Viren auf dem vernetzten Computer

Einführung

Beim Überschreiten der magischen Grenze im vergangenen Jahr haben eher verhalten die Sektkorken geknallt: Ende 1996 wurde der 10.000ste Computervirus bekannt. Heute sind es ca. 12.000. Aber nicht nur die auf den ersten Blick erschreckenden Zahlen erfordern, daß wir uns mit dieser Problematik auseinandersetzen. Vielmehr bedürfen die neuen Möglichkeiten der Verbreitung von Viren, die durch die Vernetzung und die Kommunikation der Computer untereinander sowie durch die Komplexität der Anwendungen entstehen, einer genaueren Analyse und einiger Präventionshinweise.

Was sind Computerviren?

In der Biologie ist ein Virus ein Krankheitserreger, der keinen eigenen Stoffwechsel besitzt. Er greift statt dessen eigenständige Zellen an, nistet sich in ihnen ein und programmiert die DNA-Erbinformation der Wirtszelle um. Damit ist die Analogie schon erschöpft. Ein Computervirus ist einfach ein Stück Software, das sich ein Programm sucht und seinen Programmcode dort ablegt. Gelangt das Wirtsprogramm zur Ausführung, kann der Virus aktiv werden, indem er z. B. Daten löschen oder ändern, Arbeitsabläufe stören, den Absturz des PCs bewirken oder sich fortpflanzen, d.h. sich selbst kopieren kann.
Neben verschiedenen Varianten gibt es drei große Gruppen von Viren, die uns das Leben schwer machen: Datei-, Bootsektor- und Makroviren (siehe Kasten Virenarten und -varianten).

Computerviren gibt es praktisch auf allen gängigen Rechner- und Betriebssystemplattformen: DOS, Windows 95, OS/2, (auch das von Microsoft als virensicher bezeichnete) Windows NT, Mac OS, aber auch in lokalen Netzen (Banyan VINES, Novell, Windows NT u.a.) und in UNIX.

Zwei neue Gefahrenquellen waren in den letzten drei/vier Jahren auszumachen, die in ihren Auswirkungen die konventionellen Computerviren in den Schatten stellen: Makroviren und Netzviren.

Makroviren:

Der Makrovirus ist zweifellos der neue Star unter den Virenarten. Das hat verschiedene Ursachen: Zum einen hat keiner mit solchen Viren gerechnet, zum anderen ist er äußerst leicht herzustellen. Schon mit einfachen Grundkenntnissen der Makrosprache ist jeder Anwender dazu in der Lage. Es gibt sogar schon Makroviren-Baukästen, mit welchen das dialog- und fensterorientiert und fast ohne Programmierkenntnisse möglich ist.

Weiterhin stellt er sowohl weltweit als auch bei uns im Hause von der Häufigkeit des Auftretens her die größte Gefahr dar. Man spricht davon, daß 60% des Virenbefalls in den USA durch Makroviren verursacht wird, Tendenz steigend. Zum Jahresbeginn wurden ca. 200 Word-Viren gezählt, zum Jahreswechsel werden es weit über 1.000 Stück sein. Keine Virenart hat eine so große Zuwachsrate zu verzeichnen. Außerdem sind Makroviren plattformübergreifend: Bei Verfügbarkeit der entsprechenden Anwendung können sie durchaus z. B. von einem Windows 95-Rechner auf einen Apple Macintosh übertragen werden. Schließlich besteht die neue Qualität darin, daß der Virus nicht durch die Ausführung von Programmen aktiv wird, sondern durch die bloße Benutzung von Daten, von Resultaten der Anwendungsprogramme. Das erschwert den Schutz vor Verbreitung dieser Viren.

Netzviren:

Netzviren sind keine eigene Virenart, sie zeichnen sich nur durch die Besonderheit der Infektion aus: Während in der Vergangenheit nur durch das Einlegen und Benutzen von verseuchten Datenträgern eine Übertragung möglich war, bietet das Computernetz heute ganz neue Mechanismen für ihre Verbreitung. In lokalen Netzen sorgen virenbefallene Daten auf Servern für deren schnelle Fortpflanzung. Bei der Nutzung von Diensten des Internets sollte man sich praktisch bei jedem Zugriff Gedanken über eine mögliche Virenverseuchung des eigenen Rechners machen. Mehr dazu folgt im nächsten Abschnitt.

Viren - Bedrohung aus dem Internet?

Glauben wir den Medien, so müßten wir diese Frage eindeutig bejahen: Im Kino sind Filme zu sehen, in denen ganze Computersysteme über das Internet nicht nur lahmgelegt, sondern sogar physisch zerstört werden. Oder in entsprechenden Zukunftsvisionen können uns feindlich gesinnte außerirdische Zivilisationen über das Einschleusen von Computerviren besiegt werden. Auch die Printmedien werden nicht müde, dieses Thema immer wieder aufzugreifen, häufig am Rande der Seriosität. Letztlich stehen oftmals ökonomische Interessen von Dienstleistungsanbietern auf dem Antiviren-Markt dahinter, die Bedrohung aus dem Internet etwas zu dramatisieren.

Wie sind nun die Fakten? Natürlich erzeugen sowohl die neuen Dienste als auch die neuen Kommunikationswege, die uns das Internet zur Verfügung stellt, neue Gefahren für den eigenen Computer. An anderer Stelle in diesem Heft wird auf Sicherheitslücken bei der Web-Programmierung und auf Sicherheitsaspekte bei der Benutzung von E-Mail eingegangen.

Das Dienstangebot des Internet vereinfacht vor allem den globalen Datenaustausch, sei es durch die Möglichkeit, Daten als Attachment bei Mails zu übertragen oder durch den einfachen Zugriff auf Fremddateien via FTP. Das bedeutet, daß viele Büro-Dokumente (Texte, Grafiken, Tabellen, Vorträge) durch Internet-Dienste transportiert werden können. Waren in der Vergangenheit nur einzelne Arbeitsplätze von einem Virenbefall betroffen, so ist es heute möglich, ganze Bereiche mit einem einzelnen virenbehafteten Dokument, das an alle verschickt wird, zu infizieren. Als wirksame Schutzmaßnahme reicht es also nicht aus, die Attachments eingehender Mails nach Computerviren zu verifizieren, es ist auch notwendig, Dokumente, die versandt werden sollen, zu prüfen.

Die Vereinfachung der Nutzung von Internet-Diensten macht es leider auch Computerviren leicht, sich auf dem Rechner des Benutzers festzusetzen. Oftmals reicht schon ein Doppelklick an einer bestimmten Stelle auf einer WWW-Seite aus, und neben der Übertragung der Daten wird gleich die dazugehörige Applikation gestartet.

Erfreulicherweise ist ein verbessertes Abwehrverhalten gegenüber Makroviren zu beobachten. So prüfen Dienstleister von sich aus die transportierte Mail auf Makroviren, und Anwendungsprogramme checken die

Virenarten und -varianten
(kleines Virenlexikon)

Dateiviren
Dateiviren sind die bekannteste und häufigste Art der Computerviren. Sie infizieren ausführbare Programme (COM-, EXE-, OVL-, OBJ-, SYS-, BAT-, DRV-, DLL-Dateien) und können bei deren Abarbeitung aktiviert werden.

Bootsektorviren
Bootsektorviren verstecken sich im Bootsektor von Festplatten und Disketten, können sich nach dem Booten von eben diesem Datenträger resident in den Hauptspeicher verlagern und permanent Schaden anrichten.

Makroviren
Makroviren sind in Makros (d.h. in automatischen Programmabläufen) von Dokumenten, Tabellen, Grafiken, Datenbanken u.a. enthalten. Sie können bei Weiterverarbeitung dieser Dateien mit den entsprechenden Anwendungsprogrammen (z.B. Word für Windows) aktiv werden.

Hybridviren
Hybridviren sind Kombinationen von Datei- und Bootsektorviren. Damit machen sie sich verschiedene Ausbreitungsmethoden gleichzeitig nutzbar und sind somit schwerer aus dem System zu entfernen.

Link-Viren
Link-Viren manipulieren die Datenträger-Einträge so, daß vor dem Aufruf von bestimmten Programmen zuerst andere Teile des Datenträgers angesprungen werden, welche den eigentlichen Virencode enthalten.

Stealth-Viren
Stealth-Viren (auch Tarnkappenviren) sind Viren mit speziellen Mechanismen, sich vor Virensuchprogrammen zu verstecken. Sie können z.B. eine infizierte Datei vor der Überprüfung restaurieren und somit die Verseuchung unkenntlich machen.

Polymorphe Viren
Polymorphe Viren verändern in einem bestimmten Rhythmus ihr Aussehen, so daß sie für Virenscanner, die nach Erkennungsmustern arbeiten, nicht oder schwer entdeckt werden können.

Slow-Viren
Slow-Viren sind Viren, die lange Zeit unentdeckt bleiben, weil sie die Daten nur geringfügig manipulieren. Damit wird es wahrscheinlich, daß sie auch auf Sicherungsdatenträger übertragen werden, so daß der Benutzer keine virenfreien Duplikate oder älteren Versionen mehr zur Verfügung hat.

Würmer
Würmer sind keine Viren im eigentlichen Sinne, da sie keine Wirtsprogramme benötigen, sondern ausschließlich sich selbst kopieren.

Trojanische Pferde
Trojanische Pferde sind auch keine Viren im eigentlichen Sinne, sondern Software mit Virenfunktionalität, die sich hinter dem Namen von bekannten (harmlosen) Programmen verstecken.

Logische Bomben
Logische Bomben sind Programme, die beim Eintreten bestimmter Umstände (Erreichen eines Datums, Löschen eines speziellen Datensatzes einer Datenbank, Erzeugen einer Datei mit einem speziellen Namen) Schaden anrichten können.

E-Mail-Bombing
Beim E-Mail-Bombing überhäuft ein Angreifer ein Zielsystem mit Mails, so daß im Extremfall die normale Nutzung von Mail nicht mehr möglich ist.

E-Mail-Viren
E-Mail-Viren sind Viren, die sich im Attachment von Mails verstecken und die sich bei deren Benutzung auf den lokalen Rechner übertragen.

Nutzerdaten eigenständig auf verbreitete Computerviren ab. Im nächsten Abschnitt werden einige Schutzmechanismen aufgezählt.

> *„Bereits jetzt gelangen rund 20 Prozent aller Viren per Internet in die Systeme. Und das ist eher untertrieben.“* (Th. Königshofen, Datenschutzbeauftragter der Deutschen Telekom AG, 1996).

Eine abschließende Bemerkung: Es tauchen im Internet immer wieder Warnungen auf, daß Viren als Mail verschickt würden, die allein durch das Lesen der Mail aktiviert werden könnten („Good Times“, „Penpal Greetings“ u. a.). Technisch ist dies allerdings unmöglich. Durch das alleinige Öffnen einer Mail mit einem Mailprogramm können weder Computer infiziert noch lokale Zerstörungen ausgelöst werden. Weitere Informationen dazu kann man unter http://ciac.llnl.gov/ciac/CIACHoaxes.html finden.

Gibt es einen Schutz vor Viren?

Den absolut sicheren Schutz vor Viren gibt es nicht. Dazu ist die Phantasie der Viren-Autoren zu groß. Es ist nur möglich, die Gefahr des Virenbefalls einzudämmen und die negativen Auswirkungen zu minimieren.

Bei aller Unterstützung durch Virenscanner, Prüfprogramme und sonstigen soft- und hardwareseitigen Sicherungsmechanismen ist es vor allem der Anwender, der über die Wirksamkeit der verfügbaren Schutzmittel entscheidet. Ein bewußter Umgang mit den eigenen und fremden Daten ist ein wesentlicher Bestandteil der Virenvorsorge.

Wie kann man sich vor einem Virenbefall oder wenigstens weitestgehend vor dessen Auswirkungen schützen? Hier einige Empfehlungen:

- Sichern Sie regelmäßig alle wichtigen Daten.
- Überprüfen Sie regelmäßig Ihre Festplatte auf Virenbefall mit einem Virenscanner. Beachten Sie bitte, daß bei der Virenbeseitigung durch Virenscanner die Gefahr besteht, daß Dateien/Verzeichnisse/Ordner und/oder Bereiche unbrauchbar/gelöscht werden.
- Sorgen Sie dafür, daß der Virenscanner stets aktuell ist.
- Überprüfen Sie unbekannte Disketten vor Erstbenutzung auf Virenbefall.
- Aktivieren Sie in den Standardanwendungen den Virenschutz für Makroviren (MS Word für Windows ab Version 7.0a, MS Excel und MS Powerpoint jeweils ab Version 97).
- Überprüfen Sie in Mails versandte Dateien vor Erstbenutzung auf Virenbefall. Seien Sie bei Mails von unbekannten Absendern besonders vorsichtig.
- Versenden Sie keine Dokumente, die Sie nicht zuvor auf Makroviren geprüft haben.
- Betreiben Sie kein ungeprüftes „Forwarding“. Leiten Sie keine Mails weiter, deren Inhalt Sie nicht überprüft haben.
- Versehen Sie Disketten, von denen nur gelesen werden soll, mit dem Schreibschutz. Versehen Sie auch Originalsoftware auf Diskette mit einem Schreibschutz.
- Lassen Sie keine Disketten im Laufwerk stecken, wenn sie nicht benötigt werden.
- Meiden Sie die Benutzung nicht lizenzierter Software, Messe- und Testversionen.
- Legen Sie sich eine virenfreie Bootdiskette zu.

Bei Verdacht auf Virenbefall sollte der PC von der virenfreien Bootdiskette neu gestartet und anschließend die Festplatte mit einem Virenscanner überprüft werden. Bei einem hartnäckigen Befall ist der Einsatz mehrerer voneinander unabhängiger Virenscanner zu empfehlen, um die verschieden Stärken der einzelnen Programme auszunutzen. Bei einem weiterhin bestehenden Verdacht sollte ein Fachmann (DV-Beauftragter des Instituts, Mitarbeiter des Rechenzentrums) zu Rate gezogen werden.

An der HU wird der Einsatz von zwei Anti-Virenprogrammen durch eine zentrale Finanzierung unterstützt: Turbo Anti Virus und Dr. Solomon’s Anti Virus Toolkit. Diese Virenscanner können im Hause großflächig eingesetzt werden. In verschiedenen Einrichtungen sind zusätzlich auch andere Programme im Einsatz, wie z. B. McAfee und F-PROT.

Man sollte sich der Gefahr eines Virenbefalls stets bewußt sein, ohne sie überzubewerten. Bei einem vernünftigen Umgang mit dem Computer und der Einhaltung oben genannter Empfehlungen können die schädlichen Auswirkungen eines Virenbefalls begrenzt werden.

Weiterführende Informationen:

http://www.Psnw.com/~joe/	HAVS (Hartmann Anti-Virus Site)
http://www.informatik.uni-hamburg.de/AGN/	The AGN Homepage
http://www.noc.fhg.de/CERT/ws-1997.html	Erfahrungen mit Viren Scannern für Electronic Mail
http://www.uni-siegen.de/security/viren/index.html	Uni-GH Siegen - Security-Server - Viren
http://www.datarescue.com/avpbase/index.htm	DataRescue - Index for the AVP On-Line Virus Database

Lutz Stange