Grenzen eines Antivirenprogramms

Allerdings ist auch eine Software als Schutzmechanismus nicht das Allheilmittel. Ein Schutz, und sei er noch so gut, ist nur dann wirklich zuverlässig, wenn er auch gewartet wird. Dazu zählen regelmäßige ***Updates*** und aktuelle ***Virensignaturen***, die ein Erkennen von neuen Schadprogrammen überhaupt erst möglich machen.

Veraltete Virensignaturen machen Ihre Antiviren-Software unbrauchbar, da sie vor aktuellen Schädlingen nicht geschützt sind.

Aber auch damit ist der Schutz noch nicht vollständig. Selbst eine noch so gute Antivirensoftware schützt nicht davor, dass **Sicherheitslücken in Anwendungsprogrammen und Betriebssystemen** vorhanden sind und auch genützt werden können. Was nützt also ein Virenscanner, wenn ein Programm zum Abspielen von Musikdateien eine Sicherheitslücke hat und es möglich ist, aus dem Internet auf dieses Programm zuzugreifen.

Die Konsequenz daraus ist, zu erkennen, dass auch Schutzsoftware Grenzen hat, und dass es unerlässlich ist, auch Anwendungen und Betriebssysteme auf mögliche Schwachstellen hin zu prüfen. Das wäre allerdings für den Benutzer selbst fast nicht zu realisieren. Dafür sorgen im Normalfall die Hersteller selbst. Zu diesem Zweck werden in regelmäßigen Abständen entsprechende ***Software-Updates***, sogenannte ***Patches***, von den Softwareherstellern angeboten.

Es ist unbedingt notwendig darauf zu achten, dass diese **Updates und Aktualisierungen** auch installiert werden. Nur dadurch ist es möglich, auch die Sicherheitsschwächen von Systemen und Anwendungen zu beseitigen und dafür zu sorgen, dass ein Rechner möglichst von Schadsoftware frei bleibt. Aber nicht nur der Rechner und die darauf laufenden Programme wie Browser mit Plug-Ins, Apps oder andere Anwendung müssen möglichst auf dem aktuellsten Stand gehalten werden. Auch Smartphones und die darauf laufenden Systeme und Apps gehören dazu, ebenso alle anderen mobilen Geräte. Auch hier sind immer die aktuellsten verfügbaren Updates und Patches einzuspielen. Eine nicht aktuelle App kann auf einem mobilen Gerät genau so viel Schaden anrichten wie auf einem PC.

Leider sind viel zu oft **alte Softwareprodukte** im Einsatz. Die Gründe dafür können sehr unterschiedlich sein. Die daraus erwachsenden Probleme sind aber vielschichtig. Durch aktive Verwendung solcher alten Anwendungen kann es einerseits zu Inkompatibilitäten der Programme kommen, andererseits können solche Applikationen auch nicht immer auf den aktuellen Stand gebracht werden. Die daraus entstehenden Folgen können zu Datenverlust, Schwachstellen im System und hoher Gefährdung durch Malware und Schadsoftware führen.

Natürlich ist kein 100%iger Schutz möglich. Was hilft das sicherste, neueste bzw. regelmäßig gewartete Auto, wenn der Fahrer einen Fehler macht und einen Unfall verursacht? So ähnlich verhält es sich bei einem Computer oder auch bei einem Mobilgerät. Selbst noch so gute Software und die besten Schutzmechanismen sind wirkungslos, wenn der Benutzer sich der Gefahren nicht bewusst ist und dadurch Schaden verursacht.

Quarantäne

Wenn nun so eine Antivirensoftware oder ein ähnliches Schutzprogramm eine schädliche Software erkennt, ist es in den meisten Fällen möglich, das Verhalten des Schutzmechanismus zu konfigurieren.

Die meisten der verwendeten Programme sind in der Lage, die Schädlinge zu entfernen und die befallen Dateien zu „**heilen**“. Sollte das nicht möglich sein, kann die befallene bzw. verdächtige Datei samt Schadprogramm gelöscht werden oder in ***Quarantäne*** verschoben werden, die Daten landen damit in einem Quarantäne-Ordner und jeder Zugriff wird verhindert.

Löschen ist die radikalste Methode, die natürlich im Falle eines sicher erkannten Schädlings die Beste ist. Allerdings sind damit auch die Benutzerdateien verloren.

Der Benutzer ist in der Lage im Virenschutzprogramm einzelne verdächtige Dateien, beispielsweise im Kontextmenü der Datei, in Quarantäne zu stellen oder zu löschen. Es kann in bestimmten Situationen besser sein, eine Datei in den Quarantäne-Ordner zu verschieben und dann zu versuchen, die Datei vielleicht mit einem anderen Tool „desinfizieren“ zu lassen, anstatt sie gleich zu löschen. Dabei ist aber Vorsicht geboten, daher sollte eine solche Prozedur nur in Ausnahmefällen durchgeführt werden.

Virensignatur und Heuristik

Die meisten Schutzprogramme verfügen über Methoden zur „Früherkennung“ von Schädlingen, ***Heuristik*** genannt. Diese Heuristik versucht auch solche schädlichen Programme zu erkennen, die noch nicht als Signatur bestehender Schädlinge bekannt ist. Aktuelle Virensignaturen sind allerdings unbedingt notwendig, da diese Früherkennung nur relativ geringen Schutz bietet. Bei der Auswahl einer Antivirensoftware sollte daher darauf geachtet werden, dass mindestens einmal pro Tag eine aktuelle Virensignatur vom Hersteller zur Verfügung gestellt wird. Außerdem sollte in regelmäßigen Abständen eine Untersuchung des PCs durchgeführte werden.

INFO

Manche Hersteller von Virenschutzsoftware bieten auch die Möglichkeit, bei Verdacht auf einen Befall von Malware, das Gerät online über die Webseite untersuchen zu lassen. Dabei wird über das Internet eine Virenerkennung auf dem Gerät durchgeführt und bei Befall auch gleich die Schadsoftware entfernt. Links zu solchen Programmen bieten meist die namhaften Hersteller solcher Produkte selbst an, es kann auch sein, dass der Hersteller des Betriebssystems auf Partner verweist. Auch von offizieller Seite wie Behörden und Organisationen kann mitunter der Hinweis auf solche Online-Ressourcen vorhanden sein.

INFO

Notizen:

Übungsbeispiel – Computer scannen

Ein Scanvorgang kann manuell durchgeführt werden, die meisten Schutzprogramme sind aber in der Lage, einen Scanvorgang in regelmäßigen Abständen zu planen und durchzuführen.

Lernziele:

- Scans planen, nach Zeit oder ausgewählten Ordnern
- Scan spontan durchführen

Schritt für Schritt:

Da es viele Produkte im Bereich Antivirensoftware gibt, wird hier die Übung exemplarisch am Beispiel von **AVG AntiVirus FREE** durchgeführt.

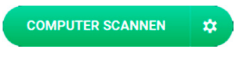
ACHTUNG

Für die Installation und Konfiguration von Antivirensoftware sind administrative Rechte notwendig.

Um einen Scanvorgang für ein bestimmtes Laufwerk oder einen bestimmten Ordner zu planen, kann ein entsprechender **Zeitplan** erstellt und aktiviert werden.

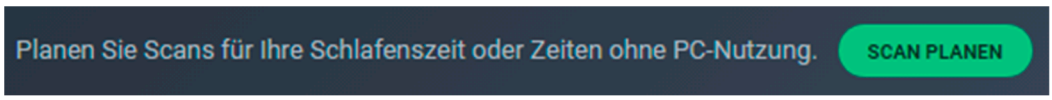
Scan planen nach Zeit

Schritt 1 Starten Sie die Konsole des Virenschutzprogramms mit einem Doppelklick auf das entsprechende Symbol im Infobereich der Taskleiste.

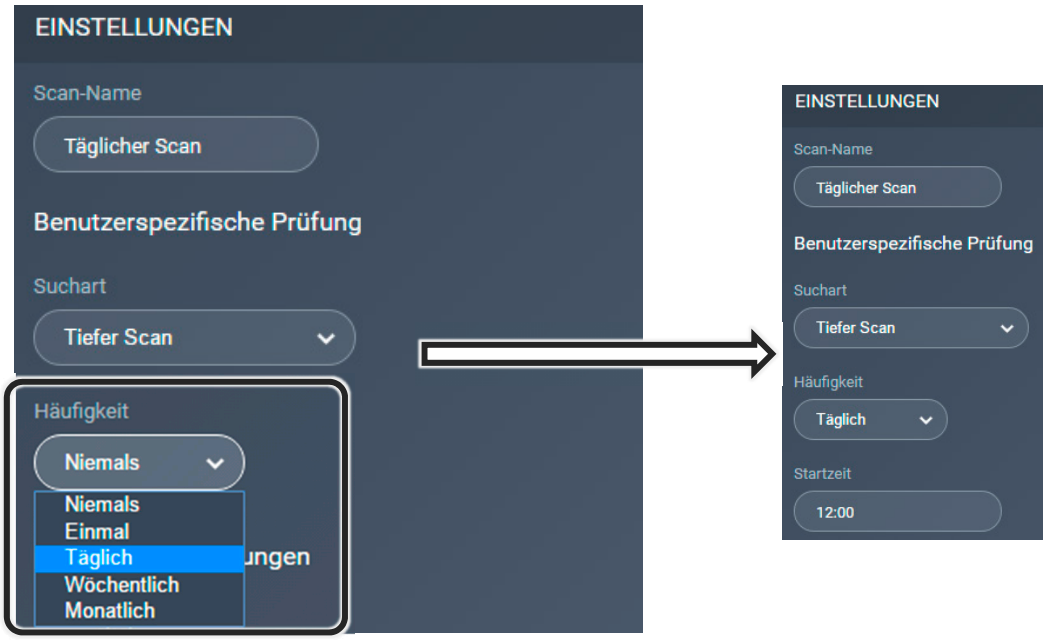
Schritt 2 Klicken Sie dann auf  neben 

.

Klicken Sie im folgenden Fenster auf SCAN PLANEN. **Schritt 3**



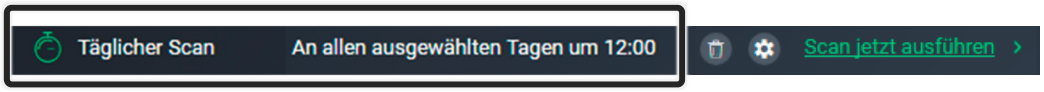
Im Fenster EINSTELLUNGEN geben Sie einen **Namen** für den geplanten Scan ein und im Menüpunkt *Häufigkeit* einen Zeitplan und bei *Startzeit* einen Startzeitpunkt für den Scan auswählen. **Schritt 4**



Günstig sind dabei Zeiten, zu denen der Computer eingeschaltet ist, aber nicht unbedingt benutzt wird (z.B. Mittagspause), da ein Scan die Leistung **Schritt 5**

TIPP

des Rechners beeinträchtigt. Ihr geplanter Scan wird dann im unteren Teil des Programmfensters angezeigt.

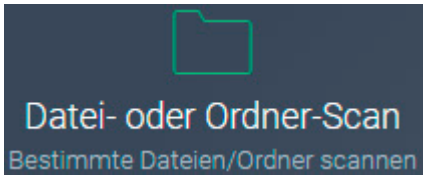


Der Scan wird nun automatisch immer am gewählten Tag und zur gewünschten Zeit durchgeführt.

Scan planen nach Ordnern

Schritt 6

Um gezielt spezielle Laufwerke oder auch ausgewählte Ordner zu scannen, aktivieren Sie die entsprechende Schaltfläche.



Schritt 7

Erweitern Sie im folgenden Fenster die entsprechenden Laufwerke, um einzelne Ordner auszuwählen und bestätigen Sie die Veränderung, um den Scan durchzuführen.