

Jürgen Schmidt

Schutzbehauptung

Antiviren-Programme auf dem Prüfstand

Nach den ersten zehn AV-Programmen im November müssen nun sechs Nachzügler zeigen, ob sie die Zeit gut genutzt haben, um sich besser für die Gefahren des neuen Jahres zu rüsten. Zusätzlich treten auch zwei verhaltensorientierte Lösungen aus der Anti-Spyware-Ecke an.



Der letzte Test ließ vor allem eine Frage offen: Kann vielleicht einer der Nachzügler den bereits getesteten Antivirenprogrammen den Rang ablaufen? Diese Chance haben jetzt Avast! 4 Professional, CA Anti-Virus plus CA Anti-Spyware 2009, Ikarus virus.utilities, McAfee VirusScan Plus 2009, Norman Antivirus & Antispyware und Trend Micro Internet Security 2009. Das Open-Source-Projekt ClamWin entspricht zwar den Anforderungen eigentlich nicht, weil es immer noch keinen Wächter enthält. Weil das zugrunde liegende, kostenlose ClamAV trotzdem einen guten Scanner für Gateways abgeben kann, haben wir dessen Scanleistung kurzerhand außer Konkurrenz mitgetestet.

Um den Test noch spannender zu gestalten, haben wir ebenfalls zum Vergleich zwei Schutzprogramme getestet, die eher aus der Anti-Spyware-Ecke stammen und ihren Schwerpunkt auf die Verhaltenserkennung legen: A-Squared Anti-Malware und PC Tools ThreatFire Pro.

Einfache Tests von Antiviren-Software beschränken sich aufs Erbsen zählen: Man jagt die Scanner über einen möglichst großen Satz böser Dateien und schaut nach, welcher wie viele davon erkannt hat. Die guten finden fast alle, die schlechten weniger; der Unterschied spielt sich oft nur im Prozentbereich ab. Dabei wird kein einziger Schädling wirklich gestartet, kein Rootkit aktiviert, kein Web-Exploit tatsächlich im Browser geladen. Das ist dann zwar einfach umzusetzen, hat aber mit der Realität wenig zu tun. Denn die ist deutlich komplexer.

Die reale Gefahr geht von neuen Schädlingen aus, die so lange optimiert wurden, bis kein Scanner mehr anschlägt. Die werden dann über Bot-Netze via Mail verteilt oder wie neulich über die Sicherheitslücke im Internet Explorer eingeschleust – lange bevor die Hersteller Signaturen dafür gebaut haben. Erst da trennt sich die Spreu vom Weizen. Selbst wenn ein Trojaner dem Wächter zunächst durchrutscht, haben die guten Schutzprogramme eine zweite Verteidigungslinie in petto: Sie durchschauen die typischen Tricks von Rootkits und erkennen Schadprogramme an ihrem Verhalten.

Um derartige Funktionen zu testen, haben wir die Antiviren-Software in Zusammenarbeit mit AV-Test (www.av-test.de) mit zehn aktiven Rootkits konfrontiert und zwanzig handverlesene Schädlinge, die zunächst nicht erkannt wurden, von Hand gestartet, um zu sehen, wie der Virenschutz reagiert. Außerdem haben wir Webseiten mit Exploits für Sicherheitslücken aufgesetzt und mit Firefox und Internet Explorer aufgerufen. Das alles ist zwar recht aufwändig, aber für einen aussagekräftigen Test unverzichtbar.

Selbstverständlich haben wir dafür auf das Erbsenzählen nicht verzichtet: An rund einer halben Million Schadprogrammen aus den letzten Monaten mussten die Scanner ihre Basisfertigkeiten beweisen. Des Weiteren mussten sie in den bewährten Tests mit alten Signaturen gegen neue Schädlinge antreten, um ihre heuristischen Fähigkeiten unter Beweis zu stellen. Darüber hinaus wurden eine ganze Reihe von zusätzlichen Funktionen überprüft, die in der großen Ergebnistabelle auf Seite 80 en Detail aufgeführt sind.

Die Tests und deren Bewertung erfolgten weitgehend analog zu dem im November, sodass sich die Ergebnisse vergleichen lassen. Um einen vollständigen Überblick über die aktuelle Produktpalette zu geben, haben wir die Ergebnistabelle auf Seite 78 nochmal abgedruckt.

Falscher Alarm

Die einzige signifikante Erweiterung betrifft das leidige Thema Fehlalarme. Da die wenigen Fehlalarme beim existierenden Testset unsere realen Erfahrungen nicht widerspiegeln, wurde ein zweites Testset mit 25 000 auf CDs und DVDs veröffentlichten Programmen erstellt und in der Tabelle dann getrennt aufgeführt.

Die Häufigkeit von Fehlalarmen ist auch schon das erste augenfällige Testergebnis. Sieben der neun Kandidaten – namentlich A-Squared, Avast, CA, ClamWin, Ikarus, McAfee und PC Tools leisteten sich mehr – teilweise sogar deutlich mehr – als zehn dieser Ausrutscher, die im besten Fall verunsicherte Anwender, im schlimmsten Fall ein zerschossenes System bedeuten können. Das ist nicht mehr akzeptabel!

Einen Mechanismus, wie es dazu kommt, illustriert ein

aktueller Fall, bei dem ein Leser gemeldet hatte, dass ein einfaches Demoprogramm aus c't zur OO-Programmierung in Delphi auf seinem Rechner einen Alarm ausgelöst hatte. Weitere Tests zeigten, dass mindestens dreizehn verschiedene Antiviren-Programme Unrat witterten. Darunter befanden sich so namhafte Hersteller wie Avast, Avira, BitDefender, G Data, F-Secure, Kaspersky, Microsoft, Eset/Nod32 und Panda. Die Schädlingsbezeichnungen zeigten, dass es sich dabei nicht um fehlgeleitete Heuristiken sondern um gezielte Signaturen für dieses Programm handelte. Wie wir später erfuhren, hatte anscheinend ein AV-Her-

steller die Datei versehentlich als Schadprogramm eingestuft und mit diesem Vermerk an die anderen weitergegeben. Und die erstellten dann offenbar ohne weitere Prüfung schnell mal eben eine Signatur für den angeblichen Bösewicht.

Wie auch im letzten Test ist aufgefallen, dass ein Komplettscan nicht zwangsläufig auch bedeutet, dass alle Dateien untersucht werden. So ignorieren Avast, CA, ClamWin, McAfee und Norman bei einem Komplettscan, den ein Nicht-Administrator anstößt, stillschweigend alle Verzeichnisse, die Administratoren gehören. Zumindest ein diesbezüglicher Hinweis wäre angebracht.

Firmenlösungen

Zumindest unterschwellig schwingt in Leserfragen oft die Erwartung mit, dass doch wohl die Firmenlösungen der Hersteller besser abschneiden würden als die bei c't getesteten Endanwenderprodukte. Doch zumindest wenn es um die Schutzwirkung geht, trügt diese Hoffnung. Denn die Firmenversionen sind in der Regel konservativer ausgelegt – und erzielen somit tendenziell eher niedrigere Erkennungsraten.

Das äußert sich beispielsweise so, dass neue Funktionen in die Firmenprodukte erst viel später eingebaut werden. So fehlen etwa bei Panda und McAfee die In-the-Cloud-Funktionen, bei anderen Herstellern fallen die verhaltensbasierten Erkennungsroutinen weg. Und schließlich verlässt man sich unter anderem natürlich auch auf externe Gateways etwa zum Filtern von Internet-Verkehr oder E-Mail.

Das ist zum Teil Performance-Erwägungen geschuldet. Denn in Firmen kommt oft noch Hardware zum Einsatz, die sich zuhause niemand mehr antun würde. Darüber hinaus steht noch stärker ein reibungsloser Arbeitsablauf im Vordergrund, der nicht durch Fehlalarme oder Warnungen mit nicht eindeutigen Befund unterbrochen werden darf.

Anwender von Norton AV 2009 bekommen mittlerweile alle sechs Minuten frische Signatu-

ren auf ihren PC geliefert. Bei der Firmenversion von Symantec gibt es je nach Version nur ein bis drei Updates am Tag. Die Reaktionszeiten bei Virenausbrüchen sind somit schlechter, was Symantec auch mit der gründlicheren Qualitätssicherung begründet, um Fehlalarme zu vermeiden.

Die Signaturen der Firmen-Produkte von Panda und Trend Micro unterscheiden sich sogar grundlegend von denen der jeweiligen Consumer-Serie. Firmenanwender bekommen hier nur eine Auswahl an Virensignaturen – die Definitionsdateien sind etwa drei- bis viermal kleiner als die der von uns untersuchten Version. In der Regel macht sich das in einem verringerten Hauptspeicherplatzbedarf und schnelleren Scans bemerkbar, aber die Malware-Erkennung ist auch um 10 bis 15 Prozent schlechter.

In der Heimanwenderversion von G Data werkeln die Engines von Avast und BitDefender, in der Unternehmenslösung sind aber derzeit noch die Engines von Avast und F-Prot integriert. Die Erkennungsraten unterscheiden sich dank der zwei Engines aber nicht wesentlich. Gar nicht als Heimanwenderprodukt ist Sophos Antivirus zu haben, das beim Signaturscan durchaus solide Ergebnisse liefert: circa 92 bei Malware beziehungsweise 93 Prozent für Ad- und Spyware. (Andreas Marx)



Aus unerfindlichen Gründen hält Avast an der unsäglichen Oberfläche im Look eines MP3-Players fest.

Avast! 4 Professional

Möchten Sie eine Ladezeit-Antivirus-Prüfung für Ihre lokalen Festplatten zeitsteuern? Die Frage zum Abschluss der Installation gibt einen ersten Eindruck von der Bedienbarkeit, den Avast dann nahtlos bestätigt: Immer ein bisschen daneben, nichts geht einfach so, wie man es sich vorstellt. Beim Aktualisieren muss man sich zwischen „iAVS Update“ und „Programm-Update“ entscheiden, auf der „einfachen“ Oberfläche im Stil eines MP3-Players sucht man ständig nach dem passenden Knopf, die „erweiterte Oberfläche“ ist nicht viel besser.

Zum Glück wirkt sich das nicht auf die Scanleistung aus: Beim Test mit unserer Schädlingsammlung lieferte der Scanner ein sehr gutes Ergebnis, bei Ad- und Spyware reichte es noch für ein gutes. Sowohl Scanner als auch Wächter bremsen dabei nur wenig. Unbefriedigend sind allerdings die heuristische Erkennung unbekannter Schädlinge und die Funktionen zum Aufspüren von Rootkits, die nur jedes zweite Rootkit bemerkten. Verhaltensbasierte Funktionen hat das Programm gar nicht aufzuweisen. Zwar filtert Avast als einziger

Testkandidat den Webverkehr von Firefox und Internet Explorer – aber leider nicht sonderlich gründlich. Der im Dezember aufgetauchte Zero-Day-Exploit für eine IE-Lücke schlüpfte noch nach einer Woche unbemerkt durch.

Nicht getestet wurde die Virus Recovery Database, die alle drei Wochen im Hintergrund eine Datenbank mit Integritätsinformationen erstellt, mit denen sich beschädigte Dateien wiederherstellen lassen sollen. Privatintern bietet Alwil nach einer Registrierung eine kostenlose Lizenz für 14 Monate an. Dabei ist unter anderem die erweiterte Oberfläche nicht verfügbar, sodass man mit der angeblich einfachen MP3-Player-Oberfläche arbeiten muss.

Die marktübliche Dreierlizenz hat der tschechische Hersteller Alwil nicht im Programm. Der überdurchschnittlich hohe Preis von 86 Euro bezieht sich folglich auf eine Zehnerlizenz, die billiger ist, als drei einzelne. Avast fischt als klassischer Signaturscanner das Größte weg; weitergehende Funktionen wie Heuristik, Webfilter, Rootkit-Erkennung und Verhaltenskontrolle sind entweder unterentwickelt oder gar nicht vorhanden. Angesichts des Prei-

ses ist das keine Empfehlung wert. Die kostenlose Version könnte man durchaus in die engere Wahl ziehen, wenn da nicht die vielen Fehlalarme wären.

CA Anti-Virus plus CA Anti-Spyware 2009

CA hat in den letzten c't-Tests eigentlich immer schlecht abgeschnitten und bleibt dieser Tradition treu. Ob Signaturscan, heuristische Erkennung oder Reaktionszeit – CA schafft es tatsächlich, in jeder dieser Kategorien nochmal signifikant schlechter abzuschneiden als der zweit-schlechteste. Wenn ein Virens scanner mit seinen Signaturen nur 58 Prozent der Schädlinge erkennt, kann man auch fast schon eine Münze werfen. Da lohnt es sich gar nicht mehr, die fehlende Verhaltenskontrolle und Ungeheimheiten bei der Bedienung im Einzelnen zu würdigen oder auf vereinzelte Abstürze einzugehen.

Bemerkenswert ist jedoch die Hartnäckigkeit, mit der CA versucht, das Produkt an den Kunden zu bringen. Im Demomodus entdeckte der Scanner beim Abschluss der Installation mehrere Tracking-Cookies von Sites wie Doubleclick, wie sie sich auf nahezu jedem benutzten Rechner finden. Für die Entfernung dieser „Spyware“ müsse man jedoch ein Abonnement abschließen, erklärt der Spyware-Scanner. Das ist natürlich absurd, ein einfaches Löschen der Cookies hat den gleichen Effekt und kostet nichts. Also Finger weg von diesem Programm.

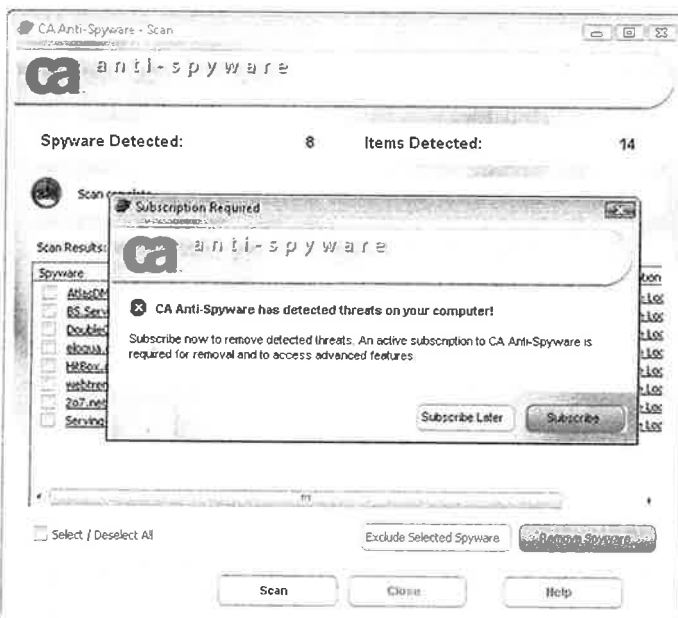
ClamWin Free Antivirus

ClamWin ist eine einfache, grafische Oberfläche für den Open-Source-Scanner ClamAV. Da es jedoch als reiner On-Demand-Scanner arbeitet, also nur nach Aufforderung aktiv wird, kann es nicht als vollwertiger Virenschutz gelten. Konsequenterweise wird es im Windows Sicherheitscenter auch nicht als solcher angezeigt.

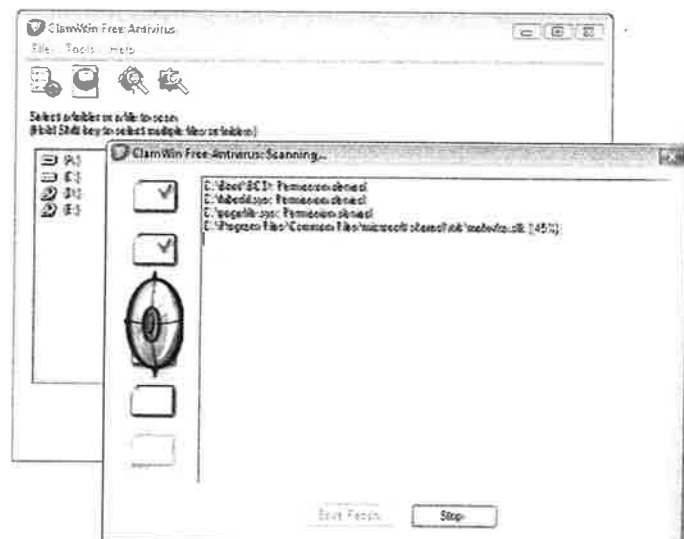
Interessant ist ClamAV somit vor allem als kostenloser Scanner für Mail- oder Web-Gateways und als Grundlage für eine frei verteilbare Version von Knoppicillin. Dafür qualifiziert es sich mit einem im Vergleich zum Vorjahr deutlich verbesserten Scan-Engine. Die CAs Antiviren-Lösung glänzt auslicht und mit Trend Micro mithalten kann. Sogar bei der Heuristik befindet man sich mittlerweile auf Augenhöhe mit den kommerziellen Herstellern. Hervorzuheben ist auch die gute Reaktionszeit von 2 bis 4 Stunden. Allerdings braucht der Scanner beim Durchsuchen große Datenbestände deutlich länger als die meisten anderen. Bedenklich ist auch die recht hohe Fehlalarmquote des Open-Source-Scanners.

Ikarus virus.utilities

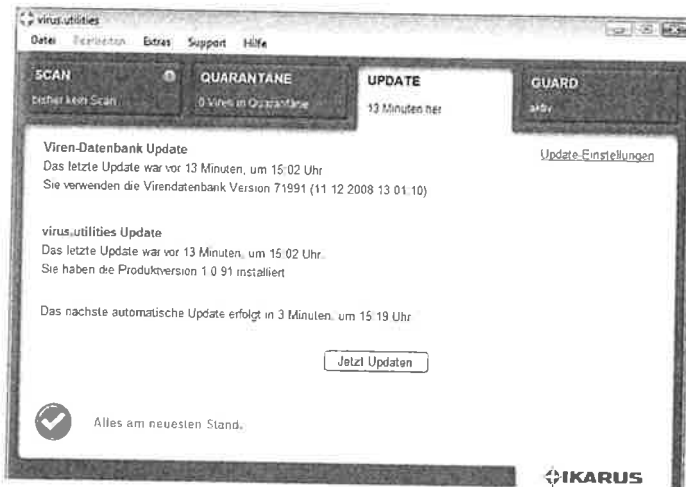
Der österreichische Hersteller Ikarus hat bei den Fehlalarmen den Vogel abgeschossen – allein vier Warnungen zu harmloser Programmen auf der DVD des iX Sonderhefts zum Thema Sicherheit. Kein anderes Programm meldete so oft unberechtigt Tro-



Für das Löschen der Cookies wollte CA ein Abonnement verkaufen.

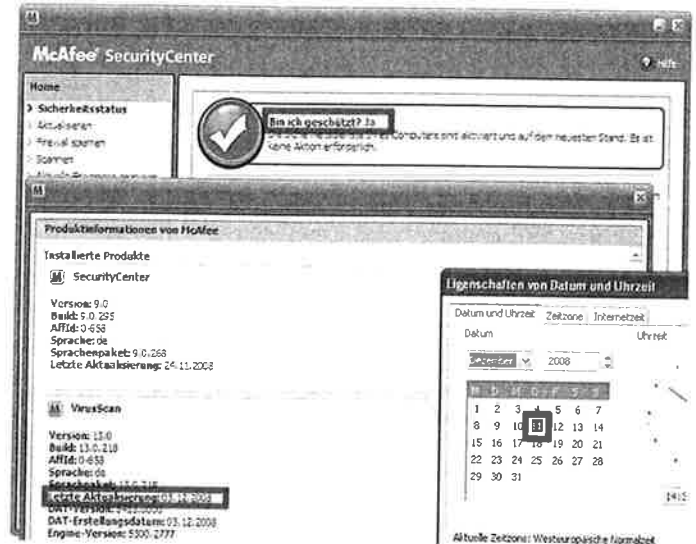


ClamWin versieht den Open-Source-Scanner ClamAV mit einer einfachen Oberfläche.



Die etwas spröde .NET-Oberfläche der Ikarus virus.utilities erfüllt ihren Zweck.

Nein! Auch wenn McAfee das behauptet, ist man mit Signaturen, die über eine Woche alt sind, nicht mehr ausreichend geschützt.



janer, Dropper, Backdoors und Viren. Hier zahlt man für die sehr guten bis guten Leistungen in den Signatur- und Heuristiktests einen zu hohen Preis.

Die einfache aber funktionale Oberfläche setzt auf .Net 2 auf, das man auf XP unter Umständen nachinstallieren muss. Wenn dann das Programm meldet: „Alles am neuesten Stand.“ kann man fast schon Wiener Schmäheraushören. Doch trotz der heimlichen Gefühle eines ausge-

wanderten Süddeutschen setzt sich die Erkenntnis durch, dass für die Wahl des richtigen Virenschutzes doch andere Kriterien wichtig sind – die schlechte Erkennung von Rootkits etwa oder die fehlende Verhaltensanalyse.

McAfee VirusScan Plus 2009

Seit Mitte November liefert McAfee an alle Installationen automatisch ein Update, das In-

the-Cloud-Funktion nachrüsten soll (siehe Kasten unten). Das klappte auf unserem XP-Testsystem allerdings erst, als wir es mit den neuesten Windows-Updates ausstatteten. Bis dahin lief der Virenwächter ohne zu klagen mit eingeschränktem Funktionsumfang. Überhaupt zeigte sich die Schutzsoftware bei den Updates sehr tolerant: Selbst nach mehreren Tagen ohne Updates zeigt das Kontrollzentrum den grünen Haken und meldet,

die Sicherheitsdienste seien „auf dem neuesten Stand. Es ist keine Aktion erforderlich.“ Falsch! In der Zwischenzeit war eine große Trojanerwelle übers Land geschwappt und obwohl McAfee eigentlich bereits passende Signaturen bereitstellte und der Testrechner sich regelmäßig und angeblich erfolgreich beim McAfee-Server nach Updates erkundigte, war das Testsystem nach wie vor ungeschützt. Eine Erklärung für das stille Versagen

Wolken am Horizont

Die Labore der Antiviren-Hersteller müssen mittlerweile mit über einer halben Million neuer Malware-Dateien pro Monat fertig werden. Daraus ergibt sich auch das Problem, dass die Signaturdatenbanken immer weiter anwachsen und damit zusätzliche Ressourcen fressen. Manche Hersteller wie Avira und Nod32 schaffen es durch kontinuierliches Optimieren und Zusammenfassen, ihre Signaturen auf 16 beziehungsweise 13 MByte zusammenzupacken. Andere wie McAfee kommen mittlerweile auf 45 MByte; die Datenbanken von Panda oder Trend Micro liegen sogar deutlich über 100 MByte.

Genau diese Hersteller mit den ausufernden Signaturdatenbanken sind ganz vorne dabei, wenn es darum geht, Erkennungsfunktionen auszulagern. Bei den sogenannten In-the-Cloud-Funktionen überträgt Antiviren-Software Informationen über ver-

dächtige oder neue Dateien – zumeist einen eindeutigen Hash-Wert – an den Server der Hersteller. Der sieht in seinen Listen nach und antwortet dann mit „gut“ oder „böse“.

Dieses Konzept ist keineswegs neu, sondern wird bereits seit Jahren gegen Spam sowie betrügerische Webseiten angewandt. Auch für die Prüfung von Mail-Anhängen werden solche Verfahren seit Jahren eingesetzt. So ist in G Data's OutbreakShield eine ähnliche Technologie von Commtouch zu finden; Unternehmenslösungen wie Ironport oder Scanservices wie die von MessageLabs arbeiten vergleichbar.

Der von den Herstellern gern beschworene Vorteil dieses Verfahrens ist die Geschwindigkeit. Auf eine akute Trojaner-Welle kann man sehr schnell mit einem passenden Eintrag auf dem Server reagieren. Was sie dabei nicht erwähnen ist, dass

das nur dann gut funktioniert, wenn die Dateien alle exakt gleich sind. Bei McAfee genügt es derzeit schon, ein Byte im Programm zu ändern, um der Erkennung durch Artemis zu entgehen. Der steigenden Zahl von Trojanern oder nachgeladenen Spionageprogrammen, die in individualisierten Versionen verbreitet werden, kann man damit kaum Herr werden. Insbesondere weil die detaillierten Analysen der aktuellen Heuristiken oder gar das Ausführen in einer Sandbox mit den übertragenen Informationen kaum möglich sind.

Einen weiteren Nachteil erwähnen die Hersteller auch nicht. Prinzipbedingt ist man nämlich plötzlich offline schlechter geschützt, obwohl man sich etwa durch bereits heruntergeladene Archive, USB-Sticks oder CDs durchaus infizieren kann. Und wer den guten Rat beherzigt, einen infizierten Rechner sofort

von Netz zu nehmen, hat ebenfalls ein neues Problem. Weil die Virenwächter die Ergebnisse ihrer Online-Abfrage derzeit noch nicht zwischenspeichern, erkennt der Scanner den gerade gemeldeten Trojaner womöglich gar nicht mehr und meldet fälschlicherweise, das System wäre sauber.

Das heißt nicht, dass das Konzept grundsätzlich schlecht wäre. Aber der von den Herstellern gern beschworene Effekt, dass mit In-The-Cloud-Techniken alles besser und vor allem schneller würde, hat zumindest derzeit mit der Realität wenig zu tun. So hatten bei einer aktuellen Trojaner-Welle mit angedrohten Sperren des E-Mail-Zugangs rund ein Drittel der Hersteller, darunter Avira, BitDefender und G Data bereits reguläre Updates parat, bevor die In-the-Cloud-Lösungen von McAfee oder Panda Alarm schlugen. (Andreas Marx)

Antiviren-Software für Windows XP und Vista aus c't 23/08

Programmname	Avira AntiVir Premium	AVG Anti-Virus Professional Edition	BitDefender Antivirus 2009	F-Secure Anti-Virus 2009	G Data AntiVirus 2009
Hersteller	Avira	AVG Technologies	BitDefender	F-Secure	G Data
Homepage	www.avira.de	www.avg.de	www.bitdefender.de	www.f-secure.de	www.GData.de
Programmversion	8.1.0.367	8.0.169	12.0.10.1	9.00 build 148	19.0.0.49
unterstützte Windows-Versionen (Herstellerangaben)	2000/XP (+ 64 Bit)/Vista (+ 64 Bit)	2000/XP (+ 64 Bit)/Vista (+ 64 Bit)	XP (+ 64 Bit)/Vista (+ 64 Bit)	XP/Vista (+ 64 Bit)	XP (+ 64 Bit)/Vista (+ 64 Bit)
Updates pro Woche / durchschnittliche Größe	35 / 95 KByte	14 / 100 KByte	100 / 95 KByte	30 / 150 KByte	160 / 110 KByte
mittlere Reaktionszeit bei Ausbrüchen	0 bis 2 Stunden	6 bis 8 Stunden	2 bis 4 Stunden	2 bis 4 Stunden	0 bis 2 Stunden
Funktionsumfang					
Prüfung bei E-Mail-Empfang/-Versand (Outlook Express und Thunderbird)	✓✓ ¹	✓✓ ¹	✓✓	✓✓	✓✓
Webtraffic-Prüfung	✓	✓	✓ ²	✓ ²	✓
Rettungsmedien: beiliegend / erstellbar / aktualisierbar	-/✓/✓	-/✓/✓	✓/✓/✓	✓/✓/✓	✓/✓/✓
Erkennung					
Signatur: Schadsoftware (469027)	99 %	97 %	98 %	98 %	99 %
Signatur: Ad- und Spyware (16224)	99 %	87 %	89 %	96 %	99 %
Heuristik bei 2 / 4 Wochen alten Signaturen	61 % / 57 %	45 % / 34 %	55 % / 45 %	37 % / 27 %	64 % / 54 %
Win32-Laufzeitpacker	63 %	66 %	86 %	83 %	92 %
Rootkits (erkannt/entfernt) (von 10/9)	8 / 8	9 / 8	9 / 8	9 / 8	9 / 7
Web-Exploits (10)	9	2	3	3	4
Fehlalarme (von 20 000 sauberen Dateien)	3	3	11	3	1
Verhaltenserkennung					
Schadsoftware blockiert / warnt (von 20)	-	-	- ⁶	8 / 0	4 / 6
harmloses Programm gewarnt / blockiert (von 20)	-	-	- ⁶	-	1 / 0
Performance					
Scanzeit 741 MByte: On-Demand/On-Access	71 s / 157 s	208 s / 101 s	115 s / 209 s	114 s / 410 s	95 s / 207 s
Test-Suite (nacktes Vista: 467 s)	626 s	581 s	690 s	1136 s	935 s
On-Demand-Scanner: Scantiefe					
modifizierte Archive erkannt (von 23)	23	21	23	23	23
einfach gepackte Archive (von 11)	11	10	11	11	11
verschachtelte Archive (von 6)	6	5	6	6	6
selbstentpackende Archive (von 6)	6	5	6	6	6
Warnung bei passwortgeschützten Archiven	✓	✓	✓	- ³	✓
eingeb. Objekte: OLE / Web-OLE / Passwort (30/21/8)	30 / 21 / 8	24 / 0 / 8	30 / 21 / 8	30 / 21 / 8	30 / 21 / 8
Bewertung					
Signatur-Erkennung Schadsoftware / Ad- und Spyware	⊕⊕ / ⊕⊕	⊕⊕ / ○	⊕⊕ / ○	⊕⊕ / ⊕⊕	⊕⊕ / ⊕⊕
Erkennung Heuristik / verhaltensbasiert	⊕⊕ / ⊕⊕	○ / ⊕⊕	⊕ / ⊕⊕	○ / ⊕	⊕⊕ / ○
Erkennung Rootkits / Web-Exploits	⊕ / ⊕⊕	⊕ / ⊕	⊕ / ⊕	⊕ / ⊕	⊕ / ○
Signatur-Updates und Reaktionszeiten	⊕⊕	⊕	⊕	⊕	⊕⊕
Bedienung	⊕	○	○	⊕	⊕
Geschwindigkeit	⊕	⊕⊕	○	⊕⊕	⊕
Preis für drei PCs (neu / Verlängerung)	50 € / 50 € ⁵	62 € / 47 € ⁵	30 € / 22 €	50 € / 40 €	40 € / 35 €

¹ standardmäßig werden ausgehende Mails nicht gescannt

² standardmäßig wird HTTP-Verkehr nicht gescannt

³ meldet nur 3 von 4 passwortgeschützten Archiven

⁴ trotz Meldung, dass die verschickte E-Mail einen infizierten Anhang enthält, nicht blockiert, Hersteller hat nachgebessert

⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊕⊕ sehr schlecht ✓ vorhanden - nicht vorhanden k. A. keine Angabe

des Update-Mechanismus konnte auch McAfee nicht liefern.

Als dann Artemis aktiv war, erkannte der Wächter tatsächlich viele Gefahren frühzeitig; McAfees sonst ungenügende Reaktionszeit von 10 bis 12 Stunden reduzierte sich auf den Spitzenwert von 0 bis 2. Doch zu welchem Preis! Ein harmloses Knoppicillin-Update-Skript, der Fast-File-Encryptor von der c't-Jubiläums-DVD und eine Reihe weiterer Programme wurden großzügig mit dem „Generic-Artemis“-Mal gebrandmarkt. Diese Fehlalarmschwemme muss McAfee schleunigst in den Griff bekommen.

Ich wollte doch nur wieder „Eine Stufe höher“.

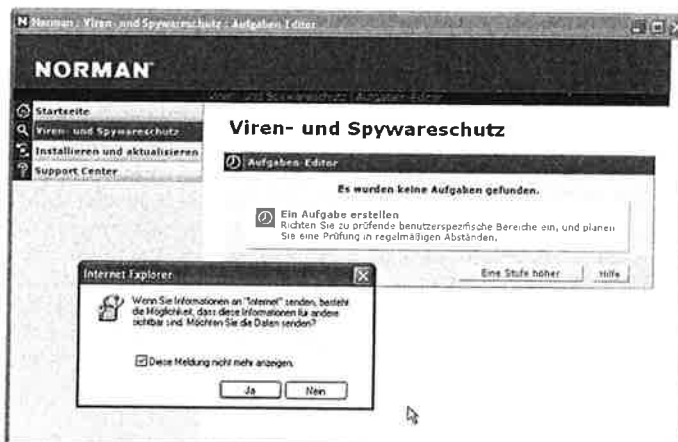
Eigentlich untypisch für ein Antivirus-Produkt ist die eingebaute Firewall mit vielen Einstellmöglichkeiten. Die Bedienung von VirusScan ist umständlich. So braucht man nach einem befundlosen Schnellscan einer Datei drei Mausclicks, bis man weiterarbeiten kann. Hat man das Scanpro-

tokoll einmal aufgespürt, erklärt es, dass zwei verdächtige Dateien gefunden und eine davon in Quarantäne gestellt wurden – welche das waren, muss man an anderer Stelle ermitteln. Schade, dass die renommierte Firma die gute Basis mit sehr guten bis guten Ergebnissen bei Signaturscans und

Heuristik nicht in ein gutes Gesamtpaket umsetzen kann.

Norman Antivirus & Antispyware

Norman wirbt besonders mit seiner Sandbox-Technik, die unbekannte Schädlinge vor dem Ausführen erkennen soll. Im Test erzielte diese Heuristik jedoch kein herausragendes Ergebnis. Die eher durchschnittliche Scan-Engine versieht Norman mit einer grauenhaften Oberfläche. Da erscheint beim Klick auf die Menüoption „Eine Stufe höher“ plötzlich eine Internet-Explorer-Warnung, dass man Informationen ans Internet sende, die für andere sichtbar seien. Den Versuch eines eingeschränkten Anwenders, ein Update vorzunehmen, quittiert



Kaspersky Anti-Virus 2009	Eset NOD32 Antivirus	Norton AntiVirus 2009	Panda Antivirus Pro 2009	Windows Live OneCare
Kaspersky Lab www.kaspersky.de 8.0.0.454 XP (+ 64 Bit)/Vista (+ 64 Bit) 160 / 85 KByte 2 bis 4 Stunden	Eset www.eset.de 3.0.672.0 2000/XP (+ 64 Bit)/Vista (+ 64 Bit) 21 / 60 KByte 2 bis 4 Stunden	Symantec www.symantec.de 16.0.0.125 XP/Vista (+ 64 Bit) 1750 / 10 KByte 0 bis 2 Stunden	Panda Security www.pandasecurity.com 8.00.00 XP(+ 64 Bit)/Vista (+ 64 Bit) 21 / 135 KByte 6 bis 8 Stunden	Microsoft http://onecare.live.com/ 2.5.2900.15 XP/Vista (+ 64 Bit) 21 / 150 KByte 6 bis 8 Stunden
✓/✓	-/- ⁴	✓/✓	✓/✓	-/-
✓	✓	✓	✓	-
-/✓/✓	-/-/-	✓/✓/✓	✓/✓/✓	-/✓/✓
99 %	94 %	99 %	97 %	97 %
98 %	94 %	90 %	96 %	97 %
56 % / 46 %	47 % / 45 %	45 % / 41 %	25 % / 25 %	57 % / 43 %
89 %	87 %	93 %	57 %	76 %
7 / 5	9 / 9	9 / 9	5 / 4	4 / 4
3	2	4	2	0
6	0	1	4	0
6 / 0	-	14 / 5	10 / 2	0 / 9 ⁷
-	-	-	1 / 2	5 / 0 ⁷
50 s / 108 s	62 s / 95 s	48 s / 105 s	48 s / 79 s	102 s / 135 s
632 s	598 s	788 s	766 s	760 s
23	18	20	23	23
11	10	10	11	11
6	6	5	6	6
6	2	5	6	6
✓	✓	-	-	-
30 / 21 / 8	4 / 3 / 8	30 / 21 / 7	30 / 21 / 8	30 / 21 / 7
⊕⊕ / ⊕⊕	⊕ / ⊕	⊕⊕ / ⊕	⊕⊕ / ⊕⊕	⊕⊕ / ⊕⊕
⊕ / ○	⊕ / ⊕⊕	⊕ / ⊕⊕	⊕ / ⊕	⊕ / ⊕⊕
○ / ⊕	⊕⊕ / ⊕	⊕⊕ / ○	⊕ / ⊕	⊕ / ⊕⊕
⊕	⊕	⊕⊕	⊕	⊕
○	○	⊕	⊕	○
⊕⊕	⊕⊕	⊕	⊕	○
50 € / 35 €	65 € / 45 €	40 € / 30 €	45 € / 35 €	50 € / 50 €

⁵ kostenlose Version mit Einschränkungen für Privatgebrauch
⁶ Behaviour Blocking per Default aus

⁷ Firewall meldet Netzwerkaktivität

Trend Micro Internet Security 2009

Trend Micro liefert zumindest in Europa kein reines Antiviren-Produkt mehr, sodass wir die Security Suite auf ihre Schutzfunktion vor Schadsoftware getestet haben. Das Ergebnis fiel erschreckend aus. Dass ein namhafter Hersteller mit seinem hochpreisigen Produkt bei den Signaturscans schlechter abschneidet als das frei verfügbare Open-Source-Projekt ClamAV, stellt seine Existenzberechtigung in Frage. Auch die Werte der Heuristik liegen weit am unteren Ende der Skala. Das können auch die guten Anti-Rootkit-Funktionen nicht ausgleichen.

Die Systembelastung durch den Virenwächter ist durchschnittlich. Der sehr hohe Tabellenwert für die Performance-Testsuite ist vor allem auf ein Problem beim Kopieren von Netzlaufwerken zurückzuführen.

Bei den Verhaltenstests konnten nur fünf Schädlinge den Rechner infizieren. In vielen Fällen schlug allerdings nur die Firewall mit unspezifischen Meldungen Alarm, wie sie auch viele harmlose Programme erzeugen. Es ist fraglich, ob da jeder Anwender wie wir auf „blockieren“ gedrückt hätte. Direkt nach der Installation auf einem sauberen System warnte die Firewall etwa vor verdächtigen Aktivitäten von svchost.exe. Echte Verhaltenswächter können das besser – wie die nächsten beiden Programme demonstrierten.

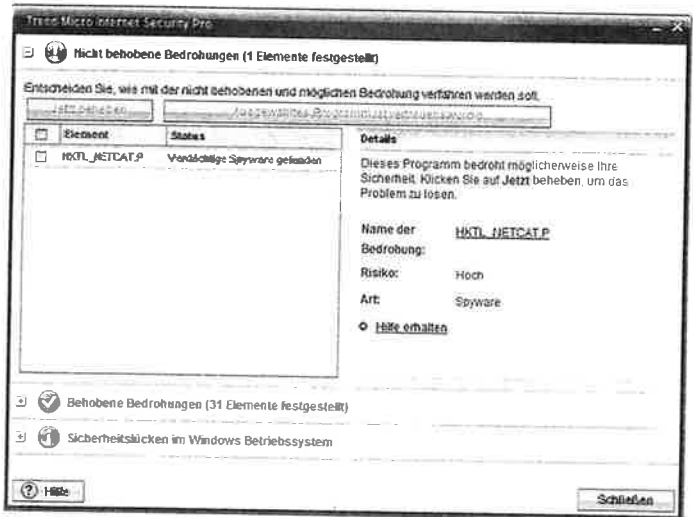
A-Squared Anti-Malware

Der österreichische Hersteller Emsi Software sammelte zunächst Erfahrungen im Bereich Dialer- und Spyware-Abwehr. Dazu entwickelte er ein Modul, das das Verhalten von Programmen in Echt-

das Programm mit der Meldung „Es fehlen die Rechte für das Download-Verzeichnis“. Zwischendurch zeigt ein roter Balken, dass bei einem Scan eine infizierte Datei nicht gereinigt

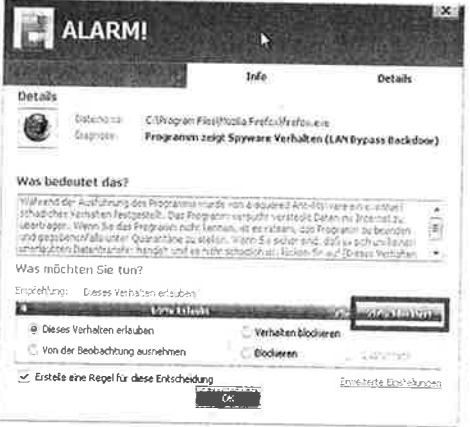
wurde. Welche? Was tun? Fehl-anzeige! Erschwerend hinzu kommt, dass Norman kein einziges der zehn Rootkits entfernen konnte und auch keine Verhaltensanaly-

se vornimmt. Außerdem ist der Scanner spürbar langsamer als seine Konkurrenten. Fazit: Das muss man sich nicht antun, vielleicht bringt die für Anfang 2009 angekündigte Version Besserung.



Wo soll das enden, wenn jetzt schon das universelle Netzwerk-Tool netcat als „verdächtige Spyware“ gemeldet wird.

Immerhin 20 Prozent der A-Squared-Nutzer hielten Firefox tatsächlich für gefährlich. Das spricht gegen den Virenschutz.



Antiviren-Software für Windows XP und Vista

Programmname	A-Squared Anti-Malware 4.0	Avast! Professional	CA Anti-Virus plus CA Anti-Spyware 2009	ClamWin Free Antivirus	Ikarus virus.utilities
Hersteller	Emsi Software	Alwil Software	CA	ClamWin	Ikarus Security Software
Homepage	www.emsisoft.de	www.avast.com	shop.ca.com	de.clamwin.com	www.ikarus.at
Programmversion	4.0.0.60	4.8.1229	10.0.0.157	0.94	1.0.91
unterstützte Windows-Versionen (Herstellerangaben)	XP/Vista	2000/XP(+64Bit)/Vista(+64Bit)	2000/XP/Vista	XP(+64Bit)/Vista(+64Bit)	2000/XP/Vista(+64Bit)
Updates pro Woche / durchschnittliche Größe	43 / 180 KByte	9 / 140 KByte	8 / 80 KByte	16 / 60 KByte	34 / 150 KByte
mittlere Reaktionszeit bei Ausbrüchen	2 bis 4 Stunden	6 bis 8 Stunden	10 bis 12 Stunden	2 bis 4 Stunden	2 bis 4 Stunden
Funktionsumfang					
Prüfung bei E-Mail-Empfang/-Versand (Outlook Express und Thunderbird)	- / -	✓ / ✓	✓ / -	- / -	✓ / -
Webtraffic-Prüfung	-	✓ ¹	-	-	-
Rettungsmedien: beiliegend / erstellbar / aktualisierbar	- / - / -	- / - / -	- / - / -	- / - / -	- / - / -
Erkennung					
Signatur: Schadsoftware (485129)	99 %	99 %	58 %	82 %	99 %
Signatur: Ad- und Spyware (23117)	95 %	92 %	64 %	84 %	95 %
Heuristik bei 2 / 4 Wochen alten Signaturen	51 % / 45 %	31 % / 30 %	18 % / 16 %	19 % / 19 %	51 % / 45 %
Win32-Laufzeitpacker	62 %	49 %	23 %	21 %	62 %
Rootkits (erkannt/entfernt) (von 10/9)	4 / 4	5 / 4	3 / 0	2 / 2	2 / 2
Web-Exploits (10)	-	4	-	-	-
Fehlalarme (von 20 000 / 25 000 sauberen Dateien)	25 / 22	3 / 11	23 / 1	26 / 9	24 / 22
Verhaltenserkennung					
Schadsoftware blockiert / warnt (von 20)	15 / 0	-	-	-	-
harmloses Programm gewarnt / blockiert (von 20)	4 / 5	-	-	-	-
Performance					
Scanzeit 741 MByte: On-Demand/On-Access	64 s / - ³	146 s / 74 s	62 s / 84 s	227 s / - ⁵	66 s / 117 s
Test-Suite vor 1. Komplettscan (nacktes Vista: 467s)	569 s	653 s	945 s	- ⁵	873 s
On-Demand-Scanner: Scantiefe					
modifizierte Archive erkannt (von 23)	11	23	20	17	13
einfach gepackte Archive (von 11)	7	11	10	9	9
verschachtelte Archive (von 6)	4	6	5	4	4
selbstentpackende Archive (von 6)	0	6	5	4	0
Warnung bei passwortgeschützten Archiven	-	✓	-	-	-
Scan eingebetteter Objekte: OLE (max. 30) / Web-OLE (max. 21) / passwortgeschützt (max.8)	9 / 2 / 7	9 / 18 / 7	27 / 6 / 8	20 / 0 / 6	7 / 2 / 7
Bewertung					
Signatur-Erkennung Schadsoftware / Ad- und Spyware	⊕⊕ / ⊕⊕	⊕⊕ / ⊕	⊕⊕ / ⊕⊕	⊕ / ⊕	⊕⊕ / ⊕⊕
Erkennung Heuristik / verhaltensbasiert	⊕ / ○ ²	⊕ / ⊕⊕	⊕⊕ / ⊕⊕	⊕⊕ / ⊕⊕	⊕ / ⊕⊕
Erkennung Rootkits / Web-Exploits	⊕ / ⊕⊕	⊕ / ○	⊕⊕ / ⊕⊕	⊕⊕ / ⊕⊕	⊕ / ⊕⊕
Signatur-Updates und Reaktionszeiten	⊕	⊕	⊕⊕	⊕	⊕
Bedienung	○ ²	○	○	○	⊕
Geschwindigkeit	⊕⊕ ³	⊕⊕	○	-	○
Preis für 3 PCs (Neu / Verlängerung)	50 € / 50 €	85 € / 60 € ^{7,8}	40 € / 35 € (Download)	kostenlos / kostenlos	34 € / 34 €
¹ nicht als Proxy	² Abwertung wegen Fehlalarm	³ Wächter prüft Dateien nicht beim Kopieren	⁴ verzerrt durch ein Problem mit Netzlaufrwerken	⁵ kein Wächter	
⊕⊕ sehr gut	⊕ gut	○ zufriedenstellend	⊕ schlecht	⊕⊕ sehr schlecht	✓ vorhanden
			- nicht vorhanden	k. A. keine Angabe	

zeit beobachtet und analysiert. In Kombination mit der AV-Engine von Ikarus wurde daraus A-Squared Anti-Malware. Allerdings ist bei A-Squared der Wächter so eingestellt, dass er Dateien beim Kopieren nicht prüft und auch beim Start einer Datei kommt der Signaturscan offenbar nicht immer zum Einsatz.

Angesichts der Verwandtschaft verwundert es kaum, dass die Scanergebnisse weitgehend

identisch zu denen der virus.utilities ausfallen – einschließlich der hohen Fehlalarmquote. Erst bei den Tests zur Verhaltenserkennung kann A-Squared seine Stärken richtig ausspielen. Nur ein einziger von zwanzig Schädlingen konnte ganz unbemerkt durchrutschen.

Der Preis, den man für diesen verhaltensbasierten Schutz zu zahlen hat, ist allerdings hoch. A-Squared konfrontiert den An-

wender auch im Normalbetrieb ständig mit Warnungen, die ihm eine Entscheidung abverlangen. So wurde im Test Firefox beim ersten Start als Programm mit „Backdoor-ähnlichem Verhalten“ denunziert. Und als wir dies akzeptierten, erschien prompt eine zweite Warnung, die ihm „Spyware-Verhalten“ attestierte.

A-Squared versucht, den Entscheidungsprozess durch Empfehlungen zu unterstützen. Diese beruhen auf Community-Feedback der Art: „69 Prozent der Anwender haben diese Warnung ignoriert“. Es ist fraglich, ob Mehrheitsentscheidungen geeignet sind, Schadsoftware aufzuspüren. Was hätten wohl diese 69 Prozent bei dem Rootkit angeklückt, das beim Abspielen von Sonys Audio-CDs installiert wurde? Und die

Tatsache, dass A-Squared über zwanzig Prozent der Anwender davon abgehalten hat, ein so bekannt gutartiges Programm wie Firefox zu starten, zeigt, wie viel Unsicherheit das Programm beim Anwender erzeugt.

PC Tools ThreatFire Pro

ThreatFire von PC Tools, das mittlerweile Symantec gehört, verfolgt einen ähnlichen Ansatz. Es ergänzt die hauseigene Verhaltenskontrolle mit einem Viren-Scanner, der auf der wenig bekannten, bulgarischen Virusbuster-Engine beruht, dessen Scan-Resultate jedoch nicht überzeugen. Auch hier schon der Wächter in der Standardeinstellung Ressourcen und mischt sich beispielsweise beim Kopieren nicht

Die Warnungen von ThreatFire geben hilfreiche Hinweise, was sie ausgelöst hat.



McAfee VirusScan Plus 2009	Norman Antivirus & Antispyware	PC Tools ThreatFire Pro	Trend Micro Internet Security 2009
McAfee	Norman Data Defense Systems	PC Tools	Trend Micro
www.mcafee.com/de/default.asp	www.norman.de	www.pctools.com/de	www.trendmicro.de
13.0 Build 218	7.10	4.0.0.8	17.0.1367
2000/XP/Vista(+64Bit)	2000/XP/Vista	2000/XP/Vista	XP/Vista(+64 Bit)
8 / 125 KByte	7 / 120 KByte	10 / 180 KByte	8 / 115 KByte
0 bis 2 Stunden ⁶	6 bis 8 Stunden	6 bis 8 Stunden	6 bis 8 Stunden
✓ / -	✓ / ✓	- / -	✓ / ✓
-	-	-	-
- / - / -	- / - / -	- / - / -	- / - / -
98 %	94 %	80 %	82 %
99 %	91 %	78 %	67 %
46 % / 43 %	42 % / 40 %	29 % / 27 %	23 % / 20 %
80 %	67 %	20 %	13 %
7 / 7	1 / 0	8 / 8	8 / 8
-	-	-	-
8 / 17	0 / 5	3 / 9	0 / 4
-	-	18 / 0	9 / 5
-	-	0 / 0	0 / 0
78 s / 135 s	215 s / 138 s	68 s / - ³	99 s / 134 s
608 s	592 s	583 s	1305 s ⁴
22	15	13	21
11	10	8	11
6	5	0	6
5	0	5	4
-	✓	-	-
30 / 15 / 8	20 / 3 / 7	19 / 3 / 7	30 / 21 / 8
⊕⊕ / ⊕⊕	⊕ / ⊕	⊕ / ⊕⊕	⊕ / ⊕⊕
⊕ / ⊕⊕	○ / ⊕⊕	⊕⊕ / ⊕⊕	⊕⊕ / ○
○ / ⊕⊕	⊕⊕ / ⊕⊕	⊕ / ⊕⊕	⊕ / ⊕⊕
⊕⊕ ⁵	⊕	⊕	⊕
⊕	⊕⊕	○	⊕
○	○	⊕⊕ ³	○
25 € / 25 €	40 € / 30 €	30 € / 30 € ⁸	50 € / 40 €

⁶ mit Artemis, sonst ca. 10–12 Stunden ⁷ kostenlose Version für Privatanwender ⁸ für 10 PCs (Listenpreis für 3 PCs 110,49 €) ⁹ nur Outlook Express

Auch die damals als allgemein recht gut befundene Erkennung und Reinigung von Rootkits ließ diesmal zu wünschen übrig. Nur McAfee und Trend Micro hatten hier etwas Präsentables vorzuweisen. Schon in der Basisdisziplin Signaturerkennung können eigentlich nur Avast, Ikarus und McAfee bestehen – aber alle mit dem Makel hoher Fehlalarmquoten behaftet. Zusammenfassend muss man konstatieren, dass keiner der Kandidaten dem Spitzentrio des letzten Tests das Wasser reichen kann.


Die Entscheidung für den richtigen Virenschutz fällt also nach wie vor zwischen Avira, G Data und Norton. Avira hat hervorragende Scan-Ergebnisse, aber noch keine Verhaltensanalyse vorzuweisen. G Data geht mit zwei Engines zu Werke, was hohe Erkennungsraten, aber leider auch mehr Fehlalarme bedeutet und Systemleistung kostet. Norton hat eine schwächere Heuristik als die beiden anderen, konnte aber mit der Verhaltenskontrolle punkten.

Bei den kostenlosen Lösungen kann sich Avast einen Platz neben Avira und AVG erobern, weil sie als einziger Hersteller darauf verzichten, bei der kostenlosen Version am Schutz zu sparen. AVG verstümmelt die Schutzfunktionen gegen Rootkits; Avira amputiert den Web-schutz und die Spyware-Erkennung. Außerdem mag nicht jeder Aviras Werbeeinblendungen hinnehmen. Dafür müssen Avast-Nutzer eine deutlich schlechtere Heuristik in Kauf nehmen – und diese Oberfläche.

Für die positiven Überraschungen dieses Tests sorgten die Außenseiter. Das Open-Source-Projekt ClamAV hat sich in den letzten Jahren konstant verbessert und steckt mittlerweile als reiner Signaturscanner manch kommerzielles Produkt in die Tasche. Eine gute Wahl für den Zweit-Scanner auf dem Mail-Gateway ist es damit allemal.

Und ThreatFire konnte als Verhaltenskontrolleur überzeugen, der auf ausreichend schlankem Fuß lebt, dass man ihn auch durchaus einem Wächter zur Seite stellen kann, der das noch nicht kann. Mehr Tipps dazu gibt der nächste Artikel. (ju)

Literatur

[1] Jürgen Schmidt, Wachwechsel, 10 Antiviren-Programme im Test, c't 23/08, S. 146 

ein. Und wie auch A-Squared meldet sich ThreatFire nicht im Windows-Sicherheitscenter an. Das erleichtert es, das Programm mit einem klassischen Virenschutz zu kombinieren.

Allerdings geht ThreatFire deutlich sparsamer mit seinen Warnungen zu verdächtigem Verhalten um. Obwohl es sich ebenfalls nur von einem Schädling austricksen ließ – einem anderen als A-Squared – gab es bei der Gegenprobe mit regulären Programmen keine Warnungen. Auch während unseres Testbetriebs machte sich ThreatFire nicht störend bemerkbar. Offenbar hat es eine deutlich besser gepflegte Whitelist als A-Squared. Erst als wir beispielsweise die Exe-Datei des Internet Controllers veränderten, warnte ThreatFire vor

den durchaus verdächtigen Aktivitäten des Sicherheits-Tools.

In ihrer Fixierung auf Anwendertauglichkeit verzichten mittlerweile viele Antiviren-Programme auf Erklärungen, was sie zu einer Warnung veranlasst hat. Nicht so ThreatFire. Hier bekommt man in der Regel durchaus hilfreiche Informationen wie die, dass gerade versucht wird, eine andere Applikation zu manipulieren.

Auch ThreatFire arbeitet mit Community-Unterstützung. Das heißt, es überträgt Informationen über Vorgänge auf dem PC und getroffene Entscheidungen an einen Server. Allerdings verzichtet PC Tools auf Entscheidungshilfen, die darauf beruhen, wie sich andere Anwender entschieden haben. Neben der getesteten Pro-Version gibt es für Privatan-

wender auch eine kostenlose, die sich vom Funktionsumfang nicht unterscheidet. Hauptunterschied ist, dass dann mit dem Abschalten der Berichte an den Server auch die automatische Aktualisierung wegfällt.

Fazit

Insgesamt haben sich vor allem die klassischen Antiviren-Programme in diesem Test nicht mit Ruhm bekleckert. Das zeigt sich schon daran, dass diesmal nur Trend Micro das Verhalten von Programmen analysiert, nur Avast den Webverkehr untersucht und kein einziger Hersteller Rettungsmedien vorzuweisen hatte. Die Programme im November-Test waren da schon deutlich weiter.