RECHNERNETZE

Viren, Würmer und Trojaner

Viren, Würmer und Trojaner

Bernd Lehle / Oliver Reutter

Die Computerviren haben etwas an Publicity in der Presse verloren, was sie allerdings nicht ungefährlicher macht. Durch die Verbreitung virenanfälliger Betriebssysteme am RUS und den Instituten der Universität ist es daher auch für die RUS-Sicherheitsgruppe an der Zeit, sich zu diesem Thema zu äußern.

Was sind Viren?

Virus ist lateinisch und bedeutet Schleim oder Gift [6]. Diese Übersetzung trifft die Sache aber nicht ganz. Viren sind submikroskopisch (20-300 nm) kleine Gebilde, die aus einem Stück Erbinformation in Form eines DNA- oder RNA-Moleküls mit einem Proteinmantel und meistens einer Schutzhülle bestehen. Einzeln betrachtet sind sie unbelebte Kristalle aus organischem Material.

Trifft so ein Kristall auf eine Zelle in einem Organismus, legt er seine Unbelebtheit ab: Er dringt in die Zelle ein und implantiert seine Erbinformation in den Zellkern. Die Zelle interpretiert den neuen genetischen Code und produziert neue Viren anstatt ihrer ei-gentlichen Aufgabe nachzugehen. Nach kurzer Zeit stirbt die Zelle, die Zellmembran platzt und die neuen Viren suchen sich weitere Zellen. Es gibt auch Viren, die die Wirtszellen zu ungehemmter Zellteilung anregen. Wird der Stoffwechsel des betroffenen Lebewesens dabei gestört, spricht man von einer Vireninfektion. Die Auswirkungen auf den Organismus können von Unbemerktheit bis zu tödlichen Erkrankungen reichen. Einige bekannte Viruskrankheiten sind Schnupfen, Grippe, Herpes, Tollwut, Pest und AIDS.

Viren sind durch ihre einfache Struktur sehr schwer mit Medikamenten zu behandeln. Der befallene Organismus muß sie durch sein Immunsystem selbst abwehren. Dies kann Tage, Wochen, manchmal sogar Jahre dauern. Jeder Mensch trägt ständig Viren in sich, die je nach aktuellem Zustand des Immunsystems aktiv werden können.

Was sind Computerviren?

Der Begriff Computervirus oder einfach Virus hat sich in der Umgangssprache für eine ganze Gruppe von Programmen eingebürgert, die vom Fachmann als Malicious Software (böswillige Software) oder kurz Malware bezeichnet wird. Je nach Funktion wird sie als Virus, Wurm, Trojanisches Pferd, Logische Bombe oder Hoax bezeichnet. Die Charakteristika seien kurz erläutert:

1. Viren sind Code-Fragmente, die sich an andere Daten anhängen und sich bei deren Ausführung oder Verarbeitung vermehren. Die Daten können Programme, Bootsektoren oder Dokumente sein. Für sich alleine ist eine Computervirus meist nicht reproduktionsfähig. Die Analogie zu den biologischen Viren liegt auf der Hand.
2. Würmer [1] sind komplette Programme, die sich aktiv fortbewegen und vermehren können. Das bekannteste Beispiel ist der Internet-Wurm, der sich 1988 in kürzester Zeit über das damalige Internet verbreitete. Würmer sind relativ selten.
3. Trojanische Pferde [4] sind Programme, die sich äußerlich wie normale Anwen-dungssoftware verhalten, intern aber Anweisungen enthalten, die Schaden an-richten können. Trojanische Pferde können sich nicht selbst vermehren, sondern werden von Anwendern kopiert.
4. Logische Bomben sind Programmfragmente, die von Entwicklern in Betriebssystemen oder Anwendungsprogrammen versteckt werden und bei Eintreten von bestimmten Bedingungen (beispielsweise Datum, Systemaktivität, etc.) anlaufen und Schaden anrichten. Diese Gruppe überschneidet sich teilweise mit allen vorher genannten, hat aber auch reine Vertreter, die zu keiner anderen Kategorie passen. Logische Bomben können sich nicht vermehren.
5. Hoaxes sind falsche Meldungen über Malware. Sie warnen vor Bedrohungen, die nicht existiert. Dadurch wird zwar kein Schaden angerichtet, aber das Beseitigen kann genauso viel Arbeit kosten wie bei echter Malware. Beispiele sind die in letzter Zeit verschickten Warnungen vor den angeblichen Viren Good Times und Penpal, die einige Mailing-Listen verstopften.

Diese Charakteristika sind nicht als Definitionen gedacht, sondern als grobe Einteilung dessen, was einem passieren kann. Es wird immer Programme geben, die in mehrere Kategorien passen und immer welche, die in keine passen. Es gibt auch genug gut gemeinte Software, die unter gewissen Bedingungen in eine der Kategorien fällt.

Wo kommt Malware her?

Malware ist natürlich keine Mutation von normaler Software sondern wird gezielt von Spezialisten programmiert. Zum Programmieren eines überlebensfähigen Computervirus oder eines Wurmes gehören sehr hohe Fachkenntnis und Wissen über das zugrundeliegende Betriebssystem. Daher gibt es wohl nur wenige Programmierer, die selbstständig solche Programme entwickeln können. Was häufiger auftritt sind sogenannte Mutationen, bei denen ein weniger erfahrener Programmierer eine bestehende Spezies abändert, ihr z. B. eine neue Botschaft oder Aktion mitgibt. Trojanische Pferde und Logische Bomben sind sehr einfach zu programmieren, da man die böswilligen Aktionen nur in beliebigen anderen Source Code einfügen muß. Ebenfalls sehr leicht zu programmieren sind Makroviren, da diese in mächtigen, leicht verständlichen Hochsprachen geschrieben sind.

Die Motivationen, Malware zu schreiben und im Umlauf zu setzen, sind schwer herauszufinden, da man von den meisten Beispielen höchstens das Herkunftsland kennt. Der klassische elektronische Vandalismus gehört sicher dazu wie politische oder gesellschaftliche Motive. So wird vermutet, daß der Israel-Virus von Sympathisanten der PLO programmiert wurde, um israelische Computer lahmzulegen. Der Stoned-Virus verbreitet die Botschaft, Marihuana zu legalisieren. Die meisten Viren wurden aber wahrscheinlich aus Abenteuerlust oder Geltungsdrang programmiert. Es gibt auch Fälle, in denen sich Forschungsprojekte verselbständigt haben.

Welche Computer und Betriebssysteme sind bedroht?

Malware ist grundsätzlich auf jedem Betriebssystem denkbar. Je stärker das Betriebssystem jedoch seine Ressourcen kontrolliert, desto weniger Schaden kann angerichtet werden. Die klassischen Opfer sind daher die Single User Desktop-Systeme. Viren und Trojanische Pferde sowie von ihnen angerichtete Schäden gibt es vor allem auf den Systemen Amiga, Atari, Macintosh, MS-DOS und OS/2. Windows 3.X und 95 sind lediglich grafische Benutzeroberflächen von MS-DOS und haben auf

die Funktion systemnaher Malware keinen Einfluß.

Auf Mehrbenutzersystemen wie UNIX, Windows NT oder VMS ist systemnahe Malware praktisch unbekannt. Hier tritt hauptsächlich anwendungsnahe Malware wie Word- oder Excel-Makroviren (NT), der Internet-Wurm (UNIX) oder der IBM Christmas Trojaner (VM/CMS) auf. Für Linux wurden in letzter Zeit verstärkt Trojanische Pferde mit wurmähnlichen Eigenschaften gefunden.

Funktionsweise von Malware

Viren
Wie bereits erwähnt, hängen sich Viren, ihren biologischen Vorbildern folgend, an bestehende Software an und vermehren sich durch Benutzung dieser Software. Es gibt drei Haupttypen von Viren, die man unterscheiden muß:

- **Boot-Sektor-Viren:** Wie Ihr Name schon andeutet, befällt diese Art von Viren den Boot-Sektor von Disketten oder Festplatten. Der Boot-Sektor besteht aus wenigen Bytes, die beim Boot-Vorgang als erstes vom BIOS in den Speicher geladen und ausgeführt werden. Der Virus ersetzt Teile des Boot-Sektors durch eigenen Code oder Zeiger auf eigenen Code und wird immer dann aktiv, wenn versucht wird, von der Diskette oder Festplatte zu booten. Der Virus kopiert sich dann in den Speicher und infiziert von dort aus weitere Disketten oder Festplatten. Diese Viren können sich unabhängig vom Betriebssystem auf alle Boot-Sektoren setzen. Sogar eine Diskette, die gar nicht bootfähig ist und nur vor dem Booten im Laufwerk vergessen wurde, kann einen Boot-Sektor-Virus verbreiten. Auch eine Linux-Boot-Diskette oder der Boot-Sektor einer NT-Festplatte können infiziert sein. Der Virus kann sich dann allerdings nicht ausbreiten, da er das Umschalten des Kernels in den Protected Mode nicht überlebt. Er könnte aber vorher eine Diskette im zweiten Laufwerk infizieren.
- **Dateiviren:** Diese Viren befallen ausführbare Dateien. Dabei kopiert der Virus sich selbst oder eine Sprunganweisung auf sich selbst an den Anfang der Da-tei und wird immer dann ausgeführt, wenn die Datei aufgerufen wird. Die Dateien werden dadurch verlängert, was sich u.U. im Verzeichniseintrag bemerkbar macht. Manche Viren manipulieren allerdings diese Einträge.
- **Makroviren:** Diese Spezies ist relativ jung. Sie trat als erstes bei dem Textverarbeitungsprogramm Word auf, das eine an BASIC angelehnte Makrosprache hat. Mittlerweile gibt es sie auch bei anderen Dokumenten, die in der Lage sind Informationen in Makros abzulegen. In der Vorgehensweise unterscheiden sich Makroviren kaum von Dateiviren. Der Virus-Code wird am Anfang beim Laden des Makros ausgeführt, kopiert sich dann auf andere Dokumente und erfüllt u. U. noch eine einprogrammierte Aufgabe. Diese Viren sind besonders gefährlich, da sie sich schnell verbreiten, wenn infizierte Dokumente mit Electronic Mail verschickt werden. So schaffte es der erste Word-Makrovirus Concept schon sechs Monate nach seiner Entdeckung der häufigste Virus überhaupt zu sein. Makroviren sind anders als andere Viren leicht zu verstehen und zu programmieren. So besteht der auch hier am RUS schon aufgetretene Makrovirus NOP:DE aus fünf Zeilen Word-Makro-BASIC. Er kann von jedem halbwegs qualfizierten Programmierer beliebig verändert werden.

Zusätzlich zu diesen grundsätzlichen Vorgehensweisen haben Virenprogrammierer im Lauf der Zeit Techniken entwickelt, Viren vor Entdeckung und Bekämpfung zu schützen. So gibt es Viren, die Ihre Anwesenheit durch Manipulation von Verzeichniseinträgen tarnen (Stealth-Viren). Ebenso gibt es Viren, die Ihren Code von Generation zu Generation ändern können (polymorphe Viren). Besonders tückisch sind Viren, die in verschlüsselter Form vorliegen und sich als erste Aktion selbst entschlüsseln, bevor sie aktiv werden (Crypto-Viren). Eine besondere Art Boot-Sektor-Viren benutzt das CMOS-RAM im BIOS als Speicher für Viren-Code.

Sehr unterschiedlich sind die sogenannten Nutzlasten (Payloads), die die Viren zusätzlich zu ihrem Reproduktionscode mit sich herumtragen. Die friedlichsten Viren tun gar nichts (z.B. der

Word-Makro-Virus NOP, was für No OPeration steht). Dies kann allerdings schon gefährlich werden, wenn bei der Reproduktion irrtümlich Daten überschrieben werden, die dann verloren gehen. Diese Gefahr besteht vor allem im Boot-Sektor. Weniger freundliche Viren machen sich durch Textbotschaften bemerkbar (z.B. "Your Computer is now stoned - legalize Marihuana!" vom Stoned-Virus). Andere Viren benutzen dazu den Lautsprecher (Yankee Doodle oder Oh Tannenbaum) oder lassen die Buchstaben wie Blätter im Herbst vom Bildschirm fallen (Herbst-Virus alias Cascade). Eine unangenehmere Spezies von Viren simuliert Hardware-Defekte (Parity Boot Virus) oder läßt den Rechner abstürzen. Die übelsten Viren löschen Daten oder komplette Festplatten, wenn sie aktiv werden.

Eine neue Qualität von Viren nutzt Online-Dienste aus, um Schaden anzurichten. Vom Chaos Computer Club wurde ein Virus INFEKT.EXE entwickelt, der gezielt Internet Banking Software stört, indem er Netscape befällt und auf Überweisungen Einfluß nimmt, bevor diese verschlüsselt werden können. Angeblich wird der Empfänger der jeweils letzten Überweisung durch Amnesty International ersetzt. Dieser Virus wurde dokumentiert als Anschauungsobjekt verbreitet, so daß noch keine Berichte über seine Wirksamkeit vorliegen.

Würmer
Diese Kategorie von Malware ist sehr selten und schwer zu programmieren. Eine einheitliche Funktionsweise läßt sich schwer definieren. Wir wollen uns daher exemplarisch auf einen Wurm beschränken, der in freier Wildbahn beobachtet wurde.

Es ist der berühmt-berüchtigte Internet-Wurm, der auch schon in früheren Artikeln erwähnt wurde. Er war wohl als Testprojekt gedacht, eine Art künstliche Lebensform im Internet. Leider hat sein Entwickler die Sicherheit der Rechner im damaligen Internet völlig überschätzt. Anstatt langsam durch das Netz zu kriechen, explodierte die Wurm-Infektion innerhalb weniger Stunden und konnte erst nach etwa einer Woche gestoppt werden. Nach Aussagen der Spezialisten, die den Wurm bekämpften, war das Programm noch unvollständig und wahrscheinlich nur eine Testversion.

Die Funktion war denkbar einfach. Der Wurm, dessen Sourcen heute offen liegen, besteht aus einem aktiven Programm namens `sh,` das sich sofort aus der Prozeßtabelle streicht, wenn es anläuft. Durch Analyse von Routing Tables, `/etc/hosts` und NIS-Information sucht sich der Wurm potentielle Opfer. Diese werden dann durch drei verschiedene Sicherheitslücken angegriffen. Führt einer der Angriffe zum Ziel, wird der Wurm auf den Rechner kopiert und versucht von dort erneut, andere Rechner zu infizieren. Seine Hauptwaffe ist ein damals weit verbreiteter Buffer Overflow Bug im finger-Daemon, dem die meisten Rechner zum Opfer fielen. Kam er damit nicht durch, versuchte er mit dem DEBUG-Loch von sendmail (s. BI. 3/4 97) einzubrechen. Schlug auch dies fehl, wurde ein Brute Force-Angriff auf schlechte Paßwörter gemacht (s. BI. 1/2 97). Ab und zu schickte er ein paar bytes an `ernie.berkley.edu`, was schließlich auf den Programmierer führte. Robert Morris jr., ein 23jähriger Doktorand an der Cornell University und Sohn des Leiters des National Computer Security Institute, der Öffentlichkeitsabteilung der National Security Agency.

Als positive Konsequenz des Wurms wurde das erste CERT (Computer Emergency Response Team) gegründet. Dies war wohl hauptsächlich eine Konsequenz der Plan- und Hilflosigkeit der betroffenen Benutzer.

Wie weit dieser Wurm im heutigen Internet käme, möchte ich an dieser Stelle lieber nicht abschätzen. Im Stile der Sicherheitstestprogramme SATAN und ISS ist es aber technisch sicher möglich einen Wurm zu programmieren, der ähnliche Effekte wie der ursprünliche Internet-Wurm hätte.

Eine Abart der Würmer sind die Kaninchen [1]. Sie sind die älteste dokumentierte Form der Malware. Es handelt sich dabei um kleine Jobs, die auf frühen Großrechnern in den Job Queues lagen. Kamen sie an die Reihe, schauten sie nach, ob der Programmierer einen Auftrag für sie hatte, den sie dann ausführten. War das das nicht der Fall, kopierten sie sich wieder an das Ende der Job Queue und

stellten so einen permanenten Platzhalter dar, der einem schnellen Zugang zur Job Queue sicherte. Insbesondere, wenn die Queue nach dem Shortest-Job-Next-Prinzip funktionierte, konnte man sich mit einem kleinen Kaninchen am Job Scheduler vorbeimogeln, das dann einen wesentlich größeren Job startete.

Trojanische Pferde und Logische Bomben

Der Vergleich mit dem historischen Vorbild [4] paßt hier ganz gut. Dem Benutzer wird ein äußerlich harmloses, oft sogar attraktiv erscheinendes Programm vorgespiegelt, daß beim Start Unheil anrichtet. Oft sind die bösartigen Teile unmerklich in normalem, funktionierenden Code versteckt, so daß sie erst später bemerkt werden. Von den Viren und Würmern unterscheiden sie sich durch die Tatsache, daß der Benutzer aktiv eingreifen muß, um das Trojanische Pferd zu starten. Manche Trojanische Pferde können sich fortpflanzen, wie das folgende Beispiel verdeutlicht.

Ein bekanntes Trojanisches Pferd auf dem als sehr sicher geltenden Mainframe-Be-triebssystem VM/CMS war Christmas. Es wurde als Mail verschickt und zeichnete einen Christbaum auf den Bildschirm. Dann wurde der Benutzer aufgefordert, die angehängte Datei XMAS EXEC auszuführen. Diese war eine in der Programmiersprache REXX geschriebene Prozedur, die den NAMES-File (Datei mit Mail-Aliases unter VM/CMS) auslas und sich an alle dort aufgeführten Benutzer weiterverschickte. Das Pferd kam vermutlich aus Deutschland und schaffte es immerhin, die komplette VM/CMS-Infrastruktur von IBM für 72 Stunden lahmzulegen.

Ein anderes Beispiel ist AOLGOLD.ZIP, das als Upgrade für die Zugangs-Software von America Online (AOL) getarnt per E-Mail verschickt wurde. Ausgepackt und ausgeführt löschte das Programm alle AOL-Software von der Platte und gab einige unschöne Kom- mentare zu AOL auf dem Bildschirm aus. Es gibt bereits eine Nachfolgeversion, die sowohl als Hoax wie auch als echter Trojaner existiert und AOL4FREE heißt.

Trojanische Pferde sind sehr einfach zu programmieren. Jeder, der Zugriff zu Source oder Object Code eines Programmes hat, kann dort ein Trojanisches Pferd einbauen. Besonders gefährdet ist daher Freeware im Internet.

Eine weitere beliebte Art, Trojanische Pferde unter die Leute zu bringen, sind böswillige Links, Java Applets oder ActiveX Controls auf Web-Seiten. Java hat zwar ein sicheres Design, allerdings fehlt es oft an der Sicherheit der Implementierung. Der Schaden, den böswillige Java Appplets anrichten können, ist relativ begrenzt, da der Zugriff auf kritische Bereiche in der Sprache gar nicht vorgesehen ist.

ActiveX hat ein völlig unsicheres Design, da es auf lokalen Betriebssystem-Calls be-ruht und vollen Zugriff auf den Rechner hat. Das heißt, ein ActiveX Control ist nichts anderes als ein ausführbares Programm, das aus dem Web geladen wird. Die Implementierung von irgendwelchen Schutzmechanismen ist daher prinzipiell nicht möglich. ActiveXfähige Browser, wie der Microsoft Internet Explorer führen bereitwillig auf Mausklick jedes beliebige Trojanische Pferd aus, das man auf eine Web-Seite packt. Davor ist man auch durch Abschalten von ActiveX und Erhöhen der Sicherheitsstufe nicht sicher, denn der Explorer hat noch eine ganze Menge anderer Schwächen, die auch ohne ActiveX vollen Systemzugriff erlauben. Die permanente Installation von Malware auf dem Rechner ist damit sehr einfach. Die Vergabe von Zertifikaten an ActiveX Controls durch Microsoft und Partnerfirmen ist dabei reine Augenwischerei. Für wenige Dollars sind diese Zertifikate zu erhalten und schützen absolut nicht vor negativen Folgen.

Eindrucksvoll demonstriert wurden die möglichen Auswirkungen dieser Schwächen Anfang des Jahres vom Chaos Computer Club. Dort wurde ein ActiveX Control entwikkelt, das im Hintergrund das Telebanking-Programm Quicken startet und eine Überweisung von DM 20,-- einfügt, die beim nächsten Login zusammen mit den anderen Überweisungen an die Bank geht. Details sind in der Zeitschrift iX in der Ausgabe 3/1997 nachzulesen. Eine weitere gute Beschreibung der horrenden

Sicherheitslöcher von ActiveX findet sich auch in der Mai-Ausgabe von Internet professionell (früher pl@net). Einige Firmen gehen schon soweit, daß ActiveX durch das Sicherheitskonzept grundsätzlich verboten ist und dessen Verwendung damit zum Kündigungsgrund wird.

Logische Bomben lassen sich meist sehr schwer von den bisher beschriebenen Verwandten unterscheiden. Klassische Vertreter werden in umfangreichen Software-Paketen versteckt und treten erst nach langer Zeit durch Eintreten bestimmter Begleitum-stände in Aktion. Ein friedliches Beispiel ist die Angewohnheit mancher Entwickler, durch bestimmte Tastenkombinationen einen graphischen Gruß vom Entwickler-Team ablaufen zu lassen. Eine unfreiwillige Logische Bombe ist die Nachlässigkeit der Software-Entwickler bei der Berücksichtigung des Jahres 2000. Die meiste Software kann Jahreszahlen nur zweistellig verwalten, was bei Altersberechnungen zu Fehlern von 100 Jahren führt. Diese Bombe wird am 1. Januar 2000 explodieren und nach Schätzungen von Experten weltweit einige hundert Milliarden US$ kosten.

Logische Bomben werden weniger im Massenbereich eingesetzt. Ihre Hauptanwendung liegt in großen Softwaresystemen von Banken oder anderen Großunternehmen, da dort wesentlich mehr Geld zu holen ist.

Abwehr von Malware

Malware verursacht weltweit etwa doppelt so viel finanziellen Schaden wie Einbrüche in fremde Systeme [5]. Daher wollen wir auch auf die Mö glichkeiten hinweisen, sich vor Schaden zu schützen.

Viren
Der beste Schutz gegen Computerviren ist, wie auch gegen die biologischen Pendants, die Enthaltsamkeit, d. h. der bewußte Verzicht auf Software oder Datentransfer, die durch Viren bedroht sind. Dies hat natürlich nur Sinn, wenn sie im Rahmen eines Sicherheitskonzeptes auch konsequent durchgeführt wird und Alternativen zu bedrohter Software bereitstehen. Am Ende dieses Artikels sind einige konkrete Beispiele aufgeführt.

Wenn man gezwungen ist, Software zu verwenden, bei der Datenverlust durch Virenbefall nicht auszuschließen ist, muß man natürlich anders vorgehen. Seit einiger Zeit hat sich eine große Menge Antiviren-Software etabliert, die auf verschiedenste Weise versucht, Daten vor Viren zu schützen. Es gibt im wesentlichen zwei Arten von Vorgehensweisen, die diese Programm verfolgen:

1. **Virenscanner**: Diese Programme durchsuchen Datenmengen oder Datenströ me auf Muster, die sie in einer Datenbank gespeichert haben. Wird eine Übereinstimmung erkannt, zeigt sie das Programm an und versucht danach, den Virus so zu entfernen, daß die ursprüngliche Funktionalität wieder hergestellt wird. Die Hauptanwendungen sind Scanner für Dateisysteme oder Scanner für Netzverbindungen wie E-Mail, FTP oder WWW. Einige Systeme be-dienen sich sogenannter heuristischer Methoden, die auch nicht gespeicherte Viren erkennen sollen.
2. **Virenschilde**: Diese Programme laufen im Hintergrund und überwachen Sy-stemkomponenten oder Betriebssystemschnittstellen , auf Anzeichen viraler Aktivität oder bekannter Virenmuster. Werden diese gefunden, schlägt das Programm Alarm und versucht den auslösenden Prozeß zu stoppen, bzw. den Verursacher zu finden und den Virus zu entfernen.

Die Virenscanner betreiben reines Pattern Matching und sind immer nur so gut, wie ihr aktuelles Virenverzeichnis. Für einige Viren sind speziellere Verfahren nötig, da ihr Code emuliert werden muß, um polymorphe, getarnte oder verschlüsselte Viren zu finden. In von unabhängigen Spezialisten durchgeführten Tests [7] erkennen gute Virenscanner im wesentlichen alle (95-100 %) in der freien Wildbahn auftretenden Datei- und Boot-Sektor-Viren. Die Erkennungsrate von Makroviren liegt meist weit darunter (60-80 %).

Die Schilde können unabhängig von ihrer Datenbank Funktionen überwachen, die für Viren typisch sind und so Viren, die nicht bekannt sind, zumindest stoppen und melden. Leider fallen diesen Schilden auch immer wieder schlecht programmierte normale Programme zum Opfer.

Wer Antivirus-Software zuverlässig einsetzen will, der sollte folgende Regeln beachten:

- Wenn irgend möglich mehrere unabhängige Scanner verwenden, die regelmäßig eine aktuelle Virendatenbank erhalten
- Jede neue Diskette und jedes per Netzwerk geladene Programm muß zuerst gescannt werden. Manche Scanner machen dies automatisch, bevor sie einen Datenträger freigeben
- Ein Virenschild sollte installiert sein
- In regelmäßigen Abständen (z.B. jede Woche oder jeden Monat) sollten alle Datenträger gescannt werden
- Ein regelmäßiges Backup schützt vor Datenverlust

Würmer
Da Würmer zu ihrer Fortpflanzung nicht auf die Mithilfe von Benutzern angewiesen sind, kann er wenig tun, um sie abzuwehren. Am Beispiel des Internet-Wurms wird deutlich, daß hier hauptsächlich die allgemeine Systemsicherheit verbessert werden muß. Die Wurmabwehr ist am ehesten mit der Abwehr von Systemeinbrüchen zu vergleichen.

Trojanische Pferde
Trojanische Pferde sind immer auf die Mitwirkung der Benutzer angewiesen. Daher sind sie am besten durch vorsichtigen Umgang mit unbekannter Software abzuwehren. Dies fängt damit an, daß bei der Verwendung von Freeware aus dem Internet vorher ein Viren-Scanner benutzt wird, da diese oft auch Trojanische Pferde finden. Dasselbe gilt für Virenschilde. Desweiteren sollte der Benutzer bei jeder ungewöhnlichen Aufforderung, ein Programm abzuspeichern oder auszuführen extrem vorsichtig sein.

Manche Entwickler von Freeware liefern zu ihrem Source Code eine digitale Signatur, mit der der Code auf Veränderungen überprüft werden kann. Das sollte, wenn möglich, genutzt werden.

Logische Bomben
Diese Spezies fällt entweder unter eine der anderen Kategorien oder ist derart exotisch und versteckt, daß es keine generellen Abwehrstrategien gibt. Es gilt hier wie allgemein, daß man sensibel gegenüber seltsamem Verhalten sein muß.

Was tun, wenn Malware aktiv wird?
Wenn der Benutzer merkt, daß Malware aktiv wurde, ist es meistens schon zu spät. Die auffälligen Zeichen von Malware wie Meldungen auf dem Bildschirm oder das Abspielen von Liedern über den Lautsprecher bilden fast immer den Abschluß der zerstörerischen Arbeit, so daß man lieber auf subtilere Zeichen achten sollte.

Einige dieser Zeichen sind:

- Ungewöhnliche Verlängerung von Dateien
- Ungewöhnliche Aktivitäten von Festplatten oder Diskettenlaufwerken
- Auffällige Verzögerungen beim Ausführen von Programmen
- Probleme beim Booten von mehreren Betriebssystemen

Leider gibt es genug Programme und Betriebssysteme, bei denen solche Anzeichen zum normalen Betrieb gehören.

Wird das Vorhandensein von Malware vermutet, empfehlen wir folgende Vorgehensweise:

1. Ruhe bewahren, es kann immer noch falscher Alarm sein
2. Rechner vom Netzwerk trennen, falls der Verdacht besteht, die Malware käme von dort oder könne sich so weiterverbreiten
3. Versuchen, wichtige Daten vom Speicher auf Platte zu sichern
4. Rechner möglichst bald ausschalten (DOS/Windows sofort, NT/UNIX nach Shut Down). Bei Makroviren das Anwendungsprogramm beenden
5. Booten des Rechners durch saubere Systemdiskette (vorher anlegen !). UNIX sollte im Single User Mode gebootet werden
6. Check der Filesysteme und des Boot-Sektors auf Befall durch Malware
7. Suche nach der Quelle (Netz, Mail, Disketten) und Bekämpfung der Malware dort
8. Information von weiteren möglichen Betroffenen

Daten, Fakten, Namen

Nach den manchmal recht theoretischen Ausführung hier noch einige konkrete Tips:

Grundsätzlich: Niemand sollte sich vor Malware sicher fühlen. Durch die Einführung von weltweiter Kommunikation und die Steigerung der Komplexität von Betriebssystemen und Anwendungen steigt die Anfälligkeit. Die Personen, die vor fünf Jahren Viren programmiert haben, über die man heute lacht, entwickeln heute mit ziemlicher Sicherheit Dinge, die uns so treffen können wie damals die ersten Viren. Der Phantasie sind wenig Grenzen gesetzt!

Einige Zahlen
Stand April 1997, Quellen [2], [5], [7]:

- Anzahl der Dateiviren (inkl. Mutationen und Abarten): ca. 10 000
- Anzahl Boot-Sektor-Viren: ca. 800
- Anzahl Makroviren: MS Word ca. 350, andere Programme ca. 10
- Anteil der Viren am Gesamtschaden im Computerbereich: 4 %

Für Malware anfällige Software

- **Extrem anfällig, nicht verwenden!:** Microsoft Internet Explorer und alle anderen Browser, die ActiveX unterstützen
- **Stark anfällig, vorsichtig verwenden oder Alternativen suchen** Microsoft Word ab Version 5 insbesondere in Verbindung mit E-Mail, MS-DOS in den Versionen 2.0 bis 7.0 (Windows 95), PC-DOS, DR-DOS
- **Software für die Makroviren existieren:** Word, Excel, PowerPoint, Access, Lotus Notes, Lotus 123, AmiPro, Ghostscript. Windows-Viewer für das Portable Document Format (PDF) sind ebenfalls anfällig für Malware, da man mit Ihnen sogar Programme starten kann [9]. Reine Word-Viewer (z.B. Netscape Plugins) sind vor Makroviren bisher sicher

Qualitativ hochwertige Viren-Scanner
Testergebnissen des Virus Test Centers der Universität Hamburg [7] zufolge sind nachfolgende als qualitativ hochwertige Viren-Scanner beurteilt worden:

Dr. Solomon Antivirus 768, AVP (Kamis) 2.2, AVAST! 77/1 (Alwil), Alert41/15 (Look) Sweep 294 (Sophos), F-PROT 2.25 (Data Fellows), Scan 2.53 (McAffee)

Scan 2.5.3 von McAffee ist als Campuslizenz erhältlich. Aus eigener Erfahrung können wir noch das Antivirenpaket von Pandasoft empfehlen.

Bekannte Hoaxes

Irina, Good Times, Ghost, Deeyenda, Penpal Greetings, Make Money Fast, Naughty Robot, AOL4FREE (Vorsicht, auch als echtes Trojanisches Pferd vorhanden!).

Literatur

[1] Brehm, A.: Das neue Tierreich nach Brehm, Meyer ,1973

[2] Cameron, D.: Security Issues for the Internet and the World Wide Web, CTR, 1996

[3] Hofmann, M.: Viren erkennen und beseitigen, Falken Verlag, 1990

[4] Homer: Ilias, 9. Jhd. vor Christus

[5] Icove, D. et.al.: Computer Crime, O` Reilly & Associates, 1995

[6] Pschyrembel, W.: Klinisches Wörterbuch, 257. Auflage, Walter de Gruyter, 1994

[7] Virus Test Center Universität Hamburg
http://agn-www.informatik.uni-hamburg.de/vtc/navdt.htm

[8] Ferbrache, D.: A Pathology of Computer Viruses, Springer, 1992

[9] Kuri, J.: Und Äktschn! Sicherheitsrisiko Acrobat PDF, c` t 6/97, S. 48, Heise
http://www.ix.de/ct/art_ab97/9706048

[10] Virus Help Munich: http://www.vhm.haitec.de/

Ansprechpartner in sicherheitsrelevanten Fragen

- sneakers@rus.uni-stuttgart.de
- dfncert-request@cert.dfn.de

Bernd Lehle, NA-5531
E-Mail: lehle@rus.uni-stuttgart.de

Oliver Reutter, NA-4513
E-Mail: Oliver.Reutter@rus.uni-stuttgart.de