



Virenschutz im Unternehmensnetzwerk

Computerviren und ähnliche schadhafte Programme sind zwar kein unbekanntes, in Zeiten weltweiter Vernetzung sind aber nicht nur deren Verbreitungsmöglichkeiten gewachsen, sondern auch die Zahl von Programmierern, die derartige Programme herstellen und verbreiten. Dass der größte Teil der beobachteten Viren für die verschiedenen Versionen von Microsoft Windows geschrieben wurden, kann leicht darüber hinwegtäuschen, dass schadhafte Programme und das Ausnutzen von Sicherheitslücken auf jedem Betriebssystem möglich sind. Auch können Rechner und Netzwerke, auf denen ein bösesartiges Programm wegen Inkompatibilitäten nicht funktioniert, immer noch als Verbreiter (über E-Mail- oder Fileserver-Dienste) missbraucht werden.

Die Schäden, die durch solche Programme entstehen, können von der Störung des Rechnerbetriebs (Verlangsamung, Abstürze) über das Ausspähen, Manipulieren und Löschen von Daten bis hin zum gezielten Manipulieren ganzer Netzwerke für Fremdzwecke (z.B. SPAM-Versand) gehen. Folgende namentliche Abgrenzungen sind derzeit üblich (wobei ein schadhaftes Programm durchaus mehrere Charakteristika in sich vereinen kann:

Übersicht

Ein **Virus** ist ein Programm, das andere Programme oder Dateien so modifiziert, dass diese Kopie des Virus enthalten, der, wenn beim Kopiervorgang absichtlich Veränderungen provoziert werden, bei der Infektion auch mutieren kann. **Infiziert** bedeutet, dass sich der Virus in die Befehlskette des ursprünglichen Programms oder in die Datenstruktur der Datei einschleust, so dass der Versuch, das Programm auszuführen oder die Datei zu öffnen, gleichzeitig oder stattdessen zur Ausführung des Virus führt.

Ein **Wurm** ist ein Programm, welches in der Regel (aber nicht zwingend) ein Virus im Sinne der obigen Definition ist, das sich selbst kopiert und verbreitet, ohne sich an ein **Wirtsprogramm** anzuhängen. Ein Wurm hangelt sich in der Regel über Netzwerkverbindungen von einer Maschine zur nächsten. Das Ziel 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 innerhalb eines Firmennetzwerks oder über das Internet zu verbreiten.

Aus jedem simplen Virus oder Wurm kann durch Hinzufügung entsprechender Zusatzfunktionen ein Trojanisches Pferd oder kurz **Trojaner** werden. Als Trojaner werden oft Programme bezeichnet, die vorgeben, etwas Nützliches oder Wünschenswertes zu tun (dies vielleicht auch wirklich machen), die jedoch gleichzeitig eine bestimmte Aktion ausführen, die vom Opfer nicht erwartet oder gewünscht wird. Zu diesen Aktionen gehören beispielsweise das Ausspähen von Kennwörtern oder die totale Zerstörung des Wirtssystems.

Eine besonders aggressive Form des Trojanischen Pferdes sind so genannte **Backdoor-Trojaner**. Diese richten auf dem Wirtssystem Ports (Backdoors) ein, durch die ein Hacker einfallen kann. Mit Hilfe von Backdoor-Trojanern kann der Hacker auf fremde Rechner zugreifen und hat dann die Fernkontrolle über praktisch alle Funktionen. Zur Gruppe der Trojaner können auch die sog. „**Dialer**“ gezählt werden, die den infizierten Rechner dahingehend manipulieren, dass ein eingebautes Modem zur Anwahl von kostenpflichtigen Telefondiensten umprogrammiert wird. Diese haben durch die neueste Rechtsprechung des Bundesgerichtshofes zwar ihren finanziellen Schrecken verloren, ärgerlich sind sie aber weiterhin.

In einer rechtlichen Grauzone operieren die Erzeuger sog. Werbetrojaner. Diese Programme werden von Shareware-Programmierern in deren umsonst abgegebene Software eingebaut und rufen beständig Werbeseiten der Finanziere des Shareware-Programmierers auf. Da vor der Installation eines solchen Programms meist auf diese Funktion hingewiesen wird, gilt ein solcher Trojaner derzeit als legal und „freiwillig“ installiert, und gängige Antivirenprogramme übersehen diese aus Angst der Hersteller vor Schadenersatzforderungen der Werbetrojaner-Hersteller.

Verbreitung von Viren

Es gibt derzeit hauptsächlich vier Verbreitungswege für bösartige Programme, wobei vorsätzliche Infektionen, d.h. das willentliche Installieren, noch hinzukämen.

Infizierte Datenträger

Das schadhafte Programm befindet sich direkt auf dem Datenträger (z.B. Diskette, CD) und infiziert den Zielrechner entweder direkt nach dem Einlegen oder über den Aufruf einer sich auf dem Datenträger befindlichen infizierten oder manipulierten Datei.

Infizierte E-Mails

Die Zahl dieser Viren hat in den letzten Monaten sehr stark zugenommen, es handelt sich derzeit größtenteils um recht einfache Viren, die eine Interaktion des Anwenders benötigen, um sich weiter verbreiten zu können. Meist enthalten diese Mails eine angehängte infizierte ausführbare Datei, einige auch einen Link auf speziell präparierte Webseiten, von denen der Virus herunter geladen würde. Denkbar wäre aber auch ein Wurm, der sich unter Ausnutzung einer Sicherheitslücke im Betriebssystem oder Mailprogramm gleich nach dem Eintreffen der Mail anfängt zu verbreiten.

Die E-Mail-Würmer versenden sich heutzutage meist mit gefälschtem Absender, den sie ebenso wie ihre Zieladressen aus den Adressbüchern infizierter Rechner zusammentragen. Gezielt programmiert, wäre ein solcher Wurm auch für Rufmordkampagnen einsetzbar.

Infizierte Websites

Entweder über das Ausnutzen von Browser-Sicherheitslücken oder mit Links auf manipulierte Programme wird eine Installation des schadhaften Programms auf dem Rechner des Besuchers der Seite erreicht

Tauschbörsen

Bei den keinerlei Kontrolle unterliegenden Tauschbörsen ist die Gefahr, auf manipulierte Daten zu stoßen, noch erheblich größer als bei dem Besuch unbekannter WWW-Seiten. Vor dem Installieren von Programmpaketen, die aus einer Tauschbörse stammen, muss daher generell gewarnt werden.

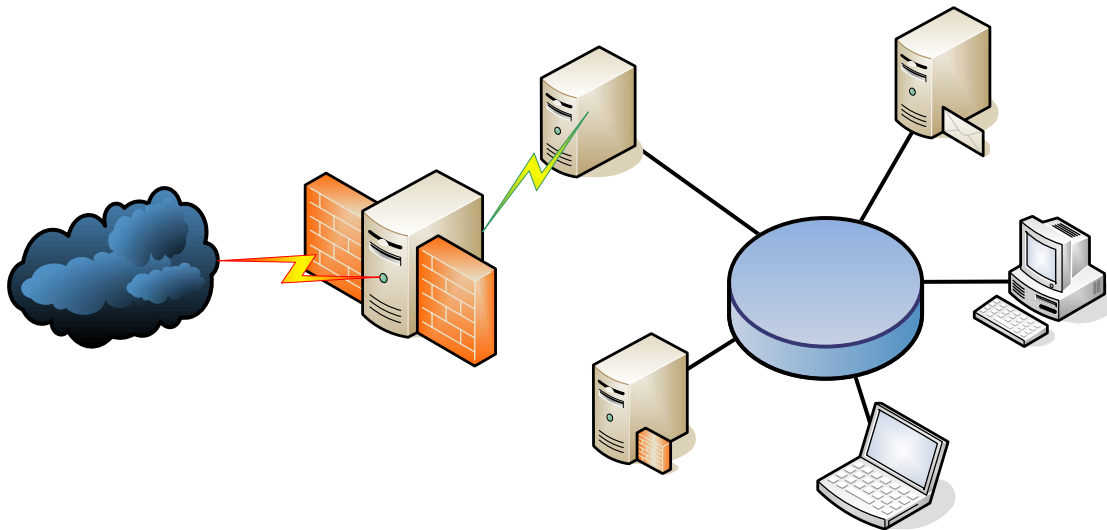
Jeder dieser Verbreitungswege könnte bei Vorhandensein einer entsprechenden Programm-Sicherheitslücke weitgehend automatisiert genutzt werden, d.h., ohne dass der Benutzer aktiv handeln muss und hierzu verführt oder getäuscht werden muss, deswegen ist es dringend anzuraten, nachträglich von Softwareherstellern veröffentlichte Sicherheitsupdates auch zu installieren.

Da aber nicht jede Sicherheitslücke allgemein bekannt wird, und da auch diejenigen Viren, die einer Benutzerinteraktion bedürfen, diese manchmal recht geschickt provozieren, kann auf ein Antivirenprogramm nicht verzichtet werden, wobei folgende Implementierungsmöglichkeiten bestehen.

Anschluss von Fremdrechnern im Netzwerk

Ein mit einem sich ohne Benutzereinwirkung im Netzwerk verbreitenden Virus infizierter Rechner kann zur Gefahr werden, wenn er an ein internes Firmennetzwerk angeschlossen wird, da damit Hindernisse in Form von Firewalls und Antivirengateways wirkungslos bleiben.

Möglichkeiten des Virenschutzes



Viruswall
- SMTP Relay
- HTTP/FTP P

Virenschutz für Server

Auf denjenigen Rechnern, die als zentrale Datenumschlagsplätze genutzt werden (Datenbank-, Datei- und E-Mail-Server), werden Antivirenprogramme installiert. Damit soll gewährleistet werden, dass keine infizierten Daten ausgetauscht oder versendet werden.

Virenschutz für Arbeitsplatzrechner

Werden nur die zentralen Server abgesichert, ist man weiterhin schutzlos gegenüber Würmern, die sich über das Netzwerk verbreiten (z.B. W32Blaster), und gegenüber manipulierten Datenträgern. Ebenso könnte ein Antivirenprogramm auf einem Server angesichts einer hereinbrechenden Welle von Viren einzelne durchlassen oder gar gänzlich seinen Dienst aufgeben, weswegen auf ein Antivirenprogramm auf den Arbeitsplatzrechnern nicht verzichtet werden kann.

Virenschutz für E-Mail-/Groupware-Systeme

Für Groupware-Server existieren spezielle Antivirenprogramme. Diese scannen sowohl ein- und ausgehende Nachrichten, als auch die Groupware-Datenbanken. Auf diese Weise können einkommende Viren schon erkannt und blockiert werden, bevor die Viren in Client-Programmen und somit zu den Client-Rechnern gelangen. Diese Programme können

AntiVirus-Verwaltung
Remote-Installation v
- Zentrale Aktualisierung
Definitionsddatein

allerdings eine erhebliche Belastung für die Leistungsfähigkeit eines Groupware-Servers dar, da sie an praktisch jedem Datenumsatz der Groupware beteiligt sein müssen.

Spezielle Antivirus-Gateways

Bei Netzwerken mit Internetanschluss sollte zusätzlich zur Verwendung einer Firewall auch die Installation eines Antivirus-Gateways erwogen werden. Insbesondere bei E-Mail-Viren sind die Angriffswellen derart umfangreich, dass ein Antivirenprogramm auf dem Groupware-Server schnell überlastet sein könnte und darauf den ganzen Server blockiert. Durch einen vorgeschalteten Filter würde dies vermieden.

Switch mit Zugangskontrolle

Um zu verhindern, dass ein Fremdrechner unautorisiert ans Netzwerk angeschlossen wird, kann man Netzwerkkomponenten verhindern, die den Zugang verweigern, wenn der Rechner unbekannt. Ein Beispiel wäre hierfür ein Switch, der MAC-Adressen ausliest und nur Daten an Ports überträgt, an denen Geräte mit einer dem Switch bekannten und autorisierten MAC-Adresse angeschlossen sind.

Zentrale Verwaltung der einzelnen AntiViren-Programme

Um gerade in Netzwerken mit vielen Arbeitsplätzen die installierten Antivirusbösungen zu administrieren sollte die verwendete Lösung eine zentrale Administrationskonsole anbieten und eine Verteilung der Software über das Netzwerk anbieten. Die Administrationskonsole bietet eine Übersicht der verwalteten Clients und ermöglicht, rasch zu erkennen, ob die Antivirenprogramme auf dem neuesten Stand sind bzw. fehlerfrei arbeiten, ohne dass ein Administrator die einzelnen Arbeitsplatzrechner aufsuchen und inspizieren muss. Die Softwareverteilung über das Netzwerk erleichtert nicht nur die Installation, sondern sie trägt auch dazu bei, die Antivirenprogramme aktuell zu halten und erspart Online-Kosten, da Antiviren-Updates nur einmal heruntergeladen werden müssen und anschließend im internen Netz verteilt werden.