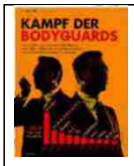


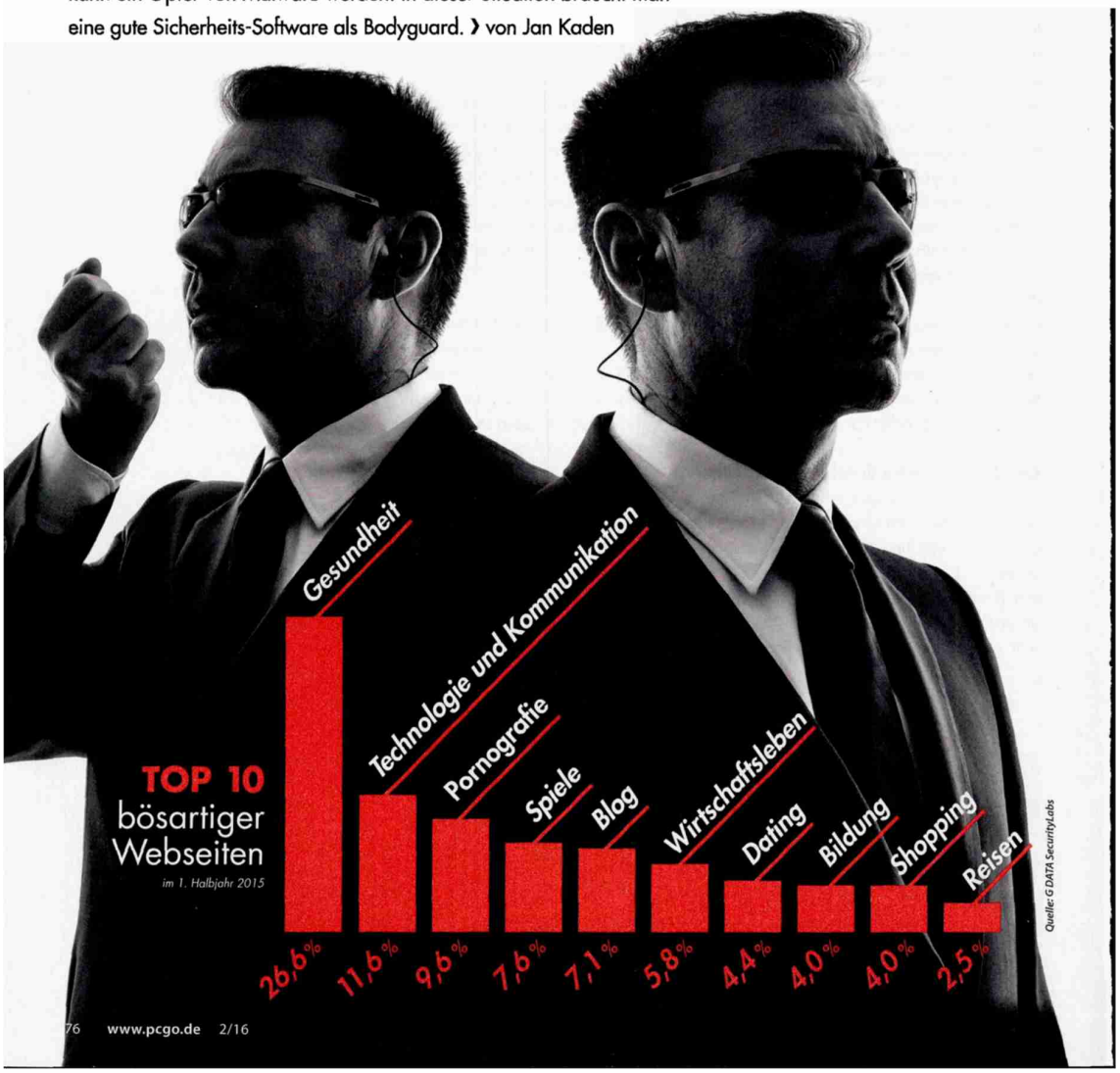
PC go - de

Print

Media type:	Magazine	Print run:	109.233
Date of publication:	02.01.2016	Paid-for circulation:	55.138
Page:	76-81	Total circulation:	55.584
		Coverage:	680.000

KAMPF DER BODYGUARDS

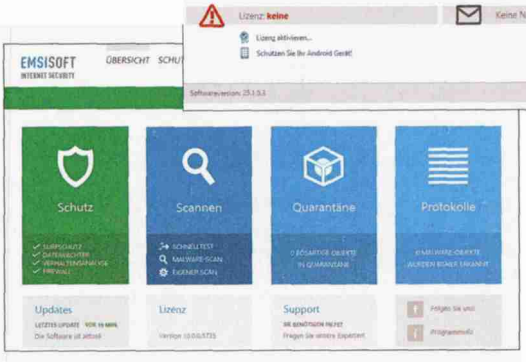
Sicherheitsexperten sind sich einig: Auch wer alles richtig macht, kann ein Opfer von Malware werden. In dieser Situation braucht man eine gute Sicherheits-Software als Bodyguard. › von Jan Kaden



Eines haben Malware-Infektionen mit echten Krankheiten gemeinsam: Wer sich infiziert, steht im Verdacht, etwas falsch gemacht zu haben. Hast Du Dir nicht ordentlich die Hände gewaschen oder Dich nicht warm genug angezogen? Bei Malware klingt das so: Du warst bestimmt auf Pornoseiten, hast Dir Raubkopien besorgt oder den Anhang einer offensichtlichen Spam-Mail geöffnet – wie dumm muss man sein! Zumindest im Computerbereich sind diese Vorurteile aber völlig falsch. Zum Thema Pornosites: Laut dem G Data Malware-Report für das erste Halbjahr 2015 gehörten prozentual die meisten bösartigen Websites zur Kategorie Gesundheit (26,6 Prozent). Im weiten Abstand folgten Sites zum Thema Technologie (11,6 Prozent). Dann erst erscheinen die berüchtigten Pornosites (9,6 Prozent). Bösartige Blogs und Spiele-Sites liegen übrigens mit 7,1 und 7,6 Prozent als Malware-Lieferanten dicht auf.

In elegantem Schwarz und Grau kommt Bitdefender einher. Die wichtigsten Funktionen wie den Bank-Browser Safepay sieht man auf den ersten Blick.

Auf der Oberfläche von G Data Total Protection wird deutsche Sicherheit als Wert angepriesen.



So aufgeräumt wie die Funktionsliste des Programms präsentiert sich auch dessen Oberfläche mit ihren vier Rubriken.

Jeden kann es treffen

Als Anwender kann man also ganz leicht Opfer von Hackern werden, ohne irgendetwas falsch gemacht zu haben. Das wurde auch im vergangenen Jahr wieder deutlich. Zum Beispiel wenn ein Online-Dienst gehackt wird und die eigenen Daten in die Hände von Kriminellen geraten. 2015 gab es einige spektakuläre Einbrüche. „Nichts falsch gemacht" haben demnach die Kunden des amerikanischen Gesundheitsversicherers Anthem. Die Server des Dienstleisters wurden im Februar 2015 gehackt, wobei die Diebe persönliche Daten von fast 80 Millionen Kunden erbeutet haben sollen. Laut Anthem waren glücklicherweise keine medizinischen Daten darunter. Man stelle sich so einen Vorfall bei einer deutschen Krankenkasse vor.

Dass sogar die Besten nicht vor Viren und Hackern gefeit sind, zeigt ein Vorfall im Juni 2015. Diesmal gehörte der Antivirenanbieter Kaspersky Labs zu den Opfern. Die Firma entdeckte nach eigenen Angaben in ihrem Netzwerk Spionagesoftware, die neueste Sicherheitstechnologien auskundschaften sollte. Weder Kaspersky-Kunden noch -Produkte seien betroffen gewesen, heißt es aus Moskau.

Immer wieder gelang es Hackern 2015 verseuchte Reklame in die weltweiten Werbenetzwerke einzuschleusen. Die Werbung erschien folglich auf absolut seriösen Websites wie eBay, Yahoo oder bei der Tageszeitung Daily Mail. Wer diese besuchte, riskierte, seinen Rechner mit Schadsoftware zu infizieren. Dazu war nur ein Browser mit installiertem Flash-Plug-in notwendig.

Gefahr durch Werbung

Die schädliche Werbung (englisch Malvertisement) nutzte eine bis dahin noch unbekannte Lücke in Adobe Flash. Wenn Kriminelle solche unbekannten und folglich ungepatchten Sicherheitslücken ausnutzen, sprechen Sicherheitsexperten von einem Zero-Day-Exploit. Diese Angriffstechnik ist besonders gefährlich, da sich der Anwender nicht mit dem Einspielen von Patches schützen kann. Obendrein haben es Antivirenprogramme schwer, die neu aufgetauchte Bedrohung zu erkennen. Die Angriffsmethode ist ja noch nicht bekannt.

Cyberkriminellen ist deshalb die Kenntnis solcher Zero-Days viel Geld wert, vor allem wenn sie in weitverbreiteten Computerprogrammen gefunden werden. Kein Wunder, dass es mittlerweile einen blühenden Schwarzmarkt für diese Informationen gibt. Ist die Sicherheitslücke einmal gefunden, ist es für Hacker relativ einfach, eine entsprechende Malware-Lösung zu produzieren. Man muss sich nur auf dem Schwarzmarkt ein Exploit Kit kaufen, einen Baukasten, in dem die nötige Technik samt aktueller Zero-Day-Exploits bereits fertig implementiert ist.

Die Opfer sind dagegen weitgehend wehrlos. Adobe Flash und die verschiedenen Web-Browser gehörten 2015 neben Adobe Reader zu den am häufigsten angegriffenen Computerprogrammen. Häufiges Angriffsziel ist auch Oracles Programmiersprache Java, die vor allem bei Firmen weitverbreitet ist. Allerdings werden die Angriffe auf Java seit längerer Zeit seltener. Dazu tragen nach Einschätzung von Experten die inzwischen eingeführten Sicherheitsfunktionen bei.

„Neu" ist auch eine uralte Form von Malware: der Microsoft-Office-Makro-Virus. Das Phänomen wurde von Pandalabs und Trend Micro beobachtet. Die Technik ist verblüffend, denn Makro-Funktionen sind in Office meist deaktiviert und müssen vom Anwender freigegeben werden. Die Cyberkriminellen wenden deshalb in E-Mails ihre gesamten Überredungskünste auf, um den Anwender dazu zu bringen, die Makros zuzulassen.

Ransomware weiter beliebt

Lösegeld-Trojaner (Ransomware) werden immer häufiger eine Bedrohung für Anwenderdaten. Laut dem Internet Security Threat Report 2015 von Symantec verdoppelte sich die Anzahl der Ransomware-Attacken 2014 weltweit von 4,1 Millionen auf bis zu 8,8 Millionen. Das bestätigt auch Trend Micro im TrendLabs 2015 Security Roundup für das erste Quartal 2015. Noch besorgniserregender ist laut Symantec und Trend Micro der steigende Anteil der Schadprogramme, die die Daten der Opfer wirksam verschlüsseln. Das macht den Zugriff auf die Daten für das Opfer tatsächlich unmöglich. Erst nach der Zahlung eines Lösegelds bekommt der geschädigte Anwender ein Passwort zugeschickt, mit dem er seine Daten wieder entschlüsseln kann.

Viele Opfer zahlen den geforderten Betrag, obwohl Experten davon abraten. Trotz der Zahlung ist nämlich nicht sicher, dass man seine Daten wiederbekommt. Entweder reagieren die Kriminellen nicht, oder es gibt technische Probleme, die das Entschlüsseln misslingen lassen. Dann hilft dem Opfer nur noch ein gutes Backup der verschlüsselten Daten weiter. Ein Hoffnungsschimmer: Sicherheitsfirmen führen mittlerweile Schlüsseldatenbanken, mit denen Betroffene mit ein wenig Glück ihre Daten wiederherstellen können. Es ist also auf jeden Fall empfehlenswert, sich bei einer Infektion mit Ransomware zunächst an die Polizei zu wenden oder online Hilfe zu suchen.

Internet der gefährlichen Dinge

Sophos, Symantec und Trend Micro weisen in ihren Berichten 2015 auf die Gefahren hin, die von computerisierten Haussteuerungsanlagen, Videoüberwachungen, Automobilen und einfachen Haushaltsgeräten wie Babyphonen ausgehen – dem sogenannten Internet der Dinge (IoT, Internet of Things). Die Bedrohung ist real. Trend Micro geht in The Fine Line – 2016 Security Predictions sogar davon aus, dass sich im kommenden Jahr der erste tödliche Unfall mit einem „smarten" Endkundengerät ereignen wird. Es gebe immer mehr Dronen im öffentlichen Luftraum und medizinische Geräte mit Computer- oder Internetschnittstellen. Viele Haussteuerungsanlagen seien inzwischen von einer funktionierenden Internetschnittstelle abhängig. Das öffnet nach Ansicht der Trend-Micro-Experten Tür und Tor für fatale Fehlfunktionen, Hackerangriffe oder Missbrauch der jeweiligen Geräte.

Schwachstellen von Haussteuerungsanlagen und anderen „smarten" Geräten werden seit längerer Zeit auf Sicherheitskonferenzen diskutiert. Zurzeit fehle es den Cyberkriminellen nur an einem Geschäftsmodell, einem Gewinnanreiz, um tatsächlich gezielte Attacken zu starten, heißt es im Bericht Security Threat Trends 2015 von Sophos. Symantec erklärt im Internet Security Threat Report 2015, dass

TESTVERFAHREN INTERNET SECURITYS

Für Virenerkennung arbeiten wir eng mit dem unabhängigen Innsbrucker Testlabor AV Comparative zusammen. Das Labor unter der Leitung von Andreas Clementi veröffentlicht seit vielen Jahren auf *www.av-comparatives.org* regelmäßig Tests von Anti-Viren-Software. 2010 hat AV-Comparatives gemeinsam mit der Universität Innsbruck einen Live-Test (*Whole-Product-Dynamic-Test*) entwickelt. Computergesteuert rufen die Tester 5000 infizierte Webseiten auf und werten das Verhalten der Sicherheitsprogramme aus. Sie beurteilen die Suiten danach, ob diese den Benutzer letztendlich vor Malware schützen oder nicht. Dabei spielt es keine Rolle, ob der Schutz durch URL-Blocker, beim Speichern auf der Festplatte oder mit Behaviour-Blocker erfolgt.

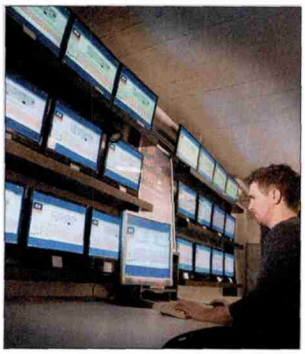
Unser Testverfahren

Wir vergeben positive Punkte nur für den reinen Virenschutz. So kann kein Produkt aufgrund anderer Merkmale wie Ausstattung ein besseres Ergebnis als das für den Virenschutz erhalten. Die Punkte dafür weisen wir in der Tabelle eigens aus. Dieser Test umfasst den Live-Test (80 Prozent), der zeigt, wie der Wächter beim echten Surfen auf verseuchte Seiten reagiert. Der Festplatten-Scan (20 Prozent) sucht nach infizierten Dateien auf dem Rechner. Abzüge gab es für Mängel bei Virenbeseitigung, Ausstattung, Performance und Fehlalarme.

„Das geht gar nicht: Einige Malware-Scanner wollen persönliche Daten von mir abgreifen."

Jan Kaden, Autor PCgo

EXPERTEN-MEINUNG Malware-Scanner sind eine gute Waffe gegen Werbe- und Spionagesoftware. Doch ab und zu verhalten sich die Wächter wie die Diebe. Der kostenlose Avira-Scanner blendet Werbefenster ein, McAfee wechselt die Browser-Startseite, Bitdefender schickt mir E-Mails mit kaputten Links. Fast alle Suiten wollen persönliche Daten von mir. Bitte nachbessern!



Das Testlabor AV Comparatives überprüft und bewertet Sicherheits-Software.

Die Kaspersky-Oberfläche ist aufgeräumt, überwältigt den Anwender aber manchmal mit der Vielfalt der angebotenen Funktionen.

Norton Security gibt sich an der Oberfläche nüchtern und spartanisch hat aber interessante Funktionen zu bieten.

Angriffe auf IoT-Geräte meist über Netzwerkschnittstellen wie zum Beispiel WLAN-Router laufen. Computersicherheit betrifft also bald nicht nur den Computer, sondern den gesamten Haushalt.

Im Zwiespalt: Leistungsfähigkeit kontra Sicherheit

Die von uns getesteten Sicherheitssuiten bieten in den aktuellen Versionen meist mehr als Malware-Scanner, Browser-Erweiterungen und Intrusion-Prevention-Systeme (verhaltensbasierte Erkennung und Blockade von Schadsoftware). Viele Pakete sind mit Backup-Funktionen ausgestattet und halten sogar Online-Speicher (Cloud) für wichtige Daten bereit. Ein Problempunkt bei Sicherheits-Suiten ist die Performance. Niemand möchte, dass sein Rechner wegen einer aufwendigen Anti-Malware-Lösung spürbar langsamer wird. Manche Hersteller gehen das Problem offensiv an und integrieren ein Tuning-Programm in ihr Produkt, das den Rechner des Users beschleunigen soll. Tuning- und Backup-Funktionen sind sicher nützlich, gehören nach unserer Auffassung aber nicht zu einer Sicherheits-Suite. Wir haben diese Funktionen daher zwar in der Tabelle aufgeführt, in die Wertung sind sie aber nicht eingegangen.

Viele Programme im Test bieten Versionen für Mobilsysteme wie Android oder iOS an. Einen Test der Mobil-Scanner können Sie in der folgenden Ausgaben lesen.

In diesem Jahr gewann Kaspersky Total Security 2016 knapp vor Avira Ultimate. Kaspersky ist auf ganzer Linie sehr gut, Avira bei der Virenerkennung sogar einen Hauch besser. Dennoch erhalten alle beide und auch der drittplazierte Bitdefender beim reinen Virenschutz die 100 Punkte. Hier ist die richtige Wahl unabhängig von der Sicherheitsfrage und hängt an Ausstattungsmerkmalen. Kaspersky bietet beispielsweise einen Tracking-Schutz, während Avira in der Performance punktet. Der Spartipp ESET überzeugt vor allem mit seiner geringen Zahl an Fehlalarmen. Stark abgefallen gegenüber den Vorjahren ist F-Secure Safe, das trotz sehr guter Virenerkennung durch viele Fehlalarme und schlechte Performance negativ auffiel. **mm**

INFO MESSERGEBNISSE AUS DEM VIRENLABOR

Verschiedene Faktoren spielen im Test eine Rolle. Virenwächter und Festplatten-Scan zeigen das eigentliche Schutzlevel eines Tools. Besonders ärgerlich sind Fehlalarme. Grün ist in jeder Spalte der beste Wert, Rot der schlechteste.

	Festplatten-Scan (%)	Virenwächter (%)	Fehlalarme (Stück)	Virenbeseitigung (Punkte)	Performance (Punkte)	Ausstattung
Avast	99,3	98,7	128	650	6,8	65
AVG	95,8	98,2	21	635	19,7	62
AVIRA	99,9	99,8	58	628	9,9	62
Bitdefender	99,8	99,9	15	650	21,9	62
Emsisoft	99,7	99,1	50	562	11,6	31
ESET	98,9	98,7	2	606	22,1	41
F-Secure	99,8	99,3	183	540	37,6	48
G DATA	99,8	95,4	48	599	41,8	44
Kaspersky	99,7	99,8	12	679	14,7	71
McAfee	98,6	94,4	45	621	22,3	48
Microsoft	88,9	91,7	6	613	34,3	9
Symantec	95,2	99,8	193	511	25,9	49

PCgo 2/16 TESTSIEGER

HERSTELLER	1 KASPERSKY	2 AVIRA	3 BITDEFENDER	4 AVAST	5 AVG
Produkt	Total Security 2016	Ultimate Protection Suite	Total Security 2016	Premier	Ultimate
Gesamtwertung	**92 Punkte**	**90 Punkte**	**89 Punkte**	**89 Punkte**	**87 Punkte**
Preis/Leistung	**gut**	**befriedigend**	**gut**	**gut**	**gut**
Punkte Virenschutz (max. 100)	**100 Punkte**	**100 Punkte**	**100 Punkte**	**99 Punkte**	**98 Punkte**
Preis (3 User/1 Jahr)	69,95 Euro	89,95 Euro	69,95 Euro	74,28 Euro	70,99 Euro (Ultimate-Abonnement)
Internet: www.	kaspersky.com/de	avira.com/de	bitdefender.de	avast.com/de-de/index	avg.com/de-de/homepage
SICHERHEITSFUNKTIONEN					
Firewall mit Regeln	●	● (Windows Firewall)	●	●	●
Passwort-Sicherung des Programms	● (mit Berechtigungen)	●	●	●	●
Spielmodus ohne Unterbrechungen	●	●	●	●	●
Touch-Oberfläche	●	●	●	●	●
WEBSICHERHEIT					
Tracking-Schutz	●	●	●	●	●
Browser-Cleaner	●	●	●	●	●
Browser-Konfigurator	●	●	●	●	●
Sichere Suchfunktion	●	●	●	●	●
Link-Checker in Suchergebnissen	●	●	●	●	●
Website-Bewertung/Rating	●	●	●	●	●
Sicherung von Kurz-URLs	●	●	●	●	●
Eigener Banking-Browser	●	●	● (Safepay)	●	●
Virtuelles Keyboard	●	●	●	●	●
Phishing-Schutz	●	●	●	●	●
E-Mail-Scanner (POP, IMAP/MAPI)	●	●	●	●	●
Spamfilter	●	●	●	●	●
WEITERE SICHERHEITSFUNKTIONEN					
Datensafe/Dateiverschlüsselung	●	●	●	●	●
Datenschredder	●	●	●	●	●
Kindersicherung	●	●	●	●	●
Webcam-Sicherung	●	●	●	●	●
Rescue Disk/Boot-CD	●	● (Avira Rescue System)	●	●	● (AVG Rescue CD)
Cloud-Backup	● (Dropbox)	●	●	●	●
Backup	●	●	●	●	●
Passwort-Manager	●	●	●	●	●
SYSTEMSICHERHEIT UND -TUNING					
Schwachstellensuche	●	●	●	●	●
System-Tuning	●	●	●	●	●
Löschen nicht benötigter Dateien	●	●	●	●	●
Treiber-Updates	●	●	●	●	●
FAZIT	Mit sehr guten Ergebnissen insgesamt und einer aufgeräumten Oberfläche holt sich Kaspersky den Testsieg.	Avira warnt vor Datensammlern und Hackern im Web. Gute Ergebnisse bei der Virenerkennung runden das Bild ab.	Bitdefender hat interessante Funktionen wie Schwachstellen-Scan und Anti-Ransomware-Funktionen.	Avast ist gut ausgestattet, liegt aber bei den Scanergebnissen nur im Mittelfeld.	Nach einem Schnitzer beim Festplatten-Scan liefert AVG solide Werte.

● = Ja ● = Nein

PCgo 2/16
SIEGER PREIS/LEISTUNG

	6 ESET	7 EMSISOFT	8 MCAFEE	9 G DATA	10 SYMANTEC	11 F-SECURE	12 MICROSOFT
	Smart Security	Internet Security	Live Safe 2016	Total Protection	Norton Security Premium	Safe	Windows Defender
	85 Punkte	**84 Punkte**	**82 Punkte**	**77 Punkte**	**76 Punkte**	**75 Punkte**	**73 Punkte**
	sehr gut	**gut**	**ausreichend**	**gut**	**gut**	**gut**	●
	99 Punkte	**99 Punkte**	**95 Punkte**	**96 Punkte**	**99 Punkte**	**99 Punkte**	**91 Punkte**
	46,08 Euro	59,85 Euro	89,95 Euro	54,95 Euro	59,99 Euro (bis 10 Anwender)	59,90 Euro	kostenlos
	eset.com/de	www.emsisoft.de/de	home.mcafee.com	gdata.de	de.norton.com	f-secure.com/de_DE	●
	●	●	●	●	●	●	●
	●	●	● (für Kinder-sicherung)	●	●	●	●
	●	●	●	●	●	●	●
	●	●	●	●	●	●	●
	●	●	●	●	●	●	●
	●	●	●	●	●	●	●
	●	●	●	●	●	●	●
	●	●	●	●	●	●	●
	●	●	●	●	●	●	●
	●	●	●	●	●	●	●
	●	●	●	●	●	●	●
	●	●	●	●	●	●	●
	●	●	●	●	●	●	●
	●	●	●	●	●	●	●
	●	●	●	●	● (Norton Family)	●	●
	●	●	●	●	●	●	●
	● (SysRescue Live)	● (Emsisoft Emergency Kit)	●	●	● (Norton-Rettungstools)	● (Rescue CD)	●
	●	●	●	●	●	●	●
	●	●	●	●	●	●	●
	●	●	● (True Key)	●	●	● (Gratisversion von F-Secure Key)	●
	●	●	●	●	●	●	●
	●	●	●	●	●	● (Gratisversion von F-Secure Booster)	●
	●	●	●	●	●	●	●
	●	●	●	●	●	●	●
	Als eines der günstigsten Programme im Test bietet Eset Smart Security nützliche Tools.	Die Performance ist Spitzenklasse. Allerdings fehlen weitergehende Funktionen wie Privacy-Schutz.	McAfee bietet neue Techniken wie zum Beispiel einen durch Gesichtserkennung geschützten Cloud-Speicher.	G Data Total Protection bietet wertvolle Funktionen, patzte leider aber bei Performance und Virenbeseitigung.	Das Programm landet bei Virenbeseitigung und bei den Fehlalarmen auf dem letzten Platz im Testfeld.	Der Scanner liefert viele Fehlalarme und liegt bei Performance sowie der Malware-Beseitigung im hinteren Testfeld.	Windows Defender ist bei den Scanergebnissen das Schlusslicht im Test.