Was leisten Virenscanner ?

Ein Beitrag von MobyDuck

In dieser Lektion wollen wir uns mit Virenscannern und anderen Programmen zur Schädlingsbeseitigung beschäftigen.

Virenscanner

Als Einstimmung erst mal eine kleine, fiktive Geschichte, die seit langem im Internet kursiert:

http://oschad.de/wiki/index.php/Virenscanner

Einiges an dieser Story mag überzeichnet sein, sie bringt jedoch die grundsätzliche Schwäche von Virenscannern auf den Punkt. Doch sehen wir uns die Funktionsweise der AV-Programme kurz an:

Die gängigen AV-Programme verfügen zunächst über einen Hintergrundwächter (On-Access-Scanner), der – wie der Name schon sagt – im Hintergrund aktiv ist und beim Zugriff auf schädliche Dateien Alarm schlagen soll. Außerdem bieten alle AV-Programme die Möglichkeit, einzelne Dateien bis hin zu ganzen Festplatten auf Malware zu durchsuchen, sog. On-Demand-Scanner. Letztere sollen vor allem die Viren im weiteren Sinne aufspüren, die, aus welchen Gründen auch immer, von dem Hintergrundwächter übersehen wurden. Teilweise wird die Meinung vertreten, ein On-Access-Scanner sei überflüssig, da man sowieso jede heruntergeladene Datei on demand scannen sollte und das automatische Ausführen von Malware bei richtiger Konfiguration (siehe Lektion 2: Einstellungen in Windows, Browser und Mailprogramm) zumindest sehr erschwert sei. Da dies jedoch einiges an Selbstdisziplin und Wissen erfordert, möchte ich mich der Meinung nicht vorbehaltlos anschließen. Es macht schon Sinn, den On-Access-Scanner mitlaufen zu lassen.

In der eingangs erwähnten Geschichte sind die Schwächen der Virenscanner anschaulich beschrieben. Es ist nun mal so, dass die AV-Programme vor allem mit Viren-Signaturen arbeiten, d.h. die Scanner vergleichen die Dateien mit Listen bekannter Malware. Dies bedeutet natürlich zwangsläufig, dass der Schädling vor der Signatur da ist.

Darüber hinaus versuchen die Malware-Autoren, den Scannern die Arbeit zu erschweren. Die einfachste Methode besteht darin, den Code der Malware abzuändern. Die Flut an Rbots ist ein naheliegendes Beispiel, bei www.sophos.de findet man inzwischen Hunderte Varianten. Es hängt zunächst von der Qualität der Virensignaturen ab, dass möglichst viele Varianten erkannt werden. Falls nicht, ist wiederum die Schnelligkeit der AV-Programmhersteller gefragt, um angepasste Signaturen nachzuschieben.

Es gibt jedoch noch jede Menge andere Tricks, die Existenz von Malware vor den Scannern zu verschleiern, einige Beispiele: Manche Schädlinge versuchen, einmal ausgeführt, die Scanner einfach abzuschalten. Oder man versteckt die Malware in gepackten, passwortgeschützten Archiven. Oder die Malware lädt sofort bei erster Gelegenheit weiteren schädlichen Code nach. Man kann sich sodann sogenannter Rootkits bedienen, um den Malwarebefall zu verbergen, vgl.

http://www.heise.de/security/artikel/38057/0

Oder man benutzt kyrillische Zeichen. Oder man versteckt den Schädling in sogenannten Alternate Data Streams. Und so weiter. Die Möglichkeiten sind grenzenlos.

Damit wird hoffentlich auch deutlich, warum ich regelmäßig meine Stirn in Falten lege, wenn User stolz behaupten, sie seien seit zig Jahren ohne Malware-Befall im Internet unterwegs. Hellseherei funktioniert nur bei den wenigsten Menschen.

Wir haben gesehen, dass zwischen dem Auftauchen eines Schädlings und dem Bereitstellen der Signatur eine gewisse Zeit vergeht. Um diese Lücke zu schließen, verwenden die meisten AV-Programme heuristische Methoden, um neue Malware dennoch zu entdecken. Vereinfachend gesagt lauert die heuristische Suche auf verdächtige Aktivitäten von Dateien, etwa ob sie andere Programme starten. Die heuristische Methode ist naturgemäß nicht sehr zuverlässig, da sie nur auf allgemeinen Erfahrungssätzen beruht. Sie ist daher ein häufiger Auslöser von Fehlalarmen.

Schließlich bieten viele AV-Programme noch die Möglichkeit, ein- und ausgehende Mails auf Malware zu scannen (Mailscan). Unbedingt nötig finde ich dies nicht. Klickt man auf einen verseuchten Mail-Anhang, dann sollte sich der Scanner sowieso melden. (Abgesehen davon, dass man sowieso nicht auf unbekannte Anhänge klickt und keine HTML-Mails empfängt.) Aber wie gesagt, das ist Geschmackssache, jedenfalls schadet der Mail-Scan auch niemanden.

So, und welches AV-Programm ist nun als „gut“ zu empfehlen? Das wichtigste Kriterium ist natürlich die Erfolgswahrscheinlichkeit. Leider machen viele Zeitschriftentests dieses Kriterium vor allem an der Erkennungsrate fest. Dies ist ein Denkfehler. Wie wir gesehen haben, kann ein AV-Programm niemals alle Schädlinge erkennen. Es ist daher statistisch zu vernachlässigen, ob ein Programm z.B. 90% oder 95% aller Schädlinge erkennt. Auch fragt sich, „95%“ von was? Die Tester bedienen sich zunächst sogenannter „Wildlists“, d.h. mehr oder weniger vollständiger Listen der bekannten Schädlinge. Dazu kommen „Zooviren“, d.h. Viren, die im Labor eben für solche Tests programmiert wurden. Ganz egal, wie vollständig diese Listen sind, wenn der User den Test liest, sind die Listen schon längst veraltert und die Erkennungsraten können aktuell ganz anders aussehen.

Darüber hinaus, was hat man von einer hohen Erkennungsrate in der Vergangenheit, wenn die Signaturen zu selten aktualisiert werden? Außerdem sollte das Programm möglichst intuitiv zu bedienen sein, damit der User auch wirklich regelmäßig aktualisiert.

Also setzt sich die Qualität – und damit die Erfolgswahrscheinlichkeit - eines AV-Programms aus den Faktoren Umfang und Qualität der Signaturen, Update-Intervalle und Ergonomie zusammen. Wie der User diese Faktoren für sich gewichtet, mag er selbst entscheiden.

Onlinescanner

Sobald der Verdacht auf Schädlingsbefall besteht, sollte man mit einem anderen Virenprogramm nochmals gegenprüfen. Häufig wird empfohlen, hierzu die von mehreren Firmen angebotenen Online-Scanner zu benutzen. Dummerweise benötigen diese Scanner zumeist den Internet Explorer, um ActiveX-Controls abzulegen. Andere begnügen sich mit j-a-v-a. Aber egal, ein Sicherheitsprogramm, das zur Ausführung unsichere Techniken braucht, ist ein Widerspruch in sich. Ich halte es für sinnvoller, für den Gegencheck auf AVG oder Antivir auszuweichen. Bewährt hat sich vor allem auch ein Check mit e-Scan . Die Programme sind für den Privatanwender kostenlos.

Stinger & Co.

Geradezu in Mode gekommen sind sogenannte Entfernungstools, die sich darauf beschränken, bestimmte Schädlinge aufzuspüren und zu löschen. Der bekannteste Vertreter ist wohl Stinger. Auch Microsoft beteiligt sich neuerdings durch den Virencheck beim XP-Update. Ich bin skeptisch. Mit etwas Glück entfernen diese Tools die angegebenen Schädlinge, nachgeladene Inhalte bleiben jedoch unbehelligt. Ist ein System durch einen Schädling mit Backdoor-Funktionen kompromittiert, dann ist meiner Meinung nach dieses System nicht mehr zu gebrauchen und man muss neu aufsetzen. Dies gilt umso mehr, desto komplexer das Zusammenspiel zwischen ursprünglichem Schädling und nachgeladenem Code wird, vgl. hierzu Lektion 1. Somit wird der User häufig nach der „erfolgreichen Reinigung“ mit derartigen Tools mit einem nach wie vor verseuchten System allein gelassen.

Spyware-Tools

Nach dem Selbstverständnis der Spy- und Adware-Hersteller handelt es sich bei ihren Programmen um keine Malware, vgl. Lektion 1. Für die Hersteller von AV-Software kann es daher rechtlich problematisch sein, entsprechende Signaturen aufzunehmen. Man muss daher meist auf spezielle Tools ausweichen. Die bekanntesten sind wohl Adaware und Spybot Search & Destroy, die meiner Meinung nach auf jedes System gehören. Die Hersteller von Spyware sind mindestens so rege wie die Wurmautoren, es tauchen laufend neue Programme auf. Allerdings haben die Autoren der Anti-Spyware-Tools nicht den riesigen Apparat der großen AV-Hersteller zur Verfügung. Sie können daher nicht laufend die Signaturen aktualisieren. Außerdem tun sich die Autoren im Einzelfall schwer, welche Programme denn nun als Ad- oder Spyware zu definieren sind. Verständlicherweise wollen sie teure Schadensersatzprozesse vermeiden. Dementsprechend leidet auch die Erkennungsrate, siehe auch hier. Man sollte daher beide Tools installieren. Was das eine Tool nicht findet, erkennt – hoffentlich – das andere. Manchmal helfen die Tools auch bei der Beseitigung von Hijackern.

HijackThis

Allerdings bestehen nahezu unbegrenzte Möglichkeiten, einen Hijacker zu fabrizieren, d.h. den Browser auf unerwünschte Seiten zu „entführen“. Daher setzen die wenigen Tools, die das Entfernen von Hijackern versprechen, überwiegend auf heuristische Methoden oder sind auf die Entfernung ganz bestimmter Hijacker spezialisiert. Entsprechend bescheiden ist der Erfolg. Hijackthis setzt anders an und listet die meisten Programme, die beim Computerstart mitgestartet werden und meldet weitere Veränderungen am System. Daher ist das Programm auch beim Aufspüren anderer Schädlinge nützlich. Das weitere Vorgehen muss dann der User selbst entscheiden. Eine Anleitung zum Einsatz von Hijackthis findet sich hier:

http://www.dedies-board.de/wbb2/thread.php?threadid=183

Allerdings braucht man schon ein wenig Erfahrung, um das Logfile sinnvoll auszuwerten. Es gibt zwar die Möglichkeit der automatischen Auswertung auf

www.hijackthis.de

Diese arbeitet jedoch noch nicht zufriedenstellend und ist daher allenfalls eine erste Orientierung für erfahrene User. Wer sich die Auswertung nicht zutraut, sollte erfahrene Bekannte oder im Forum fragen.

Als Ergebnis können wir festhalten: Es ist letztendlich egal, welches der gängigen AV-Programme eingesetzt wird. Man sollte allerdings konsequent auf die Aktualität der Signaturen achten und sich bewusst sein, dass ein AV-Programm keinen hundertprozentigen Schutz bietet, sondern nur ein Aspekt in einem umfassenden Sicherheitskonzept ist.