Mit DVD 4,99 €

PC Professionell

www.pc-professionell.de

Das Testmagazin

Vollversionen Gratis auf DVD

180 Top-Too
Open Source

Datei-Manager
für Profis

im Griff*

Private Daten
verschlüsseln*

Schnell zum
eigenen Shop*

Plus: 3 Toolpacks
Foto · Kopieren · Security

*kostenlose Online-Registrierung erforderlich

08/06 Österreich € 5,75 / Schweiz CHF 10,00 / Luxemburg € 5,90 €4,99

Vista Power-Tools

Tipps: Neue Profi-Funktionen für Windows S.26

Kopieren erlaubt!

Sie dürfen **mehr kopieren**, als Sie denken!

Brennen und Rippen: 20 legale Top-Tools auf DVD

Verboten gut: Die neuen Tri… …racker S.82

…CPU
…om S.92

…ns
…Tools & 1500 Plug-ins S.64

SONDERDRUCK

KASPERSKY lab

PC Professionell Empfehlung der Redaktion

Kaspersky Internet Security 6.0

Windows-Lauschangriff?

Aufgedeckt: XP sendet geheime Daten S.36

Epson-Drucker-Skandal

Gefahr: Totalschaden trotz Original-Tinte S.112

Security-Suiten im Härtetest S.132

Neue Fritzbox-Tricks für alle S.158

Windows-Tipp: Schnellstart S.152

16 CPU-Kühler im Stresstest S.130

4 196209 004997 08

Rundum virensicher

Security-Suiten sind beliebte All-Inclusive-Sicherheitslösungen. Welche der Pakete wirklich gegen Hacker, Spammer, Phisher und Virenschreiber helfen, testet PC Professionell in einem Mega-Test mit drei Etappen.

RÜDIGER PEIN

In diesem Artikel

Security-Suiten im Malware-Test
So gut schützen Sicherheitspakete gegen Viren und Spyware **133**

Darauf müssen Sie achten
90 Prozent Erkennungsrate sind auch für Heim-PCs viel zu wenig **135**

Virus mit tausend Gesichtern
So bringt ein polymorpher Virus Scan-Engines aus dem Tritt **136**

Sicherheitspaket auf Heft-CD/DVD
PCpro-Sicherheitspaket gegen Viren, Spyware und Rootkits auf Heft-CD (PCP-Code: AVTOOLS)

Virenscanner, Firewall sowie ein Filter gegen Spam- und Phishing-Mails, dazu ein Anti-Spyware-Programm und ein Rootkit-Detektor: Den Gefahren aus dem Internet begegnen Privatanwender wie Firmen mit unterschiedlichsten Programmen, die alle auf dem aktuellen Stand gehalten werden wollen. Internet-Security-Suiten vereinen all diese Tools unter einer Oberfläche und locken zudem mit einem Rabatt gegenüber dem Einzelkauf. Weiterer Vorteil: Der Kunde hat in Sicherheitsfragen nur noch einen Hersteller als Ansprechpartner.

Doch gibt es ein Sicherheitspaket, das in jeder Disziplin top ist? Um dies zu überprüfen, treten im PCpro-Test zehn Security-Suiten über mehrere Monate hinweg in drei verschiedenen Disziplinen gegeneinander an. Aktuell in dieser Ausgabe müssen sie ihre Fähigkeiten bei der Bekämpfung von Viren, Würmern, Trojanern und Spyware unter Beweis stellen. In der PCpro 9/2006 folgt ein Test der Antispam-Module. Abschließend werden in Ausgabe 10/2006 die Firewalls der Pakete unter die Lupe genommen.

Im Test: 10 Rundumschutz-Pakete

Am Vergleichstest nehmen zehn Einzelplatzversionen deutschsprachiger Security-Suiten teil. Diese müssen zumindest die Module Antivirus, Antispyware, Antispam sowie eine Firewall unter einer gemeinsamen Oberfläche anbieten. Nicht im Test sind Programmsammlungen ohne einheitliches zentrales Benutzermenü. Ebenso nicht mit dabei sind Suiten, die lediglich ältere Versionen der getesteten Programme unter einer neuen Oberfläche verstecken: Data Becker Internet Security Suite 2006 sowie Bullguard Internet Security bedienen sich der Bitdefender-Engine, Steganos Internet Security 2006 enthält eine ältere Kaspersky-Suite.

Bereits beim ersten Testparcours, der Abwehr von Viren und Spyware, trennt sich die Spreu vom Weizen. Das schlechte Abschneiden der Zonealarm Internet Security Suite 2006 zeigt dabei, dass ein guter Name als Firewall-Anbieter nicht gleichzeitig für ein gutes Antivirenmodul bürgt. Das Spitzentrio Kaspersky, G Data und F-Secure überzeugt in der ersten Disziplin, hat aber noch zwei weitere vor sich. So bleibt es spannend, wer am Ende als Sieger aus dem Wettbewerb hervorgeht und rundum schützt. *RPE*

Virenbekämpfer im Detail

Erkennung, Desinfektion und Prophylaxe: Neben diesen Grunddisziplinen sind bei Virenscannern auch Selbstschutz und eine übersichtliche Bedienung nötig.

Ein geschickt programmierter Wurm kann sich binnen Minuten über den gesamten Erdball verbreiten. Die Antivirenhersteller reagieren dann schnell mit Signaturupdates. Doch schnell ist nicht immer schnell genug, wie die PCpro-Tests zeigen.

Zwei bis 18 Stunden für Updates

Die Messungen der Reaktionszeiten von Januar bis Mai 2006 zeigen deutliche Unterschiede: G Data und Kaspersky versorgen den User im Durchschnitt in weniger als 2 Stunden nach einem Ausbruch mit den entsprechenden Signaturen – das ist top. Softwin Bitdefender und F-Secure schaffen dies immerhin in 2 bis 4, Panda in 4 bis 6 Stunden. Mit 8 bis 10 Stunden deutlich zu lange Zeit lassen sich McAfee, Symantec sowie Trend Micro. Bei CA und Zonelabs muss sich der Anwender gar 16 bis 18 Stunden lang gedulden – das ist zu langsam.

Die Praxis zeigt jedoch: Weitaus gefährlicher als eine globale Epidemie sind lokal begrenzte Trojaner-Attacken. Durch die Beschränkung auf wenige Opfer – Mitarbeiter einer Firma oder Kunden eines kleinen Bankhauses – bleiben solche Infektionen oft lange unerkannt. Aktuelles Beispiel ist der Schädling Ginwui, der in einer japanischen Firma als DOC-Datei über eine Sicherheitslücke von Microsoft Word auf den Rechner gelangte und dort eine Backdoor installierte. Ein Schwerpunkt in der Testwertung bilden daher Verfahren zum Aufspüren neuer Viren.

Kaspersky liefert ein gutes Handbuch, McAfee viel Luft in der Schachtel

Signaturbasierte Virenerkennung

Vor der Kür prüft PCpro aber noch das kleine Einmaleins der Virenscanner ab: die signaturbasierte Erkennung bekannter Malware. Einige Produkte werben auf ihren Schachteln mit einem Logo für hundertprozentige Erkennungsraten. Dieses bezieht sich jedoch ausschließlich auf die so genannten In-The-Wild-Viren (ITW), die von mehreren Virenforschern in freier Wildbahn gesichtet wurden. Eine Liste jener Parasiten veröffentlicht regelmäßig die Wildlist Organization *(www.wildlist.org)*. Zudem erhalten Antivirenhersteller und einige unabhängige Experten die offiziellen ITW-Samples. Beim ITW-Test sind den Kandidaten also die »Fragen« vorab sehr genau bekannt.

ITW-Viren: Erkennung ist Pflicht

Das Testergebnis von PC Professionell fällt daher wenig überraschend aus: Alle Suiten erkennen die offiziellen ITW-Samples zu 100 Prozent – sowohl mit dem On-Demand-Scanner als auch mit dem On-Access-Wächter. Extrapunkte gibt es dafür nicht; wer hier patzt, fliegt aus dem Mega-Test.

Am Beispiel des polymorphen Computervirus Polip (Infos im Kasten »Polip(os) – Die polymorphe Gefahr« auf Seite 136) sieht man deutlich, dass fehlerlose ITW-Erkennung allein kein Gütesiegel darstellt: Mitte März entdeckt und bereits Ende April sehr häufig in Tauschbörsen anzutreffen, wurde der Virus bis Redaktionsschluss dennoch nicht in die Wildlist aufgenommen. Wäre dies passiert, hätten die getesteten Security-Suiten von Computer Associates (CA), Panda, Trend Micro und Zonelabs die 100-Prozent-Marke bei den ITW-Viren verfehlt: Sie haben zum Testzeitpunkt noch Probleme bei der Erkennung aller Polip-Samples. Erst seit Mitte Mai haben alle getesteten Hersteller diese Probleme im Griff. So aber hinkt die Wildlist der aktuellen Virenausbreitung hinterher. Hersteller, die sich auf die ITW-Viren konzentrieren und den Rest vernachlässigen, erhalten so trotzdem ein 100-Prozent-Logo.

Testcocktail aus über 120 000 Viren

Interessanter wird es dann schon beim Aufspüren von Schadprogrammen, die zwar öffentlich kursieren, aber nicht in der Wildlist aufgeführt sind. Erste Prüfung ist ein Testset aus über 120 000 Samples, allen voran Datei- und Makroviren. Mit hervorragenden Erkennungsraten von 99,98 beziehungsweise 99,97 Prozent glänzen in dieser Disziplin die Suiten von G Data, F-Secure, Kaspersky, McAfee und Symantec. Erst mit deutlichem Abstand folgen CA und Trend Micro (jeweils 99,4 Prozent) sowie Panda (99,3 Prozent). Softwin Bitdefender schafft es gar nur auf 98,0 Prozent: Ausgerechnet bei den 32-Bit-Windows-Viren übersieht die Software über 5 Prozent der Samples. Völlig indiskutabel ist das Abschneiden der Zonealarm Security Suite, die im Test nur knapp 43 Prozent der Dateiviren entdeckt und so 69,6 Prozentpunkte bei der Virenerkennung einheimst.

Selbst zahlenmäßig kleine Unterschiede bei den Scanergebnissen wirken sich in der Praxis deutlich auf die Systemsicherheit aus. Lesen Sie dazu den Kasten auf Seite 135 »Infektionsrisiko minimieren«). Bei der Auswahl des Virenscanners rät PCpro zu Produkten mit über 99 Prozent Erkennungsrate.

Empfehlung der Redaktion

PC Professionell – Empfehlung der Redaktion – bei Viren- und Spyware-Schutz

Kaspersky Internet Security 6.0

Beim Kampf gegen Viren und Spyware liegt Kaspersky im Testfeld ganz vorne. Unter der durchdachten Oberfläche wartet der Virenscanner mit hervorragenden Erkennungsraten auf, auch Archive und andere Verstecke durchforstet er. Schnelle Reaktionszeiten und ein guter proaktiver Schutz minimieren das Infektionsrisiko abermals. Das über 300 Seiten dicke Handbuch lässt keine Fragen offen. So verdient sich die Kaspersky-Suite in der Disziplin Viren- und Spywareschutz die »Empfehlung der Redaktion«.

Die Security-Suiten mit den besten Antiviren-/Antispyware-Modulen

	Hersteller Produkt	maximal 100 Punkte
1	**Kaspersky** Internet Security Suite 6.0	**93,7**
2	**G Data** AVK Internet Security 2006	**92,0**
3	**F-Secure** Internet Security 2006	**83,1**
4	**Softwin** Bitdefender 9 Internet Security	**76,8**
5	**Panda** Platinum 2006 Internet Security	**70,0**

Keine Updates ohne Administratorrechte: Suiten, die deshalb mit veralteten Virendefinitionen arbeiten, bieten keinen ausreichenden Schutz

Obwohl auch Trend Micro fehlende Admin-Rechte bemängelt, funktionieren Updates hier problemlos

Im nächsten Schritt lassen die Tester eine Festplatte mit über 170 000 Backdoorprogrammen, Bots (Zombies) und anderen trojanischen Pferden scannen. Mit deren Hilfe können Hacker an Ihre Daten gelangen oder Botnetze zum massenhaften Spamversand aufbauen. Das Spitzentrio beim Scan bilden hier F-Secure mit sehr guten 99,5 Prozent sowie Kaspersky (98,5 Prozent) und G Data (98,4 Prozent). Einigermaßen mithalten kann nur noch McAfee mit 95,8 Prozent. Die Suiten von CA und Zonelabs sind die Schlusslichter: Ihr ähnlich schlechtes Abschneiden liegt an der von beiden Programmen eingesetzten Virenengine namens VET. Während CA aber bereits Version 12.4 nutzt, setzt Zonelabs noch auf VET 11.9. Für Juni – kurz nach Redaktionsschluss – ist ein Update auf die aktuelle VET-Version geplant.

Zu viele Fehlalarme

Scanner mit einer hohen Erkennungsrate neigen gleichzeitig stärker dazu, einen Fehlalarm auszulösen. In einer Sammlung aus 20 000 harmlosen Programmdateien und Skripten stuft das G Data Antivirenkit ganze 18 Exemplare als gefährlich ein (0,09 Prozent), F-Secure und Bitdefender immerhin noch 14 beziehungsweise 13 Dateien (etwa 0,07 Prozent). Lediglich die Suiten von CA und Trend Micro lassen sich nicht in die Irre führen. Bis zu ein Fehlalarm pro 1000 Dateien – das klingt viel, fällt in der Praxis aber deutlich geringer aus. Das Testset besteht zu etwa 80 Prozent aus gewöhnlichen Windows- und Office-Dateien: Hier glaubt kein einziger Virenscanner, einen Schädling zu erkennen. Die restlichen 4000 sind ausgewählte Samples, die bereits in der Vergangenheit für falschen Alarm sorgten oder leicht als potenzieller Virus gedeutet werden könnten.

Neue Wege gegen neue Viren

Varianten bekannter Schädlinge versuchen moderne Virenscanner anhand von Heuristiken zu erkennen. G Data führt hier mit einer Erkennungsrate von 55,4 Prozent, was sicherlich der eingesetzten Bitdefender-Engine zu verdanken ist: Softwin Bitdefender selbst liegt mit 50,8 Prozent ebenfalls deutlich vor der Konkurrenz. Am unteren Ende präsentieren sich hier abermals CA mit 6,1 Prozent und Zonelabs mit 4,9 Prozent.

Darüber hinaus haben einige Suiten auch proaktive Erkennungsmethoden eingebaut, die einen laufenden Virus anhand verdächtiger Aktionen identifizieren und stoppen sollen. Panda nennt dieses Modul TruPrevent, Kaspersky einfach proaktiven Schutz. In der Zonealarm-Suite übernimmt die Application Firewall diese Aufgabe. Wie die Tester feststellen, arbeiten alle drei sehr ordentlich: Zehn bis dato unbekannte Schadprogramme, die keinerlei verdächtige Verbindung ins Internet aufbauen, werden auf den Laborrechnern gestartet. TruPrevent gibt in neun Fällen eine Warnmeldung aus, Kaspersky schlägt achtmal Alarm. Bei Zonealarm folgen auf sieben Programmstarts diverse Warnmeldungen, die der Benutzer aber erst einmal richtig interpretieren muss. Bitdefender hat für die kommende Version 10 auch einen proaktiven Schutz namens B-Have angekündigt. Für den proaktiven Schutz gilt jedoch: Er ist definitiv nur eine Ergänzung zu regelmäßigen Updates und Heuristiken. Der Komplettschutz ohne Virenscanner-Updates ist Marketing, vertrauen Sie nicht darauf.

Verstecke der Virenschmuggler

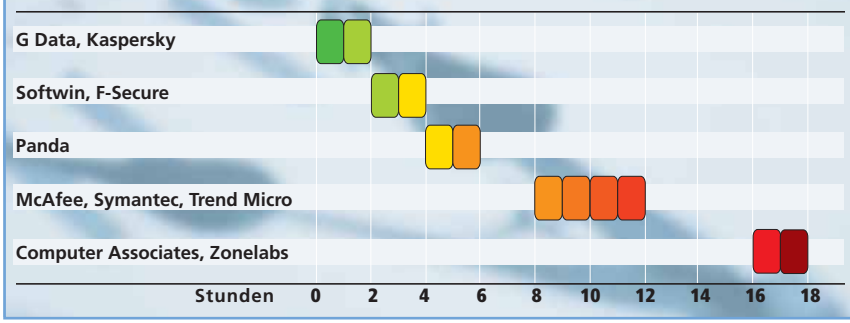
Die Suche in den wichtigsten Archivformaten klappt bei den aktuellen Scannern weitgehend ohne Probleme. Lediglich CA, Norton und Zonelabs ignorieren das Kompressionsformat ACE, Trend Micro kann nicht in selbstentpackende ACE- und RAR-Archive hineinsehen. Norton und Zonealarm kennen zusätzlich die Unix-Formate B2 und TBZ nicht.

Spannend und zugleich sehr durchwachsen fällt das Ergebnis bei laufzeitgepackten Programmdateien aus – dort gibt es unzählige Formate. Mit sage und schreibe 2941 unterschiedlichen Kompressionsalgorithmen verstecken die Tester einen Virus, den die Security-Suiten nun finden sollen. Am besten schlägt sich G Data (86,5 Prozent), gefolgt von F-Secure (82,5 Prozent) und Kaspersky (80,4 Prozent). Am anderen Ende der Leistungsskala enttäuschen erneut CA (7,7 Prozent) und Zonealarm (1,5 Prozent) mit ungenügenden Ergebnissen.

Nicht nur für Makroviren bieten sich in Office-Dokumente eingebettete OLE-Objekte als ideales Versteck an. Neben DOC, XLS,

Reaktionszeiten bei Viren-Outbreaks

Bei einer weltweiten Wurmepidemie sind schnelle Updates seitens der Antivirenhersteller gefragt. Länger als 4 Stunden sollten die Reaktionszeiten auf Outbreaks daher nicht ausfallen.



»Ein eingeschränktes Benutzerkonto und abgeschaltetes ActiveX erhöhen die Sicherheit unter XP. Security-Suiten, die in dieser Konfiguration die nötigen Updates verweigern, sind ein Sicherheitsrisiko.«

RÜDIGER PEIN, REDAKTEUR INTERNET

PPT und VBS binden die Tester auch verseuchte COM- und EXE-Dateien ein. Wieder patzen CA und Zonealarm: Programme (COM und EXE) sowie VBS-Skripte bleiben in Office-Dateien ungeprüft. Ebenso ignoriert werden XLS-MSO- und PPT-MSO-Dateien. Keinerlei Schwächen gibt es beim Scannen passwortgeschützter OLE-Objekte: Alle Programme im Test finden Viren in den unverschlüsselt gespeicherten Makros.

Raffinierte Virenverstecke aufspüren

Nur wenige Windows-Programme nutzen die Alternate Data Streams (ADS) des NTFS-Dateisystems – dafür einige Viren, die sich so unbemerkt an Datei- und Verzeichniseinträge hängen. Dort suchen aber lediglich CA, G Data, Kaspersky und Symantec. McAfee und Softwin beachten ADS aus unerklärlichen Gründen nur an Dateien, nicht jedoch an Ordnern. Mit dem Programm Streams (PCP-Code: ADS) aus dem PCpro-Sicherheitspaket auf Heft-CD finden Sie alle versteckten ADS einer NTFS-Partition. Nach den Kopierschutz-Skandalen mit Rootkits auf CDs von Sony BMG sowie auf der DVD »Mr & Mrs Smith« von Kinowelt halten auch Virenscanner vermehrt Ausschau nach unsichtbaren Systemkomponenten. Seltsamerweise erkennen nur F-Secure und Kaspersky einen mit dem einfachen Rootkit Hacker Defender versteckten Wurm. Wird der Schädling mithilfe des XCP-Kopierschutzes von Sony BMG versteckt, findet ihn nur noch McAfee. Kaspersky weist nur auf ein potenziell gefährliches, von XCP verstecktes Objekt im System32-Verzeichnis hin. Hat sich hingegen der Feebs-Wurm mit Rootkit-Technologie auf dem System eingenistet, finden F-Secure, Kaspersky, McAfee, Softwin und Zonelabs den verborgenen Trittbrettfahrer. Als Freeware-Ergänzung zum Aufspüren von Rootkits finden Sie Rootkit Revealer auf Heft-CD/DVD (PCP-Code: ROOTKIT).

Eine Sammlung aus 868 inaktiven Ad- und Spyware-Samples dient als Testbasis für die Erkennung von Spionagesoftware. Sowohl die Viren- als auch eventuell vorhandene Spywarescanner ergänzen sich hierbei gegenseitig. Sehr gute Resultate erzielen Panda (96,2 Prozent) und Kaspersky (95,8 Prozent), die Nächstplatzierten McAfee (82,6 Prozent) und Symantec (67,2 Prozent) sind bereits weit abgeschlagen.

Reinigung von Spyware

Das Säubern eines infizierten Rechners gelingt nur in wenigen Fällen: Die Adware Maxfiles beispielsweise tilgen nur Kaspersky, McAfee, Norton und Trend Micro komplett vom Rechner. Softwin und Panda löschen immerhin alle Dateien, hinterlassen aber hunderte von Registryeinträgen im System.

Spitze beim Entfernen von sechs aktiven ITW-Würmern ist Trend Micro: Es löscht alle Dateien, Registryeinträge sowie Änderungen an der *hosts*-Datei. Zonealarm an zweiter Stelle führt nur beim Lovgate.AC-Wurm keine Registrybereinigung durch. Schlecht: CA, F-Secure, Kaspersky, McAfee und Norton lassen sogar die Programmdateien von Lovgate.AC stehen, Bitdefender reinigt weder bei Lovgate.AC- noch Mydoom.O-Befall.

Updates nur gegen Sicherheiten

Die Installation klappt bei allen Testkandidaten ohne größere Probleme. Besonders kompliziert fällt sie jedoch bei McAfee aus: Mehrfache Neustarts sind dazu notwendig, Firefox-Nutzer müssen für die Updatefunktion ein Plug-in installieren. Wer jedoch die Sicherheitsstufe im Internet Explorer auf *Hoch* setzt, erhält keine Aktualisierungen mehr: Auch bei Firefox als Standardbrowser möchte das McAfee Security Center seine Fensterinhalte mithilfe von ActiveX-Steuerelementen darstellen. Ein On-Demand-Scan funktioniert dann ebenfalls nicht mehr – ein unhaltbarer Zustand bei einem Sicherheitstool.

Doch auch beim sicheren Arbeiten mit eingeschränkten Benutzerrechten (siehe auch PC Professionell 8/2005 ab Seite 138) versagt so manche Updatefunktion: Neben McAfee bleiben dann auch die Engines und Signaturen von CA und Symantec auf dem alten Stand. Bei der Suite von CA sind sowohl ezAntivirus als auch das Antispywaremodul Pestpatrol davon betroffen. Für Verwirrung sorgt das LiveUpdate von Symantec, das ebenfalls nur mit Admin-Rechten

So wichtig ist die Erkennungsquote

Infektionsrisiko minimieren

Greifen Sie zu Hochprozentigem: Auf den ersten Blick passable Erfolgsquoten beim Virenscan sind auf Dauer oft ungenügend.

Eine hohe Erkennungsrate beim Aufspüren von Schädlingen ist für einen guten Virenscanner extrem wichtig. Unterschiede von wenigen Prozent beeinflussen das Risiko einer Vireninfektion bereits um ein Vielfaches.

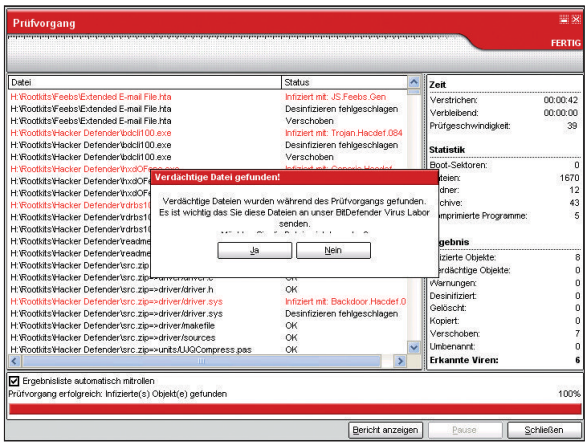
Ein einfaches Beispiel veranschaulicht dies: Zwei Virenscanner A und B (siehe Rechnung unten) werden mit jeweils zehn unterschiedlichen Bedrohungen konfrontiert. Scanner A (99,9 % Erkennungsrate) wehrt mit 99 Prozent Wahrscheinlichkeit alle Schädlinge ab, während Scanner B (90,0 % Erkennungsrate) mit hoher Wahrscheinlichkeit (über 65 Prozent) mindestens einen Virus durchlässt. Gleichzeitig zeigt dieses Beispiel jedoch auch, dass selbst der beste Virenscanner auf Dauer eine Infektion nicht hundertprozentig verhindern kann. *RPE*

Virenscanner A

Erkennungsrate: 99,9%
Infektionsrisiko bei 10 verschiedenen Virenattacken:
$100\% - (99{,}9\%)^{10} = 100\% - 99{,}0\% = 1{,}0\%$

Virenscanner B

Erkennungsrate: 90,0%
Infektionsrisiko bei 10 verschiedenen Virenattacken:
$100\% - (90{,}0\%)^{10} = 100\% - 34{,}9\% = 65{,}1\%$



Bitdefender versteckt die Frage hinter den Antwortmöglichkeiten (links)

Vier Module, vier Icons in der Taskleiste: Die Integration der verschiedenen Einzelkomponenten ist in der Suite von Computer Associates nicht sehr ausgeprägt (rechts)

funktioniert: Im Test erscheint trotz acht Tage alter Datenbanken die Meldung »Ihre Virendefinitionen sind auf dem neuesten Stand«.

Selbstschutz vor Abschaltung

Viele Viren und Trojaner versuchen, die auf einem Rechner installierten Sicherheitspakete auszuschalten. Im Labor von PC Professionell versuchen die Tester deshalb, laufende Prozesse der Security-Suiten mit der Freeware ProcessExplorer *(www.sysinternals.com/Utilities/ProcessExplorer.html)* zu beenden. Was sich auf diesem Weg manuell deaktivieren lässt, könnte ein Schädling ebenso automatisiert durchführen. Beängstigendes Resultat: Ohne Schutz vor derlei Aktionen quittieren die Wächter von F-Secure, McAfee, Softwin Bitdefender und Trend Micro ihren Dienst. Bei G Data lässt sich lediglich das Tray-Icon entfernen.

In einem weiteren Szenario versuchen die Tester, laufende Dienste der AV-Tools anzuhalten. Lediglich CA, Kaspersky sowie Zonelabs vereiteln dies komplett. Bei G Data können zwar die Antivirenkit-Services beendet werden, das Programm funktioniert aber weiterhin. Auch Norton Internet Security arbeitet nach dem Anhalten einiger Dienste zunächst weiter, stürzt aber nach einem Virenfund ab und beendet sich daraufhin.

Sicherheit bremst den Rechner aus

Security-Suiten kosten immer auch Systemperformance. Bei G Data mit seinen beiden Scanengines von Bitdefender und Kaspersky zeigt sich dies am deutlichsten: Während das Testsystem (Pentium 4 mit 3,2 GHz und 2 GByte RAM) beim Benchmark ohne installierte Schutzprogramme einen Winstone-Wert von 30,4 erzielt, liegt dieser mit aktiver G Data-Suite ganze 5,8 Punkte darunter (Winstone-Wert: 24,6). Vergleichsweise wenig belasten Kaspersky (Winstone-Wert: 27,0) und vor allem F-Secure (Winstone-Wert: 28,3) den Rechner. Als Etappensieger bei der Abwehr von Viren und Spyware steht die neue Kaspersky Internet Security 6 ganz oben auf dem Treppchen: Neben der zweitbesten Erkennungsrate spürt der proaktive Schutz zusätzlich acht von zehn unbekannten Schädlingen auf. Die Suche in Archiven und ADS ist vorbildlich, auch bei aktiven Rootkits wird der Scanner noch fündig. Alle Module sind zudem gut gegen unbefugtes Deaktivieren gesichert.

Silber und Bronze gehen an die Antivirenkomponenten von G Data und F-Secure, die ebenfalls mit hervorragenden Erkennungsraten überzeugen. G Data zeigt sich jedoch blind gegenüber aktiven Rootkits, F-Secure sucht nicht in Alternate Data Streams und lässt sich zudem leicht beenden. Deutliche Verlierer aufgrund miserabler Erkennungsraten sind die Suiten von CA und Zonelabs. Ohne Chancen auf einen Gesamtsieg gehen auch McAfee und Symantecs Norton Internet Security aus dem Rennen, die – ebenso wie die CA-Suite – beim Arbeiten mit eingeschränkten Benutzerrechten keine Updates mehr herunterladen.

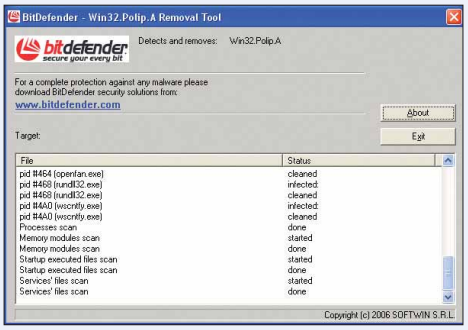
Mit Spambekämpfung und Firewall-Test stehen noch zwei wichtige Disziplinen im Mega-Vergleichstest von Security Suiten aus. In der nächsten Ausgabe folgt ein Anti-Spam-Test mit zehntausenden E-Mails. *RPE*

Polip(os) – Die polymorphe Gefahr

Virus mit tausend Gesichtern

Der in P2P-Netzwerken beheimatete Polip-Virus verändert ständig sein Aussehen und erschwert so seine Entdeckung.

Mit der Textzeile »Win32.Polipos v1.2 by Joseph« hat sich der Virenautor selbst im Code verewigt. Da es üblich ist, Namensvorschläge durch Malware-Programmierer nicht direkt zu übernehmen, heißt der Schädling nun Win32.Polip.A. Vor allem in Tauschbörsen wie eDonkey oder Gnutella ist er häufig anzutreffen.



Das Removal Tool biegt die API-Calls infizierter Prozesse wieder zurecht

Als echter Dateivirus hängt er sich an ausführbare EXE- und SCR-Dateien, die etwa um 60 bis 70 KByte an Größe zunehmen. API-Calls laufender Prozesse werden auf die Startadresse des Virencodes umgeleitet. Das Besondere an ihm ist jedoch sein Polymorphismus: Jede Kopie des Virus sieht anders aus. Um ihn zu erkennen, reicht daher eine Signatur allein nicht aus, auch die Suchengine braucht ein Update. Polip hindert jedoch verschiedene Sicherheitstools am Update. Damit die Aktualisierung auf einem infizierten Rechner dennoch klappt, säubern Sie zuvor mit dem kostenlosen Tool *www.bitdefender.de/bd/AntiPolip-A-en.exe* alle infizierten Prozesse. *RPE*

Produkt	Internet Security 6		InternetSecurity 2006		Internet Security 2006		Bitdefender 9 Internet Security		Platinum Internet Security 2006	
Hersteller	**Kaspersky**		**G Data**		**F-Secure**		**Softwin**		**Panda**	
Internet	www.kaspersky.de		www.gdata.de		www.f-secure.de		www.bitdefender.de		www.panda-software.de	
Preis (1 PC, 1 Jahr)	40 Euro		70 Euro		60 Euro		69 Euro		80 Euro	
Update (1 PC, 1 Jahr)	30 Euro		30 Euro		40 Euro		44 Euro		60 Euro	
Gesamturteil (Note/Punkte)	**sehr gut**	**93,7**	**sehr gut**	**92,0**	**gut**	**83,1**	**befriedigend**	**76,8**	**befriedigend**	**70,0**
Leistung (70 %)	sehr gut	94,9	sehr gut	91,4	gut	80,7	befriedigend	72,4	ausreichend	63,0
Ausstattung (15 %)	gut	88,7	sehr gut	93,3	gut	83,3	gut	82,7	sehr gut	90,7
Bedienung (15 %)	sehr gut	93,1	sehr gut	93,7	sehr gut	94,3	sehr gut	91,2	gut	82,0
Fazit										
	Testsieger beim Virentest: Sehr gute Malwareerkennung auch bei aktiven Rootkits, guter Selbstschutz gegen unbefugtes Beenden.		**Top Erkennungsraten auch in gepackten Dateien, schnelle Reaktion auf Viren-Outbreaks, vergleichsweise hohe Systembelastung.**		**Prima Erkennung von Viren, Trojanern und Rootkits. Mangelnder Selbstschutz und fehlende ADS-Suche verhindern besseren Platz.**		**Ausgewogene, im oberen Mittelfeld angesiedelte Leistung, Schwächen bei Selbstschutz und bei Trojaner- und Rootkit-Erkennung.**		**Schneller Virenscanner mit ordentlicher Leistung, guter proaktiver Schutz, Schwächen unter anderem bei ADS und Rootkits.**	
Virenerkennung (Scanner)										
Erkennung von ITW-Viren	100 %		100 %		100 %		100 %		100 %	
Erkennung von Dateiviren	99,96 %		99,98 %		99,96 %		95,29 %		98,43 %	
Erkennung von Makroviren	99,98 %		99,98 %		99,99 %		99,62 %		99,87 %	
Erkennung von Skriptviren	99,83 %		99,52 %		100 %		97,47 %		98,99 %	
Erkennung polymorpher Viren	99,97 %		99,98 %		99,98 %		98,00 %		99,32 %	
Erkennung von Trojanern	98,52 %		98,37 %		99,46 %		93,20 %		85,43 %	
Erkennung von Ad- und Spyware-Installern	95,74 %		32,37 %		43,66 %		61,87 %		96,20 %	
Fehlalarmquote	0,04 %		0,09 %		0,07 %		0,07 %		0,02 %	
Scandauer bei einer 75-GByte-Partition	13:11 Minuten		89:15 Minuten		26:21 Minuten		14:08 Minuten		6:40 Minuten	
Suche in Archiven										
Suche in einfach gepackten Archiven (getestet: ACE, ARJ, B2, CAB, GZ, LHA, RAR, TAR, TBZ, TGZ, ZIP)	alle		alle		alle		alle		alle	
Suche in mehrfach verschachtelten Archiven (getestet: ACE, ARJ, CAB, LHA, RAR, ZIP)	alle		alle		alle		alle		alle	
Suche in selbstentpackenden Archiven (getestet: ACE, ARJ, LHA, RAR16, RAR32, WinZIP)	alle		alle		alle		alle		alle	
Erkennung laufzeitgepackter Viren	80,35 %		86,54 %		82,49 %		76,84 %		60,97 %	
Erkennung in ADS/bei Rootkits										
Suche in ADS an Datei/an Verzeichnis	ja/ja		ja/ja		nein/nein		ja/nein		nein/nein	
Erkennung unter Hacker-Defender-Rootkit	ja		nein		ja		nein		nein	
Erkennung unter XCP-Rootkit	nein		nein		nein		nein		nein	
Erkennung unter Feebs-Rootkit	ja		nein		ja		ja		nein	
Selbstschutz										
Schutz vor Beenden der Prozesse	ja		ja		nein		nein		ja	
Schutz vor Anhalten der Dienste	ja		ja		nein		nein		nein	
Updates										
Zahl der Updates März 2006/April 2006	664 Updates/549 Updates		1000 Updates/974 Updates		63 Updates/62 Updates		350 Updates/393 Updates		46 Updates/37 Updates	
Durchschnittliche Reaktionszeiten	0 bis 2 Stunden		0 bis 2 Stunden		2 bis 4 Stunden		2 bis 4 Stunden		4 bis 6 Stunden	
kostenlose Updates auf Folgeversionen	ja		nein		ja		ja		ja	
Update möglich ohne ActiveX	ja		ja		ja		ja		ja	
Update möglich unter Benutzerkonto	ja		ja		ja		ja		ja	
Sonstiges										
Deutsches Handbuch gedruckt/auf CD	314 Seiten/314 Seiten (PDF)		223 Seiten/223 Seiten (PDF)		164 Seiten/164 Seiten (HTML)		198 Seiten/207 Seiten (PDF)		16 Seiten/16 Seiten (PDF)	
Bootfähige CD mit Virenscanner	nein, aber Menüpunkt zum Erstellen einer Notfall-CD		ja		ja		ja		ja	
Speichern kompletter Reportdateien	ja		ja		ja		ja		ja	
Online-Virenlexikon	www.viruslist.de/viruses/encyclopedia		www.antiviruslab.com		www.f-secure.com/v-descs		www.bitdefender.de/html/virusinfo.php?menu_id=1		www.pandasoftware.com/virus_info	
Unterstützte Betriebssysteme	Windows 98, Me, NT, 2000, XP		Windows 98 SE, Me, 2000, XP		Windows 98, Me, 2000, XP		Windows 2000 SP4, XP		Windows 98, Me, 2000, XP	
Service										
Hotline	(08 41) 98 18 90		(018 01) 00 06 60[1)]		(089) 787 46 73 67		(075 42) 94 44 60		keine	
E-Mail-Support	support@kaspersky.de		hotline@gdata.de		support-de@f-secure.com		support@bitdefender.de		technik@panda-software.de	

[1)] 1,99 Euro pro Minute

Produkt	Internet Security Suite		Norton Internet Security 2006		PC-Cillin 14 Internet Security		Zonealarm Internet Security Suite		eTrust Internet Security Suite	
Hersteller	**McAfee**		**Symantec**		**Trend Micro**		**Zonelabs**		**Computer Associates**	
Internet	www.mcafee.com/de		www.symantec.de		http://de.trendmicro-europe.com		www.zonelabs.de		www.blitzbox.de	
Preis (1 PC, 1 Jahr)	80 Euro		70 Euro		59 Euro		50 Euro		60 Euro	
Update (1 PC, 1 Jahr)	30 Euro		50 Euro		39 Euro		35 Euro		60 Euro	
Gesamturteil (Note/Punkte)	**befriedigend**	**65,9**	**befriedigend**	**65,6**	**ausreichend**	**57,3**	**ausreichend**	**56,0**	**ausreichend**	**51,3**
Leistung (70 %)	befriedigend	67,1	ausreichend	60,0	mangelhaft	49,2	mangelhaft	49,7	mangelhaft	46,5
Ausstattung (15 %)	ausreichend	53,3	gut	82,0	befriedigend	67,3	ausreichend	60,0	ausreichend	52,7
Bedienung (15 %)	befriedigend	72,8	befriedigend	75,2	gut	85,1	gut	81,4	befriedigend	72,2
Fazit										
	Hervorragende Virenerkennung. Aufwändige Installation, leicht zu deaktivieren und keine Updates ohne ActiveX und Adminrechte.		**In einigen Bereichen sehr gute Erkennungsraten, keine Updates unter Benutzerkonto. Schwächen bei Rootkits.**		**Schlechte Ergebnisse bei der Suche in Archiven, in ADS und bei aktiven Rootkits. Bei erkannten Viren gute Reinigungsfunktion.**		**Ungenügende Erkennungsraten und lange Reaktionszeiten auf Virenoutbreaks. Guter Schutz gegen unbefugtes Abschalten.**		**Schnelle Viren- und Spywarescanner, ungenügende Erkennungsraten und lange Reaktionszeiten, keine Updates ohne Adminrechte.**	
Virenerkennung (Scanner)										
Erkennung von ITW-Viren	100 %		100 %		100 %		100 %		100 %	
Erkennung von Dateiviren	99,99 %		99,99 %		99,25 %		42,80 %		99,31 %	
Erkennung von Makroviren	99,98 %		99,98 %		99,52 %		85,13 %		99,86 %	
Erkennung von Skriptviren	100 %		98,48 %		95,86 %		74,32 %		72,13 %	
Erkennung polymorpher Viren	99,98 %		99,97 %		99,37 %		69,56 %		99,38 %	
Erkennung von Trojanern	95,80 %		92,13 %		66,84 %		33,32 %		44,77 %	
Erkennung von Ad- und Spyware-Installern	82,60 %		67,17 %		59,68 %		65,55 %		20,39 %	
Fehlalarmquote	0,01 %		0,01 %		0 %		0,01 %		0 %	
Scandauer bei einer 75-GByte-Partition	10:05 Minuten		9:20 Minuten		5:38 Minuten		5:24 Minuten		8:24 Minuten	
Suche in Archiven										
Suche in einfach gepackten Archiven (getestet: ACE, ARJ, B2, CAB, GZ, LHA, RAR, TAR, TBZ, TGZ, ZIP)	alle		ARJ, CAB, GZ, LHA, RAR, TAR, TGZ, ZIP		alle		ARJ, CAB, GZ, LHA, RAR, TAR, TGZ, ZIP		ARJ, B2, CAB, GZ, LHA, RAR, TAR, TBZ, TGZ, ZIP	
Suche in mehrfach verschachtelten Archiven (getestet: ACE, ARJ, CAB, LHA, RAR, ZIP)	alle		ARJ, CAB, LHA, RAR, ZIP		alle		ARJ, CAB, LHA, RAR, ZIP		ARJ, CAB, LHA, RAR, ZIP	
Suche in selbstentpackenden Archiven (getestet: ACE, ARJ, LHA, RAR16, RAR32, WinZIP)	ARJ, LHA, RAR16, RAR32, WinZIP		ARJ, LHA, RAR16, RAR32, WinZIP		ARJ, LHA, WinZIP		ARJ, LHA, RAR16, RAR32, WinZIP		ARJ, LHA, RAR16, RAR32, WinZIP	
Erkennung laufzeitgepackter Viren	79,53 %		42,13 %		31,11 %		1,50 %		7,68 %	
Erkennung in ADS/bei Rootkits										
Suche in ADS an Datei/an Verzeichnis	ja/nein		ja/ja		nein/nein		nein/nein		ja/ja	
Erkennung unter Hacker-Defender-Rootkit	nein		nein		nein		nein		nein	
Erkennung unter XCP-Rootkit	ja		nein		nein		nein		nein	
Erkennung unter Feebs-Rootkit	ja		nein		nein		ja		nein	
Selbstschutz										
Schutz vor Beenden der Prozesse	nein		ja		nein		ja		ja	
Schutz vor Anhalten der Dienste	nein		nein		nein		ja		ja	
Updates										
Zahl der Updates März 2006/April 2006	24 Updates/20 Updates		33 Updates/30 Updates		32 Updates/33 Updates		28 Updates/25 Updates		28 Updates/25 Updates	
Durchschnittliche Reaktionszeiten	8 bis 10 Stunden		8 bis 10 Stunden		8 bis 10 Stunden		16 bis 18 Stunden		16 bis 18 Stunden	
kostenlose Updates auf Folgeversionen	nein, nur während der ersten drei Monate		nein		ja		ja		nein	
Update möglich ohne ActiveX	nein		ja		ja		ja		ja	
Update möglich unter Benutzerkonto	nein		nein		ja		ja		nein	
Sonstiges										
Deutsches Handbuch gedruckt/auf CD	2 Seiten/149 Seiten (PDF)		30 Seiten/30 Seiten (PDF)		4 Seiten/70 Seiten (PDF)		217 Seiten/nein[1]		keines/12 Seiten (PDF)	
Bootfähige CD mit Virenscanner	nein		ja		nein		nein		nein	
Speichern kompletter Reportdateien	nein		ja		ja		nein		nein	
Online-Virenlexikon	http://vil.nai.com		www.symantec.com/avcenter/vinfodb.html		http://de.trendmicro-europe.com/enterprise/vinfo/encyclopedia.php		www3.ca.com/securityadvisor/virusinfo		www3.ca.com/securityadvisor/virusinfo	
Unterstützte Betriebssysteme	Windows 98, Me, 2000, XP		Windows 2000, XP (enthält Version 2005 für Windows 98, Me)		Windows 98, Me, 2000, XP		Windows 98 SE, Me, 2000, XP		Windows 98 SE, Me, 2000, XP	
Service										
Hotline	(09 00) 110 14 86[2]		(09 00) 11 01 30[2]		(09 00) 186 37 22[3]		(018 05) 33 97 90[4]		(09 00) 100 03 86[5]	
E-Mail-Support	info_Deutschland@mcafee.com		Supportformular unter www.symantec.com/region/de/techsupp		Supportformular unter http://support.antivirus.co.uk/trendmicro/home_europe.jsp		emea_support@zonelabs.com		support@blitzbox.de	

[1] Link auf 294-seitiges Online-PDF-Handbuch [2] 0,59 Euro pro Minute, 18-9 Uhr: 0,025 Euro pro Minute [3] 0,62 Euro pro Minute [4] 0,12 Euro pro Minute [5] 1,50 Euro pro Minute