Skriptum zur Vorlesung

DATENSCHUTZ UND DATENSICHERHEIT

Angriffe auf (geheime Daten) und die Verfügbarkeit

Wintersemester 2001/2002

Vortragender:

Dr. Jörg Pflüger

Weitere Angriffe auf (geheime) Daten und die Verfügbarkeit

A. Andere Spähangriffe

A1. Nicht richtig gelöschte Daten

Die Art und Weise, wie Daten von verschiedenen Betriebssystemen gelöscht werden, ist von System zu System unterschiedlich.

Wenn man eine Klartext-Datei verschlüsselt und danach löscht, löscht das Betriebssystem die Daten nicht physikalisch. Es markiert nur diejenigen Datenblöcke der Festplatte oder Diskette als "gelöscht", die den Inhalt der "gelöschten" Datei enthalten, so daß sie für die Speicherung anderer Daten freigegeben werden. Das ist das gleiche, als würde man vertrauliche Papiere einfach zum Altpapier legen, anstatt sie von einem Reißwolf klein häckseln zu lassen (-> "Dumpster Diving"). Die Blöcke auf der Festplatte enthalten nach wie vor die originalen vertraulichen Daten und werden vielleicht in naher oder ferner Zukunft durch neue Daten überschrieben. Wenn ein Angreifer diese "gelöschten" Datenblöcke kurz nach ihrer Freigabe liest, hat er einige Aussicht, den kompletten Klartext zu erhalten.

Die meisten Textverarbeitungsprogramme legen zusätzlich zu den Files auch noch aus technischen Gründen temporäre Dateien. Werden diese Dateien vom Textverarbeitungsprogramm automatisch gelöscht, steht der Text weiterhin in den auf der Festplatte oder Diskette für ein Überschreiben freigegeben Blöcken.

Einige Textverarbeitungsprogramme - wie Word - speichern in bestimmten Modi ältere Versionen von Textpassagen im Dokument, so daß man aus dem fertigen Dokument eventuell die Geschichte seiner Erstellung auslesen kann. (Beispiel: Microsofts Jahresbericht auf einem Mac erstellt. ;-)

Auch in den von vielen Betriebssystemen angelegten swap-Files (Auslagerungsdatei) können Textreste vorhanden bleiben, die ein potentieller Angreifer zum Gewinnen von vertraulichen Daten verwenden kann.

Die einzig wirkungsvolle Maßnahme, sich vor solchen Attacken zu schützen, ist sicherzustellen, daß die Blöcke mit den Textresten auch wirklich überschrieben werden. Jedoch kann ein entsprechend gut ausgerüsteter Angreifer auch aus überschrieben Blöcken immer noch Informationen über die "gelöschten" vertraulichen Daten gewinnen. Spuren der Original-Daten bleiben auch nach einem Überschreiben auf der Festplatte oder Diskette.

A2.Tempest-Angriffe

Im Englischen nennt man Techniken, mit denen elektromagnetische Strahlung reduziert werden kann, Tempest (Transient Electromagnetic Pulse Emanation Standard). Mittlerweile wird der Ausdruck sowohl für Lauschangriffe als auch für Schutzmaßnahmen verwendet.

Tempest-Angriffe und Schutzmaßnahmen wurden ursprünglich im militärischen und Geheimdienstbereich ("nationale Sicherheit") entwickelt. Durch zunehmende kommerzielle und privaten Interessen an Abhörmöglichkeiten und billigere "Spionage"technologie sind heute Informationen über diese Bedrohungen der Privacy und des Datenschutzes und entsprechende Schutzmechanismen erforderlich.

Natürlich gibt es bereits seit langem Möglichkeiten, Computer vor der Tempest-Belauschung zu schützen. Solche Tempest-Schutzschilder aus Metall einzurichten, ist normalerweise aufwendig, teuer und unhandlich. Es gibt aber einfachere Möglichkeiten wie etwa "SecuDat" von Hans-Georg Wolf (siehe dazu http://www.ix.de/ct/99/04/182). Damit läßt sich die Abstrahlung der Geräte durch zufällige Störsignale überlagern, so daß Lauscher nichts mehr mitbekommen.

> *“TEAPOT: A short name referring to the investigation, study, and control of intentional compromising emanations (i.e., those that are hostilely induced or provoked) from telecommunications and automated information systems equipment."*

Markus Kuhn und Ross Anderson, die Patente für Tempest-Schutztechniken eingereicht haben, behaupten, daß Lauschangriffe auf Abstrahlung inzwischen billig mit Bauteilen aus einem Bastlerladen durchgeführt werden können und so prinzipiell vielen Menschen zur Verfügung stehen.

Sie selbst haben bereits Programme geschrieben, die sich sowohl zum Schutz als auch zum Abhören der Abstrahlung einsetzen lassen. Man kann etwa

> *"einen Tempest-Virus schreiben, um den PGP-Schlüssel des Feindes zu erhalten und ihn ohne sein Wissen abzustrahlen, indem man die Muster auf seinem Bildschirmschoner manipuliert. Die Signale lassen sich bereits mit einem billigen Kurzwellenradio empfangen."*

Man könne beispielsweise nicht nur den Text auf einem Bildschirm lesen, sondern auch die Lizenznummer des Textprogramms. Das ließe sich auch so machen, daß nur diese abgehört werden könne, was er "Bill G." vorgeschlagen habe, damit Microsoft die Existenz von Raubkopien feststellen könne, ohne Probleme mit dem datenschutz zu bekommen. Microsoft habe abgelehnt.

Ross Anderson entwickelte auch einen eigenen Tempest-Font, der die Abstrahlung der Schriftzeichen auf dem Bildschirm auf ein Minimum reduziert, sodaß die Texte nicht "geskannt" werden können.

A3. Probleme mit Chip-Karten (SmartCards)

Eine typische Chipkarte besteht aus einem 8 Bit Mikroprozessor mit ROM, EEPROM und RAM. Dabei werden Schlüsseldaten im EEPROM abgelegt. Sie werden heutzutage in allen möglichen Bereichen verwendet, wie im Bankwesen, als Telefonwertkarten, bei Versicherungen, Identitätskarten und vielem mehr.

Anderson und Kuhn beschreiben eine Reihe von Angriffsszenarien auf Chipkarten und andere Sicherheits-Prozessoren:

Die Chips können in ihrer Funktionsweise beeinflußt werden, indem man sie unüblichen Spannungen oder Temperaturen aussetzt.

Kurzzeitige Störungen der Spannungs- und Taktversorgung können gezielt eingesetzt werden, um kleine Änderungen im Code vorzunehmen und die im Chip gespeicherten geheimen Schlüssel zu ermitteln.

Durch Zeit- und Stromverbrauchsmessungen können Teilinformationen über Schlüssel gewonnen werden.

Nach dem Extrahieren des Chips aus seiner Umhüllung sei es mit Hilfe von Mikroprobennadeln im laufenden Betrieb möglich, beispielsweise Signale auf dem chipinternen Datenbus abzugreifen.

Auch Elektronenmikroskope würden eingesetzt, um Leiterbahnen und anliegende Spannungswerte auszuspähen.

In professionellen Halbleiter-Labors seien Ausrüstungen vorhanden, die für weiterreichende Angriffe genutzt werden können.

Einzig und allein bei Atomsprengköpfen ist eine Technik eingebaut, die Chips wohl wirklich sicher macht: Bei einem Einbruchsversuch werden die Siliziumbauteile in die Luft gesprengt.

Markus Kuhn und Ross Anderson meinen deshalb, daß man sich auf keinen Fall bei SmartCards darauf verlassen darf, daß sie ihre gespeicherten Geheimdaten für sich behalten.

B. Angriffe auf die Verfügbarkeit

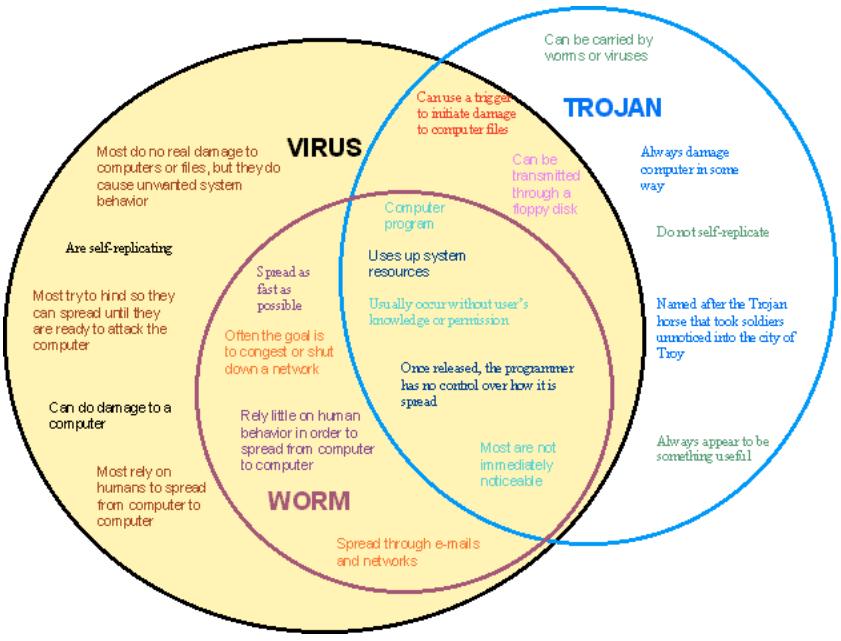
1. Malware
2. DoS-Attacken

1. Malware

Der Begriff Computervirus oder einfach Virus hat sich in der Umgangssprache für eine ganze Gruppe von Programmen eingebürgert, die als "malicious software" oder kurz "Malware" bezeichnet wird. Je nach Funktion handelt es sich um Viren, Würmer, Trojanische Pferde, logische Bomben, Zeitbomben (oder Hoaxes).

Die Begriffe werden nicht trennscharf verwendet, und heutige Malware mischt zunehmend die verschiedenen Elemente.

Böser Zoo:



Wir behandeln im folgenden die Malware-Sorten:

- Viren
- Trojanische Pferde
- Würmer
- Logische Bomben und Zeitbomben

Damit Malware Schaden anrichten kann, sind

- Vertrauenseeligkeit bzw. Dusseligkeit der User
  (z. B. ausführbare Attachment von Email öffnen) oder
- Sicherheitslücken von Server- oder sonstiger Software
  (berüchtigt: Microsofts IIS ("Internet Information Server"))

erforderlich.

20 Top Vulnerabilities (The SANS Institute, 2001) Quelle: http://66.129.1.101/top20.htm

All Systems (G):	G1 - Default installs of operating systems and applications
	G2 - Accounts with No Passwords or Weak Password
	G3 - Non-existent or Incomplete Backups
	G4 - Large number of open ports
	G5 - Not filtering packets for correct incoming and outgoing addresses
	G6- Non-existent or incomplete logging
	G7 - Vulnerable CGI Programs
Windows Systems (W):	W1 - Unicode Vulnerability (Web Server Folder Traversal)
	W2 - ISAPI Extension Buffer Overflows
	W3 - IIS RDS exploit (Microsoft Remote Data Services)
	W4 - NETBIOS - unprotected Windows networking shares
	W5 - Information leakage via null session connections
	W6 - Weak hashing in SAM (LM hash)
Unix Systems (U):	U1 - Buffer Overflows in RPC Services
	U2 - Sendmail Vulnerabilities
	U3 - Bind Weaknesses
	U4 - R Commands
	U5 - LPD (remote print protocol daemon)
	U6 - sadmind and mountd
	U7 - Default SNMP Strings

Viren

Computerviren sind Programme, die sich selbst reproduzieren, indem sie sich an andere Programme anhängen. Sie brauchen also einen (ausführbaren Wirt, durch den sie aaktiviert werden. Fast immer enthalten Computerviren einen Programmteil, der Schaden verursacht.

;-)

Man unterscheidet zwischen verschiedenen Typen:

- Systemviren (Bootsektor-Viren)
- Programm/File-Viren
- Makro-Viren
- Script-Viren
- multipartite Viren (Bootsektor- und Programmviren zugleich)
- polymorphische Viren (verändern ihre Gestalt bei der Verbreitung)
- residente Viren (bleiben auch nach Beendigung des Wirts (im RAM) aktiv)
- Stealth-Viren (tarnen sich gegenüber Antiviren-Software durch nicht-infizierte Kopien oder Größenangabenveränderungen)

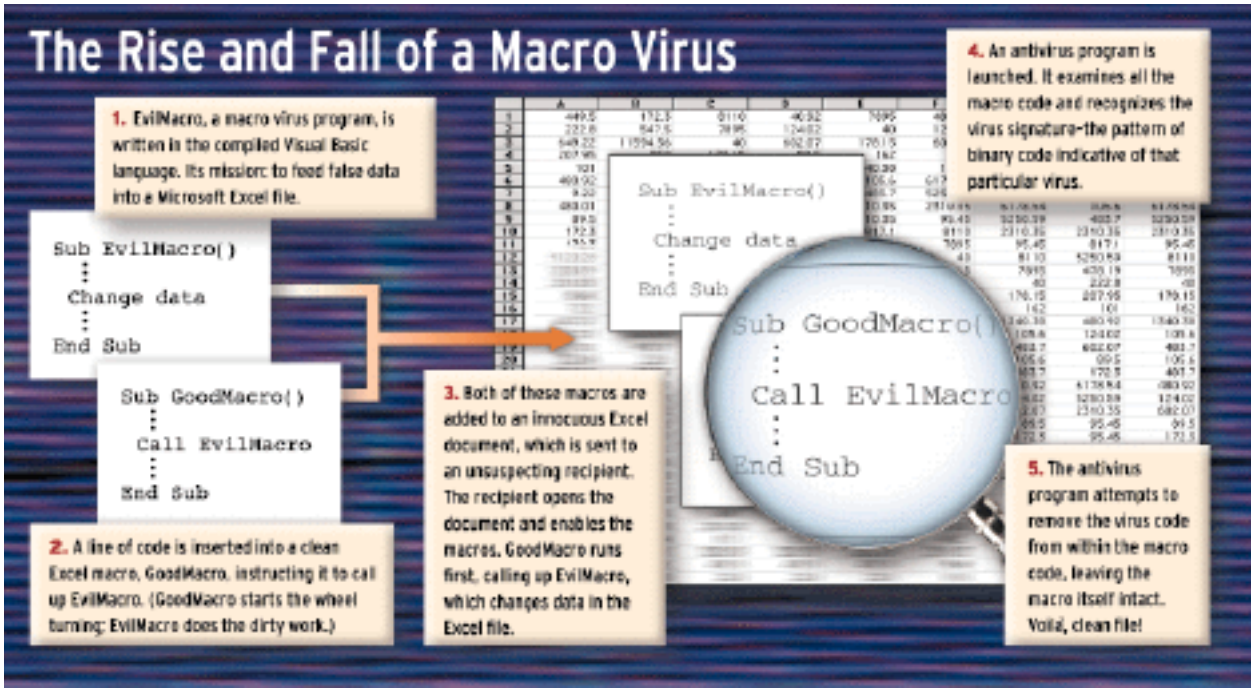
Systemviren befallen Systembereiche von Disketten und Festplatten. Bei solchen Systembereichen handelt es sich um den Bootsektor bzw. Master-Bootsektor (Partitionstabelle). In diesen Bereichen befinden sich Programmteile, die schon beim Starten des Computers ausgeführt werden. Infiziert ein Computervirus einen solchen Bereich, wird der Virus aktiviert, sobald der Computer eingeschaltet wird.

Ein **Programmvirus** hängt sich an eine ausführbare Datei an und wird Teil davon. Wird nun das Programm ausgeführt, tritt auch der Virus in Kraft und verursacht dann unterschiedliche Schäden, die bis zum kompletten Verlust aller Daten auf der Festplatte führen können.

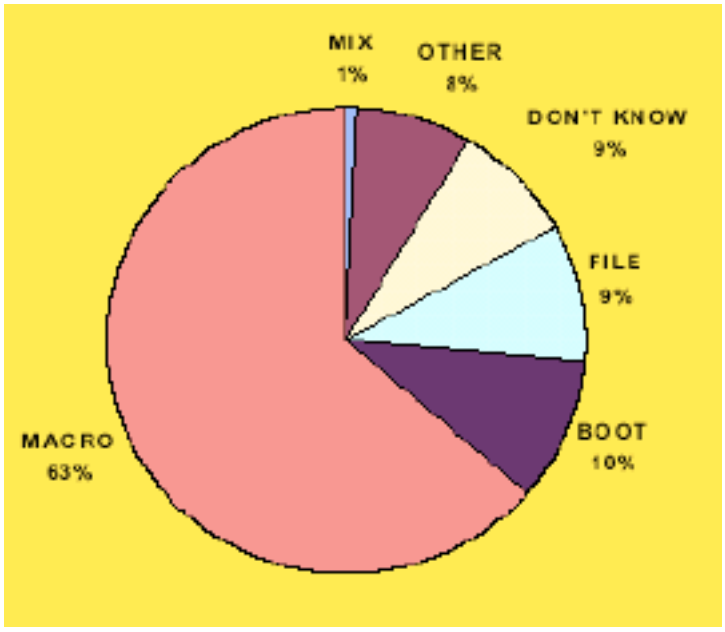
Makroviren betreffen Anwendungen, die über eine eigene Makrosprache verfügen. Vielfach sind die Microsoft Office-Programme davon betroffen, da in der aktuellen Version 2000 eine komplette Entwicklungsumgebung (Visual Basic for Applications) vorhanden ist. Mit Hilfe dieser Programmiersprache sind Systemzugriffe sehr leicht zu programmieren und in Dokumenten zu verstecken.

Script-Viren greifen auf die Programmiersprachen Visual Basic Script und JAVA zurück. Während JAVA eine reine Netzsprache ist, mit der sich beispielsweise eine Web Site mit vielfältigen Funktionen ausrüsten läßt und weniger für den lokalen Betrieb ausgelegt ist, wird VB Script mit Hilfe des Windows-Scripting Host gerne für automatische Aktionen innerhalb des lokalen Rechners eingesetzt. Hier verbirgt sich eine große Gefahr, da selbst simpelster Code bereits äußerst destruktive Funktionen ausführen kann.

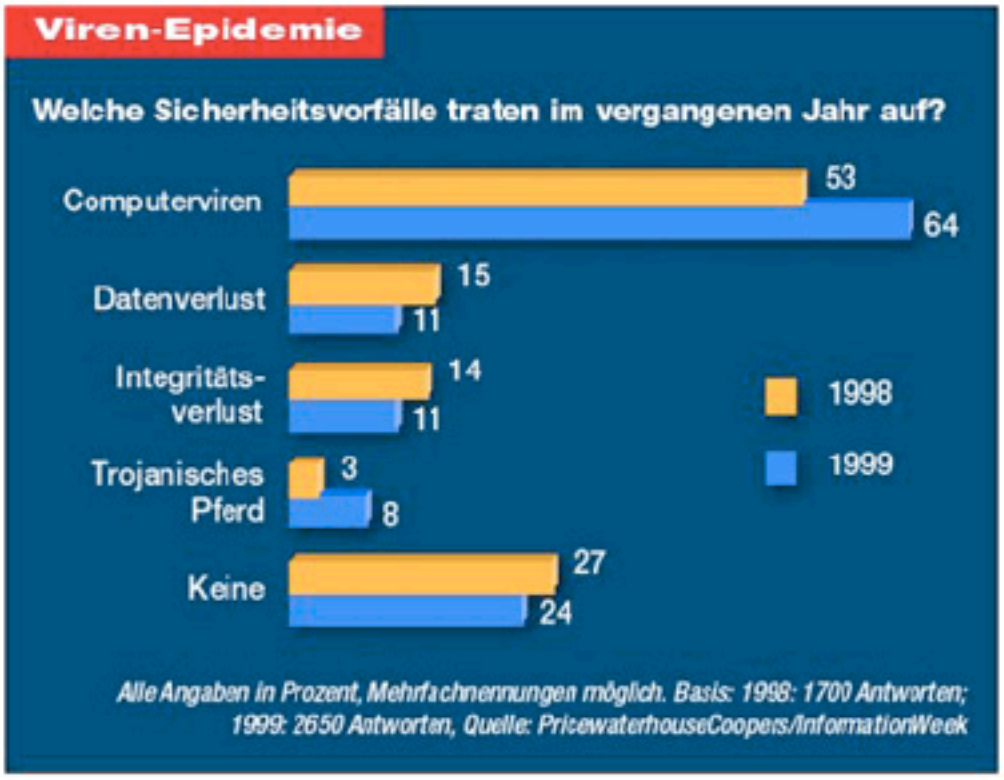
Zum Schutz vor solchen Viren eignen sich (mehr oder weniger) die handelsüblichen Virenscanner, von denen man aber regelmäßig Updates der Definitionen über das Internet nachladen muß. Sie schützen nur gegen bekannte Viren, da sie die an charakteristischen Merkmale erkennen müssen.



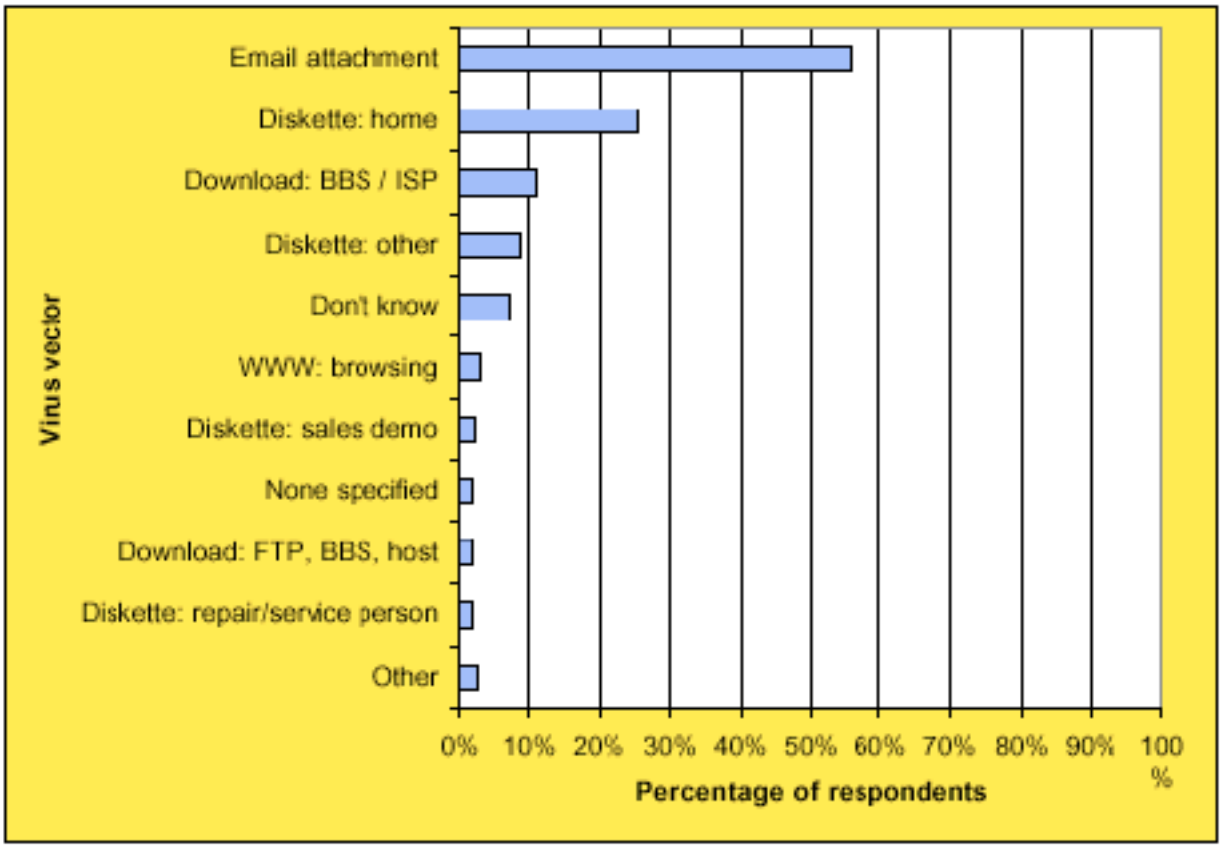
Etwas Statistik (mit Vorsicht zu genießen):



Verteilung der Virenarten



Elf Prozent mehr Viren-Zwischenfälle als im vergangenen Jahr melden die Unternehmen. Dramatischer ist der Zuwachs nur noch bei Trojanischen Pferden – die haben sich mehr als verdoppelt.



Übertragungswege

Angeblich existieren ca. 18000 Varianten (meist im Labor), 250-400 "in-the-wild"

(Zahlen schwanken enorm!).

Wahrscheinlichkeit infiziert zu werden: p=1/30

Trojaner

Trojaner sind im Gegensatz zu vielen Viren vollständig eigene Programme mit mehr oder weniger destruktiver Energie. Ihre schädigende Komponente ist in ein Programm eingebaut, das eine nützliche Funktion vorspiegelt. Ein trojanisches Pferd gibt sich als Bildschirmschoner, Paßwortverwaltung, Spiel oder anderes nützliches Tool aus, um im Hintergrund sein bösartiges Handwerk zu betreiben.

Mit Hilfe eines Trojaners gelingt es, die vollständige Kontrolle über einen infizierten PC zu erhalten und beliebige Funktionen (auch über das Internet getriggert) auszuführen. Aus diesem Grund werden Trojaner von Hackern auch als "Remote-Access-Controls" bezeichnet - also eine Art Fernsteuerungs-Software.

Ein bekanntes Beispiel:

> Anfang 1998 entschlüsselten zwei 16jährige Schüler die Verschlüsselung des T-Online-Paßworts. Anschließend programmierten sie die T-Online Power Tools, ein Hilfsprogramm für den T-Online

Decoder. Das Tool fand rasch Verbreitung. Jedoch: Sobald jemand die Online-Registrierung benutzte, schickte der Trojaner über das Internet auch die Zugangsdaten zum jeweiligen T-Online Anschluss mit. So kamen in kurzer Zeit 600 Paßwörter zusammen. Zum Glück für die Ausgespähten ging es den Schülern nur darum, die Möglichkeit nachzuweisen. Sie veröffentlichten ihre Erkenntnisse in der Presse.

Außer zum Erlangen von Paßwörtern, werden Trojaner auch eingesetzt zum

Kontrollieren des Dateisystems (kopieren, löschen, überschreiben),
Herunterfahren des Betriebssystems,
Öffnen und Schließen des CD-ROM Laufwerks,
Einfügen von Viren in das infizierte System
Koordination von DoS-Attacken und zur
Erlangung der vollständigen Kontrolle über die Peripherie (z.B. Webcams).

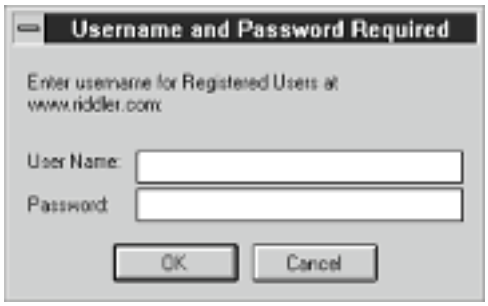
Trojanische Pferde benutzen häufig auch Techniken des Social Engineering:

Übertölpelung durch ein vorgespiegeltes Java-Applet, das ein Paßworteingabefeld simuliert

-> Kenntlichmachung des unsicheren Applets

Ein Applet, das, nachdem es geladen wurde, normales Browsen vorspiegelt und im Falle eines Logins in einem Standardfenster sein eigenes Login-Fenster unterschiebt.

Geht das?



Schützen kann man sich vor Trojanern eigentlich nur, wenn man überhaupt keine Software (aus dem Internet oder aus einem möglicherweise infizierten LAN) auf seinem Rechner installiert. Besonders fremde Dateien (z. B. E-Mail Attachments) sollte man nur öffnen, wenn man sich 100%ig sicher ist, daß sie keine Trojaner oder Viren enthalten (Viren/Trojanerscanner).

Würmer

Ein Wurm ist ein eigenständiges Programm, das sich selbständig übers Internet oder per Email wie ein Virus ausbreitet. Der Wurm wird durch den Empfänger, Systemfunktionen oder idiotische bzw. fehlerhafte Software aktiviert.

Bestandteile eines Wurms:

- Erkundungskomponente
- Angriffskomponente
- Kommando-Interface
- Kommunikationskomponente
- Nachrichtenkomponente
- unbenutztes Attackenreservoir

Der erste Wurm, der das damals noch kleine Internet ziemlich lahm legte, war der Morris Worm, 1988. Er nutzte Schwachstellen in Unix (sendmail, finger) aus.

Unter dem Namen ExplorerZip bzw. *ZippedFiles* verbreitete sich Anfang Juni 1999 ein Wurm für Windows 95/98 Systeme:

> Das Opfer bekommt eine - englische - E-Mail mit persönlicher Anrede, an die eine exe-Datei mit dem Namen ZippedFiles angehängt ist. Das wirkt wie ein normales Zip-Archiv, das sich per Doppelklick öffnen läßt. Statt dessen aktiviert ein Doppelklick den Wurm. Der gibt eine Fehlermeldung aus, die ein defektes Zip-Archiv bemängelt. Im Hintergrund kopiert er eine Datei namens explore.exe ins System-Verzeichnis von Windows und ändert die Win.ini. Damit wird der Wurm bei jedem PC-Start aktiv. Ist der Wurm aktiv, wartet er auf den Start von Outlook. Dann durchsucht er den Posteingang und schickt an alle Absender eine Antwort. Dabei benutzt er den Vornamen als Anrede und verspricht eine baldige Antwort auf die ursprüngliche Mail. In der Zwischenzeit soll der Empfänger einen Blick auf das angehängte Zip-Archiv werfen - schon ist ein neuer PC infiziert.

Innerhalb eines Netzwerkes hat ein Wurm andere Optionen. Das Peer-To-Peer-Netzwerk von Windows 95/98 und NT4.0 erlaubt den Zugriff auf die Festplatten fremder PCs. Standartmässig ist diese Freigabe gesperrt, aber viele Anwender haben die Option aktiviert.

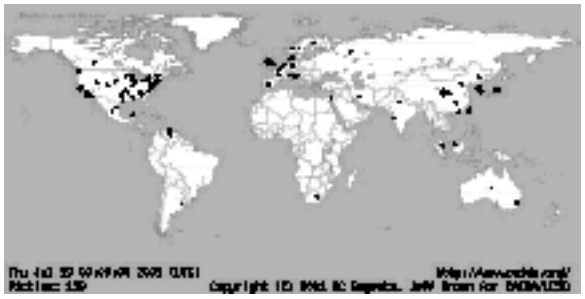
> Der Wurm *ExploreZip* sucht gezielt nach freigegebenen Laufwerken und installiert sich dann selbstständig auf solchen Windows-Laufwerken. Er durchsucht dann gezielt alle verfügbaren Laufwerke - auch die Netzlaufwerke - nach Dateien folgenden Typs: asm, c, cpp, doc, h, xls, ppt - diverse Quelldateien von Programmiersprachen sowie von Word, Excel und PowerPoint. Der Schaden, den er anrichtet, besteht darin, die Länge dieser Dateien auf Null zu setzen. Das erschwert im Gegensatz zum einfachen Löschen das Wiederherstellen der Dateien erheblich.

Der seit Juli 2001 grassierende *W32.Sircam* Wurm wird per Email verschickt.

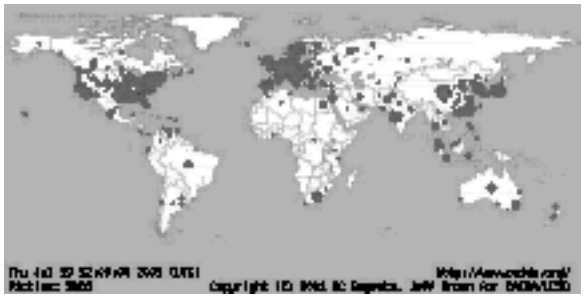
> Er versendet, einmal aktiviert, mit seiner eingebauten SMTP-Engine an alle Kontakte, die er sich aus den gängigsten Windows-Email-Programmen heraussucht, ein kurzes Email in englischer oder spanischer Sprache. Darin verweist er auf das angehängte Attachment, das aus einem zufällig gewählten File aus den Dateien des infizierten Rechners besteht und dem der Wurm angehängt wurde. Email-Filter sind wirkungslos, da das "Subject" der Name des Attachments ist und man immer ein anderes Attachment bekommt. Der Schaden: Es lassen sich keine exe-Files mehr starten, und es bleibt nur noch eine Neuinstallation des Systems.

Code Red:

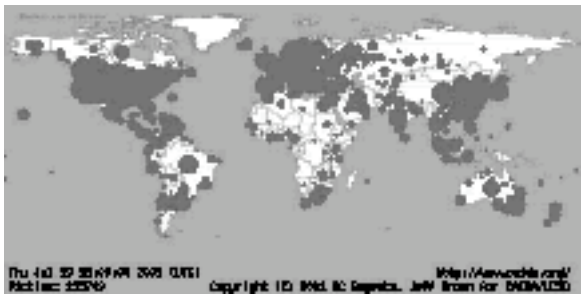
13. 7. 2001	Der erste Code-Red Wurm verbreitet sich auf IIS Webservern, er benutzt den am 18.6. entdeckten "buffer overflow" Fehler, Ausbreitung mit "static seed" für random IP-Adressen (Absicht?), bei US Windows NT/2000 Versionen gibt er die Nachricht: *"Welcome to http://www.worm.com!, Hacked By Chinese!"* aus; er versucht 4 Stunden lang eine DDoS-Attacke auf www.whitehouse.gov, die scheitert, weil sie IP-Adresse benutzt.
19.7. 2001	CodeRed Variante mit "random seed" (CRv2), er infiziert in 14 Stunden mehr als 359000 IIS-Webserver
1.8. 2001	neue Welle, 1/3 der infizierten Server sind nicht gepatched (> 140000)
Anfang August	Code-Red II Wurm, funktioniert nur auf Windows 2000; der neue Wurm installiert "back door" für ein Remote Login



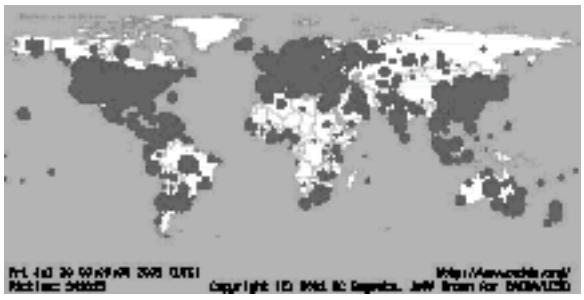
19.7. 2001 0 Uhr: 159 Opfer



19.7. 2001 12 Uhr: 5083 Opfer



19.7. 2001 18 Uhr: 235749 Opfer



19.7. 2001 24 Uhr: 341015 Opfer

Die Ausbreitung spiegelt die tatsächliche Dichteverteilung des Internets wider.

Sekundäre Folgen: Drucker, Router, DSL Modems u. Ä. wurden beschädigt,
150000 IIS-Sites auf 80000 IP-Adressen waren im September verschwunden.

Die Ausbreitungsgeschwindigkeit von Code Red kann weit übertroffen werden. Es existieren zeitliche Abschätzungen von theoretisch möglichen Würmern

Warhol Worms < 15 Minuten

Flash Worms < 30 Sekunden,

die ausreichen, das gesamte (verletzliche) Internet zu infizieren.

Auch ist eine bessere Tarnung möglich, sodaß der Wurmverkehr nicht von normalem Verkehr unterschieden werden kann.

Gegen solche Malware gibt es keinen Schutz, wenn die Netz-Software Sicherheitschwachstellen aufweist. Erforderlich ist, daß die allgemeine Systemsicherheit verbessert wird, darin ist die Wurmabwehr ist am ehesten mit der Abwehr von Systemeinbrüchen zu vergleichen.

Am Beispiel des Nimda Wurms kann man ersehen, welch unterschiedliche Sicherheitsschwachstellen (wieder mal von IIS) ein Wurm ausnutzen und auf welch verschiedene Arten er sich dementsprechend ausbreiten kann.

Analyse des Nimda Wurms

Angriffspunkte:

MS IIS/PWS Escaped Characters Decoding Command Execution Vulnerability

MS IE MIME Header Attachment Execution Vulnerability

MS IIS/PWS Extended Unicode Directory Traversal Vulnerability

MS Office 2000 DLL Execution Vulnerability

A*ngriffsweisen:*

Email mit Attachment "readme.exe" mit MIME-Type "audio/x-wav"

Open network shares (readme.exe, readme.eml, riched20.dll, admin.dll)

Modifikation von "common executables" (+ DLL-Files)

Modifikation von Web-Seiten: hängt an gefundene .html-Files folgendes an:

<html><script language= "JavaScript"> window.open("readme.eml", null, ...)
</script></html>

Direkte Infizierung: Download von "admin.dll" durch "Unicode Directory Traversal Vulnerability" oder Backdoor von Code Red II

Lange Zeit galten pdf-Files als sicher, heute nicht mehr:

"(Aug. 08, 2001) A worm that infects Portable Document Format (PDF) files ... was identified Tuesday ... So far, that type of file had been considered safe and immune from virus infections. The virus is called Outlook.pdf ... the worm uses Outlook to send itself hidden in a PDF file. When opened using Acrobat, the file will launch a game that prompts the user to click on the image of a peach. After the user clicks on the image, a Visual Basic script is run and the virus gets activated, ..."

Logische Bomben und Zeitbomben

Logische Bomben und Zeitbomben schlummern auf der Festplatte und erwachen bei einer Aktivität des Anwenders (zum Beispiel bei einem bestimmten Zählerwert) beziehungsweise an einem Datum.

Bekannt ist Michelangelo, der am Geburtstag des Meisters die Festplatte formatiert.

Eine logische Bombe kann aber auch ausgelöst werden, wenn zum Beispiel die Festplatte einen gewissen Speicherplatzgröße überschreitet (zum Beispiel bei 2 Gbyte wird die Festplatte formatiert).

Nach der (derzeit in einigen Bundesstaaten gültigen) amerikanischen Copyrightregelung UCITA können Software-Hersteller ihre Programme remote abschalten, wenn sich vertragliche Unstimmigkeiten ergeben. Das ist nichts anderes als eine legalisierte Bombe.

B2. DoS-Attacken

"Denial-of-Service" Attacken (DoS-Attacken) bestehen darin, den Zugriff oder Nutzen eines Computers oder eines Subnetzes zu be- oder verhindern. Damit wird die Verfügbarkeit von Informationen oder Dienstleistungen eines Servers blockiert.

Die häufigstn Form der "Distributed Denial-of-Service" Attacke (DDoS-Attacke) nutzt Sicherheits-schwachstellen von anderen Rechners aus, um das unschuldige Opfer mit vielen infizierten Rechnern (Trojaner, Würmer) gleichzeitig anzugreifen.

Man kann folgende Attacken unterscheiden:

Mailbombing

Broadcast Storms

DDoS - Distributed Denial of Service

Mailbombing

Eine der ältesten Versionen von DoS.

Hierbei schickt man einem Empfänger Massen an gleichen oder automatisch modifizierten Emails (mit unterschiedlichen falschen Adressen), sodaß deren Empfang den betroffenen Rechner lahm legt.

(Zusätzlich wird der versendende SMTP-Server überlastet.)

Eine Variante besteht darin, eine Newsgroup oder eine Mailingliste mit gepostetem Schwachsinn zuzumüllen; dies wurde vor einigen Jahren (wahrscheinlich) von der Scientology Sekte mit einer Newsgroup, die sich kritisch mit Scientology auseinandersetzt, praktiziert.

Eine andere Version ist das ungewünschte Eintragen in Unmengen von Mailinglisten. Das Opfer hat dann die leidige Aufgabe sich aus allen wieder händisch auszutragen. Dies entspricht der RL-Aktion, für jemanden telefonisch 100 Pizzas zu bestellen.

Broadcast Storms

Broadcast Storms bestehen darin, an jeden Rechner in einem lokalen Netzwerk eine Flut von IP Packeten zu schicken, die alle an nicht existierende Ziele adressiert sind.

Durch den Versuch diese Datenströme aufrechtzuerhalten, ist das Netzwerk recht schnell überlastet.

DDoS - Distributed Denial of Service

Eine effiziente Form der DoS-Attacke ist die auf viele Hosts verteilte Version. Dabei nutzt ein Hacker die Bandbreiten vieler Einzelrechner, deren Besitzer davon keine Ahnung haben, um ein Opfer von allen Rechnern aus gleichzeitig anzugreifen. Die unfreiwilligen Helfer werden Bots oder Zombies genannt.

Der Hacker kann seinen Zombies zum Beispiel befehlen, gleichzeitig einen Dauer-Ping oder irgendwelche Pakete an eine vorgegebene IP-Adresse zu schicken und durch die so entstehende Datenflut den Webserver mit dieser IP aus dem Internet zu werfen.

Ein Zombie ist im Grunde ein Trojaner, der sich durch einen Download oder durch den Empfang eines Emails bei einem achtlosen User eingenistet hat. Sobald nun dieser User sich mit seinem PC ins Internet einklinkt, verbindet der Bot sich mit gespeicherten Zugangsdaten zu einem geheimen IRC-Channel (Internet Relay Chat), von wo aus der Hacker seine "Untoten" zum Leben erwecken und befehligen kann.

Bekanntes Beispiel:

Im Februar 2000 wurden Yahoo, Amazon, eBay, CNN.com, Buy.com, ZDNet, E*Trade und Exite.com durch eine DDoS-Attacke an drei Tagen für Stunden völlig lahmgelegt.

DoS-Attacken können auch von "Script-Kiddies" durchgeführt werden, die die Bots nicht selbst programmiert haben, weil entsprechende Skripts im Web zur Verfügung stehen.

DDoD-Attack-Scripts: Trinoo, TFN (Tribal Flood Network), Stacheldraht

Analysiertes Beispiel: Angriff auf den Webserver von "grc.com"

Sein Besitzer Steve Gibson beschreibt in einem Bericht ausführlich eine solche DDoS-Attacke (Quelle: http://grc.com/dos/grcdos.htm):

Angriff von 474 Windows PCs ("Zombies"),
im Laufe von 8 Tagen ca. 2,4 Mrd. "malicious packets",
Angreifer: 13-jähriges "script-kiddie",
Hilfsmittel: Sub7Server Trojan,
Strategie: Koordination über IRC-Server (secret channel für IRC-Bots)

Gibson streicht heraus, dass Windows 2000/XP noch viel gefährlicher für solche Attacken eingesetzt werden kann, als seine Windows9x-Vorgänger, da im Gegensatz zu den alten Windowsversionen, die gesamte Unix-Sockets Spezifikation ausprogrammiert ist, und somit noch viel mehr Möglichkeiten ("spoofing" und bösartige TCP-Packets) für Hacker bestehen, DDoS Attacken zu "designen".

Wirklich wehren kann man sich gegen solche Attacken eigentlich nur durch gute Filter bei den Internet-Routern, was aber nur möglich ist, wenn man einen auf Sicherheit bedachten ISP (Internet Service Provider) mit kompetenten Technikern hat.