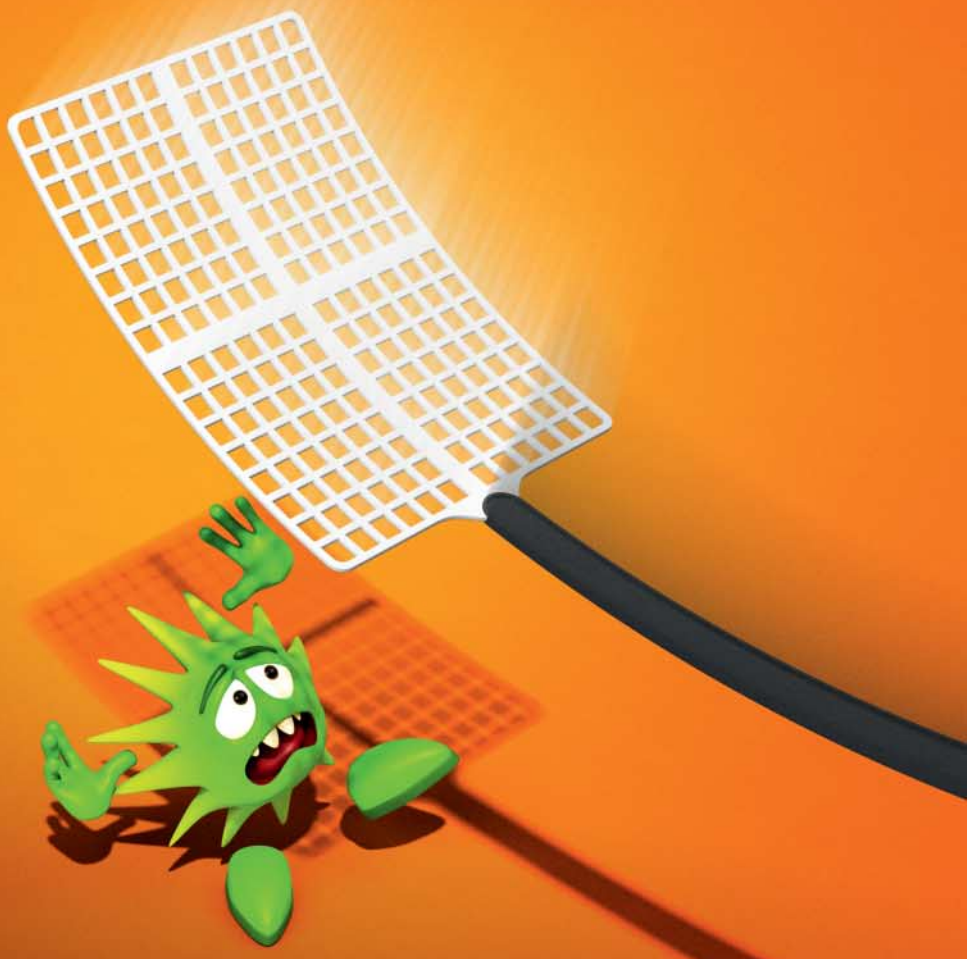
Virenschutz: Zahlen oder sparen?

Der Rest der Welt gegen den Windows Defender



Virenschutzprogramme für Windows gibt es wie Sand am Meer – von gratis bis teuer. Inzwischen drängt sich allerdings die Frage auf, ob man überhaupt noch ein Schutzprogramm installieren muss. Denn der vorinstallierte Windows Defender hat mächtig aufgeholt. Wir haben nach einer Antwort gesucht.

Von Ronald Eikenberg

Virenschutz zählt seit jeher zur Grundausstattung eines jeden Windows-Rechners. Für das sichere Gefühl zahlen viele Nutzer gern, wie ein Blick in die Software-Charts großer Online-Händler zeigt. Doch ist das überhaupt noch nötig? Es gibt doch seit Jahren kostenlose Virenschutzprogramme. Die größte Konkurrenz macht den Bezahlprogrammen jedoch Microsoft: Seit Windows 8 gehört mit dem Windows Defender eine Schutzsoftware zum Lieferumfang.

Die anfängliche Theorie, dass dieser Schritt der Redmonder zu einem Massensterben der Antivirenfirmen führen könnte, hat sich nicht bewahrheitet: Die Erkennungsraten des Defender waren zu Beginn viel zu schlecht. In unserem umfangreichen Virenscanner-Test in c't 26/2014 (siehe ct.de/yj2s) erkannte der Microsoft-Schutz gerade einmal 60 Prozent der Schädlinge, die wir ihm vorsetzten. Die besten im Test verhinderten hingegen 98 Prozent der Infektionsversuche. Vor dem Defender mussten also weder Antivirenhersteller noch Cyber-Ganoven zittern.

Doch diese Zeiten sind längst vorbei. Rund ein halbes Jahr später machte der Windows Defender bemerkenswerte Fortschritte. Ablesen kann man dies an den Ergebnissen der unabhängigen Prüfinstitute AV-Test und AV Comparatives, die sich auf darauf spezialisiert haben, Antivirensoftware auf Herz und Nieren zu testen. So kletterte die Schutzleistung des Defender in der AV-Test-Bewertung von zwischenzeitlich null Punkten Anfang 2015 zunächst auf drei von sechs möglichen Punkten. Von da an ging es bergauf: Vor rund einem Jahr erzielte der Microsoft-Schutz erstmals die volle Punktzahl bei AV-Test, seitdem hält er sich im oberen Bereich der Punkteskala. Auch im Testlabor von AV-Comparatives schneidet der Defender regelmäßig gut ab. Das ist Grund genug, die Situation auf dem Antivirenmarkt neu zu bewerten.

Auferstanden aus Ruinen

Der Aufstieg des Defender ist kein Zufall. Microsoft erklärt in seinem Security-Blog, dass die Schutzsoftware hinter den Kulissen komplett überarbeitet wurde (siehe ct.de/yj2s). Demnach geht ein großer Anteil am Leistungssprung auf das Konto künstlicher Intelligenz (KI) und maschinellen Lernens (ML). Mit diesen Verfahren versucht ein Schutzprogramm anhand vieler verschiedener Dateieigenschaften wie den Metadaten einzuschätzen, wie hoch die Wahrscheinlichkeit ist, dass von einer Datei eine Gefahr ausgeht. Bei einer hohen Wahrscheinlichkeit kann der Virenschutz eine intensivere Analyse durchführen und die Datei etwa in einer Sandbox ausführen, um Gewissheit über die Absichten zu erlangen.

Künstliche Intelligenz gegen reale Bedrohungen

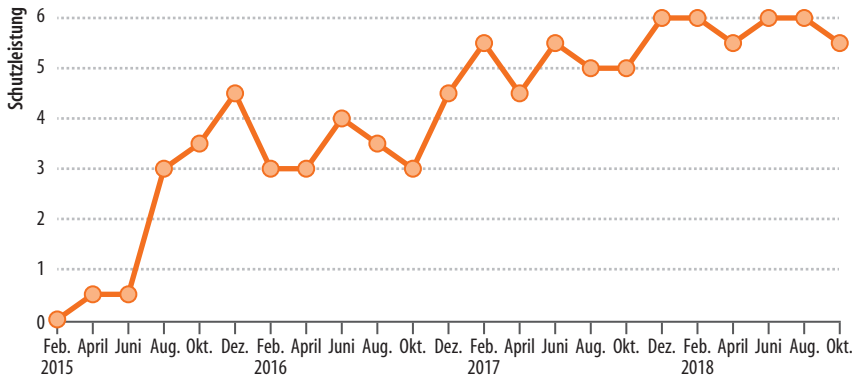
Auf diese Weise können auch zuvor unbekannte Schädlinge überführt werden, während die zur Verfügung stehenden Rechenkapazitäten möglichst effizient genutzt werden. In seinem Blog dokumentiert Microsoft detailliert, wie KI und ML konkret dazu beigetragen haben sollen, Schädlingswellen wie Emotet zu stoppen. Microsoft hat den Einsatz speziell trainierter ML-Modelle bei der Virenjagd jedoch nicht erfunden, auch die traditionellen Antivirenhersteller setzen seit Längerem darauf, um der Schädlingsflut Herr zu werden.

Je nach Hersteller wird die KI-Magie unterschiedlich eingesetzt, teilweise laufen einfache KI-Modelle lokal auf dem zu schützenden Client, während aufwendigere Operationen in der Hersteller-Cloud ausgeführt werden. Sinnigerweise ordnet man die verschiedenen Schutzverfahren von einfach und schnell bis hin zu aufwendig und langsam hintereinander an. Nur, wenn ein Schritt nicht ausreichend Klarheit verschafft, wird der nächste bemüht.

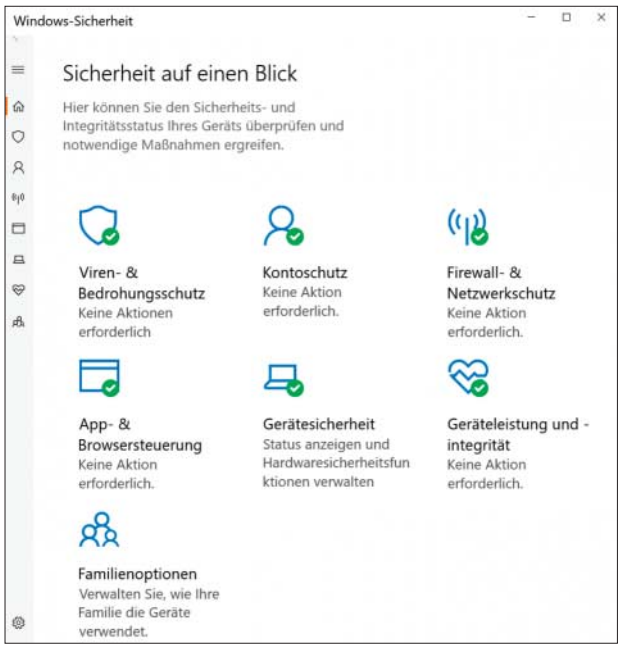
Aber auch bewährte Erkennungsverfahren wie Virensignaturen, Verhaltensüberwachung und Heuristik kommen weiterhin zum Einsatz. Die signaturbasierte Erkennung war lange der Maßstab für die Schutzleistung einer Antivirensoftware. Dem Schutzprogramm wird dabei eine Sammlung tausender Schädlinge vorgesetzt, die im Vorfeld zusammengetragen wurde. Es gilt, möglichst viele davon zu erkennen. Diese Ergebnisse sind inzwischen jedoch nur noch wenig aussagekräftig. Die Antivirenindustrie ist gut untereinander vernetzt und so dauert es nicht lange, bis ein Schädling in den Virendatenbanken aller wichtigen Hersteller auftaucht.

Schutzleistung des Windows Defender

Der Windows Defender hatte einen schweren Start, steht der Konkurrenz in puncto Schutzwirkung inzwischen jedoch in nichts nach.



Daten: www.av-test.org



Im Laufe der Zeit ist der Windows Defender nicht nur zuverlässiger, sondern auch sichtbarer geworden. Über das Security Center hat man alle Schutzfunktionen im Blick.

Erkennungsraten von 100 Prozent sind daher nicht die Ausnahme, sondern die Regel. Weiter an Relevanz verlieren die Virensignaturen durch die Tatsache, dass die Wahrscheinlichkeit abnimmt, auf eine bereits bekannte Virendatei zu stoßen. Denn auch die Cyber-Ganoven haben Zugriff auf alle Virenscanner und manipulieren die Malware vor dem Inverkehrbringen so lange, bis kein oder nur noch wenige Schutzprogramme darauf anspringen. Im einfachsten Fall nutzen sie dafür einen der zahlreichen Exe-Packer. Das erfordert keine Änderungen am eigentlichen Schadcode. So erhält jedes potenzielle Opfer sogar eine individuelle Kopie des Schädlings.

Hopp oder top

Als wichtigster Indikator für die effektive Schutzleistung einer Antivirensoftware gilt daher inzwischen der sogenannte Real-World-Test. Dabei wird der Virenschutz mit realen, aktuellen Bedrohungen konfrontiert, etwa mit verseuchten Webseiten oder virenbehafteten Mails. Anschließend überprüfen die Tester, ob das System infiziert ist oder ob die Antivirensoftware den Angriff erfolgreich vereiteln konnte. Durch welche Schutzkomponente die Attacke verhindert wurde, spielt dabei keine Rolle. Das Ergebnis der Real-World-Tests ist natürlich nur eine Momentaufnahme.

Darüber hinaus überprüfen die Testlabore den Einfluss der Antivirensoftware auf die Geschwindigkeit des Systems und die Häufigkeit von Falscherkennungen (False Positives). Das sind Fälle, in denen der Virenjäger eine harmlose Datei oder Website für schädlich hält.

Darfs ein bisschen mehr sein?

Mittlerweile schlagen sich alle namhaften Schutzprogramme, einschließlich des Windows Defender, auch in den Real-World-Tests von AV-Test und AV Comparatives gut. Je nachdem, auf welchen Testzeitraum man schaut, ist mal der eine, mal der andere Kandidat geringfügig besser. Meist liegt die Infektionsrate nach 200 bis 300 Angriffsversuchen bei lediglich 0 bis 1 Prozent, selten darüber.

Größere Unterschiede gibt es hingegen beim Funktionsumfang: Die Hersteller versuchen, ihre Produkte den potenziellen Kunden mit allerhand Zusatzfunktionen schmackhaft zu machen. Das beginnt bei Features wie einem besonders abgesicherten Online-Banking-Browser und endet bei Funktionen wie Passwort-

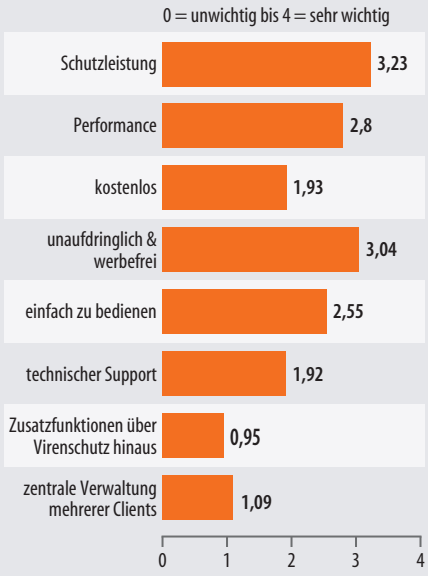
Virenschutz: Darauf legen unsere Leser Wert

Um herauszufinden, wie unsere Leser ihre Windows-Systeme schützen und worauf sie dabei Wert legen, haben wir im Vorfeld unseren c't-Leserbeirat dazu befragt. Dieser setzt sich aus rund 300 Lesern verschiedener Altersklassen zusammen.

Die Umfrageteilnehmer achten vor allem auf eine gute Schutzleistung und einen niedrigen Einfluss auf die Systemperformance. Zudem sollte die Schutzsoftware unaufdringlich und werbefrei sein. Auch eine einfache Bedienbarkeit ist vielen Lesern wichtig.

Der technische Support des Herstellers spielt für die Umfrageteilnehmer hingegen eine eher untergeordnete Rolle, kaum relevant sind Zusatzfunktionen wie Jugendschutzfilter, VPN-Dienste oder die Möglichkeit, mehrere Clients zentral verwalten zu können. Alle Ergebnisse beziehen sich auf den Schutz privat genutzter Systeme.

Die Auswertung zeigt auch, dass rund 40 Prozent der Windows-Nutzer nach wie vor Geld für den Virenschutz ihrer privaten Systeme in die Hand nehmen. Um sicherzustellen, dass wir alle für unsere Leser relevanten Produkte ins Testfeld aufnehmen, fragten wir auch, welcher Virenschutz konkret zum Einsatz kommt. Ungefähr jeder Dritte nutzt den Windows Defender (oder die Microsoft Security Essentials). Darauf folgt mit erheblichem Abstand Avira mit rund 16 Prozent. Alle anderen Hersteller tummeln sich im einstelligen Prozentbereich.



Manager, Datei-Schredder oder System-Tuning, die nichts mehr mit dem Virenschutz zu tun haben. Die meisten Hersteller bieten gar mehrere Editionen ihrer Schutzsoftware an: je teurer, desto mehr Extras. In vielen Fällen erhält die zahlende Kundschaft auch technischen Support. Dieser hilft nicht nur bei Fragen zum Schutzprogramm weiter, sondern unterstützt auch bei der Desinfektion verseuchter Systeme.

Der geschenkte Gaul

Neben den kostenpflichtigen Programmpaketen bieten Hersteller wie Avast, Avira und Kaspersky auch gänzlich kostenlose Versionen ihrer Virenjäger an. Darin werkeln die gleichen Antiviren-Engines wie in der Kaufsoftware, es sind jedoch die meisten Zusatzfunktionen deaktiviert, die über Virenschutz hinausgehen. Die Gratis-Programme werden nicht müde, diese aufpreispflichtigen Extras zu bewerben. Wer den Defender durch einen anderen kostenfreien Virenschutz ersetzt, muss mit Werbung leben.

Man hat also die Qual der Wahl – entweder bleibt man beim Defender, greift zu einer Kauf-Software oder installiert einen werbebehafteten Gratisschutz. Für viele Nutzer dürfte der Defender die beste Wahl sein, da er nicht nur vorinstalliert, sondern auch unaufdringlich und kostenlos ist. Ein kostenpflichtiges Schutzprogramm lohnt sich dann, wenn man sich nicht auf den Microsoft-Schutz verlassen möchte, auf technischen Support angewiesen ist oder den zahlreichen Zusatzfunktionen etwas abgewinnen kann. Zu den Gratis-Scannern der AV-Herstellern sollte man nur noch greifen, wenn man in puncto Werbung einigermaßen schmerzfrei ist. Gut geschützt ist man in allen drei Fällen.

Ein Grund, der gegen den Defender-Einsatz sprechen kann, ist seine enorme Verbreitung. Angreifer suchen sich meist das größte Ziel – deshalb gibt es deutlich mehr Schädlinge, die es auf Windows abgesehen haben als für alle anderen Betriebssysteme zusammen. Das Gleiche gilt für den Virenschutz: Ein Malware-Entwickler wird im Zweifel immer zuerst versuchen, den Defender zu überlisten, bevor er sich um die weniger verbreiteten AV-Programme kümmert. Mit zunehmender Verbreitung des Defender wird sich dieser Effekt weiter verstärken. Auch der erste Schädling, der im großen Stil eine Schwachstelle in einem Virenschutz-Programm ausnutzt, wird vermutlich die Defender-Nutzer treffen. In den Laboren von Sicherheitsforschern funktionieren solche Attacken bereits: So hat etwa Tavis Ormandy von Googles Security-Team Lücken in diversen namhaften Virenschutzprogrammen entdeckt. Durch diese Schwachstellen hätten Angreifer nicht nur den Virenschutz umgehen, sondern das Schutzprogramm sogar zur Infektion missbrauchen können.

Vertrauensfrage

Damit ein Antivirenhersteller seine Kunden bestmöglich vor aktuellen Bedrohungen schützen kann, benötigt er vor allem drei Dinge: Daten, Daten und Daten. Diese erhält er unter anderem von seinen Kunden, was ein gewisses Vertrauensverhältnis voraussetzt. Dem einen mag ein kalter Schauer bei der Vorstellung über den Rücken laufen, noch mehr Informationen als ohnehin schon nach Redmond zu schicken, der andere traut vielleicht Bratislava, Moskau oder Tokio nicht über den Weg. In diese Kerbe schlagen hiesige AV-Hersteller, die gar mit Slogans wie „IT-Security made in Germany“ werben und versprechen, möglichst wenig Daten zu übertragen. Inwieweit die Herkunft des Herstellers die Wahl des Virenschutzprogramms beeinflusst, muss jeder individuell entscheiden.

Um Ihnen die Wahl der Schutzsoftware zu erleichtern, lassen wir auf den folgenden Seiten acht Antivirenprogramme gegen den Windows Defender antreten. Da die Schutzleistung in allen Fällen auf hohem Niveau ist, haben wir die Bedienbarkeit im Alltag in den Vordergrund gestellt. *(rei@ct.de)*

Hintergrundinfos: ct.de/yj2s

Viren-Notfallsysteme

Wenn Windows infiziert ist, sollte man das System nicht mehr booten – ansonsten richtet ein Schädling womöglich noch mehr Schaden an. In so einer Situation kann man neben Notfallsystemen von AV-Anbietern auch auf das langjährig bewährte c't-Sicherheitstool Desinfec't (siehe ct.de/yj2s) zurückgreifen.

Dabei handelt es sich um ein Live-System auf Linux-Basis, das anstelle von Windows bootet. Desinfec't bringt vier Virenscanner von Avira, Eset, F-Secure und Sophos mit, die Windows aus sicherer Entfernung untersuchen können. Das System startet direkt von DVD oder einem USB-Stick. Die Virensignaturen kann man ein Jahr lang ab Verkaufsstart des Heftes beziehen. Neben der Virensuche kann man mit Desinfec't auch verunglückten Windows-Installationen wieder aufhelfen oder versehentlich gelöschte Dateien wiederherstellen.

Des Sicherheitstool liegt jährlich in der Regel der zwölften c't-Ausgabe bei. Jeden Herbst gibt es dann noch mal eine überarbeitete Version mit einem c't-Sonderheft. Bei der Herbst-Ausgabe von Desinfec't ist geplant, das System auf einem direkt einsetzbaren USB-Stick anzubieten.

Auch unser Notfall-Windows auf Basis von Windows PE (siehe ct.de/yj2s) kann nach der Infektion des Rechners erste Hilfe leisten. Es startet ebenfalls vom USB-Stick und enthält Notfall-Tools mehrerer Antivirenhersteller.

(des@ct.de)

Quelle: avast.com

Von 0 bis 120 Euro: Die Auswahl an Virenschutzpaketen ist schier grenzenlos – selbst, nachdem man sich für einen Hersteller entschieden hat.