Institut für Informatik
LS IV - Software and Systems Engineering

Proseminar Software Desasters

Computerviren

Baowen Yu

Ausarbeitung

13. November 2002

Inhaltsverzeichnis

I. Was sind Computerviren?

I.1 Definitionen

Biologischer Virus [8]: Ein Virus ist ein infektiöser Erreger, der nur innerhalb einer Wirtszelle wachsen kann. Es reproduziert sich durch Nutzung der Wirtszelle als Produzent und verlässt die Zelle je nach Art, durch Zerstörung oder in einer nicht destruktiven Weise. --Biologie Website

Computervirus [2]: Viren sind Programmstücke in Maschinencode, die sich vervielfachen, in andere Programme hineinkopieren und zugleich schädliche Funktionen in einem Rechnersystem ausüben können. Ein Virus ist in der Regel Bestandteil eines anderen Programms (Wirtsprogramme) und führt seine eigenen Anweisungen vor oder während des Ablaufs des Wirtsprogramms aus.

Computerviren sind Programme, genau wie Textverarbeitungssysteme, Web-Browser oder Spiele, das heißt, sie werden von Menschen programmiert. Verbreitet werden sie durch das Weiterreichen bereits infizierter Programme (Wirtsprogramme) oder Datenträger. Virenprogrammierer sind an einer möglichst schnellen und möglichst weitreichenden Verbreitung ihrer Programme interessiert. Je beliebter Anwendungen sind, desto besser dienen sie ihren Zwecken. Die Chance, dass ein Spiel, das millionenfach rund um den Erdball gespielt wird, Opfer einer Virusattacke wird, ist demnach größer, als dass eine seltene Spezialanwendung befallen wird. Ebenso eignet sich ein weit verbreitetes Office-Paket wie das von Microsoft besser als Zielscheibe für einen Makrovirus als eine exotische Textverarbeitungssoftware.

I.2 Herkunft und Geschichte von Computerviren

Geschichte der Computerviren [4]

Der erste PC-Virus tauchte Mitte der achtziger Jahre in Pakistan auf und verbreitete sich von dort per Diskette über die ganze Welt. Inzwischen gibt es weltweit über 10.000 Computerviren.

1982

Drei Versionen von Apple Computerviren tauchen in freier Wildbahn auf.

Jon Hepps und John Shock von Xerox PARC generieren Würmer für verteilte Rechenoperationen, die für den internen Gebrauch bestimmt sind. Die Würmer geraten außer Kontrolle, viele Systeme müssen heruntergefahren werden.

1983

Fred Cohen definiert den Begriff "Computervirus" formal.

1986

Entdeckung des ersten PC-Virus. Name: „Brain“. Herkunft: Pakistan. Typ: Boot-Virus. Besonderheit: benutzt Tarntechniken.

Dezember: Entdeckung des ersten Datei-Virus. Name: „Virdem“. Herkunft: Deutschland.

1987

Oktober: "Brain" taucht in freier Wildbahn, an der Universität von Delaware, USA, auf.

November: Der "Lehigh"-Virus wird an der Lehigh-Universität in den USA entdeckt. Er ist der erste Virus, der command.com infiziert.

Dezember: Der Wurm „CHRISTMA EXEC“ verbreitet sich auf IBM VM/CMS-Systemen. Er zeigt einen Weihnachtsbaum und versendet sich dann heimlich per E-Mail. Obwohl der Wurm auf menschliche Mithilfe angewiesen ist, erzwingt er das Herunterfahren vieler Systeme.

Dezember: Der Jerusalem-Virus, der erste speicherresistente Virus, der in viele Varianten bekannt wird, taucht an der Hebräischen Universität in Israel auf.

Der berüchtigte "Stoned"-Virus, der erste MBR-Virus (Master Boot Record), stammt von einem Studenten der Universität von Wellington, Neusseland.

1988

März: Entdeckung des ersten Antivirus-Virus: “Den Zuk“ von Denny Yanuar Ramdhani aus Bandung, Indonesien, erkennt und entfernt den Brain-Virus.

November: Robert Morris, 22, startet den Internet-Wurm. Er befällt 6000 Computer, das sind 10% aller Computer im Internet. Morris wird zu drei Jahren auf Bewährung, 400 Stunden gemeinnütziger Arbeit und 10.000 US$ Geldstrafe verurteilt.

“Cascade“, der erste sich Selbstverschlüsselnde Virus, wird in Deutschland entdeckt.

1989

Januar: Der Virus „Dark Avenger.1800“, in Sophia, Bulgarien geschrieben, ist der erste schnell infizierende Virus, der jedoch nur sehr langsam Daten beschädigt.

Oktober: Aus Haifa, Israel, wird die Entdeckung des Virus „Frodo“ berichtet. „Frodo“ ist der erste Tarnkappen-Virus, der Dateien infiziert.

1990

In den USA finden sich polymorphe Viren, darunter „V2Px“, „Virus-90“ und „Virus-101“.

Mit „Anthrax“ und „V1“ werden die ersten mehrteiligen Viren entdeckt. Der Virus Flip ist der erste dieses Typs, der sich erfolgreich verbreitet.

1991

März: Entdeckung des Michelangelo-Virus.

März: Veröffentlichung des Virus-Construction-Sets, das den Zusammenbau eigener, neuer Viren ermöglicht.

Oktober: Entdeckung des ersten Cluster-Virus, „DirII“.

1992

Januar: „Dark Avenger“ veröffentlicht seine „Mutation Engine“ (MtE), die es ermöglicht, aus einfachen Viren polymorphe zu machen.

März: „Michelangelo“ wird am 6. März aktiv, weltweit vorausgesagte Schäden bleiben jedoch aus.

“WinVir 1.4“, der erste Windows-Virus, wird entdeckt.

Der erste Virus, der SYS-Dateien infiziert, erscheint auf der Bildfläche und bekommt den Namen "Involuntary".

1993

Juli: Die Antivirus-Industrie veröffentlicht ihre erste Wild-List.

Der Virus „SatanBug“ infiziert PCs in Washington, DC. Die Behörden können den Autor „Little Loc“ nach San Diego zurück verfolgen. Da er noch minderjährig ist, wird von Strafmaßnahmen abgesehen.

1994

Ein Virenprogrammierer benutzt das Internet, um seinen Virus zu verbreiten. Der Virus „Kaos4“ wird in der Newsgroup alt.binaries.pictures.erotica platziert.

Der SMEG.Paragon-Virus verbreitet sich in England. Scotland Yard stellt den Virusautor Christopher Pile (auch als „Black Baron“ bekannt). Er wird wegen Computerkriminalität in elf Fällen angeklagt.

1995

August: „Concept“, der erste Makro-Virus, infiziert Microsoft-Word-Dokumente. Der im Virus enthaltene Text lautet: "That’s enough to prove my point.”

November: "Black Baron" bekennt sich schuldig und wird zu 18 Monaten Haft verurteilt, gemäß Paragraph 3 des britischen Computermissbrauchsgesetzes von 1990.

1996

Entdeckung des Boza-Virus. Der erste Virus für Windows 95 wurde von Quantum geschrieben, einem Mitglied der Virusprogrammierergruppe VLAD in Australien.

Juli: Der erste Excel-Virus kommt in Alaska und Afrika ans Tageslicht. Er bekommt den Namen „XM.Laroux“ und infiziert Tabellen von Microsoft Excel.

1997

mIRC-Script-Würmer treten in Erscheinung. Die Virusprogrammierer schreiben mIRC-Scripte, die sich automatisch wurmartig unter den Benutzern des Internet Relay Chats verbreiten.

1998

Januar: Der erste Excel-Formel-Virus namens „XF.Paix.A“ taucht auf. Der Virus benutzt nicht die klassischen Makro-Fähigkeiten von Excel, sondern ein spezielles Formelblatt, das bösartigen Code enthalten kann.

März: Carl-Fredrik Neikter veröffentlicht „Netbus“, ein Hintertür-Programm, das Hackern Fernzugang zu infizierten Rechner verschafft.

April: Der erste Virus für Microsoft Access nebst den Varianten „A2M.Accessiv“ für Access 2.0; „AM.Accessiv.A,B“, „AM.Tox.A,B“ für Access 97 wird entdeckt.

Juni: Entdeckung des „W95.CIH“ in Taiwan, ein Virus mit einer der bösartigsten Schadensfunktionen: Er versucht das BIOS eines Computers am 26. April zu überschreiben, was oft einen Austausch der Hardware erfordert.

Juli: AOL-Trojaner tauchen auf. Das erste von vielen Trojanischen Pferden stiehlt Informationen von AOL-Benutzern. AOL-E-Mail-Adressen werden mit infizierten Dateianhängen überflutet.

August: „JavaApp.StrangeBrew“ ist der erste Java-Virus, der *.class-Dateien infizieren könnte. Er wurde jedoch nie in freier Wildbahn gesichtet.

August: Die Gruppe „Cult of the Dead Cow“ veröffentlichen „Back.Orifice“, ein getarntes Fernsteuerungsprogramm, das die Ausführung von Programmen sowie die Überwachung eines Computers ermöglicht. Die Medien lenken die Aufmerksamkeit auf das bereits vorher bekannte Netbus, das ähnliche Funktionen aufweist.

Oktober: „VBS.Rabbit“ wird losgelassen. Als erster von vielen Script-Viren, die den Windows Scripting Host nutzen, ist er in in der Sprache Visual Basic Script geschrieben und zielt auf andere *.VBS-Dateien.

November: „HTML.Prepend“ beweist, dass es mit VBScript möglich ist, HTML-Dateien zu infizieren.

Dezember: Entdeckung des ersten Virus für Microsoft PowerPoint „P97M.Vic.A“. Weitere Viren folgen, die sämtliche Office-97-Anwendungen infizieren.

1999

März: „W97M.Melissa.A“ verbreitet sich sehr schnell weltweit. Der Virus infiziert Word-Dokumente und versendet sich per E-Mail an bis zu 50 Adressen im Outlook-Adressbuch, was zum Zusammenbruch vieler Mailserver führt. David L. Smith wird als Verbreiter dieses Virus verhaftet.

April: „NetBus 2 Pro“ wird als kommerzielles Programm veröffentlicht. Der Autor Carl-Fredrik Neikter verlangt für sein Produkt Geld, um Antivirus-Hersteller davon abzuhalten, es als Virus zu melden. Die Hersteller fügen trotzdem eine Erkennungsroutine ein, da es sich um ein bösartiges Programm handelt.

26. April: „W95.CIH“ wird aktiv. Aus Asien werden erhebliche Schäden gemeldet. Aus den USA, Europa, dem Nahen Osten und Afrika kommen nur sporadische Meldungen. Chen Ing-Hau, ein Student, wird als Autor des Virus identifiziert. China (bzw. Taiwan) unternimmt keine rechtlichen Schritte.

Juni: Der Wurm „ExploreZip“ wird zuerst in Israel entdeckt. Mit der Geschwindigkeit von Melissa breitet er sich via Outlook aus und zerstört Dateien mit den Endungen DOC, XLS, PPT, C, CPP und ASM.

Juli: „Back.Orifice 2000“ wird auf der DefCon in Las Vegas von „Cult of the Dead Cow“ veröffentlicht. Die neue Version des Fernsteuerungsprogramms funktioniert jetzt auch unter NT.

August: David l. Smith bekennt sich schuldig, Autor des Melissa-Virus zu sein.

August: Der polymorphe, speicherresidente Virus „W32/Kriz“ wird nur einmal im Jahr aktiv und zwar am 25.12. Er überschreibt das Flash-BIOS, löscht oder zerstört

den CMOS-Speicher, überschreibt Daten in allen Dateien auf allen Laufwerken. Der PC muss im Fall einer Infektion sofort gesäubert werden. Ansonsten lässt sich der Rechner nicht mehr starten, und das BIOS muss ausgetauscht werden.

November: „VBS.BubbleBoy“ ist der erste Virus, der nur durch Lesen der E-Mail aktiv wird. Der Virus nutzt einen Fehler in einer Microsoft-Programmbibliothek, durch den das Abspeichern und Starten der E-Mail-Anlage unnötig wird. Einfaches Anklicken der E-Mail bei aktivem Vorschau-Modus startet den Virus.

2000

Januar: Die befürchtete Jahr-2000-Katastrophe bleibt aus, existierende Y2K-Viren bleiben weitgehend wirkunglos.

April: „VBS.BubbleBoy“ wird in freier Wildbahn gesichtet.

Juni: Mit einer Geschwindigkeit, die nur mit der von Melissa vergleichbar ist, breitet sich „VBS.Loveletter“ weltweit aus. Der als ILOVEYOU-Virus bekannt gewordenen Variante A folgen ungezählte weitere. Wieder brechen zahlreiche Mailserver zusammen. In den folgenden Wochen entsteht um jeden neu entdeckten Virus ein großer Medienrummel.

Juli: „VBS.Stages“, der erste Virus, der mit SHS-Dateien (Shell Scrap) arbeitet, nutzt die OLE-Fähigkeiten von Windows, um sich in einer scheinbaren Textdatei zu verbergen. Die Endung .SHS wird von Windows nicht angezeigt.

August: „W32.Pokey.Worm“ heißt der jüngste Wurm, der zwar bereits Ende Juni registriert wurde, jedoch erst jetzt für Aufregung sorgt. Ähnlich wie ILOVEYOU erscheint er als E-Mail-Anhang. Er nutzt Outlook Express, um sich zu verbreiten.

September: Der erste Trojaner für PDAs (Personal Digital Assistant) taucht auf. „Palm.Liberty.A“ verbreitet sich nicht von selbst, sondern gelangt beim Synchronisationsprozess auf den Kleincomputer und löscht Aktualisierungen. Herkunftsland ist Schweden. Entwickelt wurde er versehentlich von einem Beschäftigten der Universität von Gavle namens Aaron Ardiri.

November: Navidad.EXE ist ein Wurm und pünktlich zur Weihnachtszeit aufgetaucht. Am 3. November zum ersten Mal entdeckt verbreitet sich Navidad zwar nicht sehr schnell, ist aber dennoch gefährlich. Er nutzt Outlook oder Express um sich zu verbreiten und alle Arten von Windows-Rechnern können infiziert werden.

2001

Februar: Der Computerwurm „VB.SST@mm“ erscheint als E-Mail-Anhang „AnnaKournikova.jpg.vbs“. Versucht der Anwender den Dateianhang mit einem

angeblichen Bild der russischen Tennisspielerin zu öffnen, dann kopiert sich der Wurm in das Windows Directory und verschickt sich anschließend eigenständig via MS Outlook an das gesamte Outlook-Adressverzeichnis.

März: „W32/Naked“ tarnt sich als Flash Animation und verschickt sich nach der Aktivierung als E-Mail-Wurm mit dem Attachment „NakedWife.exe“ an das gesamte MS Outlook-Adressbuch. Indem er verschiedene Windows- und Systemverzeichnisse löscht, macht er das System unbrauchbar und erfordert eine Neuinstallation.

Juli: Der Massenmailer "Code Red" und sein Ableger "Code Red II" (Verbreitung im August) nutzen eine Sicherheitslücke in der Web-Software "Internet Information Server" von Microsoft aus, die unter Windows NT oder 2000 läuft. "Code Red II" attackiert nicht - wie das Original - die Web-Site des Weißen Hauses, sondern installiert eine Hintertür in das System, durch das Hacker den Rechner kontrollieren können.

Juli: Der Wurm „W32/SirCam“ verbreitet sich via MS Outlook Express und tangiert die Plattformen WIN 9x, WIN NT sowie WIN 2000. Wird er ausgeführt, platziert er sich im Systemverzeichnis und wird jedes mal aktiviert, wenn der Anwender ein Programm mit der Dateiendung .EXE starten will. Er kann sich aber auch selbstständig auf freigegebene Laufwerke im Netz kopieren und dort vom betreffenden Anwender aktiviert werden. "SirCam" verschickt nicht nur sich selbst, sondern zusätzlich auch noch persönliche Dateien, die er auf dem infizierten Rechner findet. Außerdem ist er der erste Wurm, der mit einem eigenen Mailserver (SMTP-Engine) ausgestattet ist.

September: Der aggressive Computerwurm „Nimda“ rast durchs World Wide Web. Die Innovation besteht darin, dass für seine Verbreitung keine Benutzerinterventionen mehr erforderlich sind. Stattdessen nutzt er bekannte Software-Schwachstellen und unterschiedliche Formen der Infektion. Er verbreitet sich über E-Mail und kann sich zudem über das Internet auf fremden Rechnern einnisten. Die rasante Verbreitung des Wurms belastet den Internetverkehr, führt zum Zusammenbruch der betroffenen Websites und kompromittiert die Sicherheit des Filesystems indem er die lokalen Laufwerke im Netzwerk freigibt.

November: Der speicherresidente Internetwurm „W32.Badtrans.B@mm“ ist eine Variante des „WORM_BADTRANS.A“ (Verbreitung April 2001), der ein bekanntes Sicherheitsloch in E-Mail-Applikationen (MS Outlook/MS Outlook Express) nutzt. Nach der Infektion registriert sich der Wurm als Systemservice und beantwortet eingehende E-Mails, spioniert Passwörter aus und installiert einen Key-Logger.

Besonders gut getarnt sind so genannte Stealth-Viren, die ihre Anwesenheit im System verschleiern. Dazu überwachen sie z.B. Zugriffe auf Programmdateien und das Inhaltsverzeichnis.
Versucht das Betriebssystem, z.B. beim Befehl DIR, die Größe einer infizierten

Programmdatei zu ermitteln, subtrahiert der Stealth-Virus von der tatsächlichen Dateilänge die Länge des Viruscodes und täuscht so eine korrekte Programmlänge vor. Wird eine Programmdatei nicht ausgeführt, sondern nur gelesen, z.B. von einem Virenscanner, entfernt der Virus aus der zu lesenden Datei den Viruscode, so dass der Virenscanner den Virus nicht in der Programmdatei finden kann.
Alle Stealth-Viren nutzen die Technik der Residenz um die Zugriffe des Betriebssystems zu kontrollieren.
Viele Viren verschlüsseln inzwischen bei einer Infektion den gesamten Virus oder Teile davon (z.B. lesbare Zeichenketten). Dabei verwenden einige Viren bei jeder neuen Infektion neue Schlüssel zum Ver-/Entschlüsseln. Solche polymorphen Viren verhindern, dass Virenscanner nach einer speziellen, für den Virus typischen Bytefolge suchen können. Um Monitorprogramme zu umgehen, versuchen einige Viren sich zwischen BIOS und Monitorprogramm einzuklinken. Dazu unterwandern sie die Monitorprogramme mit einer Technik, die als Tunneling bezeichnet wird. Da solche Viren vor dem Monitorprogramm aktiv werden, kann ein Monitorprogramm ihre Aktivitäten nicht feststellen.

I.3 Funktionsweise eines Virus

Ein Virus ist ein kleines Programm, das von einem Programmierer mit meist bösen Absichten geschrieben wurde. Das Wesentliche an einem Virus ist, dass es sich in Wirtsprogramme kopiert. Wenn ein infiziertes Wirtsprogramm gestartet wird, wird auch das Virus aktiv und repliziert sich, indem es sich an andere, bisher noch nicht infizierte Programme anhängt.

Einige Viren begnügen sich damit, sich weiterzuverbreiten. Der Schaden, den sie anrichten beschränkt sich auf das Belegen von Systemressourcen (wie z.B. Speicherplatz). Andere Viren richten durch eingebaute Zerstörfunktionen zusätzlichen Schaden an, indem sie beispielsweise Daten löschen oder verfälschen.

Viren befallen in der Regel ausführbare Dateien, wie z.B. Dateien mit der Endung EXE. Manchmal schreiben sich Viren auch in den Bootsektor von Disketten oder Festplatten, um beim Neustart des Rechensystems sofort ausgeführt zu werden.
Viren können prinzipiell auch auf das CMOS-RAM zugreifen. Da dieser Speicher jedoch bei vielen Betriebssystemen nicht im Adressraum abgebildet ist, eignet er sich nicht zur Programmausführung - ein Virus ist dort kaum anzutreffen.

I.4 Schäden durch Computerviren

Je nach Schutzmechanismus der zugrunde liegenden Ausführungsplattform können Viren mehr oder weniger starken Schaden anrichten:

-Datenverlust durch Löschen oder Verfälschen von Dateien.

-Ausspionieren von geheimen Daten, wie z.B. Passwörtern oder Kreditkartennummern.

-Beschädigung von Hardware (z.B. durch Abändern von Bios- oder Treiberparametern)

-Blockierung von Kommunikationskanälen, wie z.B. Email- Systemen

-Verbrauch von Speicherplatz und Rechenzeit.

I.5 Folgeschäden

-Wartungsaufwand für **Virenentfernung**

-Wartungsaufwand für **Virenschutz**

-Panik-Reaktionen und Verunsicherung von Anwendern

-Vertrauensverlust bei Kunden

-Ausfallschäden (Blockierung von Arbeitsabläufen, geplatzte Geschäfte, …)

I.6 Wie hoch ist der jährliche finanzielle Schaden von Viren?

Computerviren verursachen jährlich einen Schaden von ca. 10 Milliarden Dollar. [9]

Insgesamt hat das „Code Red“ Virus, das im vergangenen Monat sein Unwesen im Netz trieb, rund 2,6 Milliarden US-Dollar (5,5 Milliarden DM) an Schaden angerichtet.
Im laufenden Jahr, so die Experten eines unabhängigen Marktforschungsunternehmens, seien bisher für „angegriffene“ Unternehmen Schäden in Höhe von insgesamt rund 10,6 Milliarden US-Dollar (22,5 Milliarden DM) zusammengekommen (im Jahr 2000 lag der Wert bei 17,1 Milliarden US-Dollar (36,4 Milliarden DM)). „Sollten nun keine weiteren großen Viren im Netz auftauchen, dann werden wir vermutlich unter dem Wert des Vorjahres bleiben. So etwa bei 15 Milliarden US-Dollar (31,9 Milliarden DM)“, Ein weiterer Viren-Ausbruch könnte mehrere Milliarden kosten. [9]

Das „ILoveYou“ Virus, das heftigste Virus bis zum Jahr 2000, trat in insgesamt etwa 50 verschiedenen Versionen im Netz auf. Insgesamt wurden weltweit rund 40 Millionen Computer vom Virus in Mitleidenschaft gezogen. Das „ILoveYou" Virus war mit seinen angerichteten Schäden in Höhe von 8,7 Milliarden US-Dollar (18,5 Milliarden DM) das bisher „teuerste" Virus. [3]

Der „Melissa-„ und der „Explorer-Virus“ waren die schädlichsten des Jahres 1999. Im laufenden Jahr hatten die beiden Virentypen „Code Red" und „SirCam" etwa 2,3 Millionen Computer infiziert. Die Kosten entstehen durch das „Säubern" der Festplatten der Computer und durch die verminderte Produktivität der Computer während der Infektionsphase.

„Code Red“ hatte im vergangenen Juli in lediglich neun Stunden bereits mehr als 250.000 Systeme infiziert. Experten befürchteten daraufhin, dass, sollte das Virus

noch einmal auftauchen, das gesamte Internet Schaden leiden könnte. Das Virus war ursprünglich derart angelegt, dass es sich zum Ende des Monats selbst zerstören sollte. Doch Anfang August verbreitete es sich erneut. Grund: an zuvor infizierten Computern falsch eingestellt Uhrzeiten und Datumsanzeigen.

„Code Red II“ trat seinen Zug durchs Internet am vergangenen 4. August an. Das Virus installierte auf den angegriffenen Computern eine Art „Hintertür". Durch diese sind die infizierten PCs zukünftigen Virenangriffen noch schutzloser ausgesetzt. Die zweite Variante hatte jedoch keinen so großen Erfolg wie das Original, da viele User nach dem ersten Angriff ihren PC mit Anti-Viren-Programmen ausgestattet hatten.

(1 US-Dollar = 2,13 DMark)

Wie viele Computer werden pro Jahr von Viren befallen?

„Code Red“ hatte im vergangenen Juli in lediglich neun Stunden bereits mehr als 250.000 Systeme infiziert. [12]
Im laufenden Jahr hatten die beiden Virentypen „Code Red" und „SirCam" etwa 2,3 Millionen Computer infiziert. [12]

I.7 Varianten von Viren und andere Schädlinge

Mittlerweile hat sich "Virus" umgangssprachlich als Oberbegriff für Schädlinge aller Art etabliert. Genau genommen ist das allerdings nicht ganz richtig, da ein Virus ein Schädling mit speziellen Eigenschaften ist.

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

Makroviren gehören zu einer neueren Generation von Computerviren, den Dokumentviren. Sie sind in der Makrosprache einer Applikation (z.B. WinWord, Excel, Access, AmiPro, WordPerfect, StarOffice) geschrieben und können sich (mit Ausnahmen) auch nur dann verbreiten, wenn die entsprechende Applikation aktiv ist. Die Verbreitung erfolgt im Normalfall über die Dokumente der Applikation. Diese Viren können unter Umständen auch plattformübergreifend "arbeiten", nämlich dann, wenn der entsprechende Dokumenttyp im gleichen Format auf anderen Plattformen verwendet wird. Als Beispiel seien hier MS Word Makroviren genannt, die sich sowohl auf Windows PC wie auch auf dem Apple Macintosh verbreiten können.

Hoaxes sind Emails mit falscher Viruswarnung. Neben tatsächlichen Schädlingen landen auch immer wieder so genannte Hoaxes in der E-Mail. Bei diesen "Verarschungs-Mails" handelt es sich um Warnungen vor angeblichen oder vermeintlichen Viren. Die Faustregel zur Erkennung von Hoaxes ist einfach: Virenwarnungen, die unaufgefordert eintreffen, sind nicht ernst zu nehmen. Solange Sie also keinen Newsletter eines Antivirus-Unternehmens abonniert haben, sind solche Warnungen meist falsch. Ein weiteres Indiz für Hoaxes ist die Aufforderung,

die Mail an "alle Freunde und Bekannte" weiterzuschicken. Einige dieser Hoaxes fordern den Nutzer auf, bestimmte Dateien zu löschen, weil es sich angeblich um einen Virus handelt.

Würmer sind vollständige Programme, die in Rechnernetzen leben. Ein Wurm kann eine Kopie von sich an einen anderen Rechner schicken. Dazu muss er natürlich das Protokoll und die Adressliste des Rechnernetzes kennen. Der am häufigsten genutzte Verbreitungsweg ist E-Mail: Die Würmer verschicken sich als (meist direkt ausführbare) Anlage an mehr oder weniger zufällig ausgewählte Mail-Adressen.

Trojanische Pferde sind auch keine Viren im eigentlichen Sinne (da sie sich in der Regel nicht selbst reproduzieren), sondern Software mit Virenfunktionalität, die sich hinter dem Namen von bekannten (harmlosen) Programmen verstecken. Sie können Viren einschleusen oder Daten ausspionieren (z.B. Passwörter). Bei einem Trojanischen Pferd handelt es sich um eine Software, die vorgibt, etwas Nützliches zu tun, aber tatsächlich das System kompromittiert (etwa mit einer Backdoor versieht). Viren befinden sich meist im Betriebssystem. Trojaner sind besonders gefährlich, da sie kaum zu entdecken sind und über lange Zeiträume schlafen können.

Dateiviren (Programmviren, COM-Viren)
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 (Bootviren) verstecken sich im Bootsektor von Festplatten und Disketten sowie im Master Boot Record (MBR) von Festplatten, können sich nach dem Booten von eben diesem Datenträger resident in den Hauptspeicher verlagern und permanent Schaden anrichten.

Scriptviren
Eine ganz neue Generation von Viren sind neben den schädlichen JAVA Applets vor allem die auf Visual Basic Script basierenden Script Viren. Diese können in VBS-Dateien und sogar in HTML-Code versteckt sein.

II. Beispiel: I love you Virus

II.1 Was ist der ILoveYou Virus?

Das IloveYou Virus war und ist der wohl berühmteste Massenvirus schlechthin! Er tarnt sich als Liebesbrief. Nach der Ausführung der angehängten Datei verbreitet er sich über das Outlook-Adressbuch. Der 4. Mai 2000 war ILoveYou-Tag. Binnen weniger Stunden verbreitete sich der Virus via E-Mail über die ganze Welt, legte die Mailserver großer Firmen lahm und griff JPEG- und MP3-Dateien an.

II.2 Wie funktioniert das ILoveYou Virus?

Das Virus konnte jede Art Sicherheitssystem von internationalen Konzernen überwinden, indem es per e-Mail andere Dateien infiziert.

II.2.1. Infizierung

Das Virus beginnt zuerst sich zu vermehren, bevor es irgendwelche Daten beschädigt. Auf diese Weise verbreitet der ahnungslose Benutzer das Virus, bevor er überhaupt merkt, dass er selbst infiziert ist. Und genau dies passiert bei”ILoveYou“.

Unser”Liebesbrief“ verschickt sich automatisch und unbemerkt an die Einträge des E-Mail-Adressbuches eines infizierten Benutzers. So bekommt ein neues Opfer zuerst eine E-Mail von einer bekannten Person. Weder der Absender noch der harmlose Betreff ”ILoveYou“ lassen Böses erahnen.

II.2.2. Aktivierung

Wer jetzt allerdings auf den Link des Anhangs klickt, sieht zunächst einmal wenig - bis auf eine nette Liebesbotschaft.

Im Hintergrund nutzt das Virus allerdings die Sicherheitslücken vom Windows-Betriebssystem und nistet sich in der Systemregistrierung ein. Dazu nutzt ”I Love You“ die Programmiersprache Visual Basic, welche dazu gedacht ist, Arbeitsabläufe zu vereinfachen.

Nach einem Neustart und einer erneuten Benutzung der Microsoft-Programme „Internet Explorer“ und „Outlook“ lädt „ILoveYou“ eine Datei namens „WIN-BUGSFIX.exe“ aus dem Internet. Sie sorgt dafür, dass sich der Virus an alle Outlook-Einträge versendet.

II.2.3. Schädliche Funktionen

Nach der Vermehrung kommt die Zerstörung. Bisher hat der ahnungslose User noch nichts von der Vireninfektion seines Computers bemerkt. Erst jetzt beginnt ”I Love You“ damit, alle Dateien mit der Endung ”*.js“, ”*.jse“, ”*.css“, ”*.wsh“, ”.*sct“, ”*.hta“, ”*.jpg“, ”*.jpeg“, ”*.mp3“ und ”.*mp2“ zu zerstören.
So hat "I Love You“ gerade bei großen Unternehmen für doppelten Ärger gesorgt: Erstens wurden die Mailserver durch ein irrsinnige Zahl von E-Mails in die Knie gezwungen - man stelle sich vor, dass 2000 User mit jeweils 100 Adressbuch-Einträgen gleichzeitig das Virus öffnen! Und zweitens wurden auf allen infizierten Rechnern wichtige Dateien gelöscht. [10]

Erstaunlicherweise hat sich "ILoveYou“ auch weitaus schneller verbreitet, als die Hersteller von Anti-Viren-Software vermutet hätten. Denn es war eine große Zahl deutscher und internationaler Unternehmen nicht mehr per E-Mail erreichbar.

II.3 Wer hat das ILoveYou Virus erfunden?

Die Frage nach dem Autor ist nach wie vor unklar. Es gab zahlreiche mutmaßliche Hacker, welche verhaftet wurden. Die Spur führte nach Manila in den Philippinen, wo auch letztendlich ein 22-jähriger Informatikstudent festgenommen wurde. Er selbst bezeichnete sich als "Spider" und sagte nach der Verhaftung aus, er habe "versehentlich" die bösartige Mail verschickt. [3]

II.4 Schaden durch das ILoveYou Virus?

ILoveYou, das zerstörerische E-Mail-Virus ruinierte Privatrechner, blockierte Unternehmen und Verwaltungen.

Die Schäden werden auf zehn bis 30 Milliarden US-Dollar geschätzt. Aber wie beziffert man den Schaden durch einen Virus? Ausfall von Arbeitszeit? Datenverlust? Zeitverlust durch das Einspielen von Backups? Image-Verlust bei einem Systemhaus, das Viren an seine Kunden verschickt? Geplatzte Geschäfte aufgrund nicht verschickter Mails, weil der Mailserver in die Knie gegangen ist? Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) spricht davon, dass solche Schätzungen immer `etwas unseriös´ seien.

Nach Schätzungen von Experten wurden weltweit etwa 45 Millionen Computer infiziert. [11]

III. Fazit

Es kommen ständig neue Ideen für Viren. In der Tat wird die Gefahr nicht weniger, sondern mehr. Es herrscht ein zunehmender Einzug von Computern in Alltags- und Geschäftswelt.

Mit technischen Maßnahmen alleine lässt sich keine hundertprozentige Sicherheit erreichen.

Pessimisten malen sich Horrorszenarien aus: zum Beispiel ganz aktuell Terroranschläge durch Einschleusen von Viren in sicherheitskritische Systeme (Kernkraftwerk, Autopilot von Flugzeugen, Krankenhäuser, Banken, …).

Auch eines sollte man nicht vergessen: immer noch tragen zwischen 0,6 und 0,7 Prozent aller E-Mail gefährliche Viren in sich!

IV Referenzen

[1] C’T Magazin

[2] **Duden** Informatik

[3] **c't**: www.heise.de/ct/antivirus

[4] **Norton Antivirus**, Symantec

[5] **McAfee VirusScan**, McAfee.com

[6] **Kaspersky Antivirus**, Kapersky

[7] **Panda Antivirus**, Panda Software

[8] Biologie Webseite
[9] Computer Economics
[10] http://www.scoolz.de
[11] http://sicheres.web.glossar.de
[12] www.asysta.de