IT-ADMINISTRATOR.DE

02/2011

iT administrator

Das Magazin für professionelle System- und Netzwerkadministration

Im Test:

Sechs Antivirus-Suiten

Wettstreit der Schädlingsbekämpfer

Sonderdruck für AVG

Jakobsoftware – Authorized Distributor

4 196583 212605 02

Im Vergleichstest: Sechs Antivirus-Suiten

Wettstreit der Schädlingsbekämpfer

von Thomas Bär und Hendrik Pilz

Quelle: Ioannis Kounadeas - Fotolia.com

Ohne einen Virenschutz kommt kein Unternehmen aus – angesichts der geschätzten 40 Millionen digitaler Schädlinge. Zu groß ist das Risiko, das von bösartigen Programmen ausgeht. Während Antiviren-Lösungen für den heimischen Privat-PC mit vielen Zusatzfunktionen wie einer verbesserten Firewall oder einem Anti-Spam-Filter aufgewertet werden, sind solche All-in-one-Suiten im Unternehmensumfeld nicht immer erwünscht. Hier zählen andere Werte, allen voran die zentrale Administrierbarkeit. In unserem Vergleichstest betrachten wir sechs professionelle Antiviren-Lösungen.

Für Antiviren-Software im Unternehmensumfeld bedarf es hauptsächlich einer zentralen Management-Lösung, die möglichst automatisiert die AV-Signaturen und Programmaktualisierungen an die Client-Systeme verteilt. Weiter findet sich auf der Wunschliste der Administratoren die zentrale Übersicht über alle Client- und Serversysteme. Für unseren Test haben wir daher die nach einer Marktanalyse [1] des IT-Dienstleisters OPSWAT sechs gebräuchlichsten Antivirus-Suiten unter die Lupe genommen, die sich an KMUs richten und die nötigen Administrationsfunktionen bieten: AVG Internet Security Business Edition 2011, Avira AntiVir Professional, ESET Smart Security 4 Business Edition, G Data AntiVirus Enterprise 10, Kaspersky Anti-Virus 6.0 für Windows Workstation und McAfee Total Protection for Endpoint.

In Bezug auf die Management-Funktionen installierten wir die AV-Lösungen auf einem aktuellen Windows Server 2008 R2 in der x64-Ausprägung. Nach der Installation wurde die AV-Client-Software auf einen Windows XP x86- und Windows 7 x64-Client verteilt. Die Management-Software musste Client-Computer, die in einer Windows-AD-Domäne verwaltet werden, direkt auffinden können. Ein zweiter Test besteht darin, einen Windows XP-Rechner außerhalb der Domänenstruktur mit einem AV-Client per "Push"-Kommando auszustatten. Allen Lösungen ist die verschlüsselte Kommunikation zwischen Management-Konsole und den Clients gemein.

Mehrstufiges Testverfahren

Das Testverfahren für die Erkennung und Performance-Messung führte das Magdeburger Institut AV-Test [2] durch. Alle Tests wurden auf einem typischen Rechner unter Windows XP Professional 32 Bit in vier Rubriken durchgeführt. Die erste Rubrik namens "Webseiten-Attacken" simuliert den direkten Zugriff auf 13 infizierte Webseiten. Diese Webseiten sind zwar nicht unbedingt repräsentativ im statistischen Sinne, jedoch sehr typisch für Gefährdungen, der sich ein Internet-Surfer im Unternehmen im "Vorbeiklicken" aussetzt. Das Blockieren der Schädlinge auf diesen Seiten trennte im Test die Spreu vom Weizen – in keiner anderen Rubrik waren die Unterschiede in der Leistungsfähigkeit größer.

Die zweite Testrubrik bestand aus mehr als 200.000 aktuellen Viren, Würmern und Trojanern aus den verschiedenen Gattungen. Dieser als "Zoo Malware-Erkennung" bezeichnete Test zeigt, wie effektiv die Programmierer einer AV-Software ihre Lösung auf den Praxiseinsatz trimmen konnten. Da es auch in dieser Kategorie zu nennenswerten Unterschieden kam, sei darauf hingewiesen, dass jede AV-Lösung in ihrer vom Hersteller gewählten Standardeinstellung ans Werk ging. Verfügt die AV-Lösung bei-

spielsweise über die Technik zum Versand von verdächtigen Elementen an spezielle, im Internet gehostete Server, so durfte die AV-Software dies auch in der Teststellung nutzen, um das Ergebnis zu optimieren. Der Trend der AV-Hersteller hin zu einer verstärkten Nutzung der "Cloud-Technologie" ist unübersehbar. Dies hat Auswirkungen auf die Parametrierung. Administratoren sollten künftig davon ausgehen, dass Antivirenserver viel häufiger größere Datenmengen mit dem Internet austauschen.

Rubrik 3, die so genannte "Wildlist" [3], lieferte für alle sechs Testkandidaten ein absolut identisches Ergebnis. Alle 5.084 Schädlinge – sowohl einmal per On-Demand-Scanner als auch einmal mit dem On-Access Virenwächter geprüft – wurden von jeder Lösung zu 100 Prozent erkannt. Dass ausgerechnet dieser Test ein so phantastisches Ergebnis erfährt, erklärt sich dadurch, dass Schädlinge, die auf der "offiziellen Wildlist" stehen, von allen Herstellern garantiert erkannt werden, da sie die notwendige Datenquelle gemeinschaftlich mit Informationen füttern. Somit ist beinahe ausgeschlossen, dass eine professionelle AV-Lösung diese digitalen Plagegeister nicht entdeckt. Bedingt durch das einheitlich gute Ergebnis in dieser eher unrealistischen Disziplin verzichteten wir darauf, diese Ergebnisse in die Kalkulation der Leistung einzubeziehen.

Die vierte Testrubrik widmet sich dem Thema der Performance. Es liegt auf der Hand, dass eine Schutzsoftware, die alle Dateien und Prozesse genau überwacht, dafür Zeit benötigt. Im Performance-Test wird die zeitliche Auswirkung in verschiedenen Verfahren geprüft. Dabei wurden typische Vorgänge eines Benutzers wie PC starten, Word öffnen, Dateien bearbeiten oder Webseitenzugriffe gemessen. Während einige Testbereiche nur minimale Verzögerungen beim Einsatz einer AV-Lösung offenlegten, kam es in anderen Tests zu teilweise dramatischen Verlangsamungen.

AVG Internet Security Business Edition 2011

AVG besteht als Unternehmen bereits seit 1991 und hat sich auf Sicherheitssoftware spezialisiert. Gänzlich neu im Funktionsumfang ist die "Protective Cloud-Technologie". Diese Technologie nutzt gleichzeitig verschiedene Scan-Engines und Verhaltenserkennung, um aufkommende und bisher unbekannte Bedrohungen zu identifizieren. Nachdem eine Bedrohung erkannt wurde, will der Hersteller zeitnah Abwehrmittel entwickeln und die AVG-Clients aktualisieren. Neben dem Abgleich mit der Internetdatenbank als "Cloud-Computing"-Technik bietet die Software die bekannten Suchmethoden über Signaturen, Heuristiken sowie Generiken und wertet das Verhalten von Programmen aus. Somit ist ein Schutz vor Schadsoftware auch dann gewährleistet, wenn Rechner keinen Zugriff auf das Internet haben.

Für den Unternehmenseinsatz bietet der Hersteller zwei Editionen. Die "AVG Anti-Virus Business Edition" bietet den Virenschutz auf Workstations und Fileservern und ist somit eine klassische Antivirensoftware. Die aktuelle "Internet Security Business Edition" bietet darüber hinaus Spam-Schutz für E-Mail-Clients und eine zentral zu verwaltende Firewall. AVG beschränkt sich bei der Produktunterstützung auf aktuelle Windows-Versionen. Zwar bietet AVG kostenfreie AV-Lösungen für Mac OS und Linux an, beide sind jedoch nicht für ein zentrales Management geeignet.

Die Installation der Server-Software ist sehr einfach. Nach einem Doppelklick auf den Installer ist lediglich die Eingabe einer Lizenznummer notwendig. AVG bietet, wie viele andere Hersteller auch, nunmehr eine Erweiterung für den Browser in Form einer "Security Bar" an. Bisher waren in erster Linie kostenlose Programme durch diese mehr oder minder sinnvolle Erweiterungen aufgefallen. Gemäß der guten Gepflogenheit, auf Server so wenig Software wie notwendig einzuspielen, verzichteten wir auf dieses Add-On. Die komplette Installation des 178 MByte großen Installers dauerte auf dem Testsystem keine

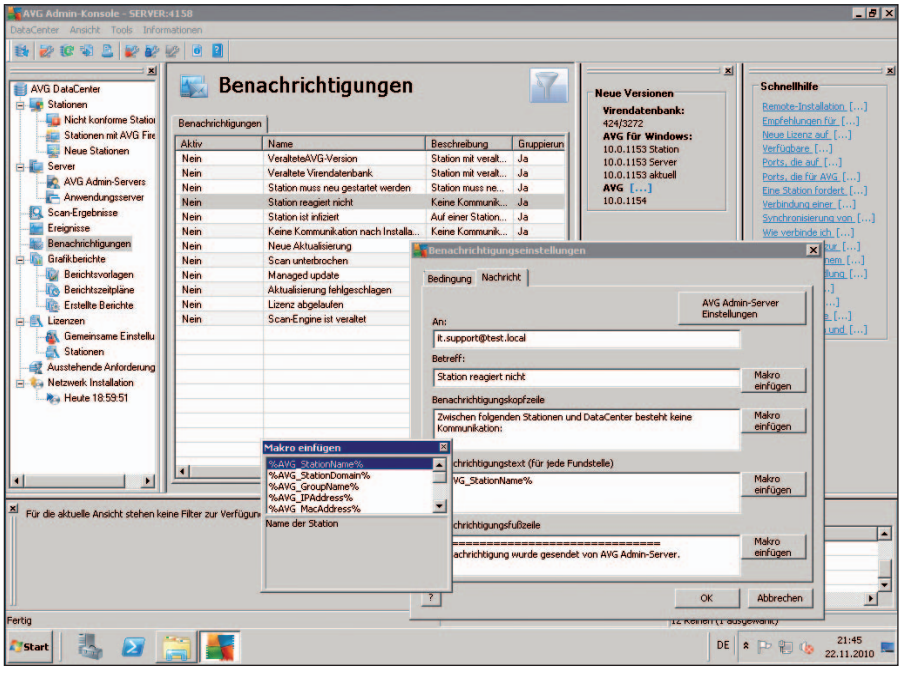

Bild 2: Wie Administratoren über Missstände informiert werden, ist bei AVG sehr genau steuerbar

Links

[1] Marktanalyse OPSWAT
B2T21

[2] AV-Test.org
B2T22

[3] Wildlist
B2T23

zwei Minuten. Direkt nach der Einrichtung versorgte sich die Software automatisch mit aktuellen AV-Pattern.

Um mit der AVG-Lösung zentral Clients zu verwalten, ist die Installation der Remote Administration Console (RAC) erforderlich. Der Admin-Server-Implementierungsassistent unterstützt den Administrator bei der Einrichtung der beiden zur Verfügung stehenden Serverdienste. In der Testinstallation wählten wir sowohl die "DataCenter-Rolle" als zentrale Management-Oberfläche als auch die "UpdateProxy-Rolle", die Client-Computer mit Updates und AV-Pattern ausstattet. Die Rolle als Datacenter benötigt für den Betrieb eine Datenbank. Zur Auswahl stehen Firebird, Microsoft SQL und SQL Express, Oracle 10g oder 11g oder MySQL 5. Die Firebird-Datenbank für rund 150 Clients wird vom Assistenten auf Wunsch des Administrators automatisch eingerichtet. Der folgende Schritt des Assistenten führt den Administrator zur Übernahme von Client-Informationen. Ist bereits eine Installation vorhanden, so können aus einem Backup alle Informationen ausgelesen werden. Eine Verknüpfung zu einem Active Directory steht als weitere Option zur Verfügung.

Im Test verlief die Verteilung der Client-Software ohne Schwierigkeiten. PCs, die in der Domäne organisiert sind, lassen sich durch den Administrator über das aus Windows bekannte Domänenfenster suchen und für die Verteilung auswählen. Eine Gruppierung der Computer und Server über die Management-Konsole ist ebenfalls problemlos möglich. Eine Einteilung von Computern in Gruppen ist in jedem Unternehmen wichtig, in dem der Virenschutz oder andere Sicherheitsregeln feiner eingestellt werden sollen. Besonders einfach hat AVG die Aktualisierung der Installationspakete realisiert. Durch einen einzigen Mausklick lädt die Software aus dem Programmfenster heraus die neueste Version herunter. Um Details wie x64- oder x86-Version muss sich der Administrator dabei nicht kümmern – das übernimmt die Software automatisch. Ebenfalls für den Administrator sehr angenehm umgesetzt sind die Benachrichtigungsfunktionen. Die typischen zwölf Ereignisse, darunter "Station infiziert", "Scan unterbrochen" oder "Veraltete Virendatenbank", stehen zur Auswahl, um E-Mail-Benachrichtigungen an den IT-Support zu versenden. Je nach Ereignisart können verschiedene Werte eingestellt werden, bei deren Erreichen oder Unterschreiten die Nachricht versendet wird.

Fazit

Die AVG-Lösung lieferte im Test ein sehr gutes Ergebnis ab. Die 13 infizierten Webseiten wurden allesamt blockiert, ehe es zu einem Schaden auf dem Computer kommen konnte. 96,65 Prozent aller getesteten Schädlinge wurden erkannt und vernichtet. Das ist im Vergleich zur Konkurrenz ein insgesamt überzeugendes Ergebnis. Die Performance-Auswirkungen durch die Software liegen in einem vertretbaren Bereich. Lediglich das Kopieren lokaler Dateien verlangsamt sich um die Hälfte und die Berechnung von MD5-Hashes für eine Auswahl von Dateien ist um 77 Prozent langsamer als ohne den Schutz. Insgesamt handelt es sich bei AVG um eine gut gelungene und ausgewogene Antivirus-Software.

Hersteller
AVG
www.avg.com/de-de/

Preis
Für 100 Windows-Clients, Server, inklusive Mailserver mit 120 Mailboxen kostet AVG AV Business Bundle 1.929,87 Euro sowie AVG ESE für 120 Mailboxen 2.043,70 Euro.

Technische Daten
www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator *(max. 10 Punkte)*

Erkennungsrate Web-Attacken	10
Erkennungsrate Malware	8
Handhabung / Management	9
Installation und Client-Unterstützung	8
Leistung	7
Gesamtbewertung	**8,4**

AVG Internet Security Business 10.0.1153