Schutz vor Malware - Antivirensoftware

Um sich vor Malware zu schützen, gibt es mehrere Möglichkeiten.

Manchmal reicht es schon, einfach nicht jede Meldung und jedes Popup, das beim Surfen im Internet auftaucht, zu akzeptieren. Ein einfaches **Nein** zu einer Installationsaufforderung oder ein wachsameres Surfen auf diversen Webseiten kann schon einiges verhindern.

Funktionsweise von Antivirensoftware

INFO

Was aber auf Dauer unbedingt notwendig ist, ist ein ***Antivirenprogramm***, das Schadsoftware erkennt und auch bereits einen Download blockiert, noch bevor die Schadsoftware auf dem Computer gelandet ist. Zusätzlich sollte so ein Antivirenprogramm, nicht nur Viren und Schadprogramme erkennen, sondern auch Mails, Downloads und optimaler Weise auch das System vor bösartigen Programmen schützen und es kann mögliche Schädlinge aufspüren, blockieren und beseitigen.

Das muss nicht unbedingt ein teures und aufwändig zu konfigurierendes Programm sein. Bei Windows 8 ist bereits ein Programm für den Schutz ins Betriebssystem integriert. Der **Defender** ist ein Tool, das zum einen das System kontrolliert und überwacht, damit es nicht kompromittiert wird und zum anderen einen Virenschutz enthält, der vor den meisten Bedrohungen schützt.

Trotzdem ist es nicht von Nachteil, wenn zusätzlich eine Antivirensoftware eines Drittanbieters installiert wird. Für den privaten Bereich ist ein kostenloses Produkt, welches von manchen Anbietern erhältlich ist, meist ausreichend.

In einem Unternehmen ist in der Regel eine Reihe von Schutzmechanismen vorhanden, die zentral verwaltet werden und somit Clients und Server schützen.

Grenzen eines Antivirenprogramms

INFO

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.

Natürlich ist auch damit kein 100%iger Schutz möglich. Was hilft das beste und sicherste Auto, wenn der Fahrer einen Fehler macht und einen Unfall verursacht? So ähnlich verhält es sich bei einem Computer. 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 oder verdächtige Datei samt Schadprogramm entweder gelöscht werden oder in ***Quarantäne*** verschoben werden, die Daten landen damit in einem Quarantäne-Ordner und jeder Zugriff wird unterbunden.

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

Daher kann es in bestimmten Situationen besser sein, eine solche Datei in den Quarantäne-Ordner verschieben zu lassen und dann zu versuchen, die Datei vielleicht mit einem anderen Tool „desinfizieren“ zu lassen. 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.

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 von Ordner und Laufwerken planen
- Einen Scan durchführen

Schritt für Schritt:

Da es viele Produkte im Bereich Antivirensoftware gibt, wird hier die Übung exemplarisch am Beispiel von **AVG AntiVirus FREE 2013** durchgeführt, weil der Defender unter Windows 8 leider keine Möglichkeit bietet, Zeitpläne zu erstellen.

ACHTUNG

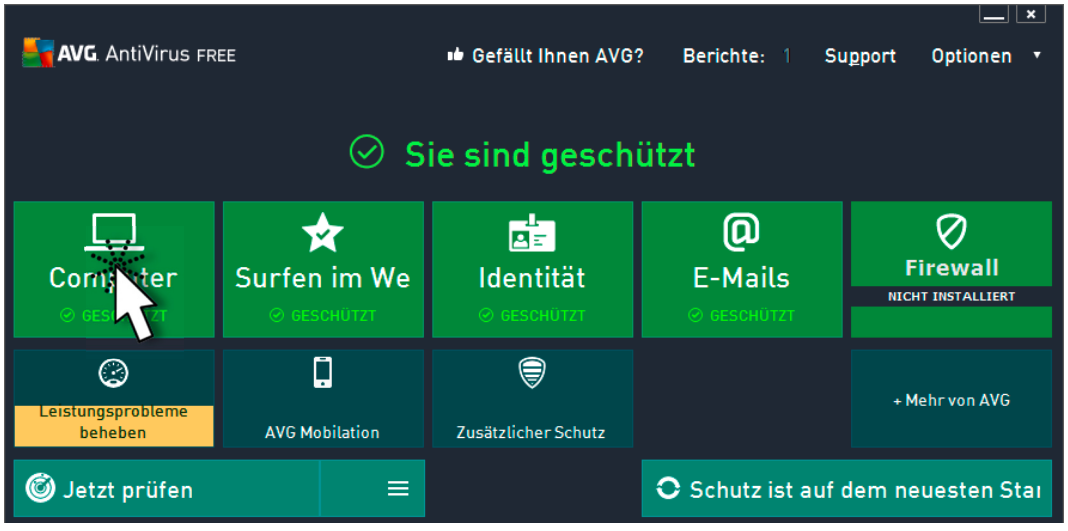
Für die Installation und Konfiguration von Antivirensoftware sind administrative Rechte notwendig.

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

Scan planen

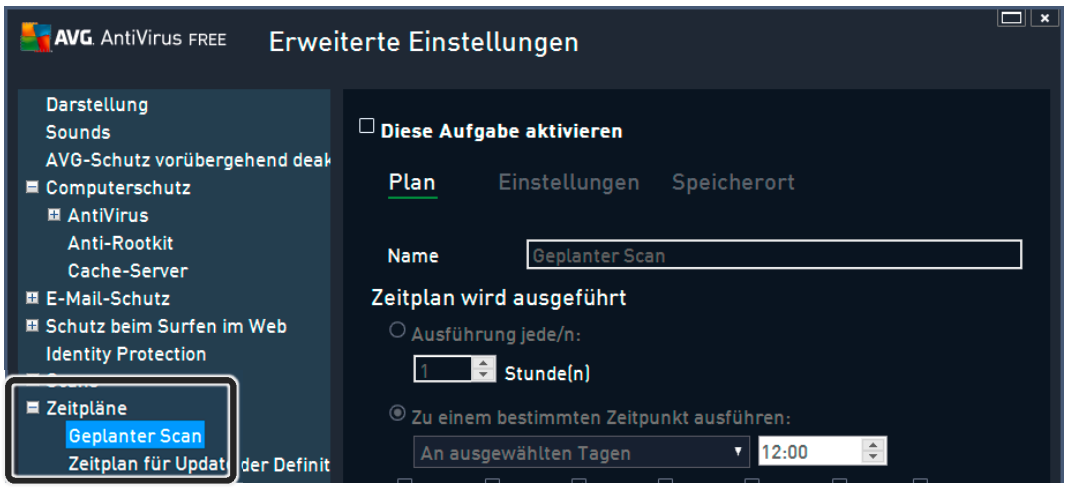
Schritt 1 Starten Sie die Konsole des Virenschutzprogramms mit einem Doppelklick auf das entsprechende Symbol im Infobereich der Taskleiste.

Schritt 2 Klicken Sie dann auf die COMPUTER.



In dem darauf folgenden Fenster klicken Sie auf EINSTELLUNGEN. **Schritt 3**

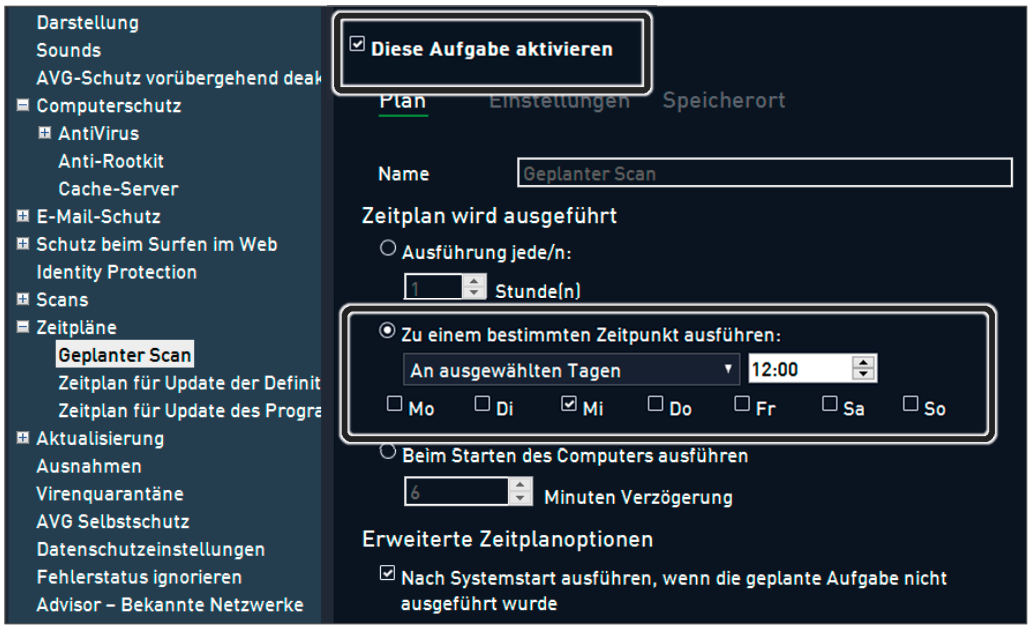
Um regelmäßige Scanvorgänge zu planen, erweitern Sie den Eintrag ZEITPLÄNE und wählen den Unterpunkt GEPLANTER SCAN. **Schritt 4**



Um die Einstellungen zu ändern, aktivieren Sie das Kontrollkästchen DIESE AUFGABE AKTIVIEREN. Danach können Sie die gewünschten Einstellungen für Uhrzeit und Wochentag einstellen bzw. aktivieren. **Schritt 5**

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

TIPP



Schritt 6 Um gezielt spezielle Laufwerke oder auch ausgewählte Ordner regelmäßig zu scannen, aktivieren Sie im Bereich SPEICHERORT die Option BESTIMMTE DATEIEN ODER ORDNER SCANNEN und erweitern Sie die entsprechenden Laufwerke, um einzelne Ordner auszuwählen.

Schritt 7 Bestätigen Sie dann die Veränderung der Einstellungen

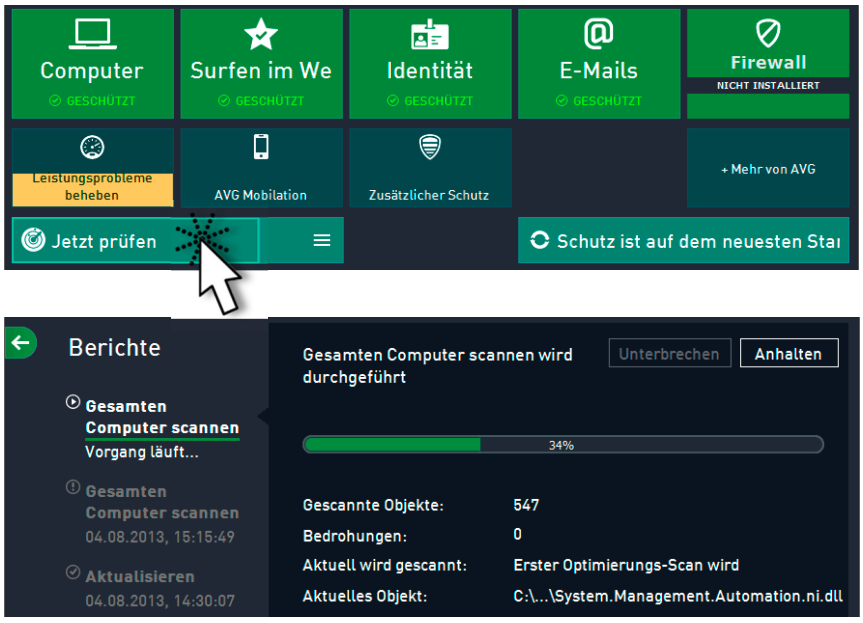
Der Scan wird nun automatisch immer am gewählten Tag und zur gewünschten Zeit in den gewählten Ordnern durchgeführt.

Scan durchführen

Um einen Scanvorgang bei Bedarf auch ohne Zeitplan durchzuführen, kann der Scan einfach mit entsprechenden Einstellungen gestartet werden.

Schritt 8

Starten Sie erneut die Konsole und klicken Sie auf JETZT PRÜFEN, um einen Scanvorgang zu starten, der den ganzen Computer mit allen Laufwerken prüft.



Wenn Sie spezielle Einstellungen für einen sofortigen Scan definieren wollen, können Sie auf

SCAN-OPTIONEN klicken. Hier haben Sie die Möglichkeit, gezielt nur bestimmte Laufwerke, Ordner und Dateien zu wählen und zu scannen.