Computer Reseller News

14 Antivirenlösungen im Test:

So gut sind Security-Suites wirklich

von magnus.de

08.02.2011

Mit der wachsenden Nutzung des Internets steigern sich auch die potentiellen Gewinne für Hacker und die kriminelle Energie, die sie in ihre Angriffe stecken. Verschiedenste Anbieter versprechen, mit ihren Security-Suiten sicheren Schutz vor solchen Angriffen – nicht immer zu Recht, wie unser Test der 14 größten Lösungen zeigt.

Die Zeiten, als sich die Virenschreiber gegenseitig am Schulhof auf die Schultern klopften, sind vorbei. Die Internetkriminellen sind inzwischen so gut organisiert wie die Cosa Nostra. Den Tätern geht es heute nicht mehr um Anerkennung unter Skript-Kiddies, sondern darum, in möglichst kurzer Zeit viel kriminelles Geld zu machen. Mit Attacken auf Kreditkartendaten, Bankkontoverbindungen oder dem Verkauf von vorgetäuschter Antiviren-Software (siehe: »Das Geschäft mit Fake-AV blüht« [1]) werden Millionen umgesetzt.

Was früher die Entführung reicher Millionärssöhne und -töchter war, ist heutzutage die durch falsche Sicherheitssoftware verursachte Festplattenverschlüsselung mit anschließender Freipressung des Entschlüsselungscodes. Hier kann man wirklich von Online Organized Crime sprechen. Es geht hier nicht um Einzelfälle – es trifft zigtausende Anwender. Der Schaden wird weltweit auf circa 55 Milliarden Dollar geschätzt, allein in Deutschland redet man von 18 Milliarden Dollar. Und die Zahlen steigen stetig.

Den Kriminellen wird es teilweise auch sehr einfach gemacht. Oft öffnet ein ungepatchtes Windows den Eindringlingen Tür und Tor, mitunter mangelt es an Security-Software oder diese versagt, weil sie veraltet ist. Ohne Absicherung durch eine Security-Suite oder die Kombination Antiviren-, Anti-Spyware- und Firewall-Tool, sollte man sich gar nicht mehr ins Internet trauen.

Unsere Schwesterzeitschrift PC Magazin hat die neuen Versionen von 14 Internet-Security-Suites und den dazugehörigen Pendants an Gratisversionen getestet. Vorweggesagt, die Free-Versionen der einzelnen Hersteller (Ausnahme Panda) stehen in der Malware-Erkennung den kostenpflichtigen Versionen in nichts nach. Sie haben aber den entscheidenden Nachteil, dass gewisse komfortable Features fehlen, wie z.B. E-Mail-Scanner, Spam-Filter, Browser-Filter oder Firewall (siehe auch "Kostenlos vs. kostenpflichtig").

DIE TESTERGEBNISSE IM SCHNELLDURCHLAUF

BILDERGALERIE: ANTIVIREN-TEST



Klicken Sie auf ein Bild, um die Bildergalerie zu öffnen.

DIE FREIHEIT ÜBER DEN WOLKEN

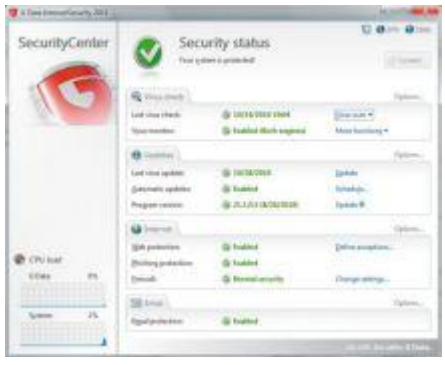
Immer mehr Hersteller setzen auf Cloud-Funktionen. Der Virenscanner erzeugt auf dem PC eine Prüfsumme von verdächtigen Dateien und schickt diese zusammen mit Zusatzinformationen an den Cloudserver. Dieser Server stellt in Millisekunden fest, ob die Datei bereits bekannt und gegebenenfalls auch infiziert ist.

Dies verringert die Signatur-Datei-Größe auf dem PC, birgt jedoch auch Gefahren in sich. Die alte Weisheit, dass man einen PC vom Internet trennen soll, sobald ein Virus entdeckt wurde, gilt heutzutage bei diesen Produkten nicht mehr. Hier kann es passieren, dass das Tool ein Virus in der Cloud entdeckt hat, diesen aber nach dem Trennen der Internetverbindung auf einmal nicht mehr kennt.

Das erschwert das Säubern eines infizierten PCs mit diesen Produkten unter Umständen. Ohne Internetverbindung ist der Anwender bei Weitem nicht so gut geschützt wie mit, das spielt vor allem beim Datenaustausch via DVD oder USB-Stick eine große Rolle.

Was passieren kann, wenn es einem Hacker gelingen sollte, den Fingerprint eines Virus in die White-List-Datenbank eines Herstellers einzuschleusen, möchte man sich gar nicht ausdenken. Unserer Meinung kann der Cloud-Service als Ergänzung gesehen werden, der Anwender sollte sich jedoch nicht allein auf die Cloud-Technologie verlassen. Maßgeblich sind immer noch eine gute lokale Erkennungsrate und eine solide Heuristik.

MEHR FEHLALARME IN DER CLOUD



G-Data hat die höchste Erkennungsrate im ganzen Testfeld. Die zwei Engines verlangsamen aber den Einsatz.

Obwohl nach wie vor DVDs und USB-Sticks eine regelmäßige Infektionsquelle darstellen, hat sich in der letzten Zeit der Infektionsvektor in Richtung Internet und E-Mail verlagert.

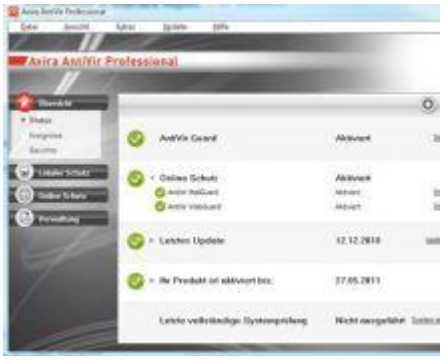
Wir verwenden hierfür die Ergebnisse eines Tests, den AV-Comparatives in Zusammenarbeit mit der Fakultät für Informatik der Uni Innsbruck entwickelt hat, den Whole-Product-Dynamic-Test (siehe "Testergebnisse"). Dabei werden 5.000 infizierte Web-Seiten aufgerufen und das Verhalten der Sicherheitsprogramme ausgewertet.

Die Grundausstattung einer Security-Suite ist immer noch die Virensuche, die Erkennung von Schadsoftware. Die Tester ließen die Scanner auf über 900.000 Virensamples los, die jeweils nicht älter als sieben Monate waren. Vor allem bei der heuristischen Erkennung muss der Hersteller die richtige Balance zwischen Aggressivität und Gutmütigkeit finden, um Fehlalarme zu vermeiden.

Im gesamten Testfeld hat sich leider kein einziges Produkt gefunden, das komplett ohne falschen Alarm auskommt. Ein solcher kann zu größerem Schaden als eine Infektion führen. Manche Hersteller setzen hier auf die Cloud, indem sie durch den Abgleich der Hashes mit der White-List gegenchecken.

Allerdings konnten wir beobachten, dass cloudgestützte Programme deutlich mehr Fehlalarme erzeugten. Viele Hersteller führen eine lokale Whitelist, die bekannte Programme privilegieren. Zudem bieten viele Suiten einen Spielemodus, der Meldungen unterdrückt und nur wichtige Schutzfunktionen aufrechterhält.

SYSTEMBREMSEN



In den kostenlosen Versionen der Antiviren-Programme fehlen Features wie Firewall, Spam-Filter und Webguard.

Idealerweise läuft die Securtiy-Suite im Hintergrund. Das heißt aber nicht, dass sie keine Leistung braucht. Die Überprüfung des Internetverkehrs und der Dateien kann im Gegenteil erhebliche Leistungseinbußen zur Folge haben. AV-Comparatives hat im Labor diese Systemfresser getestet.

Mit Alltagsaufgaben wie dem Kopieren von Dateien, dem Öffnen von Office-Dokumenten, dem Encodieren von Musik und Videos sowie dem Downloaden von Dateien und Internetsurfen wurde dem Übel auf den Grund gegangen.

Um für alle Anbieter die gleichen Voraussetzungen zu schaffen, wurde der Test auf einem einzigen PC durchgeführt, der in einem klimatisierten Raum mit exakt gleichbleibender Temperatur betrieben wurde. Jeder Hersteller wurde mit zehn Durchläufen getestet, woraus ein Durchschnittswert ermittelt wurde, um Schwankungen zu vermeiden.

Auch auf systeminterne Beschleunigung wurden die Hersteller überprüft. Einige Hersteller setzen auf Prüfsummenbeschleunigung. Wird eine Datei einmal als sauber klassifiziert, wird dies bis zum nächsten Update, das heutzutage oft in sehr kurzen Abständen erfolgt, nicht mehr überprüft. Andere verwenden Whitelisting von bekannten Programmen und Dateien.

Egal ob Fingerprinting oder Whitelisting, beide Methoden führen zu spürbaren Geschwindigkeitsvorteilen, die im Performance-Test berücksichtigt wurden. Hier fanden jeweils Testdurchläufe ohne Fingerprinting und mit Fingerprinting statt. Aus diesen Läufen wurde ein Durchschnittswert ermittelt.

DIE MESSERGEBNISSE

Geschwindigkeit ist jedoch nicht alles: Der schnellste Antiviren-Scanner nützt nichts, wenn er nichts erkennt. Man sollte unbedingt einen Scanner, der eine hohe Erkennungs-rate hat, einem Scanner, der zwar schnell ist, aber weniger erkennt, vorziehen.

Drucken (Wählen Sie bitte bei Bedarf die Option "Querformat" in Ihren Druckeinstellungen)

	Virensuche (in %)	Wächter (in %)	Fehlalarme (Stück)	Performance (Punkte)	Ausstattung (Punkte)
Avast	99,3	96,4	9	179	324
AVG	98,3	97,1	19	177	279
AVIRA	99,8	98,7	10	175	286
Bitdefender	99,3	95,2	4	146	345
ESET	98,6	96,1	6	160	335
F-Secure	99,2	98,8	2	177	306
G DATA	99,9	97,7	15	152	274
Kaspersky	98,3	98,3	46	160	352
McAfee	99,4	97,4	24	172	268

Microsoft MSE	97,6	98,7	3	179	133
Panda	99,2	96,8	98	172	329
PC Tools	98,1	95,8	7	123	302
Symantec	98,7	98,5	9	177	334
TrendMicro	90,3	95,8	23	143	280

TESTVERFAHREN

Testlabor von AV-Comparatives wird Sicherheitssoftware auf Fehler überprüft.

Details zum Testverfahren: Für die Virenerkennung und Performance-Messung arbeiten wir mit dem unabhängigen, österreichischen Testlabor AV Comparatives unter der Leitung von Andreas Clementi zusammen. Das Labor veröffentlicht seit über sieben Jahren auf www.av-comparatives.org regelmäßig Tests von Anti-Viren-Software.

Die Ergebnisse stehen kostenlos zur Verfügung. 2010 hat AV-Comparatives gemeinsam mit der Universität Innsbruck den Whole-Product-Dynamic-Test entwickelt. In den Monaten Juli bis November 2010 wurden 5000 infizierte Web-Seiten aufgerufen und das Verhalten der Sicherheitsprogramme ausgewertet.

Das Labor beurteilte die Suiten danach, ob sie den Benutzer vor der Malware schützen oder nicht. Ob das durch URL-Blocker, beim Speichern auf die Festplatte oder mittels Behaviour-Blocker beim Ausführen der Schadsoftware passiert, machte für die Tester keinen Unterschied.

Manche Produkte wollten teilweise die Entscheidungen dem Benutzer aufbürden, allen voran Norton und Kaspersky. Solche Meldungen sind auch für Computerexperten oft schwer verständlich, wie soll sich ein Laie damit auskennen? Im Test wurde solch eine unvollständige Erkennung nur zur Hälfte gewertet, da der Laie hier auch nur eine Trefferquote von 50 Prozent hat.

Um die Performance der Produkte zu ermitteln, erledigten wir auf identischen Testplattformen eine Reihe von rechenintensiven Arbeiten, die die Leistung der Virenprogramme ausgiebig forderten, insbesondere Daten entpacken, entschlüsseln, kopieren, verschieben und konvertieren.

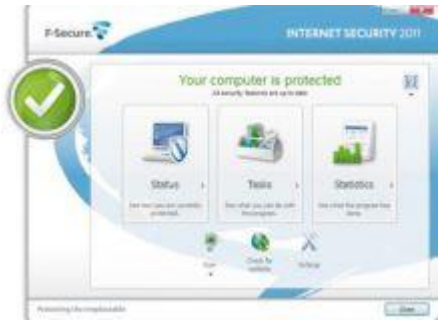
Hinzu kam ein Test mit PC-Mark (www.futuremark.com). Jedes Anti-Viren-Programm musste den kompletten Performance-Test zehn Mal durchlaufen. Der Wert in der Tabelle ist ein Punktewert.

BEWERTUNG UND FAZIT

So bewerten wir

Positive Punkte gab es nur für Virensuche (on demand) und den Wächter (Whole-Product-Dynamic-Test) und zwar höchstens jeweils 50. Von da ab gab es nur noch Abzüge, um sicherzustellen, dass kein Produkt besser sein kann als die Virenerkennung. Für Fehlalarme gab es bis zu zwanzig Punkte Abzug.

Diese drei Kriterien: Virensuche + Wächter – Fehlalarme führen zur Wertung Virenschutz (in der großen Übersichtstabelle auf den folgenden Seiten). Für die Gesamtwertung spielten Performance, Ausstattung und Bedienung eine Rolle, aber auch nur negativ, als Abzüge bei Mängelerscheinungen.



Testsieger F-Secure glänzt mit dem besten Gesamtschutz und einer guten Performance.

Punktemäßig liegt das Schwergewicht der Wertung eindeutig auf dem Virenschutz, da man sich an eine Bedienung gewöhnen kann und die Ausstattung für den Anwender nur beim Kauf eine Rolle spielt. Er sollte sich vorher überlegen, welche Features er benötigt, und dann das passende Produkt wählen.

Fazit:

Bei der reinen Virenerkennung sind alle Programme auf der sicheren Seite, ganz vorne mit dabei Avira, F-Secure, Kaspersky und Symantec. Deutliche Unterschiede treten erst bei den Fehlalarmen auf. 98 Fehlalarme bei Panda während des Tests oder 46 bei Kaspersky sind sehr stark verbesserungswürdig.

Als Gesamtpaket liegt F-Secure an der Spitze und verbindet eine sehr gute Erkennung mit hoher Performance und guter Ausstattung. Dabei ist es nicht einmal teuer und ergäbe rechnerisch auch den Preistipp. Wer auf Geschwindigkeit aus ist, landet unweigerlich bei Avast oder dem kostenlosen Security Essentials von Microsoft. Beide sind auch bei der Erkennung ganz oben dabei.

DIE TESTERGEBNISSE AUF EINEN BLICK

Drucken (Wählen Sie bitte bei Bedarf die Option "Querformat" in Ihren Druckeinstellungen)

Hersteller	F-Secure	Symantec	Avast	Avira	ESET	AVG	Bitdefend
Produkt	Internet Security 2011	Internet Security 2011	Internet Security 5	Premium Security Suite 10	Smart Security 4	Internet Security 2011	Internet S 2011
Preis 1 User (3 User)/Jahr	29,95 (39,95) Euro	39,99 (59,99) Euro	44,95 (59,95) Euro	39,95 (60,15) Euro	33,53 (41,93) Euro	43,95 (54,95) Euro	39,95 (49
Betriebssysteme	Win XP (nicht 64 Bit), Vista, 7	Win XP, Vista, 7	Win XP, Vista, 7	Win XP, Vista, 7	Win XP, Vista, 7	Win XP, Vista, 7	Win XP, V
Internet	www.f-secure.de	www.symantec.de	www.avast.de	www.avira.de	www.eset.de	www.avg.de	www.bitd
Ranking im Testfeld	1. Platz (Testsieger)	2. Platz	3. Platz	4. Platz	5. Platz	6. Platz	7. Platz
Gesamtwertung [100 max.]	sehr gut 90 %	sehr gut 90 %	sehr gut 89 %	sehr gut 88 %	sehr gut 86 %	gut 85 %	gut 84 %
Punkte Virenschutz	[99]	[97]	[96]	[97]	[96]	[94]	[96]
Sicherheitsfunktionen							
On-Demand Scan	✓	✓	✓	✓	✓	✓	✓
On-Access Scan	✓	✓	✓	✓	✓	✓	✓
Intrusion Prevention	✓	✓	✓	✓	✓	-	✓
Browser Sandbox	✓	-	✓*	-	-	-	-
Cloud Funktionen	✓	✓	✓	✓	✓	✓	✓
Scan-Beschleuniger (Fingerprinting etc)	✓	✓	✓	-	✓	✓	✓
E-Mail Scanner	✓	✓	✓	✓*	✓	✓	✓

BILDERGALERIE: ANTIVIREN-TEST

Klicken Sie auf ein Bild, um die Bildergalerie zu öffnen.

[1] http://www.crn.de/security/artikel-83398.html

VERWANDTE ARTIKEL

- **Cyberangriff auf US-Technologiebörse – Russischer Hackerangriff auf das Nasdaq-Netzwerk (http://www.crn.de/security/artikel-88736.html)**
- **Praxistipps: Mobile Rechner konfigurieren – So richten Sie ihr Notebook optimal ein (http://www.crn.de/hardware/artikel-88713.html)**
- **Unified-Content-Security-Lösung – Eine für alles (http://www.crn.de/security/artikel-88717.html)**
- **Einsatz von iOS- und Android-Geräten – Mobile Sicherheitsplattform für Unternehmen (http://www.crn.de/security/artikel-88749.html)**
- **Bilanz für 2010 – Check Point überspringt die Milliardenmarke (http://www.crn.de/security/artikel-88690.html)**
- **EU-Kommission – Intel darf McAfee übernehmen - unter Auflagen (http://www.crn.de/hardware/artikel-88530.html)**
- **Sophos-Veranstaltungsreihe – Lohnendes Geschäft Cyberkriminalität (http://www.crn.de/security/artikel-88483.html)**
- **Befragung des Eco-Internetverbands – Cloud-Sicherheit ist Top-Thema 2011 (http://www.crn.de/security/artikel-88664.html)**
- **Münchner Sicherheitskonferenz – Cyberwar nicht mehr nur Science-Fiction-Szenario (http://www.crn.de/panorama/artikel-88655.html)**