Viren, Würmer und Trojaner

Über die Unterscheidung und Bekämpfung von Viren, Würmern und Trojanern

Jan Manuel Tosses

Datum

Zusammenfassung

Viren, Würmer und Trojaner stellen nach jüngsten Umfragen den größten Kostenblock in aktuellen IT-Sicherheitsrechnungen dar. Durch sie erwägen geplagte Manager immer öfter einen Umstieg auf alternative Betriebssysteme, wie zum Beispiel Linux und MacOS X. Tatsächlich ist das Microsoft Windows Betriebsystem derzeit das einzige, das unter ernstzunehmenden Computerviren und Würmern leidet. Dies liegt sicher an seiner weiten Verbreitung, nicht zuletzt aber auch an mangelndem Sicherheitsbewusstsein seiner Nutzer und unsicheren Einstellungen nach einer frischen Installation.

1 Unterschiede zwischen Viren, Würmern und Trojanern

1.1 Viren und Würmer

Der Hauptunterschied zwischen Computerviren und Computerwürmern ist, dass der Virus eine Nutzeraktion voraussetzt, der Wurm jedoch Lücken in der Computersicherheit nutzt und sich so völlig autonom ausbreitet. Beide Schädlinge streben die weitest mögliche Verbreitung an.

1.2 Trojaner

Unter Trojanern versteht man Programme, die neben einer scheinbaren Hauptfunktion eine weitere versteckte Funktion ausführen.

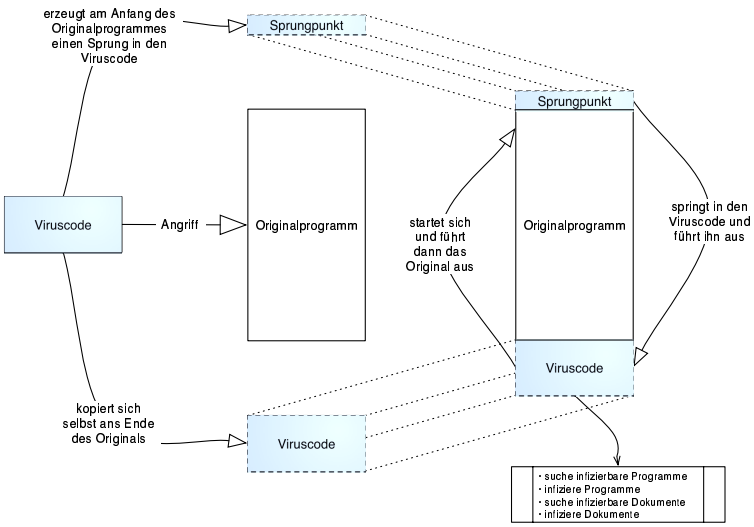
2 Wie funktioniert ein Computervirus?

Stark vereinfacht ausgedrückt legt sich der Computervirus nach seinem Start in ausführbaren Programmen und infizierbaren Dokumenten ab, versucht andere Systeme über das Internet zu infizieren und wartet schließlich auf ein Signal, seine Schadroutine auszuführen.

Er hat nach seinem Start mehrere Ziele. Er muss sich verbreiten, weshalb er nach möglichen Wirten im Adressbuch des befallenen Computers Ausschau hält und sich selbst an jene per Email versendet. Er muss nach einem Neustart des Computers weiterarbeiten können. Daher versteckt er sich in Programmen und Dokumenten auf dem Computer (siehe Abbildung 1). Dabei zögert er seine

Entdeckung möglichst lange hinaus, indem er sich tarnt. Ausserdem sorgt der Virus für seinen automatischen Aufruf beim Systemstart. Er versucht bekannte Schutzmechanismen zu unterwandern und hebelt Antivirus Software aus. Der Virus soll allerdings schon bekannt werden, daher wartet er auf ein Signal, das seine Schadroutine auslöst. Diese kann zum Beispiel die Festplatte formatieren oder Dokumente ins Internet versenden. Ein mögliches Signal kann das Öffnen einer bestimmten Anzahlt von Dokumenten sein.

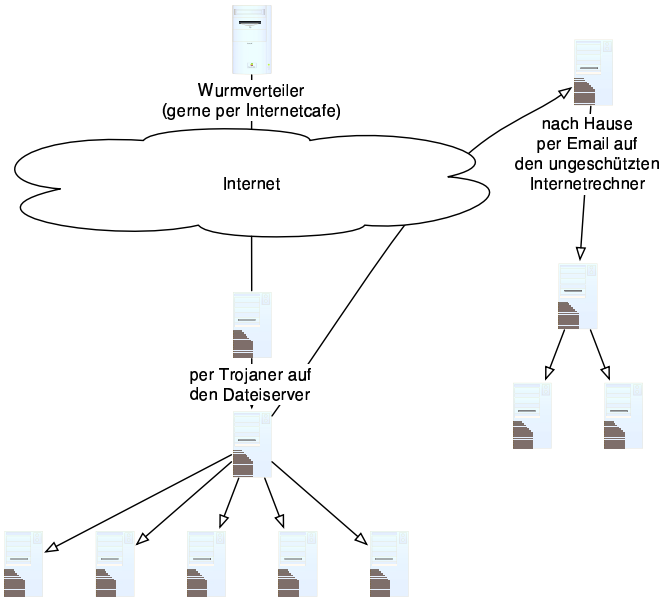
Abbildung 1



3 Wie funktioniert ein Wurm?

Der Wurm sucht nach seiner Freisetzung im Netzwerk automatisch nach ungeschützten Computern, die er angreifen kann. Auch sein Ziel ist die maximale Verbreitung. Er befällt in der Regel nur den Programmspeicher des Computers und legt sich selten auf der Festplatte ab (siehe Abbildung 2). Der Wurm hat meistens keine Schadroutine, erzeugt aber durch seine Verbreitung so viel Last in Netzwerk und Internet, dass der Datenverkehr nahezu zum Erliegen kommt. Würmer greifen Schwachstellen in Netzwerkdiensten an und benötigen zur Verbreitung keine Computerbenutzer.

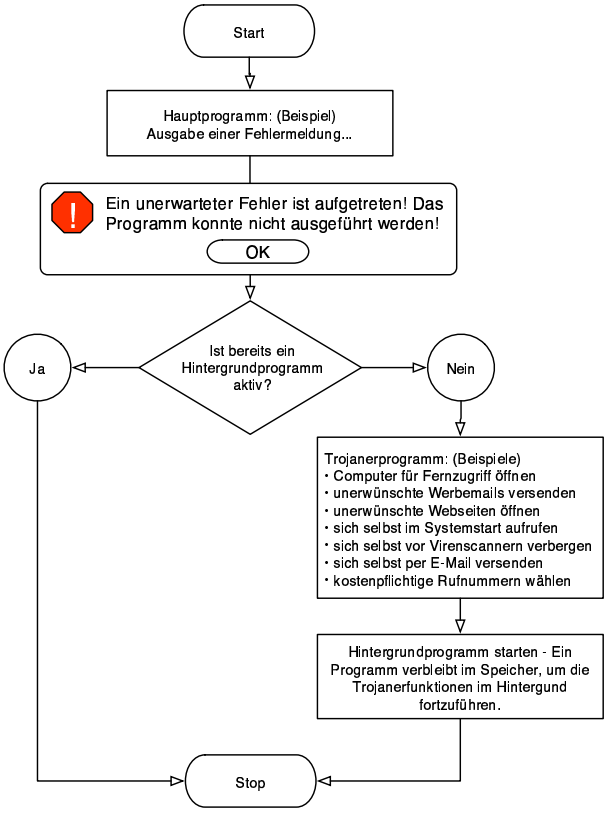
Abbildung 2



4 Wie funktioniert ein Trojaner?

Der Trojaner tarnt sich als harmloses Programm, als Animation, Video, Bild, oder einfach als Fehlermeldung. Bei seinem Programmstart erscheint für den Anwender dann nur die Tarnung (zum Beispiel eine belanglose Fehlermeldung, siehe Abbildung 3), doch im Hintergrund prüft der Trojaner, ob er bereits gestartet wurde und führt dann das eigentliche Programm aus. Dieses Programm kann die Freisetzung eines Computerwurmes, eines Virus, oder auch die Öffnung des Computers für den Fernzugriff sein. Über solche offenen Schnittstellen wird heute der Hauptanteil aller unerwünschten Werbenachrichten (Spam) im Internet verschickt. Je nach Zweck des Trojaners setzt er sich wahlweise wie der Computervirus im System fest, um seine Arbeit nach einem Neustart fortsetzen zu können und bleibt im Programmspeicher aktiv, oder er beendet sich einfach.

Abbildung 3



5 Aktuelle Trends

Während Virenautoren früher überwiegend technisch interessierte Jugendliche waren, deren Viren sie bekannt machen sollten, so sind heutige Schädlingsprogrammierer immer häufiger kriminelle Geschäftemacher. Aktuell werden Viren, Würmer und Trojaner zur Erpressung von Onlinebanken, Spielkasinos und Wettbüros eingesetzt. Ebenso liegen Industriespionage, das Versenden von unerwünschten Werbenachrichten und das Einblenden und Öffnen ungewünschter Werbeseiten aus dem Internet im Trend. Gesamtwirtschaftlich geht es hier um Millionen. Natürlich kommen einige der Viren noch aus der Feder pubertierender Jugendlicher, die im Wunsch nach Anerkennung entwickelt und freigesetzt werden, doch für die Unmengen aktualisierter und modifizierter Viren aus so genannten Viren Toolkits sind zunehmend Kriminelle und nicht selten organisierte Verbrechervereinigungen verantwortlich. Viren Toolkits sind einfache Baukästen mit denen auch Laien höchst effiziente Viren und Würmer bauen können. Geld scheint eine starke Motivation zu sein Schädlinge in Umlauf zu bringen. Auch sabotierende und scheidende Mitarbeiter wählen den Computervirus immer öfter als "Abschiedsgeschenk". Und in der Schule bietet ein Virus eine willkommene Ausrede für nichterledigte Hausarbeiten.

6 Wo bestehen die größten Gefahren?

Die gefährdetste Plattform für Virenbefall ist heute das Microsoft Windows Betriebssystem. Windows ist durch seine hohe Verbreitung und viele bekannte Sicherheitslücken ungemein attraktiv für Virenautoren. Unter Virenautoren gelten seine Nutzer als ebenso unwissend wie unbelehrbar.

7 Wie kann ich mich vor Computerviren schützen?

Derzeit ist der beste Schutz vor einem Virus sicherlich der Einsatz alternativer Betriebssysteme. Ist man auf Microsoft Windows wirklich angewiesen, sollte man folgende Programme dringend meiden und diese Ratschläge befolgen:

1. Statt des Internet Explorers alternative Webbrowser benutzen, zum Beispiel Firefox, oder Mozilla (kostenlos), oder Opera (kommerziell).
2. Statt Outlook, oder Outlook Express besser ein weniger verbreitetes Emailprogramm benutzen. Hier bieten sich Thunderbird (kostenlos), oder Eudora (kommerziell) an.
3. Anhänge in Emails nicht doppelklicken, sondern mit der rechten Maustaste anklicken und aus dem Menü "öffnen mit..." verwenden. Hierdurch können getarnte Trojaner nicht ausgeführt werden.
4. Anhänge in Emails nur nach Rücksprache mit dem Versender öffnen! Viele Viren tarnen sich als Email ihrer Opfer.
5. Auf die Versendung von Microsoft Office Formaten (Word-DOC, Excel-XLS, etc.) dringend verzichten. In solchen Formaten können sich Viren verbergen.
6. Microsoft Windows nicht direkt mit dem Internet verbinden. Zwischen Windows und dem Internet sollte stets eine Firewall stehen.
7. Auf einem Microsoft Windows System sollte immer mindestens ein Antivirus Produkt installiert sein. Dieses Programm muss regelmäßig aktualisiert werden, da es nur bekannte Viren entdecken kann. Einmal am Tag sollte aktualisiert, einmal in der Woche das komplette System untersucht werden.
8. Auch Microsoft Windows sollte immer auf dem aktuellen Stand gehalten werden. Leider führt dies mitunter zu Inkompatibilitäten.

8 Wie rette ich ein infiziertes System?

Der einfachste Weg ist eine Neuinstallation. Dieser Weg steht nicht jedem immer offen. Die Entfernung von Viren, Würmern und Trojanern ist ein aufwändiger und zeitraubender Prozess. Die erste Maßnahme muss die Abschaltung des Systems sein. Danach sollte das Gerät von Netzwerk und Telefon getrennt werden. Hiernach muss auf einem anderen, garantiert virenfreien (!) System ein Startdatenträger mit aktuellster Antivirus Software erstellt werden. Dies lässt man

nach Möglichkeit einen Fachmann erledigen. Diesen Datenträger kann man für gewöhnlich nur einmal verwenden, da er schon am nächsten Tag wieder veraltet ist! Nun sollte das infizierte, von jeglichen Kommunikationswegen getrennte System mit dem erstellten Datenträger gestartet werden. Auch dieser Schritt ist bevorzugt durch einen Fachmann verrichten zu lassen. Darauf wird das System von der Antivirus Software auf dem erstellten Datenträger nach Viren durchsucht. Hierbei sollten alle Dateitypen überprüft werden! Der gesamte Vorgang kann Stunden und manchmal auch Tage dauern, je nach Geschwindigkeit des Computers und Anzahl der Dateien darauf. Es gibt Viren, die das Dateisystem verschlüsseln, um das Entfernen zu verhindern. Hier kann nur ein Fachmann helfen. Zum Abschluss sollte die Antivirus Software vom Originaldatenträger neu installiert werden und von CD, oder Diskette aktualisiert werden. Auch das Betriebssystem sollte mittels CD, nicht aber aus dem Internet, aktualisiert werden. Jetzt kann das System wieder mit dem Netzwerk und Telefon verbunden werden. Alle bekannten Viren sollten nun gelöscht oder inaktiviert sein.