Virenschutz

Antworten auf die häufigsten Fragen

Von Ronald Eikenberg

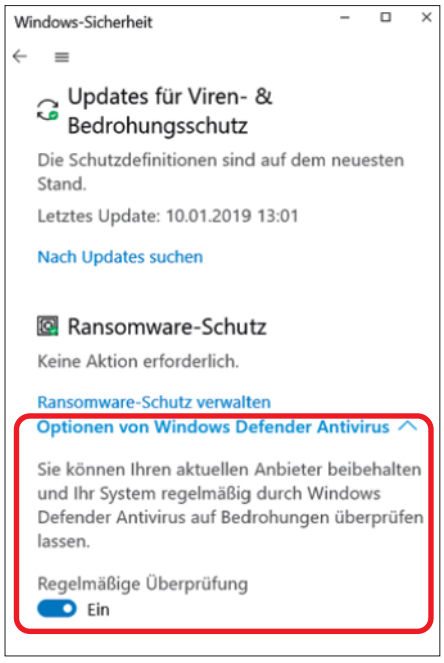
Doppelter Schutz

Kann ich zwei Virenschutz-Programme parallel installieren?

Das funktioniert in aller Regel nicht, da sich die Echtzeitschutz-Komponenten der Virenjäger gegenseitig in die Quere kommen würden. Sie müssen sich also für ein Virenschutzprogramm entscheiden und die alte AV-Software vor der Installation einer neuen entfernen. Um den unter Windows 8 und 10 vorinstallierten Defender müssen Sie sich jedoch nicht kümmern, er wird bei der Installation einer alternativen Schutzsoftware von Windows weitgehend deaktiviert, sodass keine Probleme auftreten können. Nach der Deinstallation der nachgerüsteten AV-Software schaltet Windows den Defender wieder ein.

Um sich eine zweite Meinung einzuholen, können Sie sogenannte Second-Opinion-Scanner nutzen. Diese sind für den Betrieb neben einem vollwertigen Virenschutz-Programm ausgelegt. Dazu zählen etwa Malwarebytes, HitmanPro oder Norton Power Eraser.

Auch der Defender ist inzwischen als Second-Opinion-Scanner nutzbar: Sie können mit ihm auch nach der Installation eines anderen Virenscanners das Dateisystem nach Schädlingen durchsuchen. Sie finden die Funktion unter Windows 10 durch eine Startmenü-Suche nach „Defender“ und einen Klick auf „Windows Defender Security Center“ (bis Windows-Build 1803) oder „Windows-Sicherheit“ (ab Build 1809). Wählen Sie dort „Viren- & Bedrohungsschutz“. Unter „Aktuelle Bedrohungen“ können Sie sofort eine Schnellüberprüfung starten; „Scanoptionen“ führt Sie zu intensiveren Scanverfahren. Automatische Scans können Sie veranlassen, indem Sie ganz nach unten schrollen und dort die „Optionen von Windows Defender Antivirus“ ausklappen. Aktivieren Sie dort die „Regelmäßige Überprüfung“.



Auch wenn Sie sich für einen anderen Virenjäger entscheiden, kann der Defender von Zeit zu Zeit nach dem Rechten sehen.

Schutzpaket

Früher musste ich allerhand Programme auf meinem Windows-System installieren, ehe es einigermaßen sicher war. Neben dem Virenschutz war etwa eine Firewall-Software essenziell. Was benötige ich wirklich?

Die Zeiten, in denen Sie eine Personal Firewall wie ZoneAlarm auf Ihrem Rechner installieren mussten, sind lange vorbei. Einerseits ist heutzutage fast kein Client mehr direkt über das Internet erreichbar, da die Internetverbindung in aller Regel über einen Router läuft. Andererseits ist Windows bereits seit Windows XP SP2 mit einer Firewall ausgestattet. Diese sortiert den eingehenden Datenverkehr zuverlässig und sorgt etwa dafür, dass andere Nutzer in einem öffentlichen Hotspot-Netz nicht auf Ihre Netzwerkfreigaben und andere Dienste zugreifen können. Und das Konzept, ausgehenden Datenverkehr auf dem Client zu filtern, gilt inzwischen als überholt. Eine ähnliche Entwicklung hat gerade beim Virenschutz stattgefunden: Der unter Windows 8.1 und 10 vorinstallierte Virenschutz Windows Defender hat in puncto Schutzleistung inzwischen zu den Produkten der Antiviren-Hersteller aufgeschlossen. Geht es rein um den Schutz, sind Sie mit einem Windows 10 im Auslieferungszustand also bereits gut aufgestellt. Warum sich die Installation eines anderen Virenschutzprogramms dennoch lohnen könnte, erfahren Sie ab Seite 30.

Wichtiger als die Wahl des Virenjägers ist, dass Sie auch andere Aspekte wie regelmäßige Updates, Backups und individuelle Passwörter bei der der Absicherung Ihres Rechners beachten. Auf Seite 42 finden Sie eine Zusammenfassung.

Erste Hilfe

Ich habe das Gefühl, dass mein Rechner verseucht ist. Was kann ich tun?

Am besten untersuchen Sie das potenziell infizierte System, indem Sie ein Livesystem von DVD oder USB-Stick booten. Dazu können Sie zum Beispiel Desinfec’t nutzen (siehe ct.de/yvgx), welches das System mit bis zu vier Virenscannern überprüft, ohne dass ein Virus eingreifen kann. Haben Sie den Schädling gefunden, können Sie ihn damit auch gleich entfernen. Darüber hinaus können Sie dem System im laufenden Betrieb mit Tools wie AutoRuns (siehe ct.de/yvgx) zu Leibe rücken. Es listet alle Prozesse auf, die Windows beim Systemstart ausführt. Unter „Options/Scan Options ...“ können Sie die Prozesse auch einem Online-Virencheck durch Virustotal.com unterziehen lassen. Detaillierte Informationen über laufende Prozesse finden Sie mit Process Explorer heraus, den Sie ebenfalls über ct.de/yvgx finden.

Grundsätzlich gilt, dass Sie sich nach einer Desinfektion nie sicher sein können, dass der Rechner definitiv wieder sauber ist. Möglicherweise hat der aufgespürte und entfernte Schädling etwa weiteren Schadcode nachgeladen, der dem Virenscanner entgangen ist. Am besten spielen sie ein sauberes Festplatten-Image ein oder fangen ganz von vorn an, indem Sie die Platte formatieren und Windows neu installieren. Es besteht die Gefahr, dass der Virus Tastatureingaben belauscht und Passwörter abgegriffen hat. Wenn Sie auf Nummer sicher gehen möchten, ändern Sie bei allen Online-Diensten, die Sie mit dem infizierten Rechner genutzt haben, Ihre Passwörter.

Kostenfrage

Muss ich für einen guten Virenschutz Geld ausgeben?

Nein. Wenn Sie Windows 8.1 oder 10 nutzen, dann ist Ihr System bereits mit dem Windows Defender ausgestattet, der inzwischen eine gute Schutzwirkung bietet. Auch die kostenlosen, werbefinanzierten Virenschutz-Programme der AV-Hersteller bieten einen guten Schutz. Sie nutzen unter der Haube die gleichen Antiviren-Engines wie die kostenpflichtigen Schutzprogramme der jeweiligen Hersteller. Eine Hilfestellung bei der Wahl des Virenschutzprogramms liefert Ihnen der Artikel auf Seite 30 sowie unser großer Vergleichstest auf Seite 34.

Erpressungstrojaner

Auf meinem Rechner hat ein Erpressungstrojaner zugeschlagen und meine Daten verschlüsselt. Für die Entschlüsselung soll ich ein Lösegeld in Bitcoin zahlen. Was kann ich jetzt tun?

Im Idealfall haben Sie ein Backup Ihrer Daten und können die Festplatte formatieren, Windows neu installieren und die Daten einfach zurückspielen (siehe „Erste Hilfe“). Wenn Sie keine Sicherheitskopie der verschlüsselten Daten haben, wird es knifflig. Zahlen Sie auf keinen Fall das Lösegeld, da es keine Garantie dafür gibt, dass die Kriminellen ihr Wort halten. Versuchen Sie stattdessen herauszufinden, um welchen Schädling es sich genau handelt und ob im Netz bereits ein kostenloses Entschlüsselungs-Tool kursiert. Die erste Anlaufstelle hierfür ist die Website ID Ransomware (siehe ct.de/yvgx). Wenn Sie dort die Datei mit der Erpresserbotschaft oder eine der verschlüsselten Dateien hochladen, versucht die Website den Schädling zu identifizieren und zeigt im Erfolgsfall nicht nur die Schädlingsfamilie, sondern auch etwaige Rettungs-Tools an. Wenn dieser Weg ins Leere führt, können Sie Ihr Glück noch mit Datenrettungs-Tools wie Recuva oder ShadowExplorer probieren (siehe ct.de/yvgx).

Wenn Sie die verschlüsselten Daten nicht retten können, sollten Sie diese trotzdem aufbewahren. Mit etwas Glück entdeckt ein findiger Sicherheitsforscher in Zukunft einen Weg, die Verschlüsselung zu knacken. Ziehen Sie also ein Image von dem betroffenen Datenträger, ehe Sie ihn formatieren – oder Sie legen ihn in den Schrank und nutzen für die Neueinrichtung eine andere Platte/SSD.

Sicherheit für unterwegs

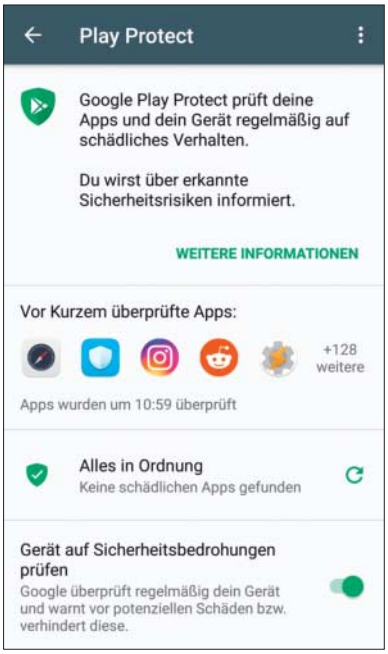
Brauche ich auf meinem Smartphone oder Tablet einen Virenscanner?

Normalerweise nicht. Auf iPhones und iPads läuft iOS, für das so gut wie keine Schädlinge existieren. Sie können im Normalzustand ausschließlich Software aus dem App Store installieren, die von Apple überprüft wurde. Bei Android-Geräten ist die Lage anders, da Sie hier beliebige Apps aus beliebigen Quellen im APK-Format installieren können. Solche Dateien können verseucht sein. Wenn Sie jedoch darauf verzichten und ausschließlich Apps von Google Play herunterladen, dann kann ihnen wenig passieren. Auf Android-Geräten ist standardmäßig Google Play Protect installiert, das alle Apps automatisch einem Virenscan unterzieht. Findet es dabei eine Infektion, erhält man einen Hinweis und kann den Schädling leicht entfernen. Ganz gleich, welches Mobil-Betriebssystem Sie einsetzen: Halten Sie es stets auf dem aktuellen Stand, da die meisten Updates Sicherheitslücken schließen.

Aus der Schusslinie

Bin ich mit Linux oder macOS wirklich auf der sicheren Seite?

Windows ist mit Abstand das beliebteste Angriffsziel. Nicht, weil es besonders unsicher ist, sondern aufgrund seiner schieren Verbreitung. Für macOS und Linux gibt es deutlich weniger Schädlinge, weil die Anzahl der potenziellen Opfer viel geringer ist. Sie sollten dennoch darauf achten, was Sie installieren und grundlegende Schutzvorkehrungen treffen, denn hin und wieder tauchen durchaus Viren für diese Plattformen auf.



Das unter Android vorinstallierte Play Protect hält Smartphones & Co. virenfrei. Sie finden es im Menü des Play Store (Knopf oben links).

Halten Sie das System und die Anwendungen auf dem aktuellen Stand. Achten Sie darauf, welche Software Sie auf Ihrem System ausführen und woher sie stammt. Unter macOS beziehen Sie Software am besten aus dem Mac App Store, da diese von Apple vor der Veröffentlichung überprüft wird. In der Linux-Welt stehen vor allem Server im Visier der Angreifer, die über das Internet erreichbar sind. Stellen Sie also sicher, dass insbesondere Server-Anwendungen stets aktuell sind.

Wenn Sie unsicher sind, ob eine Datei infiziert ist, können Sie diese zum Beispiel bei dem Virenscan-Dienst Virustotal.com hochladen. Virenschutz-Programme gibt es auch für macOS und Linux, sie sind dort jedoch aufgrund der überschaubaren Bedrohungslage nicht so essenziell wie unter Windows. Sie können damit allerdings verhindern, unwissentlich Windows-Schädlinge an Ihre Bekannten weiterzugeben.

Rettungs-Tools: ***ct.de/yvgx***