte weiterhin so konfiguriert sein, dass E-Mails als Text angezeigt werden und nicht im HTML-Format. HTML-Mails können Skripts enthalten, die beim Öffnen automatisch ausgeführt werden. MBA

GLOSSAR

Heuristik Heuristiken analysieren alle ausführbaren Programme nach virenrelevanten Aktionen. Dafür beschränken sich die Verfahren meist auf den Beginn oder das Ende des Programmcodes. Während der Zugriffe werden bestimmte Sequenzen in Assembler-Befehle übersetzt.

Prüfsumme Berechneter Wert von Datenobjekten, mit dem festgestellt werden kann, ob irgendwelche Daten verändert wurden.

VB-Script (Visual Basic Script) Code innerhalb einer Anwendung, eines Dokuments oder einer Website, der ausgeführt wird, sobald jemand die entsprechende Seite anklickt.

Virensignaturen Über Signaturen impfen die Hersteller ihre Programme gegen neue Viren. Die Signaturen beinhalten Informationen über eindeutige Merkmale eines Virus, anhand deren der Scanner den Schädling erkennen kann.

Wertung & Ausstattung

	PLATZ ①	PLATZ ②	PLATZ ③	PLATZ ④
				
Produkt	**McAfee Security Active Virusscan Suite SBE**	**Kaspersky Anti-Virus Business Optimal**	**F-Secure Anti-Virus Client Security**	**Trend Micro Client Server Suite for Small and Medium Businesses 2.0**
Hersteller	**Network Associates**	**Kaspersky**	**F-Secure**	**Trend Micro**
Gesamturteil [Punkte]	**gut 84,7**	**gut 83,7**	**gut 83,1**	**gut 80,2**
Leistung (40 %) [Punkte]	2. Platz 89,7	3. Platz 89,2	1. Platz 91,2	9. Platz 81,3
Ausstattung (25 %) [Punkte]	4. Platz 81,3	3. Platz 83,9	5. Platz 79,3	1. Platz 91,9
Bedienung (25 %) [Punkte]	3. Platz 75,7	2. Platz 77,6	6. Platz 69,0	4. Platz 71,9
Service (10 %) [Punkte]	1. Platz 95,3	4. Platz 76,7	1. Platz 95,3	7. Platz 66,9
Info	(089) 370 70	(08 41) 88 19 71 70	(089) 78 74 67 00	(089) 37 47 97 00
Internet	www.networkassociates.de	www.kaspersky.de	www.f-secure.de	www.trend-micro.de
Preis (15 Clients)	1200 Euro	820 Euro	1400 Euro	840 Euro
Manager-Funktionen				
Windows NT/2000/XP	●/●/●	●/●/●	●/●/●	Webbrowser
Windows NT Server/2000 Server	●/●	●/●	●/●	Webbrowser
Windows 2003/Linux	●/○	○/○	●/●	Webbrowser
Unterstützte Groupware	optional	optional	optional	optional
Remote-Installation (Log-in-Skript)	●	●	●	●
Remote-Installation (Website)	○	○	●	●
Remote-Installation (NT, 2000, XP Pro)	●	●	●	●
Update der Clients aktiv	●	○	●	●
Update der Clients passiv	●	●	●	●
Installations-Packager	●	●	●	●
Rollback-Funktion (Update-Rücknahme)	●	○	●	●
Einstellungen der Clients	●	●	●	●
Suchfunktion für Clients	○	●	●	●
Alle Clients scannen	●	●	●	●
Client-Gruppen	●	●	●	●
Outbreak Monitor	●	●	○	●
Log-Funktion Updates	●	●	●	●
Log-Funktion Virenfund	●	●	●	●
Benachrichtigung	E-Mail, SNMP, Windows-Ereignisanzeige, Pager	E-Mail	E-Mail, SNMP, Windows-Ereignisanzeige, Tivoli	E-Mail, SNMP, Windows-Ereignisanzeige, Pager
Zentrale Quarantäne	●	●	○	●
Client-Funktionen				
Windows 95/98/Me	●/●/●	○/●/●	○/●/●	○/●/●
Windows NT/2000/XP	●/●/●	●/●/●	●/●/●	●/●/●
Windows NT Server/2000 Server	●/●	●/●	●/●	●/●
Windows 2003/Linux	●/●	●/○	●/●	●/○
Sonstige Betriebssysteme	Netware, DOS, HP-UX, SCO, AIX, Solaris	○	○	○
Virenscanner	●	●	●	●
Virenwächter	●	●	●	●
Update direkt per Internet	○	●	●	●
Outlook-Plug-in	●	● nur Mapi	○	●
POP3-Mail-Scanner	○	○	●	●
Sperrung für Anwender/Passwort	●/●	●/●	●/○	●/●
Zeitplaner	●	●	●	●
Kontextmenü im Explorer	●	●	●	○
Backup vor Reparatur	●	●	○	●
Service				
Hotline	(069) 66 40 43 30	(08 41) 88 19 71 70	(089) 787 46 73 00	über Fachhändler
Fazit	Testsieger, zweitbeste Virensuchleistung	Budget-Empfehlung, bestes Preis-Leistungs-Verhältnis	einfache Installation, beste Virensuchleistung	gut und preiswert, aber eingeschränkte E-Mail-Prüfung

● = ja ○ = nein [1)]0,12 Euro pro Minute [2)]Auslandstarif [3)]19–18 Uhr: 0,046 Euro pro Minute, 18–9 Uhr 0,025 Euro pro Minute

	PLATZ ⑤	PLATZ ⑥	PLATZ ⑦	PLATZ ⑧	PLATZ ⑨
					
	Symantec Antivirus for Small Business	**Sophos Anti-Virus**	**Bit Defender Small Office Suite**	**E-Trust Antivirus 7**	**Antiviren Kit 2004 Client/Server**
	Symantec	**Sophos**	**Softwin**	**Computer Associates**	**Gdata**
	befriedigend 78,1	**befriedigend 77,8**	**befriedigend 77,7**	**befriedigend 77,1**	**befriedigend 75,5**
	6. Platz 84,8	7. Platz 84,6	3. Platz 89,2	8. Platz 82,8	5. Platz 87,9
	2. Platz 84,6	8. Platz 70,6	7. Platz 72,5	6. Platz 75,2	9. Platz 50,6
	9. Platz 65,2	8. Platz 67,1	6. Platz 69,0	5. Platz 70,0	1. Platz 81,4
	7. Platz 66,9	1. Platz 95,3	7. Platz 66,9	4. Platz 76,7	6. Platz 73,1
	(069) 66 41 03 15	(061 36) 911 93	(075 42) 94 44 44	(089) 99 61 91 10	(02 34) 976 20
	www.symantec.de	www.sophos.de	www.bit-defender.de	www.ca.com/offices/germany	www.gdata.de
	1400 Euro (20 Clients)	975 Euro	1030 Euro	555 Euro	1340 Euro
	●/●/●	○/○/○	●/●/●	Webbrowser	●/●/●
	●/●	●/●	●/●	Webbrowser	●/●
	●/○	●/○	●/○	Webbrowser	●/○
	Lotus Domino ab 5.08, MS Exchange ab 5.5, SMTP-Gateways	optional	optional	Lotus Domino ab 4.1, MS Exchange	optional
	●	●	○	●	○
	●	○	○	○	○
	●	●	●	●	●
	●	●	●	●	●
	●	●	●	●	○
	●	●	●	●	○
	●	○	○	○	○
	●	●	●	●	●
	●	○	○	●	●
	●	●	●	○	●
	●	●	●	●	●
	○	○	○	●	○
	●	●	○	●	●
	●	●	●	●	●
	E-Mail, SNMP, Windows-Ereignisanzeige, Pager	E-Mail, SNMP, Windows-Ereignisanzeige	E-Mail	E-Mail, SNMP, Pager	E-Mail, SMS, Telefon
	●	●	○	○	○
	○/●/●	●/●/●	○/●/●	●/●/●	○/●/●
	●/●/●	●/●/●	●/●/●	●/●/●	●/●/●
	●/●	●/●	●/●	●/●	●/●
	●/○	●/●	●/●	●/●	●/○
	Netware, Solaris, OS/2, Mac-OS	Netware, DOS, Mac-OS, Open-VMS	○	Netware, Mac-OS	○
	●	●	●	●	●
	●	●	●	●	●
	●	●	●	●	○
	●	○	○	○	● nicht Express
	○	○	●	○	○
	●/●	●/○	●/●	●/○	●/○
	●	●	●	●	○
	●	○	●	●	○
	●	○	○	●	○
	(069) 66 41 03 15	(061 36) 91 19 66	(075 42) 94 44 60	(02 31) 120 82 08	(01 801) 00 11 88[3)]
	mächtiges Produkt mit komplexer Installation	Ausstattung und Bedienung sind die Schwachpunkte	eingeschränkt bei Management und Ausstattung	preiswertestes Programm, schlechteste Virensuchleistung	zu teuer für die gebotenen Leistungen