Proseminar
„ Ethische Aspekte der Informationsverarbeitung“

Prof. Dr. W. Kurth

Computerviren

von
Steffen Liese 2016921
20.1.2004

Was sind Viren?

Biologischer Virus :

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.
(Neues Großes LEXIKON in Farbe, Buch und Zeit)

Computervirus :

Viren sind Programmstücke in Maschinencode, die sich vervielfachen, in andere Programme hineinkopieren und zugleich schädliche Funktionen in einem Rechnersystem ausüben können.

Geschichte der Computerviren

1949 Mathematiker John von Neuman stellt Überlegungen über sich selbstständig reproduzierende Computerprogramme an
50 Jahre Bell Labs in Kalifornien wird “Krieg der Kerne“ entwickelt, Spieler hacken sich gegenseitig
1982 3 Computerviren für Apple tauchen „ in the Wild“ auf
1983 Fred Cohen definiert den Begriff "Computervirus" formal

„Ein Computervirus ist ein Programm, das andere infizieren und verändern kann, um möglicherweise veränderte Versionen von sich selbst hinzuzufügen.“

1986 Entdeckung des ersten IBM kompatiblen Virus. Name: „**Brain**“ Herkunft: Pakistan, Typ: Boot-Virus
Entdeckung des ersten Datei-Virus, Name: „**Virdem**“ Herkunft: Deutschland
1987 "**Lehigh**"-Virus: ist der erste Virus, der command.com infiziert
Wurm „**CHRISTMA EXEC**“ verbreitet sich auf IBM VM/CMS-Systemen, versendet sich dann heimlich per E-Mail, erzwingt er das Herunterfahren vieler Systeme
Jerusalem-Virus, der erste speicherresidente Virus
"**Stoned**"-Virus, erste MBR-Virus (Master Boot Record), stammt von einem Studenten
1988 Robert Morris, 22, startet den Internet-Wurm, befällt 6000 Computer, das sind 10% aller Computer im Internet
“**Cascade**“, der erste sich selbstverschlüsselnde Virus, wird in Deutschland entdeckt
1989 „**Dark Avenger.1800**“, in Sophia, Bulgarien geschrieben, ist der erste schnell infizierende Virus
„**Frodo**“ ist der erste Tarnkappen-Virus
1990 Marc Washburn schreibt „**1260**“, den ersten polymorphen Virus
„**Anthrax**“ und „**V1**“, die ersten mehrteiligen Viren werden entdeckt

1991 Veröffentlichung des Virus-Construction-Sets, das den Zusammenbau eigener, neuer Viren ermöglicht
„**Form**“, Boot Sektorvirus, 8 Jahre lang in Top 10 Liste
1992 „**Michelangelo-Virus**“, sorgt für erste Viren Hysterie
“**WinVir 1.4**“, der erste Windows-Virus
"**Involuntary**", infiziert SYS-Dateien
1993 Antivirus-Industrie veröffentlicht ihre erste Viren-Liste
1994 „**GoodTimes**“, erster Hoax
1995 „**Concept**“, der erste Makro-Virus, befindet sich auf einer offiziellen Microsoft CD-Rom
1996 **Boza**-Virus, der erste Virus für Windows 95
„**XM.Laroux**“, der erste Excel-Virus
1997 **mIRC**-Script-Würmer treten in Erscheinung
1998 „**Chernobyl**“ –Virus, erste der Hardware beschädigt
„**AOL-Trojaner**“, das erste von vielen Trojanischen Pferden
„**JavaApp.StrangeBrew**“, erste Java-Virus, infizieren *.class-Dateien
„**P97M.Vic.A**“, erste PowerPoint -Virus
1999 „**W97M.Melissa.A**“ verbreitet sich sehr schnell weltweit, versendet sich per E-Mail, was zum Zusammenbruch vieler Mailserver führt
„**VBS.BubbleBoy**“ ist der erste Virus, der nur durch Lesen der E-Mail aktiv wird
2000 befürchtete Jahr-2000-Katastrophe bleibt aus, existierende Y2K-Viren bleiben weitgehend wirkungslos
„**VBS.Loveletter**“, als ILOVEYOU-Virus bekannt, bösartigster Virus der Computergeschichte, viele Mail-server brachen zusammen, von philippinischen Studenten
„**Palm.Liberty.A**“, erste Trojaner für PDAs (Personal Digital Assistant)
2001 "**Code Red**" und „**W32/SirCam**“, befallen binnen weniger Stunden eine viertel Millionen Rechner, erster Virus der seinen eigene Mail-Server Engine mitbringt

es gibt natürlich viel mehr Virenattacken, hier waren nur die bekanntesten oder die ersten ihres Typs

Arten 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 in der Anlage von Mails verstecken
- überträgt sich bei der Benutzung auf den lokalen Rechner

Makroviren

- gehören zur neusten Generation von Computerviren , den Dokumentviren
- sind in der Makrosprache geschrieben (z.B. WinWord, Excel, Access, WordPerfect, StarOffice)
- die Applikation muss auf den zu infizierenden System vorhanden sein
- Verbreitung erfolgt über Dokumente der Applikation

Hoaxes

- sind Emails mit falscher Nachrichten
- handelt sich meist um Warnungen vor angeblichen oder vermeintlichen Viren

Erkennung:

- Virenwarnungen, die unaufgefordert eintreffen
  (solange nicht Abonnent der Newsletter eines Antiviren-Unternehmens)
- weiteres Indiz : diese Mail an „alle Freunde und Bekannte“ weiterschicken

Würmer
- sind vollständige Programme,
- leben in Rechnernetzen
- kann eine Kopie von sich selbst an anderen Rechner schicken
- dazu muss er die Protokolle und Adressliste des Rechnernetzes kennen
- häufigste genutzte Verbreitungsweg ist die E-Mail

Trojanische Pferde
- keine Viren im eigentlichen Sinne
- reproduzieren sich in der Regel nicht selbst
- verstecken sich hinter bekannten (harmlosen) Programmen
- können Viren einschleusen oder Daten ausspionieren
- besonders **gefährlich**, da sie kaum zu entdecken sind und über lange Zeit schlafen können

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

Bootsektorviren
- 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
- ganz neue Generation von Viren
- basieren neben den schädlichen JAVA Applets vor allem auf Visual Basic Script

können sich in VBS Dateien und sogar in HTML-Code verstecken

Wie schützen sich Computerviren vor der Erkennung durch Antivirenprogramme?

Speicherresistente Viren:
Laden ihren Programmcode in den Speicher und führen sich von dort aus.

Selbstverschlüsselnde Viren:
Verschlüsseln einen Teil ihres Programmcodes, nur der Teil zum entschlüsseln des Restes wir nicht verschlüsselt. Somit wird die Erkennung sehr erschwert.

Stealth-Viren (Tarnkappenviren)
Stealth-Viren 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.

Dies sind nur einige Techniken. Wahrscheinlich werden es mit zunehmenden Vorschritt in der Technologie, neue Techniken geben.

Schäden durch Computerviren

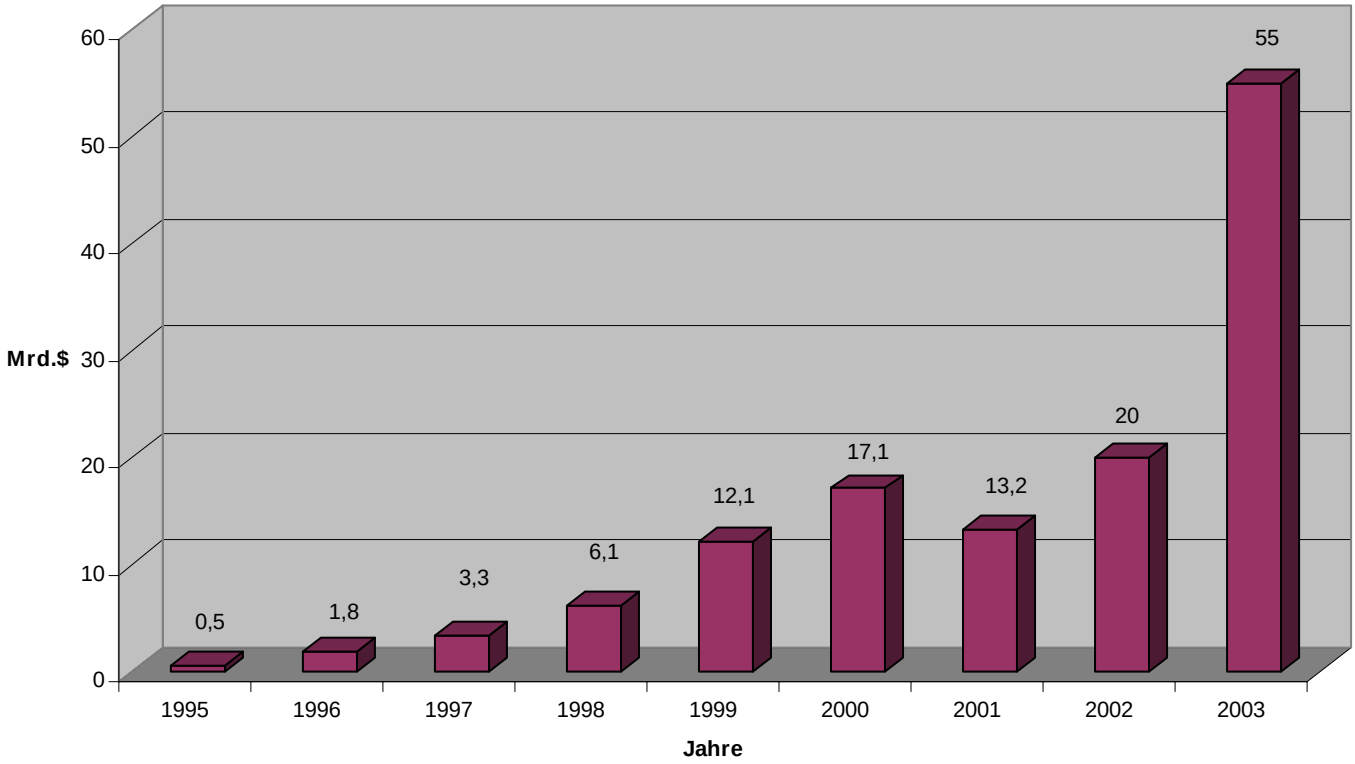
Je nach Schutzmechanismus der zugrunde liegenden Ausführungsplattform können Viren mehr oder weniger starken Schaden anrichten:

- **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.

Folgeschäden

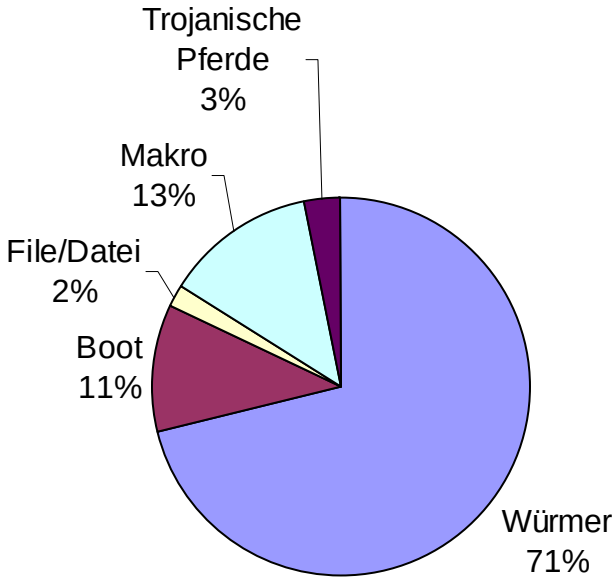
- Wartungsaufwand für **Virenentfernung**
- Wartungsaufwand für **Virenschutz**
- **Panik-Reaktionen** und Verunsicherung von Anwendern
- **Vertrauensverlust** bei Kunden
- **Ausfallschäden** (Blockierung von Arbeitsabläufen, geplatzte Geschäfte, …)

Finanzieller Schaden durch Computerviren



Häufigkeit von Viren

- derzeit gibt es **über 50.000**
- keine einheitliche Konvention für die Kategorisierung
- täglich werden 10-15 neue Viren von Forschern und Anwendern entdeckt
- dazu kommen noch Abwandlungen bekannter Viren



Computerviren sind nicht das Problem, sondern Virenschreiber

- Warum schreiben Menschen Viren?
- die eigentlichen Gründe werden uns wohl verschlossen bleiben
- aber ein Grossteil der Viren sind Abwandlungen bekannter Viren
- diese kann man leicht im Netz herunterladen
- oft sind sie auch noch gefährlicher als ihr Original
- die meisten, die diese Viren loslassen, wissen gar nicht ,welchen Schaden sie damit anrichten

Zukünftige Ziele

- Heim PC werden immer Leistungsfähiger
- eignen sich gut als Zwischenstation für weitere Angriffe
- sind meist Sicherheitstechnisch nicht auf den neuesten Stand
- weiteres Ziel sind neue Handys, die Code ausführen können (z.B. Java)
- mobile Computer der kommenden Generationen

Sieben Tipps für sichere Computer

Starke Passwörter:
- Passwörter wählen, die man nicht erraten kann
- Mischung aus Buchstaben und Zahlen
- unterschiedliche Codes für verschiedene Zugänge
- **Wichtig !** Passwörter nie aufschreiben

Datensicherung:
- sichern Sie von Zeit zu Zeit ihre Daten
- hängt ab wie intensiv ihr Rechner genutzt wird

Antiviren-Software:
- sollte auf jeden Rechner zur Virenabwehr installiert sein
- **Wichtig !** stets aktuell halten

E-Mail:
- **Nie** E-Mail-Anhänge von Fremden offen
- Achtung auch bei Anhängen von Bekannten

Virenwarnungen:
- informieren Sie sich zuerst bei Herstellern von Antivirenprogramme oder beim Bundesamt für Sicherheit in der Informationselektronik (http://www.bsi.de/av/)
- keine falsche Virenwarnungen weiterleiten

Firewall:
- sollte auch zum Standart auf jeden Rechner gehören
- dient zum Schutz vor äußeren und inneren Attacken

Updates:
- Betriebssystem auf den neuesten Stand halten(Sicherheit)
- Patches (Flicken) gegen bekante Lücken im System besorgen

Fazit

- Die Vernetzung wird weiter voranschreiten
- Zukünftige Computer werden immer kleiner und Leistungsfähiger
- in naher Zukunft wird die Anzahl der Viren zunehmen
- der dadurch entstandene Schaden wird weiter steigen
- das Einhalten der 7 Tipps muss zur Grundlage werden
- harte Strafen für Virenschreiber und Hacker

Referenzen

Computerviren, Baowen Yu
Norton Antivirus, Symantec(www.symanetec.de)
Duden Informatik
NEUES GROSSES LEXIKON in Farbe, Buch und Zeit
Bundesamt für Sicherheit in der Informationselektronik
(www.bsi.de)
Dauerclinch mit Cyber-Ungeziefer, www.messe-zeitung.com
Das Virus ist die Nachricht, www.zeit.de/2001/23/kettenbriefe
Frankfurter Rundschau, 22.01.2002