

Tod den



Killerviren

Schadsoftware wird immer komplexer und leistungsfähiger. Der halbjährlich erscheinende Security Intelligence Report von Microsoft zeigt, dass Cyberkriminelle einen hohen Organisationsgrad erreicht haben und fast ausschließlich aus finanziellen Motiven agieren. FACTS stellt daher in seiner Kaufberatung aktuelle Sicherheitspakete für Unternehmen auf den Prüfstand.



Trotz der massiven Bedrohungen aus dem Internet sind die Infektionsraten in Deutschland im internationalen Vergleich niedrig und sind zum dritten Mal in Folge sogar gesunken. Die neue Microsoft-Studie belegt, dass nur 0,22 Prozent der Computer in Deutschland im zweiten Halbjahr 2009 von Schadsoftware befallen wurden. Das ist deutlich unter dem weltweiten Durchschnitt von 0,7 Prozent.

Besonders unsicher sind Rechner in der Türkei: Dort sind immerhin 2 Prozent infiziert. Die größte Bedrohung geht in Deutschland weiterhin von Trojanern aus. Trotz eines Rückgangs um 26 Prozent im Vergleich zum ersten Halbjahr wurden in der zweiten Hälfte 2009 immer noch 373.861 Computer von Trojanern befallen. Gefolgt werden sie von Trojan-Downloadern

und potenziell unerwünschter Software, deren Aufkommen sich mehr als verdoppelt hat.

„Die aktuellen Zahlen bestätigen erneut: Der beste Schutz ist – neben einem gesunden Misstrauen und einer aktuellen Anti-Virus-Software – ein System, dessen Software auf dem neuesten Stand ist“, sagt Tom Köhler, Direktor Informationssicherheit bei Microsoft Deutschland. „Erfreulich, dass deutsche Computerbenutzer beim Thema Internetsicherheit im internationalen Vergleich einen guten Job machen.“

VIRENBEFALL PER POST

Die meisten dieser Schädlinge erreichen den PC per E-Mail. Es reicht aber schon der Aufruf einer gefälschten Internetseite oder ein unüberlegter Klick auf einen OK-Button, um sich ein Virusproblem einzufangen. Aufgrund dieser zahlreichen Bedrohungen ist für Unter-

nehmen die Sicherstellung eines aktuellen Schutzes oberstes Gebot.

In dieser Kaufberatung vergleicht FACTS insgesamt sechs verschiedene Sicherheitslösungen für mittelständische Unternehmen der Hersteller Kaspersky, McAfee, Norman, Sophos, Symantec und Trend Micro. FACTS hat die vorgestellten Schutzlösungen unter dem Nutzenaspekt für mittelständische Unternehmen betrachtet. Dazu wurde der Einsatz einer Lösung für eine Unternehmenssituation mit 25 Workstations und einem Server gefordert.

Bei der Beurteilung der Lösungen verzichtet FACTS bewusst auf die Überprüfung der Scanleistung in Bezug auf Erkennungsgeschwindigkeit und Anzahl der aufzufindenden Schadprogramme. Die Erklärung: Die größte Problematik bei Virentests ist ein fehlender Industriestandard bei der Erkennungsrate von Angriffen. Es fehlt die Definition eines schadhafte Programms und somit ist nicht geklärt, wann ein Programm wirklich darauf ausgerichtet ist, einen Schaden im System anzurichten. Das erklärt auch, dass in großen Vergleichstests die Ergebnisse mit 85 bis 98 Prozent relativ dicht beieinanderliegen. Für Unternehmen stehen ganzheitliche Lösungen im Vordergrund, die aufgrund ihrer Komplexität in Bezug auf Angriffsszenarien flexiblen Schutz bieten müssen – dazu zählen nicht nur wie eingehend erwähnt Computerviren.

OPEN SPACE SECURITY

Unter dem Namen „Open Space Security“ bietet der russische Hersteller Kaspersky Lab eine Kombination aus Schutzlösungen für sämtliche Knotenpunkte und Plattformen eines Netzwerks. Während die Einstiegsvariante „Work Space Security“ lediglich Windows- und Linux-Workstations schützt, sichert die „Business Space Security“ das gesamte Netzwerk, bestehend aus Workstations, Datei- und Mail-Servern, Groupware-Servern und mobilen Geräten. Letztere schließen sogar Smartphones und PDAs ein.

Für Administratoren bietet der Hersteller ein kostenloses „Administration Kit“ an. Hierarchische Administrationsstrukturen werden ebenso unterstützt wie die MySQL-Datenbank. Kaspersky betont den schonenden Umgang seiner Software mit Ressourcen. ➤

► Praktisch: Bei Mehrkernsystemen können Administratoren festlegen, dass nur ein Prozessor von den Kaspersky-Produkten belastet werden soll. Komfortabel ist auch die Einbeziehung von Microsofts „Active Directory“. Meldet sich ein neuer Client im Netzwerk an, werden automatisch zuvor konfigurierte Kaspersky-Softwarepakete auf dem Rechner installiert.

Optisch und vom Funktionsumfang ähnelt die zentral verwaltbare Business-Lösung auf den einzelnen Clients stark der Consumer-Variante. Alle bekannten Schutzkomponenten wie Web-Anti-Virus, proaktiver Schutz vor Rootkits, Firewall, Anti-Spyware, Anti-Spam und Anti-Phishing gehören zur Grundausstattung.

TOTAL PROTECTION

McAfee Total Protection for Endpoint blockiert neben Viren auch Malware, Rootkits, Spyware, Exploits, Bots, Spam und Hackerangriffe. McAfee Total Protection for Endpoint vereint bewährte McAfee-Technologie, hochaktuelle Gefahrenforschung durch die McAfee Avert Labs und skalierbares Management über eine einzelne zentrale Konsole.

Mit leistungsstarkem Schutz vor Bedrohungen für Server, E-Mail-Server und Desktop-Rechner ist die Lösung für alle Notfälle gerüstet. On-Access-Scannen hindert Spyware und anderen schädlichen Code daran, sich auf die einzelnen Workstations im Unternehmen zu verbreiten. Automatische Updates von Bedrohungssignaturen schirmen zudem von Zero-Day-Angriffen ab. Der hoch entwickelte Schutz vor Rootkits erkennt tief verborgene Rootkits und schaltet sie aus, ehe Hacker sie für bösartige Zwecke einsetzen können.

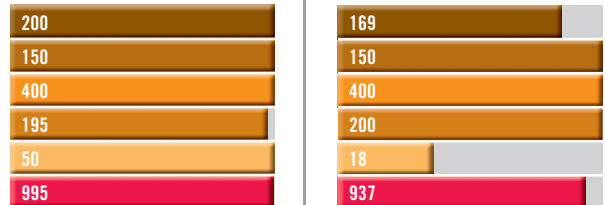
Administratoren steuern alles zentral über McAfee ePolicy Orchestrator (EPO). McAfee ePO ist eine zentrale, webbasierte Konsole zur Verwaltung von Sicherheit und zur Durchsetzung von Schutzrichtlinien. ePO bietet eine effektive und kostengünstige Verwaltung der Systemsicherheit, einschließlich grafischer Berichte, mit denen Administratoren ►



Anbieter	Kaspersky	McAfee
Hersteller	Kaspersky Labs GmbH	McAfee GmbH
Produktbezeichnung	Kaspersky Business Space Security	McAfee Total Protection for Endpoint
Preis	818,- € pro Jahr	2.262,- € pro Jahr
Anzahl der Lizenzen	25 Nodes (Clients und Server)	25 Clients + 1 Server
Lizenzierungsmodell	Lizenzierung 1–3 Jahre, nach Nodes	Lizenz 1 Jahr inkl. 1 Jahr Gold Software Support
Kosten für Update	während der Lizenzdauer kostenlos	während der Lizenzdauer kostenlos
Ausstattungsmerkmale		
Unterstützte Betriebssysteme	MS Win 2000+Server/XP/2003 Server/Vista/Win 7/2008 Server, RHEL, Fedora, SLE, openSuSE	MS Win NT/2000/XP/Vista
Zertifizierungen	Citrix, Windows Server 2008, Windows 7	nein
Schutz für Workstations · Server · Mobile Geräte	ja · ja · ja	ja · ja · ja
Virenschutz in Echtzeit	ja	ja
Virenerkennung in Packern	ja	ja
Enthaltene Firewall-Lösung	ja	ja
Scheduler	ja	ja
Boot-Disk	ja	nein
Virendatenbank	ja	ja
Prüfungen		
E-Mail (pop3)	ja	ja
Phishingschutz	ja	ja
Webdownloads	ja	ja
Scriptblocking	ja	ja
Administration		
Zentrale Installation	ja	ja
Skalierbarkeit Netzwerk	ja	ja
Skalierbarkeit Bedienungsfläche	ja	ja
Fernwartung	ja	ja
Bedienoberfläche u. Benutzerfreundlichkeit	intuitiv zu bedienen	intuitiv zu bedienen
Berichtssystem	ja, grafisch	ja, grafisch
Support		
Online Update	ja	ja
Automatische Updates	ja	ja
Updatefrequenz	1 x pro Std.	in Echtzeit - sofort
Virenmitteilungen an Labore	ja	ja
Handbücher	ja	ja
Hotline	deutscher telefonischer Support	deutscher telefonischer Support
Kosten für Hotline	normale Telefongebühren	normale Telefongebühren

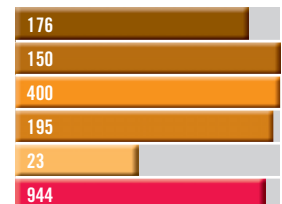
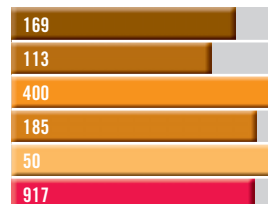
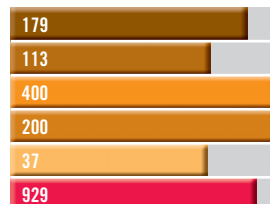
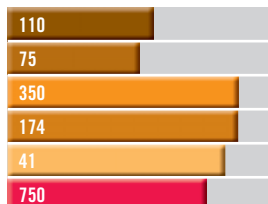
GESAMTWERTUNG: Insgesamt können 1.000 Punkte erreicht werden: 200 Punkte bei der Ausstattung, 150 Punkte bei der Prüfung, 400 Punkte bei der Anwendernutzung, 200 Punkte beim Support und 50 Punkte beim Preis.

AUSSTATTUNG: max. 200 Punkte
 PRÜFUNG: max. 150 Punkte
 ANWENDERNUTZUNG: max. 400 Punkte
 SUPPORT: max. 200 Punkte
 PREIS: max. 50 Punkte
GESAMT: max. 1.000 Punkte





Norman	Sophos	Symantec	Trend Micro
Norman	Sophos GmbH	Symantec GmbH	Trend Micro Deutschland GmbH
Norman Endpoint Protection	Sophos Computer Security SBE 4	Endpoint Protection Small Business Edition	Worry Free Business Security Advanced
999,- € pro Jahr	1.098,50 (1 Jahr) Listenpreis	810,- € pro Jahr	1.725,- € pro Jahr (bei 25 Clients + 1 Server)
25 Clients + 1 Server	25 Clients + 1 Server	25 Clients + 1 Server	25 Clients + 1 Server
Lizenzierung 1–3 Jahre	Lizenzierung 1–5 Jahre	Lizenzierung 1 Jahr, verlängerbar	Lizenzierung 1 Jahr, verlängerbar
während der Lizenzdauer kostenlos	während der Lizenzdauer kostenlos	während der Lizenzdauer kostenlos	während der Lizenzdauer kostenlos
MS Win 2000+Server/XP/Server 2003/ Vista/Server 2008/Windows 7	MS 2000/XP/Vista/7/2008(SBS/R2, Core), Mac OS X (10.4/10.5/10.6)	Windows ab 2000 (inklusive Windows 7)	MS Win 2000+Server/XP/Server 2003/Vista/Home Server/Server 2008, Client/Server Security Agent unterstützt Citrix, WFBS-A unterstützt Vmware
VB 100 / TÜV geprüfter Virenschutz/ ICSA certified	Windows-Zertifizierungen, MAC-Zertifizierung,, TÜV Zertifizierung, vb100, westcoast labs, icsa labs	nein	Windows 7
ja · ja · nein	ja · ja · Option	ja · ja · ja	ja · ja · ja
ja	ja	ja	ja
ja	ja	ja	ja
nein	ja	ja	ja
ja	ja	ja	ja
nein	ja	nein	nein
ja	ja	ja	ja
ja	Option	ja	ja
nein	Option	nein	ja
nein	ja	ja	ja
ja	ja	ja	ja, über Verhaltensüberwachung
ja	ja	ja	ja
ja	ja	ja	ja
nein	ja	ja	ja
ja	ja	ja	ja
intuitiv zu bedienen	intuitiv zu bedienen	intuitiv zu bedienen	intuitiv zu bedienen
ja, grafisch	ja, grafisch	ja, grafisch	ja, grafisch
ja	ja	ja	ja
ja	ja	ja	ja
1 x pro Tag	alle 5 Min.	1 – 3 mal täglich	1 x pro Tag
nein	ja	ja	ja
ja	ja	ja	ja
deutscher telefonischer Support	deutscher telefonischer Support	deutscher telefonischer Support	deutscher telefonischer Support
normale Telefongebühren	normale Telefongebühren	normale Telefongebühren	kostenfrei



› ständig über die aktuelle Sicherheitsleistung informiert werden. Wenn sich Richtlinien aufgrund von sich ändernden Bedrohungen und Bestimmungen ändern, kann eine Aktualisierung schnell, präzise und lückenlos erfolgen.

NORMAN PROTECTION

Die Lösung Norman Endpoint Protection besteht aus einem Client-Modul Endpoint Protection und der Management-Konsole Endpoint Manager. Das Management-Modul ermöglicht die Konfiguration und das Management bestehender Antimalware-Produkte von Norman und ist für die Einbindung künftiger Norman-Produkte vorbereitet.

Der Endpoint Manager identifiziert im Unternehmensnetzwerk alle IP-gestützten Clients und ordnet sie anhand ihrer IP-Adresse zuvor definierten Gruppen automatisch zu. Die Client-Suche erfolgt wahlweise aktiv in definierten IP-Adressen-Bereichen oder aber passiv. Der Systemverantwortliche kann alle Clients gruppieren und Policies gruppenspezifisch festlegen und konfigurieren.

Die Clients werden über das zentrale Policy Management konfiguriert und bei der Verteilung von Software und der Aktualisierung

von Signaturdateien berücksichtigt. Eine Sicherungskopie der Konsolenkonfiguration erspart Administratoren bei Hardware Schäden den Aufwand bei der Wiederherstellung aller Parameter. Ein Benachrichtigungstool hält die EDV-Abteilung per E-Mail, SMS oder anderen Formaten über Warnungen und Vorkommnisse auf dem Laufenden. Auch Reportfunktionen sind in der Lösung enthalten. Eine übersichtliche Benutzeroberfläche und eine intelligente Menüführung runden die neugestaltete Konsole ab.

SOPHOS SECURITY

Mit Sophos SBS Computer Security haben Unternehmen Rundumlösung inklusive Client-Firewall. Die Sophos Client Firewall sperrt Computer proaktiv und schützt so vor Internet-Würmern, Hackern und dem Risiko ungeschützter Computer, die sich mit dem Netzwerk verbinden und eine Infektion verursachen können.

Natürlich bietet die Lösung zuverlässigen Schutz vor Viren, Spyware und Adware. Die Software bietet Viren- und Firewall-Schutz für die Büro-PCs, Notebooks, File-Server und klinkt sich auch als Sicherheitssystem auf Microsoft Exchange ein. Auf dem Exchange-Server sor-

tiert Sophos auch gleich Spam-Mails aus. Dabei werden alle eingehenden, ausgehenden und internen Mails analysiert. Durch die sogenannte Decision-Caching-Technik prüft Sophos nur Dateien, die seit dem letzten Check geändert wurden, und spart so Ressourcen.

Die Integrated Behavioral Genotype Protection erkennt verdächtige Programmcodes und blockiert sie noch vor der Ausführung. Zudem bietet Sophos SBS Computer Security die Vorteile eines Host-Intrusion-Prevention-Systems (HIPS), ohne dass eine separate Lösung installiert werden muss.

Zentrales Bedienelement ist das Control Center, mit dem Administratoren die Installation, Konfiguration und Updates auf allen Systemen steuern. Die benötigten Updates kommen im Ernstfall auch stündlich und werden ohne Eingreifen des Benutzers auf den PCs und Servern eingespielt. Das Sophos Control Center bietet sofortigen Überblick über den Status jedes Windows- und Mac-Computers, fasst Bedrohungen auf einen Blick zusammen und stellt wichtige Tasks übersichtlich auf dem Dashboard dar. Die Bereinigung infizierter Computer können Administratoren zentral über das Sophos Control Center vornehmen.

SYMANTEC PROTECTION

Symantec Endpoint Protection Small Business Edition bietet weitestgehenden unternehmensweiten Schutz. Die Lösung sorgt für die nahtlose Integration erstklassiger Sicherheitstechnologien durch Virenschutz, Spyware-Schutz, Desktop-Firewall und Intrusion Prevention. Alle Sicherheitsmodule sind in einem einzigen Agenten untergebracht.

Somit sorgt die Symantec Endpoint Protection Small Business Edition für proaktiven, umfassenden Schutz vor bekannten und neuen Bedrohungen. Die Lösung analysiert automatisch das Verhalten von Anwendungen und die Netzwerkkommunikation, um verdächtige Aktivitäten zu erkennen und zu blockieren. Administratoren können gezielt Aktionen von Anwendungen und Endgeräten kontrollieren und nach eigener Risikoeinstufung Blockaden errichten.

Die Lösung enthält von Symantec empfohlene Sicherheitseinstellungen, sodass in erster Linie keine zusätzlichen Konfigurationen erforderlich sind. Integrierte Tools wie der Assis-



TESTSIEGER

Nur Software, die in den Kategorien Ausstattung, Support und Anwendernutzen allerbeste Leistungen zeigt, erhält das FACTS-Urteil „sehr gut“.

tent für die Client-Installation vereinfachen die Verteilung der Software auf Client-Computern und halten etwaige Installations- und Implementierungsschulungen auf einem niedrigen Niveau.

WORRY FREE

Trend Micro Worry-Free Business Security Advanced schützt Microsoft-Exchange- und Small-Business-Server, Microsoft-Windows-Server, PCs und Laptops. Die Sicherheitslösung entdeckt und entfernt klassische Bedrohungen wie Viren, Spyware, Rootkits und Bots. Zudem wird die Sicherheit von bestehenden Wi-Fi-Verbindungen geprüft und sperrt bei Bedarf den Zugriff auf ausgewählte Dateien und Ordner sowie den Zugriff auf gefährliche Websites.

Zusätzlich bietet die Lösung mit InterScan Messaging Hosted Security zuverlässigen Schutz zur Abwehr von Spam und Phishing-Angriffen. Dazu werden IP-Adressen mit der stets aktuellen Trend-Micro-Datenbank bekannter Spam-Quellen abgeglichen und dadurch Spam vor der Ankunft am Exchange-Server gestoppt. Die Spam-Abwehr auf dem Microsoft-Exchange-Server sorgt dafür, dass Netzwerkressourcen wieder für geschäftliche Zwecke zur Verfügung stehen und nicht für die Bearbeitung von Spam verloren gehen.

Frank Becker ■

Platz 1: Kaspersky Labs GmbH	995 Punkte = sehr gut
Platz 2: Trend Micro GmbH	944 Punkte = gut
Platz 3: McAfee GmbH	937 Punkte = gut
Platz 4: Sophos GmbH	929 Punkte = befriedigend
Platz 5: Symantec GmbH	917 Punkte = befriedigend
Platz 6: Norman	750 Punkte = ausreichend

