Virenbekämpfung

Einführung

Da es in letzter Zeit immer wieder zu spektakulären Virenangriffen, zumeist aus dem Internet gekommen ist, möchte ich mir dies zum Anlass nehmen euch die Grundlagen von Viren, die verschiedenen Virenarten, deren Verbreitungswege, deren Mechanismen und schließlich auch deren Bekämpfungsmöglichkeit näher zu bringen. Sicherlich wird viel über Viren im Freundeskreis und in den Medien geredet, jedoch ist deswegen nicht gewährleistet, dass jeder über Viren Bescheid weiß.

Was sind Viren?

Ein Computervirus ist im Grunde genommen das Gleiche wie ein Krankheitserreger-Virus. Zwar sind Viren Computerprogramme, doch sie legen ähnliche Vorgehensweisen an den Tag wie Viren beim Menschen. Hat man sich einen Virus über das Internet oder über Datenträger unwissentlich eingeschleppt, kopiert sich selbst, infiziert manchmal alle Dateien, so dass deren Weitergabe zur Infektion anderer Computer führt. Außerdem versuchen können sich Viren auch über E-Mail automatisch und unwissentlich weiter verbreiten und so sehr schnell sehr viele andere Computer anstecken. Wie beim Virus beim Menschen benötigt der Virus dazu einen Wirt. Dieser ist beim Computervirus der Computer. Der infiziert wird und danach für den Virus als Überträger dient.

Was für Folgen kann Virenbefall haben?

Die Viren richten Unheil auf dem Computer an, dies kann in der Form von Dateiveränderungen sein, also wichtige Word werden durch wahllose Einschübe von Wörtern unbrauchbar gemacht oder in Exceltabellen Zahlen verändert. Auch Anzeigen von Meldungen (als harmlose Folge) aber auch das jedoch auch löschen von Dateien, das können sowohl wichtige Worddateien sein oder auch Systemdateien so dass das System danach nicht mehr ordnungsgemäß arbeitet. Seit neuestem auch das Verschicken von E-Mails, ausspionieren von Benutzerdaten, das können Firmenpasswörter sein, Providereinwahldaten, wichtige Word- und Exceldateien oder auch Homebankingdaten und -passwörter. Im aller schlimmsten, aber sehr seltenen, Fall kann ein Virus auch zur Zerstörung von Hardwarebestandteilen (der CIH-Virus machte einen Bestandteil des Motherboards durch unsinniges Überschreiben von dessen Daten unbrauchbar) führen.

Wie können sich Viren verbreiten?

Viren können sich auf sehr vielen Wegen verbreiten: Über Disketten (im Bootsektor der Diskette), E-Mails (als Attachment), Worddokumente (als Makro), als "Anhängsel" an alle möglichen Dateien (durch Anfügen des Virenquelltextes in normale Programme) und seit neustem sogar durch das bloße surfen auf Webseiten infizierter Webserver (durch ein Sicherheitsleck im Internet Explorer).
Wenn du das Programm startest oder ein Dokument öffnest, wird der Virus aktiv. Er nistet sich als Erstes so im System ein, dass er von nun an bei jedem PC-Start automatisch aktiv wird - Makroviren beispielsweise in der Datei normal.dot, die Word bei jedem Start lädt. Dateiviren befallen eine Programmdatei, die Windows bei jedem Systemstart automatisch ausführt. Bootviren werden ganz automatisch noch während des PC-Startvorgangs aktiviert.

Wie sind Viren aufgebaut?

Computerviren bestehen in der Regel aus drei Modulen: Infektionsroutine, Kopierroutine sowie Statusroutine.

Der Infektorteil ist der wichtigste Bestandteil des Computerviruses. Er spürt ein geeignetes Wirtsprogramm auf und infiziert es. Außerdem beinhaltet dieses Modul die Aktivierungsbedingung (Trigger) und die Schadensroutine (Payload). Um eine frühzeitige Entdeckung des Virus zu vermeiden, versucht der Infektor auch, alle verdächtigen Aktivitäten zu tarnen.

Bei einer Infektion klinkt sich der Virus in den Code eines Wirtsprogramms ein und platziert an dessen Beginn einen Sprungbefehl. Dieser ruft beim Start der verseuchten Datei den angehängten Virus auf. Der kann nun seine Instruktionen ausführen und übergibt am Schluss die Kontrolle wieder an das ursprüngliche Programm, das ganz normal weiterarbeitet. Daher bemerkt der Anwender im Allgemeinen nichts von diesem Vorgang.

Die Kopierroutine überträgt den viralen Code in andere Wirtsdateien. Dieser Programmteil kann zusätzlich das Zwischenspeichern von Daten übernehmen, die der Virus verlagert hat, etwa aus dem Bootsektor oder dem MBR (Master Boot Record).

Die Statusroutine dient schließlich zur Kontrolle und soll Mehrfachinfektionen verhindern. In der Regel setzt der Statusteil ein bestimmtes Bit als Flag (Erkennungszeichen) in der Wirtsdatei, an dem der Virus erkennt, ob die Datei bereits infiziert ist oder nicht.

Warum ist das Internet für Viren zu attraktiv?

Das Internet ist weltumspannend und bietet dem Virus deshalb viele potentielle Infektionsopfer. Außerdem ist das Internet weitgehend unkontrolliert, so dass Programme die Viren enthalten (ob absichtlich oder nicht) nicht vor der Verbreitung geschützt werden können. Die Virenautoren bleiben darüber hinaus noch weitgehend anonym, so dass es schwer ist diese zu bestrafen.

Virenarten

Es gibt verschiedene Arten von Viren, die sich in der Funktionsweise und dem Verbreitungsweg unterscheiden.

Internetwürmer

Viren von denen man in letzter Zeit sehr viel hört, sind sogenannte Internetwürmer, diese werden als Anhang an E-Mails angehängt und werden durch ausführen des Attachments aktiviert. Die Internetwürmer verbreiten sich vorwiegend bis ausschließlich durch selbstständiges versenden von E-Mails über das E-Mailprogramm Outlook von Microsoft. Dieses Programm gehört zum Lieferumfang des Officepaket Microsoft Office oder des Internet Browers Internet Explorer von Microsoft, jedoch diesmal als Expressversion. Die verseuchten E-Mails werden ohne Wissen des Benutzers an alle Personen des Adressbuches von Microsoft Outlook (und Outlook Express) versendet.

Durch diese Vorgehensweise wird der Empfänger eher dazu animiert den Anhang zu öffnen. Er kennt ja schließlich den Absender.

Würmer infizieren keinen fremden Code, um sich fortzupflanzen. Vielmehr sind sie auf die selbstständige Verbreitung in Netzwerken (das Internet ist auch ein Netzwerk) ausgerichtet, wodurch sie sich von Viren und Trojanern unterscheiden.

Bekannte Vertreter sind W32/ExploreZip und Happy99.

Bootviren

Mit einem Bootvirus fing alles an: 1986 verbreitete sich Pakistani Brain innerhalb eines Jahres rund um die Welt, obwohl der Virus nur Disketten und keine Festplatten infizierte. Bootviren funktionieren ähnlich wie ein Betriebssystem: Beim Start eines PCs führt das eingebaute BIOS-Programm eine kleine Startroutine von der Festplatte aus. Sie ist im MBR am Anfang der Festplatte gespeichert. Dieses Startprogramm ruft den Startcode von Windows oder eines anderen Betriebssystems im Bootsektor der aktiven Partition auf.

Auch jede Diskette hat einen Bootsektor. Dort und/oder im MBR ersetzen Bootviren den Startcode. So wird der Schädling vor allen anderen Programmen aktiv und kann jede eingelegte Diskette infizieren. Danach aktiviert er den normalen Bootcode des Betriebssystems - der Anwender merkt davon nichts.

Der Infektionsweg für einen Bootvirus ist klar: Beim Einschalten des PCs liegt eine Diskette im Laufwerk, und der PC versucht, davon zu booten. Weil ein Bootvirus keine Datei zur Verbreitung benötigt, kann auch eine ganz "leere" Diskette einen Bootvirus enthalten. Da Bootviren auf diese Weise lange Zeit unbemerkt bleiben, gehören Sie zu den hartnäckigsten Vertretern ihrer Art.

Bekannte Vertreter sind der Pakistani-Brain-Virus und der Italien-Virus.

Dateiviren

Dateiviren attackieren ausführbare Programmdateien, in die sie ihren eigenen Code kopieren. Wenn das manipulierte Programm gestartet wird, aktiviert das zunächst den Virus, der nun weitere Programme infizieren oder seine Schadensfunktion ausüben kann. Dann lädt er das Originalprogramm.

Bekannte Vertreter sind der Vienna-Virus und der Datacrime-Virus.

Trojaner

Wie nach der alten griechischen Sage versteckt sich der Ausspionierungsmechanismus in vermeintlich nützlichen Programmen und zeichnen während der Laufzeit Passwörter und weitere Nutzerdaten auf. Während sich Viren und Würmer nach Möglichkeit verstecken, treten Trojanische Pferde offen auf. Sie geben sich als Bildschirmschoner, Passwortverwaltung oder ein anderes nützliches Tool aus. Diese Funktion erfüllen Trojaner gelegentlich sogar mehr oder weniger gut. Meistens geht es aber nur darum, den Empfänger dazu zu verlocken, die Programme (Malware) zu starten, so dass der Schädling zuschlagen kann: So entschlüsselten zwei 16-jährige die Verschlüsselung des T-Online-Passworts. Anschließend programmierten sie die T-Online Power Tools, ein Hilfsprogramm für den T-Online-Decoder, das rasch Verbreitung fand. Sobald jemand die Online-Registrierung benutzte, schickte der Trojaner über das Internet auch die Zugangsdaten zum jeweiligen T-Online-Anschluss mit. Die Verschlüsselung des Decoders war nur mangelhaft. So kamen in kurzer Zeit 600 Passwörter zusammen. Zum Glück für die Ausgespähten ging es den Schülern nur darum, die Machbarkeit nachzuweisen.

Der Trojaner Back Orifice nistet sich im Systemkern von Windows ein. Dann wartet das Programm, bis es ein Hacker über das Internet aktiviert. Es lässt den ungebetenen Gast Dateien kopieren, sämtliche Tastatureingaben mitlesen, Programme starten und vieles mehr.

Bekannte Vertreter sind BackOrifice und BackDoor-G2.svr

Makroviren

Viren die in letzter Zeit auch oft verbreitet werden sind Makroviren. Bei Makroviren

für Microsoft-Programme ist die Geschichte einfach: Die Makros sind Teil des Office-Dokuments. Bestimmte Makros wie AutoOpen führen Excel, Word oder Access automatisch aus, wenn du das infizierte Dokument öffnest. Und der Makrovirus klinkt sich - im einfachsten Fall - in dieses AutoOpen-Makro ein. Das Officepaket von Microsoft verfügt über eine ausgefeilte Makrosprache mit mächtigen Befehlen: VBA, Visual Basic für Applikationen. Mit diesen Befehlen kann ein Makro zum Beispiel Dateien und andere Officedokumente manipulieren oder Windows-Programme fernsteuern.
Der Knackpunkt bei MS-Office: Die Makros sind direkt im Dokument gespeichert. Wenn du ein Word-, Excel- oder PowerPoint-Dokument weitergibst, sind eventuell Makros mit dabei. Und es gibt eine Autostart-Funktion. Sobald man ein Dokument mit einem entsprechend deklarierten Makro öffnet, wird das Makro aktiv. Dann verändern die meisten Makroviren die Standard-Dokumentvorlage normal.dot so, dass der Virus bei jedem Start von Word aktiv wird. Die Vorgehensweise bei den anderen Office-Applikationen basiert auf demselben Prinzip.
Besondere Brisanz haben Makroviren, die sich selbstständig über E-Mail weiterverbreiten. Das bekannteste Beispiel dafür ist Melissa: Der Virus sucht sich aus der Outlook-Datenbank 50 Empfänger aus und schickt ihnen eine E-Mail mit dem Virus als Anhang. Wenn die Empfänger den Anhang per Doppelklick aktivieren, nistet sich Melissa im System ein. Dass die E-Mail von einem bekannten Absender stammt, vergrößert die Chance auf einen unbedachten Doppelklick. Mittlerweile gibt es etliche Nachahmer, auch für Excel.
Der Schaden, den Makroviren anrichten können, ist beträchtlich. Denke beispielsweise an eine große Excel-Tabelle mit einer statistischen Auswertung. Ein Virus könnte hier zufällig einige Werte ändern, in einen Word-Text Tippfehler einbauen oder einzelne Wörter ersetzen. Der Aufwand, die Originaldaten wieder herzustellen, kann enorm sein.
Bekannte Vertreter sind Melissa und WM/Concept.

Script-Viren

Ähnlich wie die Makroviren funktionieren auch die Scriptviren. Sie nutzen das seit Windows98 standardmäßig mitgelieferten WSH (Windows Scripting Host). Dieser WSH sollte eigentlich Windows-Standart-Aufgaben für den Benutzer auf Knopfdruck automatisch erledigen. Der WSH kann deshalb auch tief in den Systemkern eingreifen. Dies nutzen die Viren aus. Bei den Viren handelt es sich um eine ausführbare vbs-Datei, die den Virenquellcode enthält.
Wir diese Datei geöffnet wird das Script ausgeführt und verschiedene Sachen ungewollt ausgeführt. Das populärste Beispiel für einen solchen Virus ist der "I love you"-Virus, der die ganze Welt in Angst und Schrecken versetzt hat. Dieser Virus hat Unternehmen Millionen bis Milliarden gekostet und mehr oder weniger "gute" Derivate nach sich gezogen.
Bekannte Vertreter sind I love you und JS/Kak@M

Hoaxes

Die letzte hier aufgeführte Virenart, ist eigentlich gar kein "echter" Virus. Ein Hoax könne man ins Deutsche übersetzt "Ente" nennen. Ein Hoax ist eine gezielte Falschmeldung per E-Mail über einen Virus oder ein anderes Schadensprogramm. In der Regel wird der Empfänger aufgefordert, die E-Mail an alle Bekannten als Warnung weiterzuleiten. Und genau das ist die Schadenswirkung eines Hoax: Er kostet Arbeitszeit in Firmen und verbreitet sich rasend schnell. Außerdem wird unnötig Panik

erzeugt und die E-Mailleitungen und Mailfächer unnötig verstopft. Manchmal wird man auch aufgefordert wichtige Systemdateien zu löschen.
Einer der ersten Hoaxes tauchte mit "GoodTimes" Ende 1994 auf. Die Mail warnte vor einem Virus, der alleine durch Lesen einer E-Mail einen PC infizieren könne. Erkennbar sei die Nachricht durch die Worte "Good Times" im Betreff. Der Virus würde dann den Festplatteninhalt löschen oder gar den Prozessor des Computers zerstören.
Nach diesem Muster funktionieren alle gängigen Falschmeldungen über vermeintliche Viren. Oft findet sich im Text der entsprechenden Mail noch der Hinweis, dass namhafte Computerfirmen die Warnung vor dem neuen Virus ausgegeben hätten. Eine ständig aktualisierte Übersicht von Hoaxes findet sich beispielsweise auf den Internet-Seiten von VMyths.com, Hoax Info oder der TU Berlin. Daneben wird man ebenfalls bei den großen Antivirenherstellern fündig, etwa bei Network Associates oder Symantec.
Bekannte Vertreter sind GoodTimes und der SMS-Virus

Wie kann man gegen Viren vorbeugen?
Absolut sicher vor Viren ist man nur, wenn man keine fremden CDs und Disketten in den PC steckt und auch keine Dateien aus dem Internet lädt - aber wer will das schon? Selbst originalverpackte Programme direkt vom Hersteller sind gelegentlich infiziert. 1998 hat Corel mit der Mac-Version von Corel Draw 8.0 unwissentlich einen Virus ausgeliefert; Microsoft verteilte 1995 unabsichtlich einen der ersten Makroviren WM/Concept mit einem Dokument auf einer Probe-CD.
Mit einem gewissen Maß an Vorbereitungen ist man Viren trotzdem nicht hilflos ausgeliefert. Die folgenden Regeln stellen zwar keine Garantie dar, schränken Infektionswege aber drastisch ein und begrenzen den Schaden im Ernstfall.

- Lege eine virenfreie bootfähige Notfalldiskette an (Lässt sich automatisch mit dem Virenscanner machen).
- Mache regelmäßig Backups wichtiger Daten und Dokumente - ihre Wiederherstellung kostet viel Zeit und Mühe.
  Windows und Programme lassen sich relativ leicht wieder installieren.
- Schalte im BIOS das Booten von Diskette aus. Damit ist das Risiko, sich einen Bootvirus von einer Diskette einzufangen, praktisch auf Null reduziert.
  Im Bedarfsfall lässt sich die Boot-Reihenfolge leicht wieder umstellen.
- Lasse im Hintergrund immer einen Virenwächter mitlaufen. (Wird bei den meisten aktuellen Virenscannern mitgeliefert).
- Durchsuche die ganze Festplatte regelmäßig, mindestens einmal die Woche, mit dem Virenscanner. (Dazu kannst du den Terminplaner des Virenscanners verwenden.
- Besorge dir regelmäßig Updates für deinen Virenscanner. Nur so findet dieser auch neuere Viren.
- Achte auf ungewöhnliche Reaktionen deines PCs, sie könnten ein Anzeichen für eine Infektion sein.
- Verwende wenn möglich einen Virenscanner mit Heuristikfunktion (erkennt mögliche neue Viren, anhand von verbreiteten Virenalgorithmen)

Virenscanner
Wie im vorherigen Abschnitt beschrieben, sind Virenscanner eine der wichtigsten

Werkzeuge um sich vor Viren zu schützen. Moderne Antivirenprogramme bestehen meistens aus einem On-Demand-Scanner und einem On-Access-Scanner, auch Virenwächter genannt.
Der On-Demand-Scanner untersucht nach dem Start die virusgefährdeten Dateien auf Datenträgern. Da ein Virenscanner nur Sinn macht, wenn man ihn regelmäßig benutzt, ist ein Zeitplaner Standard. Er gibt vor, an welchen Tagen und zu welcher Uhrzeit der Scanner aktiv wird.
Der On-Access-Scanner läuft als Betriebssystemtreiber im Hintergrund und untersucht bei jedem Zugriff auf eine Datei, ob ein Virus enthalten ist. Zudem sind einzelne Wächterprogramme in der Lage, auch Online-Verbindungen und den E-Mail-Datenverkehr zu prüfen.
Virenscanner erkennen nur die Schädlinge sicher, die bereits bekannt sind. Deshalb ist es entscheidend, dass Sie sich regelmäßig Updates der Virensignaturen besorgen. Die Signatur ist das typische Merkmal eines Virus, anhand dessen der Virenscanner eine befallene Datei erkennt. Mindestens einmal pro Woche ist ein Update fällig. Am praktischsten sind Virenscanner, die sich die Aktualisierungen selbst über das Internet besorgen.
Noch weiter geht die heuristische Suche, die Programme auf virentypische Befehlssequenzen prüft. Das ist besonders für polymorphe Viren (d.h. für Viren die sich bei jeder Weiterverbreitung geringfügig ändern) wichtig, und auch für Makroviren sollte so eine Heuristik vorhanden sein. Mit dieser Technik kann der Scanner auch neue Viren als verdächtig deklarieren. Derartige Dateien schickst du am besten per Internet an den Hersteller, der dann innerhalb kurzer Zeit ein Update verfügbar macht.
Man sollte jedoch nicht blind auf den Virenscanner vertrauen, dieser kann schnell veraltet sein oder durch sehr geschickte Viren umgangen werden (Gibt es wirklich!). Also Vorsichtsmaßnahmen beachten!
Gute Virenscanner sind McAfee VirusScan 8 (30 €) und Norton Antivirus 2004 (49,95 €), die regelmäßig sehr gut in Vergleichtests abschneiden. Für alle die garnichts für einen Virenscanner ausgeben wollen, gibt es die Personal Edition von Antivir, die meist Preis-Leistungssieger wird.

Was tun wenn der Virus doch mal zugeschlagen hat?

Bei einem Virenvorfall gilt es zwei Zustände zu unterscheiden: Entweder der Virenscanner hat eine Datei oder Diskette mit einem Virus entdeckt, dieser ist jedoch noch nicht aktiv. Oder aber der Scanner entdeckt einen Virus, der bereits im System aktiv ist.
Im ersten Fall ist der Virenscanner meistens in der Lage, den Virus zu entfernen, bevor er Schaden anrichtet. In manchen Fällen geht dabei aber die befallene Datei verloren, weil der Virus Teile davon unwiederbringlich überschrieben hat. Ist der Virus bereits aktiv, solltest du vorsichtig vorgehen und die nachfolgende To-do-Liste berücksichtigen:
Bei einem Virenbefall gilt vor allem eins: Keine Panik, die erforderlichen Maßnahmen in Ruhe ergreifen. Das Formatieren der Festplatte ist die allerletzte Aktion - und bestimmte Viren überstehen sogar das.
Wie alt ist das letzte Backup? Im Zweifelsfall sollte man sofort ein aktuelles Backup anlegen - ohne das letzte zu überschreiben! Denn eine virenverseuchte Sicherung ist besser als gar keine. Wenn etwas schief geht, kann ein Profi vielleicht die Daten retten. Ein Disk Imager wie Drive Image oder Ghost sichert den gesamten Festplatteninhalt.
Nimm das Handbuch deines Antiviren-Programms zur Hand und lese genau durch,

was dort für den Ernstfall empfohlen wird. Bisweilen kommt es nämlich darauf an, mit welchem Betriebs- und Dateisystem (Windows NT/2000/XP mit NTFS, Windows 98/SE/ME mit FAT32 etc.) du arbeitest.
Bei Bootviren gilt: Die virenfreie Notfallbootdiskette des Virenscanners einlegen oder virenfreie Windows-Bootdiskette einlegen bevor du bootest. Nur so ist gewährleistet, dass kein Virus aktiv ist. Achte aber darauf, dass der Schreibschutz-Schieber der Diskette aktiviert ist!

Nicht vergessen: Nachsorge!

Um zu verhindern, dass der Virus in einer versteckten Datei überlebt und später erneut wichtige Dateien infiziert, solltest du alle Festplatten, Disketten und sonstige Wechselmedien einer genauen Prüfung mit dem Virenscanner unterziehen.
Versuche auch festzustellen, woher der Virus kam: via E-Mail, per Dokument auf Diskette oder über Downloads aus dem Internet. Benachrichtige dann unbedingt den Absender oder Anbieter mit möglichst genauen Angaben.
Stelle den Zeitplaner deines Virenscanners für die nächsten Wochen so ein, dass er täglich einen kompletten Scan aller Laufwerke durchführt. Damit verhinderst du die Neuinfektion des Systems aus einem bisher nicht entdeckten "Rückzugsgebiet" des Virus.
Bei Makroviren solltest du dich über den Virus und seine Schadensfunktion in der Virendatenbank deines Virenscanners oder auf der Webseite des Herstellers informieren. Denn es kann sein, dass der Virus den Inhalt von Dokumenten manipuliert hat. Es besteht die Gefahr, dass du mit den veränderten Daten weiterarbeitest.

Weitere Virusinformationen

Weitere Virusinformationen findest du z.B. bei Antivirus Online, auf dieser deutsch / englischen Portalseite findest du viele Informationen zu Viren, aber auch aktuelle News und eine Linksammlung. Viruslist bietet eine, leider englische, aber ausführliche Virenlexikondatenbank mit 30.000 Einträgen. Wer sich noch näher mit den Grundlagen von Viren befassen will, wird hier fündig: VHM Virus Help Munich. Auf dieser Seite bekommt man viel deutsches Grundlagenmaterial. Auf Sophos schließlich findest du eine umfangreiche deutsche Virenlekikondatenbank

Zum Schluss

Abschließend ist noch zu sagen, dass die Bedrohung durch Viren, Würmer und Trojaner weiter zunehmen dürfte. Selbst Laien können heutzutage Sabotage-Programme mit Hilfe von Construction-Kits erstellen: Über ein komfortables Frontend lassen sich Schädlinge nach dem Baukastenprinzip zusammenklicken. Auf diese Weise generierte Malware ist oft erstaunlich effektiv.
Als E-Mail-Anhang verbreiten sich die digitalen Parasiten in Windeseile über das Internet. Eine eindeutig gewählte Betreffzeile - etwa "Sex Pics for free" - sorgt dafür, dass möglichst viele Empfänger alle Vorsicht fahren lassen und das verseuchte Attachment starten.
Ein sicherer Schutz vor Viren bedarf einer gewissen Selbstdisziplin. Virenscanner müssen up to date gehalten werden, auf manch komfortables Software-Feature sollte man besser verzichten und nicht alles, was klickbar ist, sollte auch geöffnet werden. Doch wer sich an ein paar Grundregel hält, ist vor Virenangriffen auch in Zukunft weitgehend sicher.