

Jürgen Schmidt

# Der Trojaner-Test

## So gut schützen Virenwächter

**In unserem Trojaner-Test dürfen 20 Antiviren-Programme beweisen, dass sie tatsächlich bei einem versehentlichen Klick auf einen Trojaner schützen. Manchen gelang das deutlich besser als anderen.**

**A**ntiviren-Programme müssen gerade dann schützen, wenn der Anwender eine Dummheit macht. Also wenn er etwa auf eine Trojaner-Mail hereingefallen ist und selbst eine böartige Datei startet, die seinen Rechner mit Schadprogrammen infizieren will. Denn das Problem ist in den letzten Jahren eher schlimmer geworden als besser. Rechnungen, Lieferbenachrichtigungen oder Sicherheitsnachfragen – immer mehr Kommunikation läuft über E-Mail ab. Und immer bessere Imitate lassen sich kaum noch von den richtigen und dann auch tatsächlich wichtigen Nachrichten unterscheiden.

„Guten Tag Herr Schmidt, mit dieser E-Mail erhalten Sie Ihre aktuelle Mobilfunk-Rechnung“ – ob

das jetzt wirklich von der Telekom, von Vodafone oder Arcor stammt oder doch ein gut gemachter Versuch ist, mich zum Öffnen des Anhangs oder des Links zu verleiten, kann ich an Äußerlichkeiten nicht mehr erkennen. Der Name stimmt, Ansprache und Rechtschreibung auch. Ich persönlich würde wohl misstrauisch werden, wenn an der Mail statt einer PDF-Datei ein ZIP-Archiv dranhinge. Aber bei meiner Mutter bin ich mir schon nicht mehr sicher, ob sie nicht doch das ZIP-Archiv und die dort enthaltene Datei „Rechnung\_2014\_09\_1123539708687.pdf.exe“ öffnen würde. Selbst wenn das „.exe“ am Ende des Dateinamens ihr Misstrauen wecken würde – Windows versteckt diese infor-

mative Dateieindung standardmäßig.

### Test-Aufbau

Genau diesen Fall stellt der Trojaner-Test nach. Wir haben über zwei Wochen hinweg aus allen auf dem Heise-Server ankommenden E-Mails alle ausführbaren Dateien herausgefiltert. Diese wurden dann direkt zu einem Testlabor geschickt. Das Ganze reicherten wir mit den ausführbaren Inhalten an, die sich in den Spam-Traps des nix-Spam-Projekts der iX-Kollegen verfinden.

Interessant dabei: Es waren zwar ein paar kaputte Dateien dabei – aber keine einzige wirklich harmlose Datei, über deren

Nicht-Zustellung jemand erbost gewesen wäre. Es ist somit ernsthaft zu überlegen, ob man nicht von vornherein alle Mails mit ausführbaren Inhalten komplett sperrt.

Insgesamt fast 900 Schädlinge sammelten wir auf diesem Weg ein. Die wurden dann möglichst bald nach dem Eintreffen auf 20 Rechnern gestartet, auf denen jeweils eine Antiviren-Software mit aktuellen Updates installiert war. Das System hatte dabei eine funktionierende Internet-Verbindung – die Trojaner konnten also Unrat aus dem Netz nachladen. Genauso konnten aber auch die Wächter zusätzliche Informationen aus der Cloud einholen. Nach etwa 5 Minuten brach der Test ab und das System wurde gründlich auf Anzeichen einer Infektion untersucht. Danach wurde es für den nächsten Test wieder in einen sauberen Zustand versetzt. Die Basis war übrigens Windows 7 mit einer kleinen Auswahl zusätzlicher Software, die auf vielen PCs so anzutreffen ist.

Bei diesem Test werden die Schädlinge also tatsächlich ausgeführt und nicht wie etwa bei einem Scan mit Virustotal nur die verdächtigen Dateien analysiert. Das bedeutet, dass den Wächtern viel mehr Informationen zur Verfügung stehen als bei einem rein statischen Test. Sie können unter anderem das Verhalten des Schädlings beobachten und bei ausreichend vielen verdächtigen Aktivitäten einschreiten. Allerdings sind solche dynamischen Tests in Echtzeit sehr aufwendig. Besonders schwierig gestaltet sich die Auswertung der Ergebnisse. Wir arbeiteten dazu wie beim letzten Trojaner-Test mit dem in Österreich beheimateten Testlabor AV-Comparatives zusammen.

### Sippenhaft

Deren Virenexperten sortierten die Schädlinge bei einer nachträglichen Analyse in 82 Malware-Familien ein. Darunter fanden sich unter anderem rund 80 ZBot-Variationen. Diese gehören zum Online-Banking-Schädling Zeus, der im Untergrund als Baukasten-Trojaner gehandelt wird. Viele ambitionierte Kriminelle kaufen sich einen Zeus-Bausatz und erstellen dann über das grafische User-Interface ihre jeweils maßgeschneiderte ZBot-Version,

die sie dann in Wellen über Bot-Netze in die Mailboxen ihrer ansivierten Opfer spülen.

Besonderes interessant auch, dass sich rund 70 Exemplare des Papras-Trojaners in den E-Mails fanden. Der enthält spezielle Rootkit-Funktionen, um sich tief in Windows zu verstecken, und hat es dann vor allem auf Passwörter und andere Zugangsdaten abgesehen. Darüber hinaus gab es unzählige unspezifische Downloader und Injector-Schädlinge, die das eigentliche Schadprogramm erst übers Netz nachladen. Teilweise geschieht dies erst, nachdem die Schutzfunktion von Antiviren-Software ausgehebelt wurde.

Damit etwa die Erkennung einer häufig auftretenden ZBOT-Variante die Testergebnisse nicht allein durch ihre Masse dominiert, haben wir jede Malware-Familie nur einmal gewertet. Eine positive Bewertung gab es nur, wenn wirklich alle Varianten erkannt und blockiert wurden.

### Ergebnisse

Wer die im Kasten rechts grafisch aufbereiteten Ergebnisse betrachtet, wundert sich vielleicht, dass dort keineswegs 20, sondern nur 13 Antiviren-Programme aufgeführt sind. Das kommt daher, dass wir bei mehreren Herstellern zwei Versionen parallel getestet haben. So interessierte uns, ob die Microsoft Security Essentials auf Windows 7 anders schützen als der in Windows 8.1 eingebaute Virenschutz namens Windows Defender.

Ebenso wollten wir wissen, ob die kostenlosen Versionen von

Avast, AVG, Avira und Panda weniger Schutz bieten als die kostenpflichtigen. Und wir wollten klären, ob – wie vom Hersteller immer wieder betont – Kasperskys Internet Security Suite besser schützt als das reine Antiviren-Programm.

Um es kurz zu machen: Zumindest in diesem Test-Szenario konnten wir keinerlei Unterschiede ausmachen. Die Ergebnisse der Geschwister waren in allen Fällen identisch. Wenn das kostenpflichtige Avira einen Trojaner neutralisierte, gelang dies der kostenlosen Version ebenso. Und MSE schützt genauso gut beziehungsweise eher schlecht wie der Windows Defender. Deshalb gibt es bei den Ergebnissen pro Hersteller nur eine Spalte. Bei Avast testeten wir übrigens noch die Version 2014, nachdem uns der Hersteller versichert hatte, dass das Update auf die kurze Zeit später erscheinende Version 2015 keine gravierenden Änderungen an der AV-Engine mit sich bringen würde.

### Die Besten

Anders als beim letzten Trojaner-Test vor knapp zwei Jahren gab es dieses Mal mehrere Programme, die eine exzellente Schutzwirkung entfalteten. Esets NOD32, F-Secure, Kaspersky, Symantec und – für uns überraschend – Trend Micro konnten in über 90 Prozent der getesteten Fälle ihr System sauber halten. Avast verpasste diese Marke nur ganz knapp. Damit verfehlte der beste der auch kostenlos erhältlichen Testkandidaten nur hauch-

dünn eine Spitzenwertung; der von Avast gebotene Schutz lag aber durchaus auf Augenhöhe etwa mit dem kostenpflichtigen Norton Security.

G Data hätte sich eigentlich ebenfalls ganz oben eingereiht. Allerdings war sich der G-Data-Wächter sehr viel öfter als die anderen nicht so ganz sicher und fragte beim Anwender nach, wie er denn mit dieser Datei verfahren wolle. Dafür stehen die vielen gelben Felder in der Ergebnis-Präsentation. Der Anwender musste in rund einem Drittel der

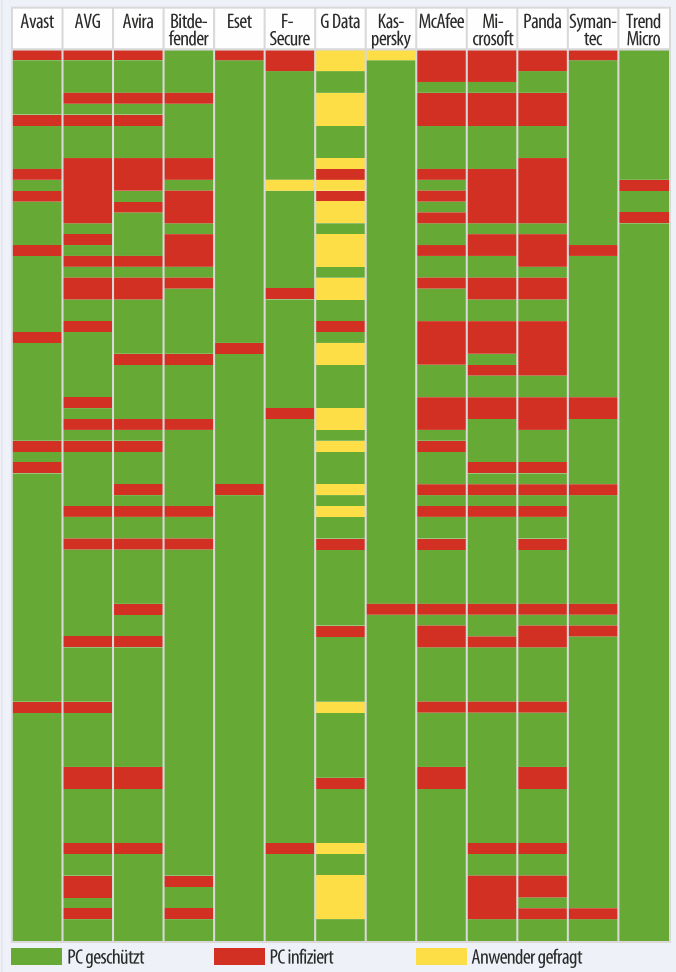
Fälle selbst entscheiden, ob er das Programm ausführen oder es blockieren und in die Quarantäne verschieben möchte. Dies werteten wir lediglich als teilweise geschützt, was zu einer Abwertung in der Gesamtnote von G Data führte.

Dass der Trojaner-Test kein harmloser Dummy ist, den jeder schafft, beweisen die schlechten Ergebnisse einiger Kandidaten. Microsofts Basisschutz versagte bei rund 40 Prozent aller Trojaner. Das wurde nur noch von der Ausfallquote von Panda

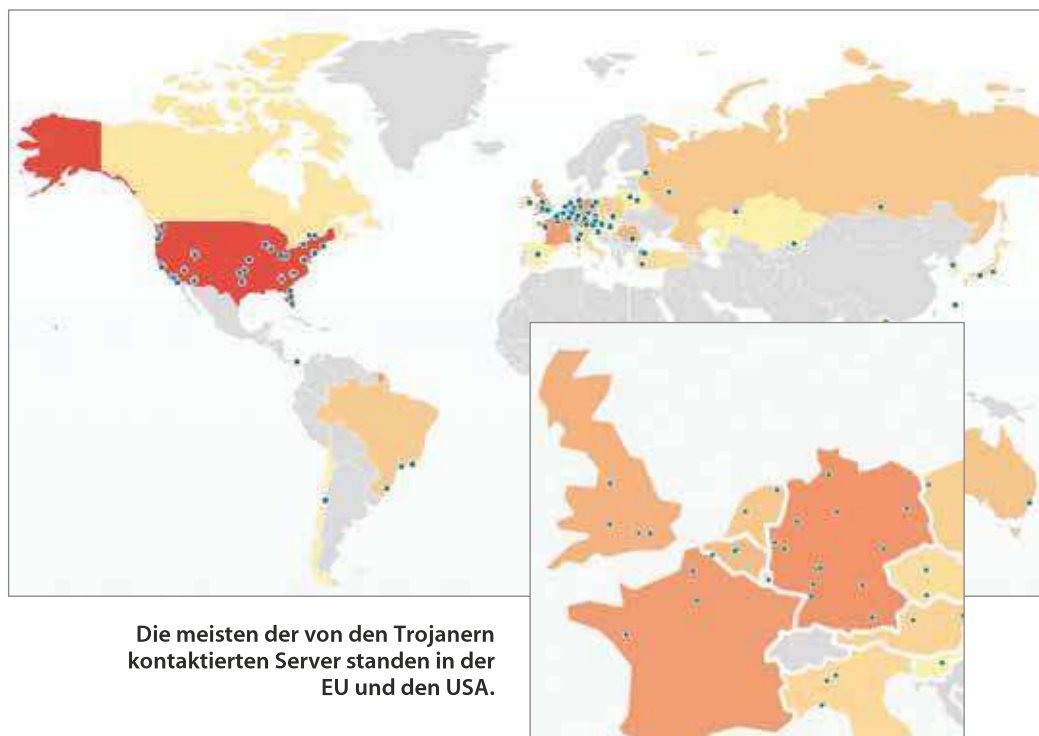
## Trojaner-Testergebnisse

Jeder Balken steht für eine Schädlingsfamilie, deren Angriffe entweder abgewehrt wurden (grün) oder zu einer Infektion des PC führten (rot). Bei gelb musste der Anwender entscheiden, was zu tun ist. Die guten Wächter haben also überwiegend grüne Spalten; bei denen mit viel Rot rutschten viele Trojaner durch.

Die Ergebnisse sind übrigens nach der Zeitspanne zwischen Eintreffen der Mail und dem tatsächlichen Start auf dem Testsystem sortiert. Man kann deutlich erkennen, dass bei den kürzeren Delays mehr Rot auftritt, während unten die komplett grünen Bereiche dominieren. Die Chancen, einen Trojaner abzuwehren, steigen also, wenn man eine Mail erst einen Tag später öffnet.



G Data überließ in vielen Fällen dem Anwender die Entscheidung, was zu tun ist.



Die meisten der von den Trojanern kontaktierten Server standen in der EU und den USA.

unterboten, dessen hauptsächlich Cloud-basierte Virenwächter kaum mehr als eine Fifty-fifty-Chance auf Schutz boten. Darauf sollte man sich genauso wenig verlassen, wie auf Intels McAfee und AVG, die bei rund einem Drittel aller Schädlinge passen mussten.

Vor der abschließenden Bewertung noch ein paar erklärende Worte zur Bedeutung dieses Tests – und zu dem, was er nicht leisten kann. Das TestszENARIO ist darauf angelegt, den Schutz vor massenhaft verbreiteter Schad-Software etwa für den Online-Banking-Betrug, der Erpressung mit verschlüsselten Daten und Ähnlichem auf die Probe zu stellen. Gezielten Attacken etwa im Bereich der Industrie-Spionage, wo maßgeschneiderte Malware-Unikate zum Einsatz kommen, hat Antiviren-Software bekann-

termaßen wenig entgegenzusetzen.

Wir haben mit diesem Trojaner-Test auch nur genau einen Infektionspfad getestet: Trojaner, die den Anwender via E-Mail erreichen. Das ist nach unserer Erfahrung ein sehr wichtiges Problem, denn viele der von uns untersuchten Rechner sind tatsächlich auf diesem Weg infiziert worden. Aber es ist nicht der einzige. Das zweite wichtige Einfallstor sind böartige Webseiten, die gezielt Sicherheitslücken in veralteter Software ausnutzen, um das System zu infizieren.

Wir fanden jedoch keinen Weg, den Schutz vor solch böartigen Webseiten sinnvoll, also herstellerunabhängig und zeitnah zu testen. Unser Eindruck ist jedoch, dass sich die Ergebnisse nicht grundsätzlich von denen des Trojaner-Tests unterscheiden

würden. Denn häufig ist das nur ein alternativer „Vertriebsweg“ für den gleichen Unrat.

Außerdem ist die Zusammensetzung der Schädlinge natürlich durch deren Ziel – also die Heise-Mail-Adressen und die Spam-Traps von nixSpam geprägt. Man muss davon ausgehen, dass die Ergebnisse insbesondere in anderen Regionen der Welt anders ausfallen würden. Überhaupt sollte man die exakten Prozentzahlen in den Testergebnissen nicht überstrapazieren. Allein durch eine etwas andere Gruppierung nach Familien schwanken diese um einige Prozent hin und her. Die Tendenz der Ergebnisse bleibt dabei jedoch erhalten und kann somit als aussagekräftig betrachtet werden.

Allerdings haben wir hier nicht getestet, wie viele Fehlalarme die Programme produzieren. Immer-

hin ist es eigentlich ganz simpel, einen Virenwächter mit hundertprozentiger Erkennungsrate zu bauen: Der verbietet dann einfach alles. Mehr dazu, wie die besseren der Virenwächter mit potenziell verdächtigen Dateien umspringen, verrät der auf Seite 126 folgende Praxistest.

### Fazit

Der Test war schwierig zu bestehen; keiner der Wächter konnte alle Schädlinge abfangen. Wirklich erstklassigen Schutz demonstrierten denn auch nur die Virenwächter von Eset, Kaspersky und Trend Micro, denen nur vereinzelte Trojaner durchrutschten.

Das breite Mittelfeld bilden F-Secure, G Data, Symantec, Avast bis hin zu Bitdefender und so gerade noch Avira. Diese Programme kann man durchaus guten Gewissens einsetzen – insbesondere, wenn man die Ergebnisse aus dem Anwendungstest ab Seite 126 mit einbezieht.

„Besser als gar nichts“ ist wohl das beste, was man über den Schutz der Virenwächter von AVG, McAfee, Microsoft und Panda sagen kann; verlassen sollte man sich darauf jedoch nicht. Wer Wert auf mehr als rudimentären Basisschutz legt, sollte sich lieber die anderen Kandidaten noch mal genauer ansehen.

Die kostenlosen Programme schnitten ohne Ausnahme genauso gut oder schlecht ab wie die käuflich zu erwerbenden Geschwister. So richtig überzeugen konnte aber nur der Schutz von Avast; Avira geht so grade noch. Microsofts Virenschutz kann da nicht mal ansatzweise mithalten und AVG AntiVirus Free 2015 und Pandas Free Antivirus sind keine Alternativen, die den Umstieg vom eingebauten Windows Defender lohnend erscheinen lassen. (ju)

## Zusammenfassung der Testergebnisse

Hersteller	Avast	AVG	Avira	Bitdefender	Eset	F-Secure	G Data	Kaspersky	McAfee	Microsoft	Panda	Symantec	Trend Micro
Produkt(e)	avast! Free Antivirus 2014 / avast! Pro Antivirus 2014	AVG AntiVirus 2015 / AVG AntiVirus Free 2015	Avira Anti-virus Pro / Avira Free Antivirus	Bitdefender Antivirus Plus 2015	Eset NOD32 Antivirus 8	F-Secure Anti-Virus	G Data Antivirus / G Data Internet Security	Kaspersky Anti-Virus 2015 / Kaspersky Internet Security 2015	McAfee Live-Safe 2015	Microsoft Security Essentials / Microsoft Windows Defender <sup>2</sup>	Panda Antivirus Pro 2015 / Panda Free Antivirus	Norton Security	Trend Micro Antivirus+ Security
blockiert	73	55	61	66	79	76	49	80	54	50	44	74	80
nachgefragt	0	0	0	0	0	1	27	1	0	0	0	0	0
infiziert	9	27	21	16	3	5	6	1	28	32	38	8	2
Schutz in %	89	67	74	80	96	93	76	98	66	61	54	90	98
Note	⊕	⊖	○	⊕	⊕⊕	⊕⊕	○ <sup>1</sup>	⊕⊕	⊖	⊖	⊖⊖	⊕⊕	⊕⊕

<sup>1</sup> deutlich besser, wenn man die Nachfragen als vollwertigen Schutz interpretiert <sup>2</sup> integriert in Windows 8.1

⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht





Jan Schübler

# Wachtmeister

## Acht Virenwächter im Praxistest

**Starke Abwehrkräfte allein machen noch keine gute Antivirensoftware: Auch schlüssige Bedienung und verständliche Hilfsfunktionen sind unabdingbar, wenn der Antivirenkampf nicht zum Krampf werden soll.**

**H**ohe Erkennungsleistung ist bei Virenwächtern wichtig, aber erst die Mischung mit Bedienkomfort und Ausstattung macht ein Produkt wirklich interessant. Im Artikel auf Seite 122 haben wir die Erkennungsraten von zwanzig Virenwächtern überprüft und dabei einige gute Kandidaten ermittelt – und klären nun die Frage, welche davon in puncto Bedienkomfort und Stressfreiheit überzeugen können.

Dazu haben wir uns acht Virens Scanner genauer angeschaut. Das sind zunächst einmal die fünf Produkte, die durch die besten Erkennungsraten aufgefallen sind: **Eset NOD32 Antivirus 8**, **F-Secure Anti-Virus**,

**Kaspersky Anti-Virus 2015**, **Norton Security** und **Trend Micro Antivirus+**. Als Gratis-Scanner mit einem guten Beschützerinstinkt kommt **Avast Free Antivirus 2015** hinzu. Einige Anwender bevorzugen zudem Antivirensoftware aus hiesiger Entwicklung. Deshalb haben wir dem Testfeld noch **G Data Antivirus** sowie das kostenlose **Avira Free Antivirus** hinzugefügt.

Die Produkte haben wir auf Windows 8.1 mit 64 Bit installiert und dabei auf Auffälligkeiten während der Installation und im laufenden Betrieb geachtet. Besonderes Augenmerk legten wir dabei auf die Verständlichkeit und Übersichtlichkeit der Bedienoberflächen, Einstellungen und

Hilfsfunktionen. Zudem haben wir mittels Testviren und harmlosen Grafikdemos, die Laufzeitpacker einsetzen, die Reaktion auf Virenfunde und das Management von Fehlalarmen geprüft und auf Auffälligkeiten bei der E-Mail-Prüfung geachtet. Wann immer der Wächter etwas bereinigt oder blockiert, sollte der Anwender das durch eine Meldung erfahren.

Uns hat auch interessiert, wie sich die im Hintergrund arbeitenden Virenwächter auf die Geschwindigkeit des Systems auswirken. Dazu haben wir eine SSD mit einem knapp zwei GByte großen Haufen von Setup-Archiven, teils in entpacktem Zustand, per USB 3.0 angeschlossen und den Inhalt auf den Desktop kopiert und dabei die Zeit gestoppt. Außerdem haben wir exemplarisch ausprobiert, wie stark die Schutzprogramme die Installation einer mittelgroßen Anwendungssoftware ausbremsen; dazu wählten wir das kostenlose 123D Design von Autodesk. Als Testsystem diente dabei ein aktuelles Notebook der 500-Euro-Klasse.

### Kleine Unterschiede

Bis auf Avira und G Data haben die Hersteller ihre Virens Scanner

werksseitig so eingestellt, dass Funde automatisch bereinigt – also im Regelfall in die Quarantäne verschoben – werden. Die beiden deutschen Hersteller fragen den Anwender in einigen Fällen, wie er verfahren will. Wem das zu sehr auf die Nerven geht, der kann eine vollautomatische Bereinigung einstellen. Bis auf G Data Antivirus haben alle Produkte zudem einen Silent- oder auch Spielmodus, der die sonst üblichen Meldungsfenster der Software zu Updates oder Funden stumm schaltet, damit sie sich bei Spielen und Videos nicht in den Vordergrund schieben.

Notfallmedien ermöglichen einen Virens Scan des PCs, wenn sich das Betriebssystem wegen einer Infektion nicht mehr starten lässt. Avira, Eset, F-Secure, Kaspersky und Trend Micro bieten dafür ISO-Dateien zum Download an, aus denen sich bootfähige CDs oder USB-Sticks erstellen lassen. Sie enthalten ein Live-Linux-Betriebssystem und ein Modul, das die Festplatten scannt, ohne Windows booten zu müssen. G Datas Notfallmedium nutzt ebenfalls Linux, lässt sich aber direkt aus der Antivirensoftware heraus erstellen.

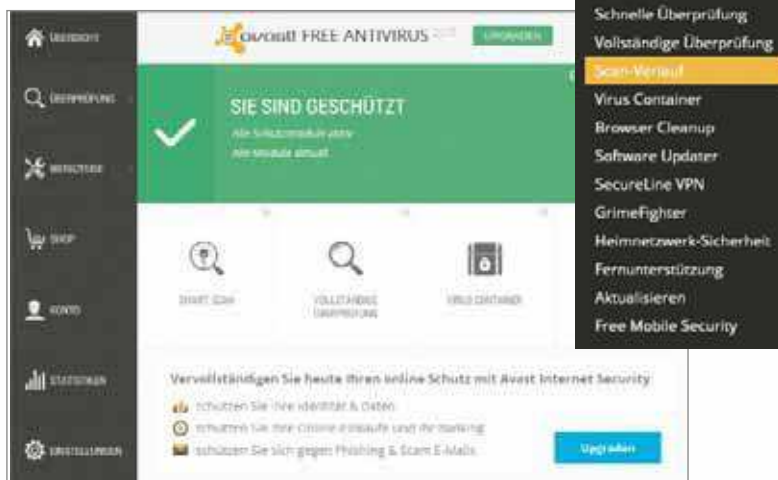
Die Assistenten von Avast, Eset und Symantec erzeugen

hingegen Notfallmedien auf Basis von Windows PE, der Installations- und Reparaturumgebung von Microsoft. Symantec liefert den Assistenten dafür allerdings nicht mit – man muss ihn erst separat herunterladen und installieren. Eset – der einzige Anbieter im Test, der sein Notfallmedium sowohl auf Linux als auch auf Windows-PE-Basis anbietet, macht's bei Letzterem richtig nervig: Läuft NOD32 auf einem 64-Bit-Windows, muss der Anwender vorher das Assessment and Deployment Kit (Windows ADK) von Microsoft herunterladen und installieren. Das erfordert fortgeschrittene PC-Kenntnisse und verschwendet ein paar GByte Speicherplatz.

### Entschleunigungstendenzen

Die Arbeitsgeschwindigkeit wurde mit keinem der Programme unerträglich zäh. Beim Kopieren unseres Testdaten-Ordners konnten wir leichte Unterschiede zwischen den einzelnen Produkten messen. So dauerte der Vorgang mit den Wächtern von Avast, Avira, Norton oder Trend Micro im Hintergrund kaum länger als ganz ohne Virenschutz. Liefen hingegen die Virens Scanner von Eset, G Data oder Kaspersky im Hintergrund mit, dauerte das Kopieren im Schnitt rund um ein Viertel länger. Einzig mit F-Secure Anti-Virus zog es sich auf das rund Drei- bis Vierfache in die Länge. Außerdem lief der Aufbau der Datei-Icons im Testdatenordner auf dem System mit F-Secure Anti-Virus spürbar zäher als üblich. In etwas schwächerer Form trat dieser Effekt auch mit Kaspersky Anti-Virus 2015 im Hintergrund auf – so etwas ist beim alltäglichen Arbeiten mitunter lästiger als die per Messung ermittelten kürzeren oder längeren Kopierzeiten.

Ähnlich verhielt es sich mit der Installationsdauer der Autodesk-Software: Auf Systemen mit Software von Eset, F-Secure, G Data oder Norton geschah das ganze minimal langsamer. In allen Fällen waren das eher graduelle Unterschiede, die sich besser messen als fühlen ließen. Im Test hatten andere Faktoren einen weit größeren Einfluss auf die gefühlte Performance – wenn etwa der Virens Scanner im Hintergrund noch wegen eines geplanten Scans auf der Platte



Avasts Gratis-Scanner bringt viel Werbung, aber auch gute Ausstattung und Flexibilität: Jeder der vier Hauptschaltflächen lässt sich eine von dreizehn Funktionen zuweisen.

herumrödelte oder Windows gerade nach neuen Updates gesucht hat. Auch ein Notebook, das über mehrere Stunden warmgelaufen ist, arbeitet unter Umständen zäher, weil der Prozessor seinen Turbo-Modus nicht mehr voll ausfahren kann (siehe Kasten im Artikel ab S. 102).

Mitunter verursachten bestimmte, teils exotische Konstellationen von Virens Scannern, Treibern und Windows-Updates Probleme. So ließ die Kombination von Avast-Wächter und Microsofts optionalem November-Update-Rollup (KB3000850) in unserem Test dauernd die Windows-Systemsteuerung und den Internet Explorer abstürzen, und die Autodesk-Software ließ sich gar nicht erst installieren. Lief G Data Antivirus in einem virtualisierten Windows 8.1 unter VMware Workstation 10, stürzte der Netzwerktreiber mit einem Bluescreen ab, wenn wir in Outlook 2013 ein E-Mail-Konto einrichten wollten. So etwas darf man aber getrost als exotischen Sonderfall betrachten.

Einige Anbieter lassen den Anwender die erworbene Lizenznummer mit einem Online-Benutzerkonto beim Hersteller verknüpfen, bei manchen ist es sogar Zwang. Das ganze entspannt allerdings den Umgang mit den Lizenzcodes, da sie sich im Internet nachschauen oder sogar während einer Neuinstallation durch Eingabe der Logindaten laden lassen. Symantec geht am weitesten: Der Anwender kann mit seinem Norton-Login sogar bestehende Installationen aus der Ferne deaktivieren – praktisch bei Gerätewechsel oder -diebstahl.

### Große Unterschiede

Bei den heuristischen Verfahren, mit denen Virens Scanner unbekannte Schädlinge aufspüren wollen, kann es ab und an zu Fehleinschätzungen kommen. Harmlose Programme kommen dann mitunter zu Unrecht in Gewahrsam. Ein guter Virenwächter muss einen entspannten Umgang mit solchen Fehlalarmen erlauben – wie Avast, Eset, Norton und Trend Micro. Landet eine harmlose Datei in der Quarantäne, lässt sie sich von dort aus wiederherstellen und direkt als Scan-Ausnahme eintragen, damit sie nicht sofort wieder beschlagnahmt wird. Avira Free Antivirus lässt sich schon bei der Erkennung eines vermeintlichen Übeltäters anweisen, den Fund zu ignorieren. In Esets NOD32 war die Option „Wiederherstellen und von Prüfungen ausschließen“ in unseren Tests stets ausgegraut – warum das so war, konnte der Hersteller bis Redaktionsschluss nicht klären.

F-Secure und Kaspersky machen es deutlich komplizierter: Funde lassen sich aus der Quarantäne zwar wiederherstellen, landen allerdings wenig später wieder automatisch dort, da es keine Option gibt, sie einer Ausschlussliste hinzuzufügen. In solchen Fällen muss der Virenwächter vorher abgeschaltet werden – dann lässt sich die Datei wiederherstellen und in eine Ausnahmenliste eintragen. G Data erdreistet sich, vermeintliche Funde ohne Nachfrage zu löschen – dazu später mehr.

### Avast Free Antivirus 2015

Avasts Gratis-Scanner bietet an, Google Chrome oder Dropbox

mitzuintallieren. Die Teilnahme an der Avast Community, der Cloud-Erkennung des Anbieters, wird automatisch aktiviert. Wer das nicht möchte, soll es nach der Installation deaktivieren. Eine Registrierung ist Pflicht; ohne Avast-Benutzerkonto lässt sich die Software nur 30 Tage nutzen. Die Lizenzbestimmungen und Cloud-Teilnahmebedingungen stehen nur auf Englisch zur Verfügung, ebenso wie die Hilfetexte – kein guter Start.

Die Oberfläche ist klar strukturiert; die Einstellmöglichkeiten sind riesig und dennoch relativ verständlich. So lassen sich zum Beispiel die Scan-Einstellungen für das Lesen und für das Schreiben von Dateien separat anpassen und der Umfang der Protokollierung ändern. Den Warnhinweis im Betreff einer infizierten E-Mail kann man individuell ändern.

Die Funktion Heimnetzwerk-Sicherheit ist bis dato einmalig in einem Virenwächter. Sie testet den Internet-Router auf Schwachstellen, die Zugang zur Router-Konfiguration ermöglichen, und versucht zusätzlich mit diversen banalen Passwörtern, in die Konfigurationsoberfläche zu gelangen. Schafft das Avast-Tool das, ist es auch für Hacker ein Kinderspiel – und der Anwender wird gewarnt. Außerdem testet die Software auf DNS-Hijacking, indem sie den Router mit ein paar Tausend gängigen URLs bombardiert und prüft, ob auch nur die dazugehörigen IP-Adressen antworten.

Plug-ins für Outlook und Thunderbird nehmen schon beim E-Mail-Abruf eine Virenprüfung vor. Funde werden mitunter unmittelbar gelöscht; wer das

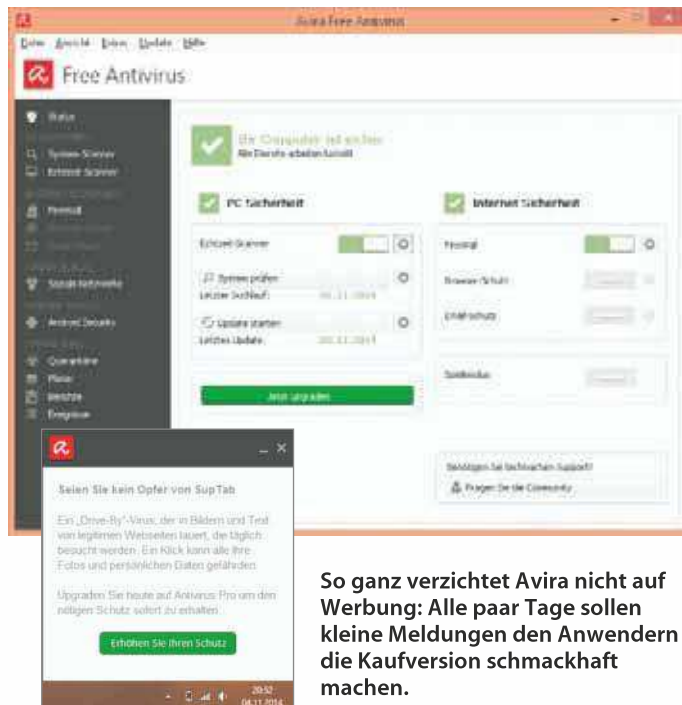
verhindern will, muss die automatische Behandlung abschalten. Einen Hinweistext auf einen Virenfund fügte im Test nur das Outlook-Plug-in ein.

Der Preis für die große Flexibilität ist eine mit Werbung beladene Bedienoberfläche. So sucht der Smart-Scan in der Werkseinstellung auch etwa nach veralteten Java- und Flash-Plug-ins. Er bringt sie aber nur automatisch auf den neuesten Stand, wenn man ein Upgrade auf Avast Premier kauft. Auch der Datenmüllschlucker GrimeFighter findet beim Smart-Scan einiges zu tun und verspricht sogar, den PC zu beschleunigen. Bevor er damit loslegen kann, sind 20 Euro Jahresgebühr fällig. Praktischerweise lassen sich die beiden Werbefunktionen in den Einstellungen des Smart-Scan-Profiles abschalten. Auch kleine Pop-ups weisen hier und dort auf die Vorzüge der kostenpflichtigen Produkte hin, und manche Fenster enthalten Werbung beispielsweise für Amazon Prime. Wer Avast Free Antivirus installiert, muss die Werbung ignorieren können und bekommt dafür eine üppige Ausstattung.

### Avira Free Antivirus

Ein Klick auf das Desktop- oder Taskleistenicon von Avira Free Antivirus öffnet ein kleines Menü, das Zugriff auf alle installierten Avira-Produkte sowie Dropbox bietet. Ein optionales und kostenloses Benutzerkonto lässt den Anwender in einer Web-Anwendung die Geräte verwalten, auf denen er Avira-Produkte nutzt.

Die Oberfläche ist aufgeräumt, Werbung ist in Maßen vorhanden: Ein „Jetzt upgraden“-Link und ein paar ausgegraute Schaltflächen erinnern daran, dass man kein Geld für das Produkt ausgegeben hat. Alle paar Tage wirbt eine kleine Pop-up-Mitteilung für die Kaufversion. Das Einstellungsmenü ist nicht sehr umfangreich, aber es ist sinnvoll strukturiert. Wir haben keine wichtige Option vermisst – bis auf die Möglichkeit, die automatische Updatefunktion temporär abzuschalten. Allerdings lässt sich der Zyklus für die Update-Automatik von den voreingestellten sechs Stunden auf maximal drei Wochen strecken. Das ist hilfreich, wenn man unterwegs das Datenvolumen einer Mobilfunkverbindung nicht belasten möchte. Die Scanfunktionen sind



So ganz verzichtet Avira nicht auf Werbung: Alle paar Tage sollen kleine Meldungen den Anwendern die Kaufversion schmackhaft machen.

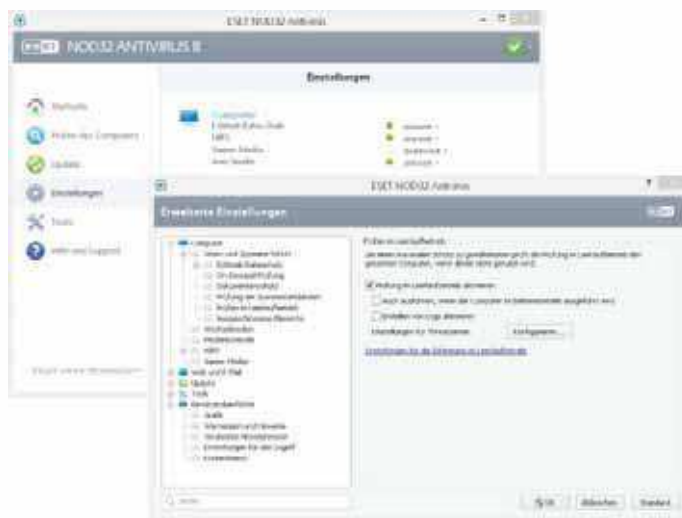
gut konfigurierbar. Auf Wunsch fragt die Cloud-Komponente nach, bevor Verdachtsfälle hochgeladen werden. Die Protokollierung ist vorbildlich und sehr komfortabel zu bedienen; sie filtert die Ereignisse nach Typ und Quelle. Avira Free Antivirus verhält sich für ein kostenloses Produkt erstaunlich unauffällig; der Funktionsumfang ist sinnvoll gewählt.

### Eset NOD32 Antivirus 8

Eset lässt den Anwender bereits bei der Installation entscheiden, ob die Software auch auf unerwünschte Programme achten soll

– also Software, die nicht per se schädlich ist, bei unachtsamer Verwendung aber ein Sicherheitsrisiko darstellen könnte. Bei Aufruf der erweiterten Setup-Optionen lässt sich zudem gleich ein Kennwortschutz für die Einstellungen des Virenwächters setzen.

An der Bedienoberfläche gibts nur Kleinigkeiten auszusetzen. So dürfte Eset den leeren Platz auf der Startseite durchaus nutzen, um Quarantäne, Protokoll und Updatefunktion direkt zu verlinken. Ein Hinweis auf den Zeitpunkt des letzten Signaturupdates könnte das Sicherheitsgefühl steigern. Die Wortwahl der Bedienoberfläche



Eset: Eine klare Struktur gibts auch tiefer in den Einstellungen, aber nicht alles ist für Laien gut verständlich.

richtet sich an erfahrene Anwender. So dürfte nicht allen auf Anhieb klar sein, was es mit der Option „Snapshots der Update-Dateien erstellen“ für das „Update-Rollback“ auf sich hat. Die Hilfefunktion erklärt alle Optionen sehr ausführlich, setzt aber ebenfalls IT-Kenntnisse voraus.

Die Einstellmöglichkeiten sind sehr umfangreich und gut strukturiert. So lässt sich die Cloud-Security-Funktion LiveGrid anweisen, keine Statistik und keine verdächtigen Programme an den Anbieter zu übertragen. Die E-Mail-Prüfung verbessert die Übersichtlichkeit, indem sie einen Ordner für infizierte Nachrichten anlegt und Funde schon beim Abruf dort hinein schiebt. Stehen sicherheitskritische Windows-Updates an, bittet das Programm den Anwender, sie möglichst bald zu installieren. Die sinnvollen Details und der recht unauffällige Betrieb haben uns gut gefallen.

### F-Secure Anti-Virus

Der finnische Anbieter liefert einen einfach zu bedienenden Virenwächter. Die Startseite ist übersichtlich; in der Registerkarte Tools stehen benutzerdefinierte Scans sowie Zugriffe auf die Quarantäne, die manuelle Updateprüfung und die von der DeepGuard-Heuristik überwachten Objekte bereit. Das „Cleanup-Tool“ soll bestimmte Schädlinge bekämpfen können, die der reguläre Virenschscan nicht entfernen kann. Was für Schädlinge das sind und warum dieses Tool dafür hilfreich ist, ist nicht ersichtlich – das stärkt nicht gerade das Vertrauen in die normalen Wächter- und Scanfunktionen.

Die Ausstattung der Software ist recht schmal und die Einstellmöglichkeiten beschränken sich auf das Nötigste. Ein Update-Protokoll legt F-Secure Anti-Virus in Form einer Textdatei an; ansonsten loggt die Software lediglich Virenfunde.

Eine einfache Ausstattung ist eigentlich eine gute Voraussetzung für eine ebenso simple Bedienung, doch leider hat der Hersteller diese Einfachheit nicht konsequent durchgezogen. So sind einige Funktionen nur über das Kontextmenü des Taskleistensymbols erreichbar, etwa der Spielmodus sowie Einstellungen zum Cloud-basierten Schutz und zu automatischen Updates

Virens Scanner					
	Avast Free Antivirus 2015	Avira Free Antivirus	Eset NOD32 Antivirus 8	F-Secure Anti-Virus	G Data Antivirus
Programmversion	2015.10.0.2206	14.0.7.306	8.0.301.3	14.115 build 100	25.0.2.3
Internet	www.avast.de	www.free-av.de	www.eset.de	www.f-secure.de	www.gdata.de
Systemvoraussetzung	XP, Vista, 7, 8, 8.1	XP, 7, 8, 8.1	XP, Vista, 7, 8, 8.1, Home Server 2003/2011	XP, Vista, 7, 8, 8.1	XP, Vista, 7, 8, 8.1
<b>Virenschutz</b>					
Scan: on-access / schnell / komplett / Auswahl	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓
scant Netzlaufwerke	✓	✓ (nur on-access)	✓	✓	✓
Komplett-Scan umfasst USB-Sticks / Netzlaufwerke	- / -	- / -	✓ / ✓	- / -	- / -
Autoscan beim Einbinden von USB-Sticks / Netzlaufwerken	- / -	- / -	✓ / -	✓ / -	- / -
Scan nach Zeitplan	-	✓	✓	✓	✓
Antiviren-Plugin Outlook 2013 / Thunderbird	✓ / ✓	- / -	✓ / -	- / -	✓ / ✓
Hinweis in gesäuberten Mails	✓ (nur Outlook)	-	✓	-	✓
<b>Ausstattung und Einstellungen</b>					
Direkt nach Installation: Update / Schnell-Scan	✓ / ✓	✓ / -	✓ / ✓	✓ / ✓ <sup>2</sup>	- / -
Update manuell anstoßen / Updates deaktivieren	✓ / ✓	✓ / -	✓ / ✓ <sup>4</sup>	✓ / -	✓ / ✓
Stummschaltung / Vollbildererkennung <sup>3</sup>	✓ / -	- / ✓	✓ <sup>4</sup> / ✓ <sup>4</sup>	✓ / -	- / -
Schutz anhaltbar	10/60 Min., bis Neustart, dauerhaft	bis Neustart	10/30/60/240 Min., bis Neustart	bis Neustart	5/10/15/30/60/120/240/480 Min., bis Neustart, dauerhaft
Kennwortschutz für Konfiguration	✓	✓	✓	-	✓
Notfallmedium nutzt	Windows PE	Linux	Linux, Windows PE	Linux	Linux
Add-On für Chrome / Firefox / IE	✓ / ✓ / ✓	✓ / ✓ / -	- / - / -	✓ / ✓ / ✓	- / - / -
Tonausgabe / abschaltbar?	✓ / ✓	✓ / ✓	✓ / ✓	- / n.v.	✓ / ✓
online Lizenzen einsehen / Installationen deaktivieren	- / - (kostenlos)	- / - (kostenlos)	- / -	- / -	✓ / -
Registrierungszwang	✓	-	✓	-	✓
<b>Verhalten bei Funden</b>					
Funde automatisch bereinigen / nachfragen	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
Nachfrage bei Virenfund bietet	Quarantäne, löschen, ignorieren, bereinigen	Quarantäne, löschen, ignorieren, umbenennen	Quarantäne, dauerhaft ignorieren, einschicken, Warnungen anzeigen	Quarantäne, löschen, bereinigen, Bericht	Quarantäne, löschen, sperren, bereinigen (wenn Bereinigen nicht möglich: Quarantäne oder sperren)
Quarantäne-Objekte lassen sich	löschen, wiederherstellen, wiederherstellen und ignorieren, erneut prüfen, einschicken	löschen, wiederherstellen, erneut prüfen, einschicken, Infos anzeigen	löschen, wiederherstellen, wiederherstellen nach, wiederherstellen und ignorieren, einschicken	löschen, wiederherstellen, Infos anzeigen	löschen, wiederherstellen, bereinigen, einschicken
Funde in Virendatenbank ansehen	-	✓	✓	✓	-
Ausnahmen für Dateien / Verzeichnisse / Laufwerke / Endungen	- / ✓ / ✓ / ✓	✓ / ✓ / ✓ / -	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	- / ✓ / ✓ / ✓
<b>Bewertung</b>					
Bedienung	○	⊕	⊕	○	⊕⊕
Einstellmöglichkeiten	⊕⊕	○	⊕⊕	⊖	⊕⊕
Protokoll	⊕	⊕⊕	⊕⊕	⊖	⊕⊕
Quarantäne	⊕⊕	⊕	⊕	⊕	⊕
Umgang mit Fehlalarmen	⊕⊕	⊕	○ (⊕⊕) <sup>7</sup>	○	⊖⊖
Schutznote	⊕	○	⊕⊕	⊕⊕	○ <sup>8</sup>
Preis (1 PC, 1 Jahr)	kostenlos	kostenlos	30 €	20 €	30 €
<sup>1</sup> Scan-Option „Lokale Laufwerke“ scant auch USB-Datenträger <sup>2</sup> Scan erfolgt vor der Installation <sup>3</sup> Herstellerangabe <sup>4</sup> Gamer-Modus, der auch alle geplanten Aufgaben deaktiviert <sup>5</sup> Meldungen in Einstellungen abschaltbar <sup>6</sup> Bildschirmtastatur als Add-On <sup>7</sup> Funktion im Test nicht voll verfügbar, siehe Text					
⊕⊕ sehr gut   ⊕ gut   ○ zufriedenstellend   ⊖ schlecht   ⊖⊖ sehr schlecht   ✓ vorhanden   - nicht vorhanden   k. A. keine Angabe					

bei Mobilfunkverbindungen. Die Hilfefunktion ist schlecht strukturiert und hin und wieder unverständlich. Den Abschnitt, der die Bedienung des Programms erklärt, nennt F-Secure „Computer wird vor schädlichen Anwendungen geschützt“; den Unterabschnitt über Scanfunktionen „Computer wird nach schädlichen Dateien durchsucht“. Einen Einstieg gibt es gleich zweimal – mit unterschiedlichen Inhalten. Wer mit der Bedienung von F-Secure Antivirus vertraut ist, kann es weiterhin nutzen und

macht nichts falsch – aber: Schön geht anders.

### G Data Antivirus

Die Antivirensoftware des deutschen Anbieters G Data überzeugt mit einer vorbildlichen Übersichtlichkeit: Auf einen Blick erfährt man den Betriebszustand der Wächterfunktionen und den Zeitpunkt der letzten Virensuche. In Werkseinstellung prüft das Produkt alle 60 Minuten, ob neue Signaturen vorliegen. Einstellungen, Protokoll

und manuelles Update sind direkt erreichbar. Ein Klick auf E-Mail-Prüfung, Webschutz, Nächstes Update und so weiter lässt den Anwender diese Funktionen ein- oder ausschalten. Die Registerkarte „Virenschutz“ bietet Zugriff auf die Scanprofile, die Quarantäne und den Assistenten für das Notfallmedium. Der Autostart Manager hilft, die Autostart-Elemente der Windows-Installation zu verwalten. Die Einstellmöglichkeiten sind gut aufgebaut und umfangreich; die Hilfsseiten im Netz sind in wei-

ten Teilen auch für Anfänger gut verständlich.

Den Umgang mit Fehlalarmen hat G Data nicht im Griff. Wählten wir bei einem angeblichen Virenfund die vorgeschlagene Behandlungsoption „Desinfizieren (wenn nicht möglich: in Quarantäne)“, wurde die Datei nur laut Protokoll desinfiziert – tatsächlich hat der Wächter sie ohne weitere Nachfrage gelöscht. Die Auswahl „Datei in Quarantäne verschieben“ tut hingegen, was sie soll. Stellten wir die Datei von dort aus wieder her, konnten wir sie trotz-

Kaspersky Anti-Virus 2015	Norton Security	Trend Micro Antivirus+ Security
15.0.1.415	22.0.2.17	8.0.1133 – USAC202006.2966
www.kaspersky.de	www.norton.de	www.trendmicro.de
XP, Vista, 7, 8, 8.1	XP, Vista, 7, 8, 8.1	XP, Vista, 7, 8, 8.1
✓/✓/✓/✓	✓/✓/✓/✓	✓/✓/✓/✓
✓	✓	✓
✓/-	✓/-	✓/-
✓/-	-/-	-/-
✓	✓	✓
✓/-	-/-	-/-
✓ (nur Outlook)	-	-
-/-	✓/✓	-/-
✓/✓	✓/✓	✓/-
-/✓	✓/✓	✓ <sup>5</sup> /-
1/3/5/15/30/60/180/300 Min., bis Neustart, dauerhaft	15/60/300 Min., bis Neustart, dauerhaft	30 Min. / bis Neustart
✓	✓	✓
Linux	Windows PE	Linux
✓ <sup>6</sup> /✓ <sup>6</sup> /-	✓/✓/✓	✓/✓/✓
✓/✓	- / n.v.	- / n.v.
✓/-	✓/✓	✓/-
-	✓	✓
✓/✓	✓/-	✓/-
Ausnahme speichern, Ignorieren, Ordner öffnen, Bericht anzeigen, in Virusdatenbank aufrufen	-	-
löschen, wiederherstellen, Ordner öffnen	löschen, wiederherstellen und ignorieren, einschicken	wiederherstellen und ignorieren
✓	✓	-
✓/✓/✓/✓	✓/✓/✓/✓	✓/✓/✓/✓
⊕	○	⊖
⊕⊕	⊕⊕	⊖
⊕	⊕⊕	⊕
⊕	○	○
○	⊕	⊕⊕
⊕⊕	⊕⊕	⊕⊕
30 €	40 €	20 €

<sup>8</sup> deutlich besser, wenn man die Nachfragen als vollwertigen Schutz interpretiert

dem nicht aufrufen, da der Virenwächter kommentarlos den Zugriff darauf sperrte. Auch das Erstellen einer Ausnahmeregel für den Ordner, in dem der vermeintliche Bösewicht lag, änderte nur wenig: Die Datei ließ sich dann zwar einmal ausführen, wurde kurz darauf aber wiederum als bösartig eingestuft und in die Quarantäne verschoben. Erst nachdem wir Virenwächter und Verhaltensüberwachung abschalteten, ließ G Data Antivirus uns gewähren. Die gute Verständlichkeit der Software macht sie ei-

gentlich zu einem großartigen Produkt. Der sperrige Umgang mit Fehlalarmen allerdings ist für erfahrene PC-Anwender eine Herausforderung und für Anfänger eine Überforderung. Daher können wir das Programm nicht empfehlen.

### Kaspersky Anti-Virus 2015

Die Startseite von Kasperskys Anti-Virus 2015 im treffend gewählten Krankenhaus-Look ist schön übersichtlich. Außer vier großen Schalt-

# BILLIGE AFFÄREN HABEN TEURE KONSEQUENZEN



## BLEIBEN SIE BEIM ORIGINAL VON KYOCERA.

Wenn Sie wirklich Qualität wollen, dann bleiben Sie beim Originaltoner von KYOCERA und lassen sich nicht auf billige Abenteuer ein, die Ihr System schädigen und die Druckqualität beeinträchtigen können. Zweitklassige Fremdtoner haben nicht die hohe Ergiebigkeit des Originals und mit dem CO<sub>2</sub>-neutralen Originaltoner von KYOCERA schonen Sie außerdem unsere Umwelt. Also, lassen Sie sich nicht von günstigen Gelegenheiten verführen. Das kann teure Konsequenzen haben.

KYOCERA Document Solutions Deutschland GmbH  
Infoline 0800 187 187 7 [www.originaltoner.kyocera.de](http://www.originaltoner.kyocera.de)  
KYOCERA Document Solutions Inc.  
[www.kyoceradocumentsolutions.com](http://www.kyoceradocumentsolutions.com)

<sup>9</sup> Nur bei Vertrieb durch KYOCERA Document Solutions Deutschland GmbH und KYOCERA Document Solutions Austria GmbH.



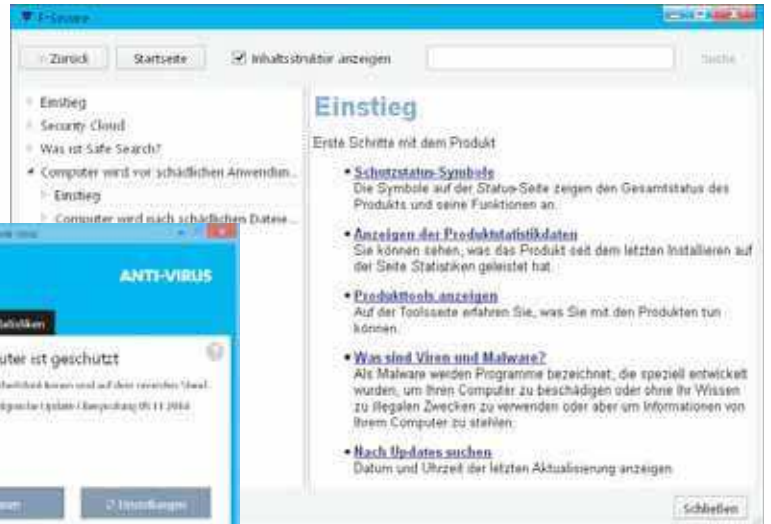
flächen für Untersuchung, Update, Berichte und eine Bildschirm-tastatur gibts noch einige Links zu Einstellungs- und Verwaltungsfunktionen und ein Menü für weitere Funktionen wie Quarantäne, Schwachstellensuche und Download eines Notfallmediums.

Ein Klick auf das Status-Banner im oberen Fensterdrillt öffnet die Mitteilungszentrale, die mit Informationen sparsam umgeht; so verrät die Aussage „Datenbanken sind aktuell“ nicht die Versionsnummer oder den Zeitpunkt der letzten Aktualisierung, und die Aussage „Lizenz ist gültig“ dürfte gerne um die Angabe der Restlaufzeit ergänzt werden.

In den Einstellungen haben wir nichts vermisst, allerdings wünschten wir uns auch hier mehr Informationen. Die Empfindlichkeit der Scan- und Wächtermodule zum Beispiel lässt sich auf minimalen, optimalen oder maximalen Schutz einstellen. Das ist nicht vertrauensbildend, gilt doch ein maximaler Schutz landläufig als optimal. Wer sich durch die Hilfeseiten klickt, erfährt, dass die maximale Schutzstufe sämtliche Dateitypen scannt – also auch solche, die nur selten Viren enthalten. Apropos Hilfe: Die wird in einem uralten Microsoft HTML-Hilfemodul dargestellt, das im Aussehen arg an Windows 98 erinnert und sich etwas altbacken bedient.

Die Schwachstellensuche tattet das System auf veraltete Programmversionen hin ab. Im Test bemerkte sie die obsoleten Ausgaben von Chrome, Firefox und Thunderbird, aber nicht den älteren Adobe Reader und 26 ausstehende Windows Updates. Au-

**F-Secure Anti-Virus ist ein schlichter Virenwächter und einfach zu bedienen – bis man doch mal die Hilfeseiten in Anspruch nehmen muss.**



ßerdem schlägt die Schwachstellensuche vor, beispielsweise das Ausführen unsignierter ActiveX-Objekte und die Autostart-Funktion für Wechseldatenträger auszusuchen. Die vorgeschlagenen Korrekturen lassen sich direkt per Klick anwenden. Die Protokollierung der Schwachstellensuche klemmt: Obwohl veraltete Programme gefunden wurden, hieß es im Bericht „Keine Bedrohungen gefunden“.

Kaspersky Anti-Virus 2015 bietet nur für Microsoft Outlook ein Plug-in an, das Viren aus E-Mail-Anhängen entfernen kann. Die in den E-Mail-Einstellungen gesetzte Option zur generellen Überwachung von POP3- und IMAP-Verkehr hinderte Thunderbird in unserem Test nicht daran, verseuchte Mails herunterzuladen – bei Zugriff auf die angehängten Schädlinge schritt der Wächter

dann aber stets ein. Insgesamt sind die Kritikpunkte nicht dramatisch; wer bisher mit Kaspersky Anti-Virus zufrieden war, dürfte es auch weiterhin sein.

### Norton Security

Symantec hat seine Produktlinie umgebaut und bietet nun Norton Security als einfachste Ausgabe seines Virenwächters an. Es kostet deutlich mehr als das alte Norton Antivirus und bringt dafür Zusatzfunktionen wie Firewall, Passwortsafe, Spamfilter und Anti-Phishing-Schutz mit.

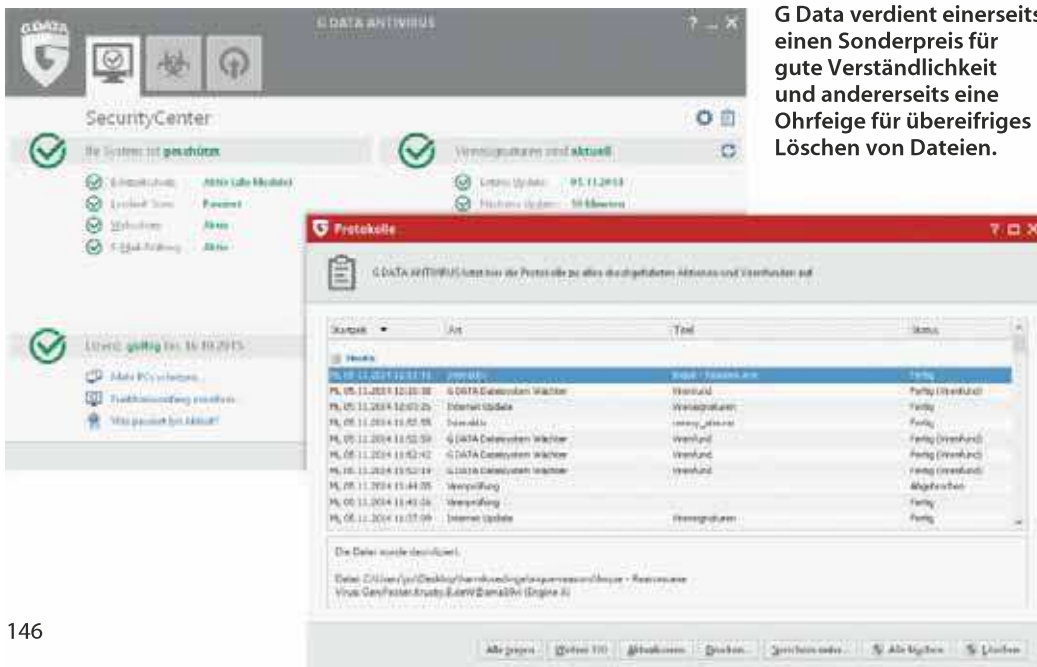
Die Startseite ist übersichtlich und erlaubt schnellen Zugriff auf wichtige Funktionen wie Scans, Signatur-Updates, Protokoll und Einstellungen. In allen Einstellungsdialogen befinden sich Hilfe-Links, die zum jeweils passenden Eintrag in der gut ver-

ständlichen Onlinehilfe führen. Der Startmanager lässt den Anwender die Autostart-Elemente des Computers verwalten. Der „Silent Mode“ kann automatisch und manuell aktiviert werden und lässt sich sogar einzelnen Programmen gezielt zuweisen.

Während die Startseite klar gegliedert ist, hat der Hersteller bei Struktur und Verständlichkeit der Einstellungen und Untermenüs geschlammpt. Betrachtet man beispielsweise ein Quarantäneobjekt im Protokoll, gibt es Links zu „Optionen“ und „weiteren Optionen“, hinter denen sich unterschiedliche Dialoge verbergen. Die Quarantäne lässt sich nur über das Protokoll aufrufen. Im Einstellungsmenü Aufgabenplanung lassen sich unsinnigerweise gar keine Virencans planen, sondern nur Zusatzaufgaben wie Browserbereinigung und Festplattenoptimierung. Unter „Erweitert“ lassen sich einzelne Schutzmodule bei Bedarf abschalten, – Unterschiede zwischen dem „Angriffsschutz“ und der „intelligenten Firewall“ oder zwischen „Browser-Schutz“ und „Sicheres Surfen“ erschließen sich erst durch Nachlesen. Norton Security wird dadurch nicht zu einem schlechten Produkt, wohl aber zu einem etwas sperrigen.

Die Festplattenoptimierung ist im besten Fall einfach eine unsinnige Funktion. Aktuelle Windows-Versionen defragmentieren Magnetfestplatten im Leerlauf ohne weiteres Zutun. Bei SSDs bringt es ohnehin nichts und verkürzt mit unnötigen Schreibzugriffen im Zweifelsfall sogar die Lebensdauer des Datenträgers – dort sollte die Funktion daher nicht benutzt werden.

**G Data verdient einerseits einen Sonderpreis für gute Verständlichkeit und andererseits eine Ohrfeige für übereifriges Löschen von Dateien.**



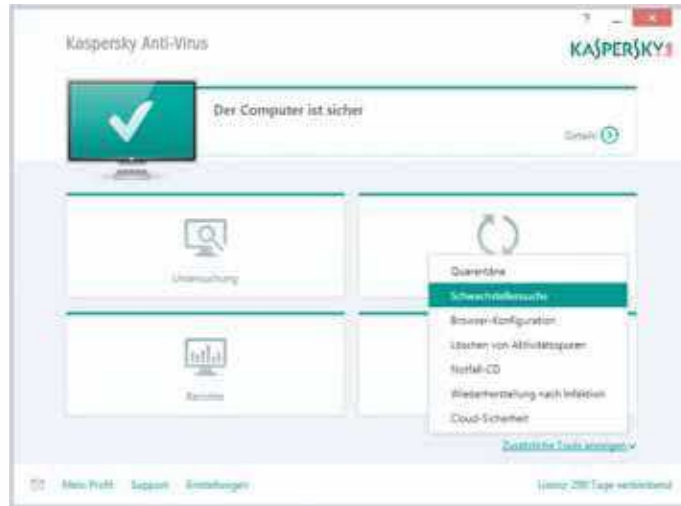
### Trend Micro Antivirus+ Security

Die Hauptseite von Trend Micros Virenwächter Antivirus+ kommt verspielter daher als die der anderen Anbieter. Hinter zwei der vier animierten Schaltflächen in der oberen Fensterhälfte, nämlich Daten und Familie, verbirgt sich Werbung für die teurere Ausgabe namens Maximum Security – bei einem Kaufprodukt darf man das durchaus als unverschämte empfinden. Die Einstellmöglichkeiten beschränken sich aufs Nötigste. Ein Spiele- oder Silent-Modus ist nicht enthalten; zumindest lassen sich aber die Warnmeldungen bei Funden manuell abschalten.

Bedienung und Darstellung sind darüber hinaus nicht gut durchdacht. So besteht die Funktion „Gerät“ aus einer zu drei Vierteln leeren Seite, die lediglich den Betriebszustand von Echtzeitsuche und Webfilter anzeigt – um die Komponenten ein- oder auszuschalten, ist ein zusätzlicher Klick auf „Konfigurieren“ nötig. Die Quarantäne ist im Security Report unter „Weitere Informationen über den Schutz Ihres Computers anzeigen“ versteckt. Das einzig Großartige an Trend Micro Antivirus+ ist die Schutzleistung – deshalb ist das Produkt eine Empfehlung für alle, denen es ausschließlich darauf ankommt.

### Fazit

Eset NOD32 Antivirus 8 überzeugt mit einer durchdachten Bedienung. Wer Erfahrung im Umgang mit Rechnern hat, dürf-



te gefallen an der Software finden. Laien könnten allerdings an einigen Stellen Probleme bekommen.

An Kaspersky Anti-Virus 2015 können wir nur Kleinigkeiten aussetzen. Die Software ist übersichtlich und leicht zu bedienen – und bietet eine exzellente Erkennungsrate. Im Alltag könnte allenfalls der etwas zähe Aufbau von Ordnern mit vielen ausführbaren Dateien lästig sein. Wer bereits Kaspersky-Software verwendet, kann damit getrost weitermachen.

Bei Norton Security hat Symantec seine Hausaufgaben nur halb erledigt. Schutzleistung und Alltagsperformance sind super, gängige Funktionen sind klar strukturiert und sehr einfach zu bedienen – aber einige Einstellungs-menüs sind zum Haare raufen. Ist man die Bedienung gewöhnt, hat man keinen Grund zu wechseln.

G Data bietet mit seinem Antivirus eigentlich die beste Benutzerfreundlichkeit im Testfeld. Bei Fehlalarmen wird die Software aber biestig, und das ungefragte Löschen von Dateien ist indiskutabel. Wer nur weit verbreitete Programme nutzt, kann die Software schmerzfrei einsetzen.

Trend Micro zeigt mit seinem Antivirus+, dass man auch mit einem kostenpflichtigen Virenwächter nicht immer vor Werbung sicher ist. Für die Software sprechen die relativ geringe Systemverschlebung, die gute Erkennungsrate und der im Vergleich zur Konkurrenz etwas geringere Kaufpreis. Die Bedienung ist allerdings nicht gut durchdacht und die Einstellmöglichkeiten sind mager. Wer einen möglichst unauffälligen Virenschoner sucht, wird bei Trend Micro fündig.

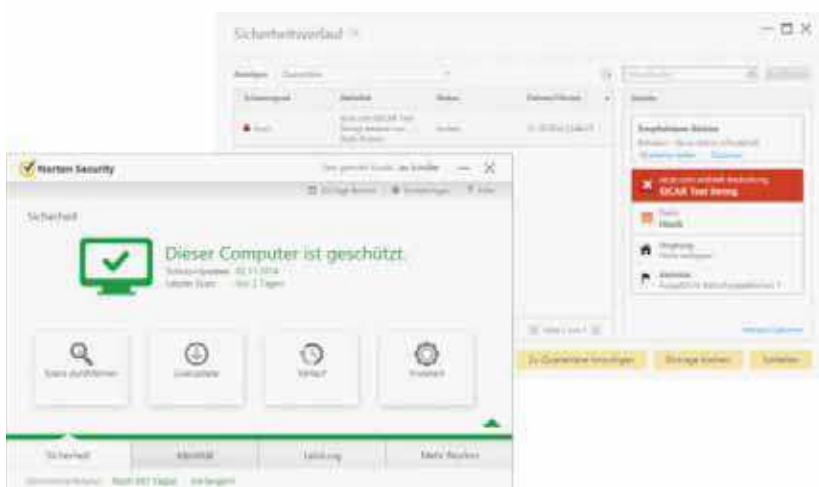
F-Secure Anti-Virus verpackt einen schnörkellosen Funktionsumfang in einer einfachen Be-

### Kühle Eleganz: An Kaspersky Anti-Virus 2015 gibts nur Kleinigkeiten auszusetzen.

dienoberfläche. Die Auslagerung einiger Einstellungen ins Taskleisteicon ist aber unnötig und die bizarre Hilfefunktion wirft mehr Fragen auf, als sie beantwortet. Das Produkt ist schlicht und unauffällig, der Performanceverlust beim Aufbau von Ordnern mit vielen großen ausführbaren Programmen und beim Kopieren großer Datenmengen kann aber lästig werden.

Von den beiden getesteten Gratis-Scannern erzielte Avast mit seinem Produkt Free Antivirus 2015 im Schutztest die besseren Werte, die Wahl des Produkts ist aber auch eine Geschmacksfrage: Avast bietet massig Konfigurationsmöglichkeiten, Plug-ins für den E-Mail-Schutz und eine Router-Prüfung, trägt aber auch in puncto Werbung dick auf. Avira Free Antivirus gibt sich wesentlich dezenter und wirbt eher subtil für das Kaufprodukt, vor allem mittels ausgegrauten Schaltflächen. Funktionsumfang und Einstellmöglichkeiten bleiben allerdings hinter Avast Free Antivirus 2015 zurück und die Erkennungsrate konnte nicht vollends überzeugen. Wer einen kostenlosen Virenschoner sucht und sich an den Werbefunktionen nicht stört, greift zu Avast Free Antivirus 2015; wer es lieber unauffällig hat, nimmt Avira Free Antivirus. (jss)

ct Testversionen: [ct.de/ycuq](http://ct.de/ycuq)



Norton Security ist oberflächlich leicht bedienbar, doch schon das Wiederherstellen und künftige Ignorieren eines Fundes hakelt etwas und erfordert unnötig viele Klicks.



Trend Micro: Die schnörkellose Ausstattung mag ihren Reiz haben, doch durch leere oder fast leere Menüs fühlt sich das Programm oft unvollständig an.