Schadsoftware

Erkennung, Arten und Bekämpfung

Inhaltsangabe

Schadsoftware aus der Sicht des Endanwenders

1. Wie infiziere ich mich mit Schadsoftware

Im Gegensatz zu einer Infektion mit biologischen Viren kann dies im Fall von Computerviren bzw. Schädlingen vermieden werden, wenn der Benutzer diesem Thema genug Aufmerksamkeit schenkt. Die meisten Viren können ein System nur befallen wenn diese vom Benutzer aktiviert werden. Hier zählen die Entwickler auf das Unwissen und die Naivität vieler PC-Benutzer.

Schadsoftware kann den PC auf 3 Arten befallen:

1.1. Internet

Der einfachste Weg für Schadsoftware auf den PC zu kommen ist wohl der Download von infizierten Dateien. Diese müssen danach allerdings erst ausgeführt bzw. bei Archiven entpackt werden um sich auf dem System installieren zu können. Auch durch den Besuch von Internetseiten kann sich unerwünschte Software auf dem PC installieren. Dabei geschieht dies meist durch so genannten „Aktiven Inhalt“, der in Skriptsprachen verfasst ist. Auch das einfache Wegklicken von nervigen Meldungen kann die Installation von Software starten.

1.2. E-Mail

Viele Viren und an andere Schädlinge erreichen den Anwender per E-Mail. In den meisten Fällen sind die Dateianhänge verseucht und durch das Öffnen dieser wird der Schädling aktiv. So kann es aber auch durch das alleinige Lesen und dem damit verbundenen Öffnen der Mail zu einer Infektion kommen. In den seltensten Fällen versenden Absender absichtlich Viren. Ist dessen PC befallen, können sich Viren automatisch an ausgehende Mails anhängen.

1.3. Wechselmedien

Der dritte Weg ist der wohl älteste und von den meisten am wenigsten bedachte. So birgt nicht nur das Internet und der Mail-Verkehr seine Gefahren, auch auf Wechselmedien wie Disketten, CD‘s, DVD‘s aber auch auf den sehr beliebten USB-Sticks können sich Schädlinge befinden und sich alleine durch das Anschließen bzw. das Einlegen des Datenträgers in ein Laufwerk auf dem eigenen PC festsetzten.

2. Wie erkenne ich Schadsoftware

Ist der Rechner mit einem Virus oder der gleichen infiziert, so kann es sein, dass man als Anwender keinen Unterschied zu vorher merkt oder aber das sich die Auswirkungen massiv bemerkbar machen.

- Im Idealfall schlägt der installierte Virenscanner Alarm und gibt eine entsprechende Meldung aus.
- Sollte kein Virenscanner installiert sein oder der Virenscanner kennt die Schadsoftware noch nicht, so kann sich diese folgender Weise bemerkbar machen:
    - Unerklärliche Fehlermeldungen oder sogar Systemabstürze.
    - Ungewöhnliche Systemlast, d.h. ungewöhnlich hohe Prozessor- und Arbeitsspeicherauslastung.
    - Ungewöhnliche Systemaktivitäten, wie automatisches Starten von Programmen oder ständiger Zugriff auf die Festplatte. Natürlich sind solche

Beobachtungen nur im Ruhezustand, d.h. ohne Benutzeraktivität, des PC‘s sinnvoll.
- Werbeeinblendungen am Desktop oder mittels Popups auch wenn der Webbrowser geschlossen ist. Ungewöhnlich viele Popups im Webbrowser, auch auf Seiten auf denen ansonsten keine Werbepopups üblich sind (z.B.: www.google.at)
- Eine der gravierendsten Auswirkungen ist es wohl wenn Dateien beschädigt oder gelöscht werden.

3. Wie kann ich Schadsoftware entfernen

Das Entfernen von Schadsoftware ist ein sehr komplexes Thema, nicht immer einfach und meistens mit sehr viel Aufwand und Zeit verbunden.

- Die von der Theorie her einfachste Variante ist wohl das Löschen von befallenen Dateien bzw. das Deinstallieren von Schadsoftware. Doch von Hand ist dies meist ein unmögliches Unterfangen.
- Besser geht es hier schon all jenen die einen Virenscanner auf dem System installiert haben und dieser den Virus erkennt und auch entfernen kann.
- Sollte der systemeigene Virenscanner auf Grund der Schadsoftware nicht mehr ordnungsgemäß funktionieren oder den Schädling erst gar nicht erkennen, kann man die befallene Festplatte auch mit Hilfe eines Zweitsystems scannen. Hierzu kann eine Live-CD, wie Knoppix oder BartPE, oder ein Zweitrechner, in den man die Festplatte einbauen und von einem sauberen System aus scannen kann, helfen. Achtung beim Einbau der infizierten Festplatte in einen anderen Rechner besteht die Gefahr, dass auch dieser infiziert wird.
- Weis man genau um welchen Schädling es sich handelt kann man auch so genannte Removaltools verwenden. Dies sind kleine Tools, meist von Antivirensoftwareherstellern, die genau für das Entfernen eines speziellen Schädlings ausgelegt sind.
- Sollten all diese Versuche fehlschlagen, hilft im äußersten Notfall dann nur noch die Neuinstallation des Systems. Dies ist nach einem starken Virenbefall auch zu empfehlen.

4. Wie kann ich mich vor Schadsoftware schützen

So weit, dass man einen Virus, Trojaner, etc. entfernen muss, sollte es erst gar nicht kommen. So gilt auch hier wieder einmal Vorsorgen ist besser als Nachsorgen.

Hier einige Dinge die man Beachten sollte bzw. tun kann:

4.1. Softwareupdates

Regelmäßige Softwareupdates und Aktualisierungen der Hersteller bessern nicht nur Anwendungsfehler sonder auch Sicherheitslücken aus. Vor allem die Aktualisierung von Betriebsystem, Office-Paket, Virenscanner und Firewall sollte regelmäßig durchgeführt werden.

4.2. Virenscanner

Die Installation eines Virenscanners ist nicht nur bei mit dem Internet verbundenen Rechnern sinnvoll. Die reine Installation ist ein guter Anfang, das war es aber auch schon. So sollten regelmäßig die aktuellen Virendefinitionen des Herstellers

eingespielt werden und auch ab und dann ein manueller Scan des kompletten PC-Systems veranlasst werden.

4.3. Firewall

Auch eine Firewall kann vor dem Befall von Schadsoftware schützen bzw. die Auswirkungen eindämmen. So blockieren diese z.B. Dialer oder Trojanische Pferde. Viele Firewalls haben auch eine Popup-Blocker integriert der mitunter sehr nützlich sein kann.

4.4. Spyware-Removal-Tool

Das Thema Spyware ist bei Herstellern von Antiviren-Software erst vor kurzer Zeit angekommen und so gibt es bereits eigenständige und sehr ausgereifte Tools (z.B.: Spybot Search&Destroy, Lavasoft AdAware) die sich darauf spezialisiert haben Spyware und Dialer zu erkennen bzw. zu entfernen. Auch hier gilt regelmäßig updaten und vor allem benutzen, da der Scanvorgang bei diesen Tools meist manuell gestartet werden muss und keine permanente Überwachung wie von Virenscannern erfolgt.

4.5. Eingeschränkte Benutzerrechte

Ein weiterer Sicherheitsfaktor ist das Arbeiten mit eingeschränkten Benutzerrechten. Hat der Benutzer keine Rechte Software zu installieren so hat diese der Virus auch nicht und kann sich somit nicht im System festsetzen. Leider ist in der großen Windowswelt genau dieser wohl am meisten Sicherheit, nicht nur im Bezug auf Schadsoftware, bringende Ansatz nicht Gang und Gebe. Viele Benutzer, nicht nur auf Privatrechnern sondern auch in Firmen, arbeiten immer noch mit Administratorrechten und betteln somit schon fast um Viren. In der Unix-Welt ist das Konzept von Benutzerrechten seit Anfang an implementiert und somit auch Standard. Man wird wohl selten jemanden mit Root-Rechten auf einem Linux-Rechner arbeiten sehen. Hier hat vor allem Microsoft noch ein großes Stück arbeit zu leisten und wird mit Windows Vista auch ein entsprechendes Rechtesystem und hoffentlich auch das dazu notwendige Denken einführen.

4.6. Aktive Inhalte deaktivieren

Durch das alleinige Betrachten von Webseiten kann man sich noch keinen Virus einfangen. HTML bietet von Haus aus keinen Möglichkeiten auf den Client-Rechner Daten zu verändern oder zu schreiben. Allerdings gibt es einige Skriptsprachen die diese fehlende Funktion auf Webseiten nachrüsten. Und so kann mittels JavaScript, Java oder ActiveX, wenn der Anwender nicht entsprechende Restriktionen setzt, nach belieben auf dem Host-Rechner herumgewerkt werden. Die einfachste Methode hier mehr Sicherheit einzuführen ist das deaktivieren dieser Elemente. Dies führt allerdings dazu, dass viele Seiten nichts mehr darstellen oder an Funktionalität verlieren, daher ist dies keine alltagstaugliche Lösung. Jedoch sollten, über die Browsereigenschaften, die Aktionen die solche Skripte ausführen dürfen so weit wie möglich (meist durch die Voreinstellungen schon getroffen) eingeschränkt werden.

4.7. Automatische Mail-Vorschau deaktivieren

Ein weiterer Punkt den viele Anwender nicht bedenken ist, dass sich Viren durch das öffnen von E-Mails bereits im System einnisten können. Hat man nun die automatische Vorschau aktiviert, werden Mails durch das alleinige anklicken schon geöffnet und so hat man, auch wenn man ein verdächtiges Mail entdeckt, nicht einmal

die Chance dieses zu Löschen bevor es geöffnet wird. Also überlegen ob man diese Funktion wirklich benötigt und am Besten deaktivieren.

4.8. Sicherungskopien

Sollte es doch zu einer Infektion kommen so ist der der über eine Sicherheitskopie, ein so genanntes Backup, verfügt auf jeden Fall immer auf der besseren Seite. So kann zur Not auch einmal das gesamte System gelöscht und vom Backup wiederhergestellt werden. Auch vor dem Verlust von Daten durch Schadsoftware oder versehentliches Löschen dieser ist man so halbwegs sicher, so lange man seine Sicherungskopien ständig auf dem aktuellen Stand hält.

4.9. Know-How

Und zu guter letzt hilft auch noch eine Portion Hausverstand und etwas Mitdenken im Umgang mit verdächtigen Mails, dubiosen Internetseiten bzw. Downloads, sowie fremden Datenträgern um sich vor Schadsoftware zu schützen. Nur der der Gefahren kennt und erkennt kann sich auch vor diesen schützen.

Schadsoftware aus der Sicht des Experten

1. Gefährdung der unterschiedlichen Betriebssysteme

Die Art des eingesetzten Betriebsystems hat großen Einfluss darauf wie hoch die Gefahr eines Viren- bzw. Schadsoftwarebefalls ist. So gibt es für Windows rund 60.000 Viren, während es für Linux gut 50 und für Mac OSX praktisch keine gibt. Wie sich der Umstieg Apples von der PowerPC- auf die Intelplattform im Bezug auf Viren für Max OSX bemerkbar macht ist noch abzuwarten.

Doch warum gibt es für Windows so viele Viren und für Linux bzw. Mac OSX so wenige. Dies beruht nicht auf der Unsicherheit einzelner Systeme sondern in dem Nichtwissen der Anwender, der Verbreitung, sowie in der falschen Konfiguration eines Systems. So haben alle drei dieser Betriebssysteme eine wirkungsvolle und ausgeklügelte Rechteverwaltung. Doch nur kaum ein Privatanwender benutzt diese auch auf seinen PC. Gerade dieser Umstand, dass viele HeimPC-Anwender mit Administratorrechten arbeiten und sich nur schlecht mit den Gefahren bzw. mit dem eigenen System auskennen macht Windows für Virenschreiber so interessant. So arbeitet ein Benutzer nach der Neuinstallation eines Windowssystems oder auch auf fertig installierten, im Fachhandel gekauften, Rechnern von Beginn an als Administrator. Ein Paradies für Viren. Im Sektor Linux, dass für allem im Serverbereich zum Einsatz kommt, ist das Arbeiten mit eingeschränkten Rechten Alltag und auch das Wissen über das System ist hier viel höher da Linux meist im kommerziellen Umfeld betrieben wird, wo Sicherheitsstandards weit aus höher und Fachkräfte am Werk sind. Anders als bei Viren sieht es jetzt bei Würmern aus. Da Internetserver meist unter Linux bzw. Unix-Derivaten betrieben werden ist dieses Betriebssystem ein beliebtes Ziel von Wurmautoren geworden.

2. Arten von Schadsoftware

Es gibt unzählige Arten von Malware (malicious = boshaft), zu Deutsch Schadsoftware. Dabei bezeichnet Malware Software die bewusst Schaden anrichtet oder sich gegen den Willen des Benutzers installiert. Nicht jede Schadsoftware löscht sofort Daten oder bringt das System zum Absturz. Viele dieser Schädlinge dienen auch zum Ausspionieren von Daten oder zum Ärgern des Benutzers durch Werbung und lästige Meldungen.

2.1. Trojaner

Trojaner sind Programme die versuchen sich mit Hilfe von harmlos aussehenden Dateien auf den PC zu schmuggeln. Dabei verstecken sie sich in Funktionen von Programmen und sind daher bei Hackern sehr beliebt, da die Chance entdeckt zu werden sehr gering ist. Viele Trojaner sind daher nicht auf das Zerstören sondern auf das Ausspähen eines Systems ausgelegt. Dabei kann man unter folgenden Arten unterscheiden:

2.1.1. Remote-Access-Trojaner

Remote-Access-Trojaner wie Back Orifice oder Netbus erlauben dem Angreifer die vollständige Kontrolle über das System zu erlangen. Angefangen über kleine Systemmanipulationen bis hin zum Neustart ist alles möglich.

2.1.2. Mail-Trojaner

Mail-Trojaner verfügen über ein eigenes Mail-Programm um Daten an den Angreifer zu senden. Diese werden vor allem zum Ausspähen von Kennwörtern

und Benutzerdaten benutzt. Kann ein Trojaner seine Informationen nicht automatisch übermitteln, ist dies ein so genannter Keylogger.

2.1.3. Telnet-Trojaner

Telnet-Trojaner öffnen einen Zugang per Telnet, das zum Fernwarten von Servern benutzt wird. Der Angreifer kann sich dann ungeniert einloggen und über die Kommandozeile Änderungen am System vornehmen.

2.1.4. FTP-Trojaner

FTP-Trojaner starten einen eigenen FTP-Server. Dadurch kann der Angreifer Dateien vom infizierten System herunterladen aber auch welche aufspielen.

2.1.5. Keystroke-Trojaner

Keystroke-Simulatoren übersetzen die Befehle eines Hackers in simulierte Tastatureingaben. Dadurch kann das System nicht zwischen den Eingaben des Benutzers und denen des Angreifers unterscheiden.

2.2. Rootkits

Rootkits werden auf einem System installiert um Malware zu verstecken oder Logins des Angreifers zu tarnen. Auch Sony BMG kam unlängst in die Schlagzeilen, da der Kopierschutz von CD‘s und DVD‘s der Firma mittels eines auf dem System installierten Rootkits verborgen wird. Auch die Firma Kinowelt verkauft im Moment DVD‘s die einen Rootkit auf dem System installieren.

Auch bei Rootkits gibt es verschiedenen Arten:

2.2.1. Kernel Rootkits

Kernel Rootkits ersetzen Teile des Kernels, also des Betriebsystemkerns, durch eigenen Code um sich selbst zu tarnen und dem Angreifer Funktionen auf Betriebsystemebene bereit zu stellen. Diese Rootkits manipulieren entweder direkt den Kernel oder werden unter Linux als Kernelmodule nachgeladen. Unter Windows werden diese meist als sys-Treiber realisiert.

2.2.2. Userland Rootkits

Userland Rootkits sind vor allem unter Windows sehr beliebt. Diese stellen meist eine DLL zu Verfügung die direkt in Prozesse injiziert wird. Wird diese DLL geladen, modifiziert sie API-Funktionen, dadurch können Informationen gezielt gefiltert und modifiziert wird.

2.2.3. Speicher Rootkits

Speicher Rootkits existieren, wie ihr Namen vermuten lässt, nur im Speicher. Ein Neustart des Systems lässt diese Rootkits dann aber auch wieder verschwinden.

2.3. Adware

Adware dient zur Zustellung von Werbematerial oder zum Ausspionieren von Benutzergewohnheiten, wie dem Surfverhalten. Dabei wird Adware des Öfteren in Zusammenhang mit Free- und Sharewareprogrammen installiert. Auch durch den Besuch einer Webseite und Scriptsprachen kann sich Adware auf dem Computer installieren. Meistens wird Adware unabsichtlich, durch Zustimmung von Lizenzbedingungen die in Verbindung mit Adware stehen, mit harmlos aussehender Software mitinstalliert.

2.4. Spyware

Spyware kann auf denselben Wegen wie Adware auf den PC gelangen. Im Unterschied zu Adware versucht Spyware unerkannt zu bleiben und Benutzerdaten wie Passwörter, Anmeldedaten oder Kontonummern auszuspähen und an Dritte zu übermitteln.

2.5. Dialer

Dialer sind Programme die über eine Modemverbindung eine gebührenpflichtige Nummer anrufen und typischer Weise Gebühren ablaufen lassen. Dabei können Dialer über dieselbe Art wie Spy- und Adware ihren Weg auf den PC finden. Meistens wählen sich diese ohne Wissen des Benutzers ein, der dann über die Telefonrechnung und die Mehrwertnummern dem Dialerbesitzer seine Anerkennung zeigen darf.

2.6. Joke-Programme

Joke-Programme stören oder manipulieren den normalen Betrieb eines PC‘s und versuchen so den Anwender abzulenken oder zu verärgern. Im Normalfall versuchen Joke-Programme keine Informationen zu sammeln oder Schaden anzurichten.

2.7. Wurm

Ein Wurm ist ein Programm, das sich selbst zu verbreiten versucht. Dazu nutzt es Datenträger, das Netzwerk, E-Mail, Instant-Messaging oder bekannte Schwachstellen von Systemen aus. Würmer infizieren somit auch keine Dateien. Im Gegensatz zu Viren warten Würmer nicht darauf vom Anwender aktiviert zu werden sondern versuchen sich selbst zu aktivieren.

2.8. Virus

Siehe Kapitel 3.

3. Das Virus

Das Virus ist ein sich selbst vermehrendes Computerprogramm. Die Klassifizierung als Virus bezieht sich hier auf die Selbstverbreitungsfunktion. Einmal gestartet können sie vom Benutzer nicht nachvollziehbare Änderungen am System durchführen. Malware wird von Anwendern oft fälschlicherweise schlicht als Virus bezeichnet, da der Unterschied zwischen den einzelnen Schädlingen oft nicht erkennbar oder bekannt ist.

3.1. Die Arten

3.1.1. Dateiviren/Linkviren

Dateiviren und Linkviren fügen sich in Dateien ein oder überschreiben diese einfach. Beim Ausführen der befallenen Datei wird zunächst das Virus und dann erst das Programm ausgeführt, damit der Anwender nichts merkt. Hat das Virus Programmcode überschrieben kann es zu Abstürzen der betroffenen Programme oder irreparablen Dateien kommen, diese lassen sich auch von Antivirussoftware nicht mehr retten und müssen gelöscht werden. Siehe Infektionsarten, um die verschiedenen Methoden von Datei- und Linkviren kennen zu lernen.

3.1.2. Makroviren

Makroviren benötigen Anwendungen die Dokumente mit eingebetteten Makros verarbeiten. Die meisten Office-Dokument-Typen unterstützen Makros und somit sind diese eine ideale Verbreitungsmethode. Vor allem ist den meisten

Anwendern nicht bewusst, dass auch ein einfaches Textdokument ausführbaren Code enthalten kann. Und so verbreitet sich diese Art von Viren rasant durch den Versand oder den Download von infizierten Dokumenten. Ein Schutz gegen Makroviren ist es nur zertifizierte Makros auszuführen. Da sich Makroviren meistens die „Funktion des automatischen Ausführens von eingebetteten Makros“ zu nutze machen, ist es am einfachsten dieses automatische Ausführen in Anwendungen zu deaktivieren.

3.1.3. Skriptviren

Skriptviren betten sich oft auf Unix-Maschinen in Bash-, Perl- oder Python-Skripte ein. Diese Viren sind aber eher selten anzutreffen, da das Skript erst von Hand ausgeführt werden muss um den Virus zu aktivieren. Eine Gefahr stellen diese für unzureichend abgesicherte Webserver die eine CGI-Schnittstelle bieten dar.

3.1.4. Bootsektorviren

Bootsektorviren nisten sich im MBR der Festplatte ein. Damit dürfen sie nicht größer als 444 Byte sein und müssen außerdem die Funktion des Bootloaders übernehmen. Ist diese Hürde erste einmal genommen kann der Virus den Start des Betriebssystem beeinflussen oder gar verhindern. Bootviren sind heute sehr selten geworden, zählen aber zu den hartnäckigsten ihrer Gattung.

3.1.5. Companionviren

Companion-Viren infizieren keine ausführbaren Dateien sondern benennen die ursprüngliche Datei um und erstellen eine Datei mit demselben Namen die den Virus enthält. D.h. es wird z.B. die Datei explorer.exe in explorer2.exe umbenannt. Danach wird vom Virus eine Datei mit dem Namen explorer.exe erstellt. Wird nun die explorer.exe aufgerufen wird zunächst der Virus ausgeführt und dieser startet dann eventuell noch die Datei explorer2.exe, also die Originaldatei, um keinen Verdacht aufkommen zu lassen.

3.1.6. Polymorphe Viren

Da Virenscanner Viren anhand von Signaturen und damit Codesegmenten identifizieren versuchen polymorphe Viren ständig ihre Gestalt zu verändern. Dies geschieht durch ständiges Verändern und Kopieren, oft in Verbindung mit variabler Verschlüsselung. Dabei muss allerdings immer ein Teil des Virus unverschlüsselt vorliegen. Nämlich jener der für die Entschlüsselung des restlichen Virus verantwortlich ist. An diesem Teil kann der Virenscanner den Virus identifizieren.

3.1.7. Retroviren

Das Ziel von Retroviren ist es Virenschutzprogramme und Firewalls zu deaktivieren. Dies geschieht oft durch löschen entsprechender Dateien. Dabei wollen sie sich nicht nur selbst vor Entdeckung schützen sondern öffnen auch allen anderen Viren und Hackern den Zugriff zum nun ungeschützten System. Diese Art von Virus ist sehr gefährlich, wenn auch noch nicht sehr verbreitet.

3.1.8. Stealthviren

Stealthviren versuchen ihre Existenz durch die Veränderung von Systemfunktionen zu verschleiern. So wird das Betriebssystem so manipuliert,

dass die veränderte Größe einer Datei nicht angezeigt wird oder das bei Aufruf der Datei immer noch die ursprüngliche Datei zurückgeliefert wird.

3.1.9. Testviren

Testviren enthalten keinen viralen Inhalt sonder sind nur per Definition als Virus zu erkennen. Jeder Virenscanner sollte eine solche Eicar-Testdatei (http://www.eicar.org/anti_virus_test_file.htm) erkennen und somit kann diese zum testen der Funktionalität eines Scanners genutzt werden.

3.1.10. Hoaxes

Hoaxes haben mit Viren im eigentlichen Sinn wenig zu tun. Hierbei handelt es sich um Falschmeldungen über Viren und deren Ansteckungsgefahren die per Mail verschickt werden. Durch den guten Willen der Leute solche Warnungen an Kollegen und Freunde weiterzusenden verbreiten sich diese Mails rasend und belasten die Infrastruktur bzw. nehmen Zeit in Anspruch, dass vor allem Betriebe wieder Geld kostet.

3.2. Der Aufbau

Viren sind unterschiedlichst aufgebaut und somit ist der generelle Aufbau schwer zu definieren. Der einzige Bestandteil der ein Computerprogramm zu einem Virus macht ist die Vermehrungsroutine.

Viren enthalten je nach Art einen oder mehrere der folgenden Funktionsteile:

3.2.1. Entschlüsselungsroutine

Die Entschlüsselungsroutine dient bei verschlüsselten Viren dazu, die verschlüsselten Daten wieder zu entschlüsseln um diese zur Ausführung zu bringen. Einige Virensignaturen machen sich diesen Teil für die Erkennung zu nutzen, da er oft einfacher als der restliche Teil des Virus erkannt werden kann.

3.2.2. Vermehrungsteil

Der Vermehrungsteil sorgt für die Vermehrung und Weiterverbreitung des Virus. Dies ist der einzige Teil den ein Virus benötigt um per Definition zu einem Virus zu werden.

3.2.3. Erkennungsteil

Mit Hilfe des Erkennungsteils wird überprüft ob eine Datei oder ein Programm bereits infiziert wurde oder nicht. Dieser Teil ist in fast allen nicht-überschreibenden Viren vorhanden. Wenn sich ein Virus immer wieder in dieselbe Datei schreiben würde, würde mit der Zeit die Dateigröße ansteigen und damit auch die Chance entdeckt zu werden. Somit wird jede Datei und jedes Programm von demselben Virus immer nur einmal infiziert.

3.2.4. Schadteil

Im Verhältnis zur Anzahl an Viren haben nur sehr wenige einen Schadteil, der auch wirklich erheblichen Schaden anrichtet. Dieser ist der Grund für die Angst vor Viren und beinhaltet den Code der z.B. Festplatten löscht oder Systeme zum Absturz bringt.

3.2.5. Bedingungsteil

Der Bedingungsteil ist dafür zuständig, dass der Schadteil ausgeführt wird. Dabei kann dieser zufällig oder mittels Trigger z.B. an einem bestimmten Datum oder bei überschreiten einer Dateianzahl ausgeführt werden. Viren ohne diesen Teil führen den Schadteil bei jeder Aktivierung aus.

3.2.6. Tarnungsteil

Der Tarnungsteil ist nur in wenigen und sehr komplexen Viren vorhanden. Er versucht durch Verschlüsselung oder Polymorphismus den Virus vor dem entdecken durch eine Antivirensoftware zu schützen. Es gibt allerdings nur eine geringe Anzahl von Viren denen dies noch gelingt.

3.3. Infektionsarten

Die Technik von Viren unter Windows oder Unix ist es einen eigenen Prozess zu starten der so unverdächtig wie möglich aussieht. Dies geschieht durch vergeben eines harmlosen Namens oder verstecken des Prozesses. Speicherresistente Viren verbleiben außerdem im Speicher auch wenn ihr Wirtsprogramm beendet wurde. Manche Viren versuchen sogar Funktionen des Betriebssystems umzuleiten oder zu manipulieren.

Nun gibt es verschiedene Arten wie eine Datei infiziert werden kann:

3.3.1. Dateien imitieren

Companion-Viren geben sich als eine bereits im System bestehende ausführbare Datei aus. Dabei wird die Originaldatei umbenannt und das Virus übernimmt deren Namen.

3.3.2. Dateien überschreiben

Überschreibende Viren überschreiben ganze Dateien oder Teile dieser. Die infizierte Datei wird dabei unbrauchbar, dieser Umstand macht es Virenscanner aber auch leicht diese zu entdecken.

3.3.3. Prepender

Bei dieser Art von Virus fügt sich das Virus am Anfang einer Datei an. Beim Ausführen wird zunächst der Virus gestartet. Dieses stellt im Arbeitspeicher dann den Originalzustand der Datei her, die normal gestartet werden kann. Außer einer kurzen Zeitverzögerung bemerkt der Anwender nichts.

3.3.4. Appender

Beim Appender-Virus fügt sich dieses an das Ende der infizierten Datei ein. Es manipuliert diese dann so, dass zunächst das Virus gestartet wird und dann mit Hilfe eines Einstiegspunkt das Wirtsprogramm ausgeführt wird. Diese Art von Viren ist relativ simple zu realisieren, da die Originaldatei nicht wie bei den Prependern im Arbeitsspeicher rekonstruiert werden muss.

3.3.5. Entry Point Obscuring

Entry Point Obscuring heißt zu Deutsch Verschleierung des Einstiegspunkts. Dabei sucht eine Routine einen Funktionsaufruf in der ausführbaren Datei, meist den zum Beenden des Programms, da dieser relativ leicht zu identifizieren ist, um diesen zu manipulieren. EPO-Viren sind schwer zu realisieren haben aber den Vorteil, dass sie sich in der Mitte der Datei befinden. Da viele Scanner, um

Zeit zu sparen, nur den Anfang und das Ende der Datei überprüfen bleiben EPO-Viren meist unentdeckt.

4. Virenscanner

Virenscanner ist nicht gleich Virenscanner und wie überall gibt es auch in diesem Bereich essenzielle Unterschiede.

4.1. Typen

4.1.1. On-Access-Scanner

On-Access-Scanner, zu Deutsch Echtzeitscanner, laufen im Hintergrund als Systemdienst (Windows) bzw. Daemon (Unix) und überwachen die Aktivitäten des Benutzers. Dabei werden alle Dateien, Programme, der Arbeitsspeicher und eventuell je nach Scanner auch der HTTP- und FTP-Transfer überwacht. Um dies zu ermöglichen werden Filtertreiber im System installiert, welche eine Schicht zwischen den Daten und den Anwendungen einziehen. Alle Dateizugriffe werden nicht mehr direkt auf das Dateisystem ausgeführt sondern über diesen Treiber abgewickelt. Somit kann der Scanner auch geöffnete Dateien scannen ohne, dass ein Programm oder das System etwas davon merkt. Der einzige Nachteil darin besteht in der dadurch etwas verminderten Systemleistung. Nun können Virenscanner eine von zwei verschiedene Strategien oder natürlich auch beide verfolgen:

- Scannen beim Lesevorgang
- Scannen beim Schreibvorgang

Die bevorzugte Strategie ist das Scannen bei Schreibvorgängen, da diese wesentlich seltener vorkommen und daher ressourcenschonender ist. Außerdem wird das Einspielen von infizierten Dateien ins System verhindert. Allerdings bietet diese Methode keinen Schutz, wenn sich bereits eine infizierte Datei im System befindet. Um die Belastung des Systems weiter zu verringern werden einige Dateiformate, oft Dateiarchive, nur zum Teil oder gar nicht gescannt. Daher sollte regelmäßig auch ein manueller Scan durchgeführt werden. Findet ein Echtzeitscanner etwas wird der Benutzer meist nach dem weiteren Vorgehen gefragt (Löschen, in Quarantäne verschieben, Reparieren).

4.1.2. On-Demand-Scanner

Der manuelle Scanner (On-Demand-Scanner) muss vom Benutzer per Hand gestartet werden. Erst dann sucht dieser nach Malware. Ein reiner On-Demand-Scanner bietet dem System also keinen ausreichenden Schutz, daher verbinden heutige Virenscanner On-Access und On-Demand.

4.1.3. Online-Scanner

Eine spezielle Form von On-Demand-Scannern sind Online-Scanner. Mit Hilfe dieser kann man sein System über das Internet scannen lassen. Viele große Antivirensoftwarehersteller bieten solche in Java oder mit Hilfe von ActiveX (nur für Internet Explorer) realisierte Scanner an. Diese sind auch hilfreich um als so genannte Second-Opinion-Scanner zu fungieren, also um sich eine zweite Meinung neben der des am System installierten Scanners einzuholen.

4.1.4. Netzwerkscanner

In großen Firmen kommen so genannte Netzwerkscanner zum Einsatz. Diese sind meist in einen Proxyserver integriert und scannen den ein- und ausgehenden Netzwerkverkehr. Hierzu zählen nicht nur E-Mails sondern eben auch der HTTP- und FTP-Transfer. So können Dateien oder E-Mails direkt am Server aussortiert oder desinfiziert werden, bevor sie den PC des Anwenders überhaupt erreichen. Allerdings ersetzten diese Netzwerkscanner den lokal installierten Scanner, gerade auf Notebooks, nicht.

4.2. Erkennungstechniken

Aufgrund der ständigen Weiterentwicklung der Schadsoftware und vor allem der Unvorhersehbarkeit der eingesetzten Techniken und Logiken kann praktisch kein Virenscanner 100%-tigen Schutz bieten. Virenscanner sollten daher immer nur als Ergänzung zu andern Vorsichtsmaßnahmen und nicht als der Schutz schlecht hin gesehen werden.

Grundsätzlich kann bei der Erkennung von Viren zwischen 2 Arten unterschieden werden:

4.2.1. Reaktiv

Die reaktive Erkennung von Viren ist die klassische Methode die in jeder Antivirensoftware zum Einsatz kommt. Dabei benötigt der Scanner erst eine Signatur (die vom Hersteller kommt) um den Virus an Hand dieser erkennen zu können.

4.2.2. Proaktiv

Unter Proaktiv bezeichnet man jene Techniken die ohne entsprechende Signaturen in der Lage sind Viren zu erkennen. Aufgrund der rapiden Zunahme und Wandlungsfähigkeit aktueller Schadsoftware wird die Zukunft der Erkennung in diesen Techniken (z.B.: Heuristik, Sandbox) liegen.

4.3. Scanengine

Die Scanengine ist jener Programmteil der Antivirensoftware die für die Untersuchung des Rechners auf Schädlinge zuständig ist. Für gewöhnlich sind diese Engines Module die sich unabhängig vom Rest des Programms aktualisieren lassen oder komplett ausgetauscht werden können. Es gibt auch Antivirus-Produkte die mehrere Scanengines von Drittanbietern unter einer Haube vereinen. Diese bieten zwar eine etwas bessere Erkennungsleistung, sind aber von der Performance sehr schlecht. Nicht nur die Aktualität der Signaturen, sondern vor allem die Fähigkeit Dateiarchive zu untersuchen kennzeichnen die Leistungsfähigkeit einer Scanengine.

Es gibt 3 bedeutende Möglichkeiten einen Virus zu entdecken:

4.3.1. Signaturen

Die Signaturen werden vom Hersteller zu Verfügung gestellt und enthalten Muster, sowie Regelmäßigkeiten, die einen Virus identifizieren können. Eine Signatur stellt also ein möglichst eindeutiges Erkennungsmerkmal dar. Dazu müssen mehrere Exemplare des Virus untersucht werden, da viele Viren mutieren, also ihren Code verändern können.

4.3.2. Heuristik

Heuristikverfahren suchen nach allgemeinen Merkmalen die Viren kennzeichnen können. Dabei gewinnt dieses proaktive Verfahren immer mehr an Bedeutung, da die Zeiträume in denen neue Varianten eines Virus auf den Markt kommen immer kleiner werden. Dabei wird die Heuristik niemals die Signaturen ersetzen, da die Chance unbekannte Malware zu erkennen sehr gering ist. Der Zugewinn an Sicherheit durch dieses Verfahren ist eher minimal bzw. beschränkt sich vor allem auf Mutationen schon bekannter Schädlinge.

4.3.3. Sandbox

Das 2001 vom Antivirensoftwarehersteller Norman entwickelte Verfahren der Sandbox zählt zu den proaktiven. Bei der Sandbox handelt es sich um eine Nachbildung der PC-Umgebung in der die verdächtige Datei ausgeführt wird. Dabei kann die Sandbox bei Bedarf auch Netzwerfunktionalitäten nachbilden. Bei der Ausführung der Datei erwartet sich die Sandbox eine typische Verhaltensweise, weicht diese einen gewissen Grad von der Vorgabe ab wird die Datei als potentielle Gefahr eingestuft. Dabei wird von der Sandbox jede Aktion und Veränderung die der Schädling auf dem System durchgeführt hätte protokolliert. Diese Informationen können auch zum Bereinigen eines infizierten Systems benutzt werden. Mit diesem Verfahren konnten im Schnitt 40% der unbekannten Schädlinge (also jene für die noch keine Signatur bereit stand) identifiziert werden.

4.3.4. Probleme

Virenscanner greifen tief ins System ein und einige Anwendungen können Probleme mit den Echtzeitscans, bei denen Programm und Engine gleichzeitig auf die Datei zugreifen, haben. Jeder Virenscanner hat daher auch eine Ausschlussliste für Dateien die nicht gescannt werden dürfen.

Häufig treten Probleme mit folgenden Anwendungen auf:

- Zeitkritischen Anwendungen
  Durch das Scannen von Dateien entsteht eine Verzögerung, für manche Programme ist diese zu groß und sie erzeugen Fehlermeldungen oder stürzen ab.
- Datenbanken
  Durch die ständigen Zugriffe versucht ein Echtzeitscanner Datenbanken dauerhaft zu scannen. Dies führt zu ansteigender Systemlast, Timeouts oder gar Beschädigungen der Datenbank. Von dem abgesehen macht das Scannen von Datenbanken wenig Sinn, da Scanner die Struktur nicht verstehen.
- Mailserver
  Viele Mailserver speichern E-Mails MIME-codiert auf der Festplatte ab. Erkennt ein Virenscanner eine infizierte Mail und kann diese nicht reparieren wird sie im Normalfall gelöscht. Der E-Mailserver wird davon aber nicht in Kenntnis gesetzt und vermisst nun diese Datei, dadurch kann es zu Funktionsstörungen kommen.

4.4. Bekannte Hersteller von Antivirensoftware und deren Produkte

Hier eine kurze Übersicht über die besten Homeanwender-Produkte verschiedener Antivirensoftwarehersteller. Die Reihung wurde von mir Aufgrund der Ergebnisse eines Tests aus c‘t 2005, Heft 26 des Heise Verlags selbst durchgeführt.

1. GData Antiviren Kit
2. Kaspersky Anti-Virus
3. NOD32 AntiVirus System
4. F-Secure Anti-Virus
5. SoftWin BitDefender
6. Symantec Norton Antivirs

Weiters sind noch folgende zu nennen: McAfee Virus-Scan, Panda Software Internet Security und Trend Micro PC-Cillin.
Im Serverbereich sind die bekanntesten Anbieter: Symantec, Sophos, Trend Micro, McAfee, und Ikarus.

Bei diesem Ranking ist eindeutig zu erkennen, dass Scanner die mehrere Scanengines enthalten wie „GData Antiviren Kit“ zum Teil etwas besser abschneiden als die Konkurrenz. Meistens sind auch Produkte die der breiten Masse unbekannt sind mit im Spitzenfeld. Symantec und MacAfee die vor allem ihre Internetsuiten mit Antivirus, Anti-Spam und Firewall als komfortable All-In-One Lösung anbieten, liegen von der Leistung her nur im unteren Bereich des Spitzenfeldes. Allerdings ist zu erwähnen, dass der Unterschied, der bewerteten Scanleistung, der angegebenen Produkte im Bereich von 0-5% liegt.

5. Computerschäden durch Schadsoftware

Computerviren und andere Schädlinge haben den Ruf Daten zu zerstören, dies ist allerdings nur in den seltensten Fällen der Fall. Meistens wollen sich Viren selbst möglichst weit verbreiten und daher erst gar nicht auffallen.

5.1. Harmlose Auswirkungen

Die harmlosen Auswirkungen von Viren und Schadsoftware sind lästige Meldungen oder die Beanspruchung von Systemressourcen. So benötigten diese Festplattenspeicher bzw. Prozessorleistung und Arbeitsspeicher um sich selbst zu verbreiten. Die meisten Viren sind allerdings so geschrieben, dass sie kaum Ressourcen benötigen um nicht aufzufallen und bei modernen Rechnersystemen ist die Beeinträchtigung meist marginal und für den Anwender nicht spürbar.

5.2. Ungewollte Schäden

Viele Viren und Schadcodes enthalten Fehler. Diese sind zwar meistens nicht beabsichtigt können aber im schlimmsten Fall zur Zerstörung von einzelnen Dateien oder ganzen Datenbeständen führen.

5.3. Existenzbericht

Manche Viren machen auch nach einiger Zeit (Tage, Wochen) auf sich Aufmerksam. Dies kann in folge von Piepsen, Musik, Meldungen, plötzlich auftauchenden Schriftzügen auf dem Desktop oder Manipulation von Bildschirminhalten geschehen. So gibt es viele Viren die für den Virenautor amüsante Nachrichten oder gar

politischen Inhalt verbreiten. Die meisten dieser Meldungen sind harmlos und erfolgen oft auch nur zu bestimmten Zeiten.

5.4. Datenzerstörung

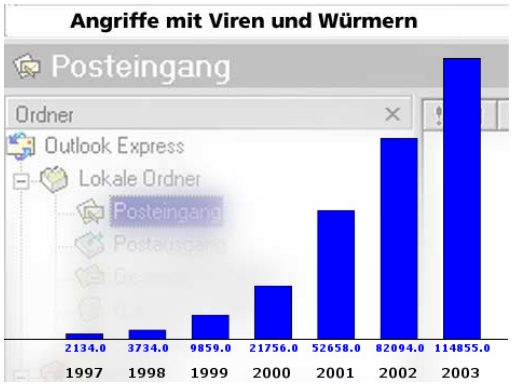
Durch das Infizieren von Dateien wird deren Inhalt manipuliert oder zerstört. In vielen Fällen ist eine Rekonstruktion möglich. Einige wenige Viren wurden speziell für das Zerstören von Daten geschrieben. Diese Löschen einzelne Dateien bis hin zur Formatierung der gesamten Festplatte. Dadurch zerstört sich der Virus dann allerdings auch selbst.

5.5. Hardwarezerstörung

Direkte Hardwarezerstörung durch Software ist eher schwierig, da dem Autor die Hardware bekannt sein müsste. Einige Beispiel hiefür währen das Übertakten von Komponenten und das damit verbundene zerstören durch Überhitzung derer, weiters können Festplatten durch inoffizielle ATA-Kommandos unbrauchbar gemacht werden. Zu guter letzt kann Schadsoftware noch das BIOS des Mainboards überschreiben. Dies zählt allerdings nur indirekt als Hardwareschaden, da hier nur der Flashbaustein ausgebaut und neu beschrieben werden muss. Kosten verursacht es in jedem Fall.

6. Wirtschaftliche Schäden durch Schadsoftware

Die wirtschaftlichen Schäden die durch Schadsoftware entstehen sind enorm. Alleine im Jahr 2003 verursachten Viren einen Schaden von 55 Mrd. US$. So sind nicht nur die Kosten die durch den Datenverlust, Ausfall der EDV oder die Arbeitszeit entstehen zu rechnen sondern auch jene die für die Vorbeugung entstehen. Alleine die jährlichen Investitionen europäischer Unternehmer zur Vorbeugung vor Schädlingen betragen 250 Mio. €. Und so steigt die Anzahl der Angriffe durch Viren und heutzutage vor allem durch Würmer, die den Hauptteil der Schädlinge ausmachen, jährlich. Waren es 1997 gute 2100 Angriffe stieg die Zahl in den letzten Jahren rapide. Im Jahre 2003 waren es bereits über 100.000 Angriffe. Geschichtlich gesehen wurde 1987 der erste Virus entdeckt, heutzutage sind rund 80.000 verschiedene im Umlauf.



Quellenverzeichnis

- http://www.smarttrain.at/web_sicherheit/arten_von_viren.htm
- http://www.waltertietz.nedam.de/cv-arten.htm
- http://www.pchilfe.org/Virena.htm
- http://www.ott-deffge.de/viren_arten.html
- http://www.it-academy.cc/article/457/Viren+Die+verschiedenen+Arten.html
- http://www.symantec.com/region/de/avcenter/security_risks/index.html#virus
- http://agn-www.informatik.uni-hamburg.de/vtc/pcvir_dt.htm

- http://www.sueddeutsche.de/computer/artikel/206/21185/
- http://de.wikipedia.org/wiki/Computerwurm
- http://de.wikipedia.org/wiki/Malware
- http://de.wikipedia.org/wiki/Virensignatur
- http://de.wikipedia.org/wiki/Rootkit
- http://de.wikipedia.org/wiki/Computervirus
- http://de.wikipedia.org/wiki/Computersicherheit
- http://de.wikipedia.org/wiki/Virenscanner
- http://de.wikipedia.org/wiki/Trojanisches_Pferd_%28Computerprogramm%29