

Begriffserläuterung

Spätestens seit „I love you“ haben die meisten PC-Benutzer ein geschärftes Bewusstsein für Malware (schädliche Software). Neben dem Ausdruck „Virus“ kursieren Bezeichnungen wie „Wurm“ oder „Trojanisches Pferd“, die die Benutzer verunsichern: Schützt mich meine Virenschutzsoftware denn auch vor Würmern und Trojanern?

Die Grenze zwischen den verschiedenen Schädlingen ist manchmal gar nicht so leicht zu ziehen, manche Schadprogramme sind zugleich Virus, Wurm und Trojaner. „Virus“ ist sowohl Oberbegriff für alle Arten von Malware als auch die Bezeichnung für ein Schadprogramm mit spezifischen Eigenschaften. Der Unterschied zwischen Virus und Wurm liegt in ihrer Verbreitungsstrategie:

Viren verbreiten sich innerhalb von PCs --- weitere Arten von Viren siehe weiter unten

Würmer nutzen die Infrastruktur eines Netzwerkes, um sich zu verbreiten,

Trojaner sind die Tarnkappenbomber unter den Viren. Sie tarnen sich meistens als nützliche Programme, um im Verborgenen ihre Schadensfunktion auszuüben.

Hoaxes, so genannte Scherzviren, kursieren immer wieder und funktionieren wie Kettenbriefe. Virenhoaxes sind **Falschmeldungen** über nicht existente Viren, wobei häufig Auswirkungen beschrieben werden, die eigentlich nicht möglich sind. Sie enthalten immer die Warnung vor einem neuen, angeblich extrem gefährlichen Virus und fordern den Adressaten dazu auf, die E-Mail-Warnung an möglichst viele Freunde und Bekannte weiterzuleiten, um sie zu warnen. Natürlich gibt es diese Viren nicht, aber das Schneeballsystem verbreitet unnötig Panik und belastet den Netzverkehr.

Computerviren lassen sich in folgende Kategorien unterteilen: **Dateiviren** infizieren Programme wie etwa eine Tabellenkalkulation oder Spiele. Wenn der Anwender die befallene Programmdatei startet, infiziert der Virus weitere Programmdateien. Dort wird er beim nächsten Aufruf aktiv.

Virus: Der Gründliche

Der klassische Virus ist ein Schadprogramm, das sich von Datei zu Datei auf einem Computer ausbreitet. Der Virus repliziert sich selbst, zum Beispiel wenn der Benutzer ein bestimmtes Programm ausführt oder den Computer hochfährt (siehe dazu auch "Wissenswertes über Viren"). Damit der Virus sich auf dem PC ausbreiten kann, muss er aktiviert werden, und dazu ist menschliche Hilfe nötig, auch wenn der PC-Benutzer natürlich nicht weiß, dass er mit dem Öffnen einer Datei oder dem Starten des Computers seinen Rechner infiziert.

Strategie des Virus: den Wirt beherrschen

Die „Absicht“ vieler Viren ist es, so viele Dateien wie möglich innerhalb eines Computers zu infizieren oder vitale Funktionen zu blockieren. Viren können nur dann von einem auf den anderen Computer übergreifen, wenn sie zum Beispiel per Diskette übertragen werden. Natürlich können sie auch per Email mit infiziertem Anhang verschickt werden.

Das bedeutet aber auch, dass der klassische Virus sich nur so schnell verbreitet, wie Menschen sich untereinander auf digitalem Wege austauschen, den Virus in ihrem Schlepptau. Es kann mitunter Tage oder Wochen dauern, bis eine Virusinfektion von einem auf den anderen PC gelangt.

Bootsektorviren kommen zwar inzwischen wesentlich seltener vor, sind aber umso zerstörerischer, da sie sich in dem Bereich einer Festplatte oder Diskette festsetzen, der beim Starten eines Computers in den Arbeitsspeicher gelesen wird.

Makroviren können sich unabhängig vom eingesetzten Betriebssystem fortpflanzen, sind relativ einfach zu programmieren und mutieren im schlimmsten Fall sogar ohne menschliches Zutun zu neuen Formen, zum Beispiel beim Upgrade von Windows 98 auf Windows 2000. Ihre gewaltige Ausbreitung in den letzten Jahren lässt sich auf den rasant zunehmenden Datenaustausch per E-Mail und die Nutzung des Internets zurückführen.

Bis 1992 waren die bekannt gewordenen Fälle von Datei- und Bootsektorviren etwa gleichmäßig verteilt, bis die Einführung des Betriebssystems Windows 3.1 die Anzahl der Dateiviren dramatisch zurückgehen ließ. Die Einführung von Windows 95 wiederum sorgte für ein Abflauen der Bootsektorviren, leistete aber gleichzeitig dem Aufkommen der Makroviren Vorschub.

Polymorphe Viren sind die Verwandlungskünstler unter den Viren. Sie lassen sich nicht mit Hilfe so genannter Virendefinitionen, der Fingerabdrücke von Viren, erkennen, da sie ihre Struktur von Infektion zu Infektion ändern.

Stealth-Viren benutzen ausgeklügelte Algorithmen zur Tarnung. Durch ihre besondere Erscheinungsform gelingt es ihnen, vor der Entdeckung und Entfernung durch einen Viren-Scanner sicher zu sein. Nur Programme, die in einer logischen Analyse die Aktionen eines Stealth-Virus prüfen, können ihn erkennen.

Wurm: Der Autonome

Ein Wurm ist ein Schadprogramm, das sich von Computer zu Computer via Netzwerk selbsttätig weiter verbreitet. Die „Absicht“ der Würmer ist es, so viele Computer wie möglich innerhalb eines Netzwerks zu befallen. Würmer brauchen, sind sie erst einmal auf den Weg gebracht, kein menschliches Zutun, um sich rasend schnell innerhalb eines Firmennetzwerks oder über das Internet zu verbreiten. Sie benutzen beispielsweise die Email-Funktionen eines Rechners, um sich an beliebige Internetadressen zu versenden. Neben ihrer Fähigkeit zur schnellen autonomen Verbreitung haben Würmer eine Ladung, das eigentliche Schadprogramm, das sich wie ein herkömmlicher Virus innerhalb des befallenen PCs austobt.

Strategie des Wurms: die Menge macht's

Während der „Internet Wurm“ im Jahr 1988 es gerade mal auf 6.000 infizierte Systeme brachte, konnte Melissa innerhalb von nur drei Tagen 100.000 Systeme lahm legen. Die Schäden sind dadurch natürlich ungleich höher als noch vor über 10 Jahren. Sind also die heutigen Würmer moderner und leistungsfähiger als ihre Vorfahren? Im Grunde genom-

men nicht: Explore Zip hat 1999 eine ähnliche Strategie verwendet wie der „Internet Wurm“ 11 Jahre zuvor. Der große Erfolg von Würmern heutzutage ist auf ihre verbesserten „Lebensbedingungen“ zurückzuführen.

Standardschädling fürs Standardsystem

Die homogene Softwarelandschaft trägt dazu bei, dass sich Würmer so weit verbreiten können. Microsoft Windows ist allgegenwärtig. Während vor gut 12 Jahren große Unternehmen ihre spezifischen Betriebssysteme mit eigenen Anwendungen hatten, ist man heute längst dazu übergegangen, standardisierte Software zu verwenden. Die Angriffsfläche für Würmer ist somit enorm gewachsen.

Würmer gedeihen heute aus vier Gründen so richtig gut:

Knapp 380 Millionen PC-Benutzer mit Internetzugang: Ins Netz gegangen

Ende des Jahres 2000 waren weltweit laut Computer Industry Almanach etwa 380 Millionen PCs durch Internetzugang miteinander verbunden. Die Kommunikationsinfrastruktur ist so gut ausgebaut, dass PC-Benutzer auf dem ganzen Globus miteinander kommunizieren können. Und sie tun es auch sehr rege. Bereits über die Hälfte ihrer Zeit verbringen PC-Benutzer online (laut einer Studie von Odyssey, L.P). Je höher die Kommunikationsdichte, umso schneller können sich Würmer verbreiten. Anders ausgedrückt: Die Geschwindigkeit von Würmern wächst proportional zur Internetgeschwindigkeit.

Fehlende Anonymität: Das „Ich war hier“-Syndrom

Immer mehr Internetbenutzer lassen sich in Internetverzeichnissen, Mailboxseiten oder Chatrooms als Besucher eintragen und geben so ihre Email-Adresse jedermann preis. Würmer zapfen jedoch nicht nur private Email-Verzeichnisse an, sondern auch öffentliche, um sich automatisch an alle diese Adressen zu versenden.

Fröhliches Heimwerken: So basteln wie uns einen Wurm

Die Programmierbarkeit von Computern hat stark zugenommen. Kaum ein fortschrittliches Office-Programm verzichtet noch auf Makros, die der Laie bequem nach Handbuch mit VBS (Visual Basic Script) anfertigen kann. Auch Würmer lassen sich mit dieser einfachen Programmiermethode rasch herstellen. Für den Loveletter dürften das Microsoft-Handbuch, ein Nachmittag und eine ordentliche Portion kriminelle Energie genügt haben, um einen Schaden von geschätzten 2,5 Milliarden Dollar weltweit anzurichten.

Trojaner: Der Heimliche

Aus jedem simplen Virus oder Wurm kann mit entsprechenden Zusatzprogrammen ein Trojanisches Pferd oder kurz: Trojaner werden. Das sind Programme, die sich als nützliche Anwendungen tarnen, im Hintergrund aber ohne das Wissen des Anwenders eine Schadensroutine ausführen. Nach dem Start des Tarn-Programms wird auch die schädliche Ladung auf dem PC aktiviert.

Strategie des Trojaners: sensible Daten aushorchen

Die „Absicht“ vieler Trojaner ist es, unbemerkt so viele sensible Benutzerdaten wie möglich auszuspähen. Wenn der Internetbesucher persönliche Daten wie zum Beispiel Passwörter für das Onlinebanking oder für Mailaccounts, Kreditkartennummern und Ähnliches übermittelt, schreibt der Trojaner mit. Die Leistungsfähigsten unter ihnen sind in der Lage, die wirklich interessantesten Informationen herauszufiltern, und übermitteln diese dann per Email an den Hacker, sprich den Absender des Trojaners.

Attacke durchs Hintertürchen

Trojanische Pferde verstecken ihre wahre Identität hinter einem normalen Programm. Was zum Beispiel zunächst als Taschenrechner erscheint, könnte zum Beispiel darauf programmiert sein, das Passwort und die Login-ID auszuspionieren und per E-Mail dem Hacker zu verraten.

Einen neuen und gefährlichen Trend stellen Würmer wie Melissa oder ExploreZip dar. Durch ihre automatische Versendung via E-Mail verbreiten sich Würmer rasend schnell und legen dadurch oftmals ganze Netzwerke lahm. Mittlerweile machen sich 9 der Top-10-Viren Netzinfrastrukturen zu Nutze, um sich zu vermehren.

Eine besonders aggressive Form des Trojanischen Pferdes sind so genannte Backdoor-Trojaner. Diese richten auf dem Wirtssystem Ports (Backdoors) ein, durch die der Hacker einfallen kann. Mit Hilfe von Backdoor-Trojanern kann der Hacker auf fremde Rechner zugreifen und hat dann die Fernkontrolle über praktisch alle Funktionen.

Moderne Virenschutzsoftware: Automatisch schneller

Würmer und Trojanische Pferde besitzen einen Vorteil: sie sind schnell. Menschliche Reaktionszeiten sind für diese High-Speed-Schädlinge zu langsam. Deshalb setzen moderne Virenschutzprogramme auf Automatisierung. Dessen Digitales Immunsystem (DIS) koordiniert und automatisiert den gesamten Virenschutz bis hin zum automatischen Update der Virensignaturen.

So geschützt können PC-Benutzer der Armada aus dem Cyberspace gelassen entgegen blicken, die zwar stark ist – aber nicht unbesiegbar.

Sollten Sie Fragen oder ein akutes Problem haben, so wenden Sie sich am besten per Email an uns: support@softwaresupport.ch

Wir werden schnellstmöglich antworten!

Wenn Sie mehr wissen wollen, wie Sie sich wirkungsvoll gegen Viren schützen können, dann klicken Sie [hier](#), um die Goldenen Regeln gegen Viren zu lesen.