



Universität Trier



Institut für Telematik

unter Betreuung der
Fraunhofer Gesellschaft

Vorlesung SS 2001: "Sicherheit in offenen Netzen"

3.9 Viren, Würmer und Trojanische Pferde

Prof. Dr. Christoph Meinel

Informatik, Universität Trier & Institut für Telematik, Trier



3. Schwachstellen und Angriffspunkte

- 3.1 Menschliches und technisches Versagen
- 3.2 Beschaffung von Systeminformationen
- 3.3 Account- und Paßwortangriffe
- 3.4 Angriffspunkte im Netzwerkbereich
- 3.5 Design- und Programmierfehler in Applikationen
- 3.6 Schwachstellen in Unix/Linux
- 3.7 Schwachstellen in Windows NT/2000
- 3.8 Angriffspunkte im World Wide Web
- 3.9 Angriffe durch Viren, Würmer, Trojanische Pferde**



3.9 Viren, Würmer, Trojanische Pferde (1 von ...)

(1) Einleitung (1 von ...)

Mit der zunehmenden weltweiten Vernetzung von Computer-Systemen nimmt die Bedrohung der elektronischen Informationsverarbeitung durch Viren und Artgenossen stark zu.

- In den 80er Jahre verbreiteten sich Viren über Programme, die von Diskette zu Diskette kopiert wurden
- Heute werden Anwendungsprogramm hauptsächlich von einem zentralen Server auf die Anwenderstationen geladen oder in Form von CD-ROMs ausgeliefert. Neueste Virengenerationen befallen deshalb bevorzugt Benutzerdaten und mißbrauchen Standardbefehle von Anwendungen wie Word, Exel oder Postscript-Befehlsfolgen.



3.9 Viren, Würmer, Trojanische Pferde (2 von ...)

(1) Einleitung (2 von ...)

Ziel der Viren-Aktivitäten:

- **früher**: meist Destruktion und Zerstörung der Daten
- **heute**: meist Vorbereitung von Einbrüchen
z.B. Modifikation von Systemdateien, Aufzeichnen von
Paßwortdateien

Viren und Artgenossen stellen erhebliche Bedrohung dar und müssen professionell bekämpft werden.



3.9 Viren, Würmer, Trojanische Pferde (3 von ...)

(1) Einleitung (3 von ...)

Würmer und Trojanische Pferde sind mit Viren verwandt:

- **Viren:** Befehlsfolge, die bei Ausführung eine Kopie des Virus einem bereits existierenden Programm hinzufügt (Infektion). Daneben enthalten Viren meist einen Schadensteil, der ein bestimmtes Ereignis auslöst
- **Würmer:** Würmer sind lauffähige Programme, das sich bei Abarbeitung über das Netzwerk auf andere angeschlossene Rechner kopiert und Kopie startet
- **Trojanische Pferde:** sind Programme, deren Ist-Funktionalität nicht mit der Soll-Funktionalität übereinstimmt. Verborgene Funktionen lesen oder verändern z.B. Benutzerdaten

Angriffsmechanismen sind bei Viren, Würmern und Trojanischen Pferden gleich, so daß Bekämpfung durch Mustererkennung mittels Virenschanner erfolgen kann



3.9 Viren, Würmer, Trojanische Pferde (3 von ...)

(2) Verbreitung von Viren (1 von ...)

- etwa 70% des Virenbefalls betrifft PCs und MS-Windows-Betriebssysteme, dann folgen Macintosh-Computer und abgeschlagen Unix-Systeme
- modern Benutzerdatenorientierte Viren agieren oft schon plattformunabhängig
- 1999 waren 99% aller großen und mittleren Unternehmen Opfer (Quelle: ICISA), obwohl 55% der Unternehmen alle PCs mit Virenschutzprogrammen ausgestattet haben
- starke Zunahme des Virenbefalls in den letzten Jahren zu beobachten

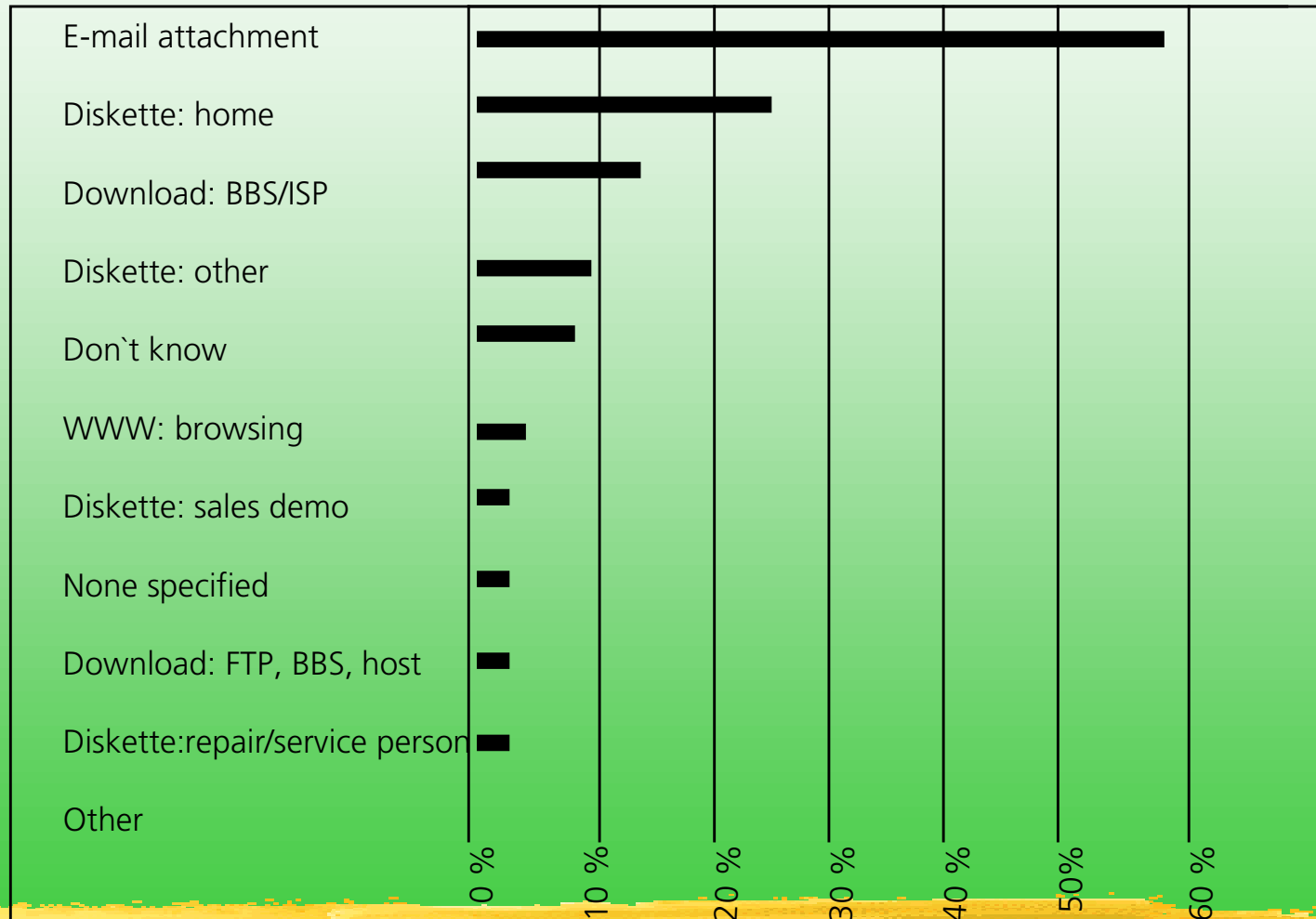


Verbreitete Virentypen:

Virus	Meldungen in Prozent
Melissa	16 %
Class	13 %
Laroux	12 %
Etan	7 %
Word Macros	7 %
Cap	5 %
Happy99	5 %
CIH	4 %
Excel Macros	2 %
sonstige	29 %

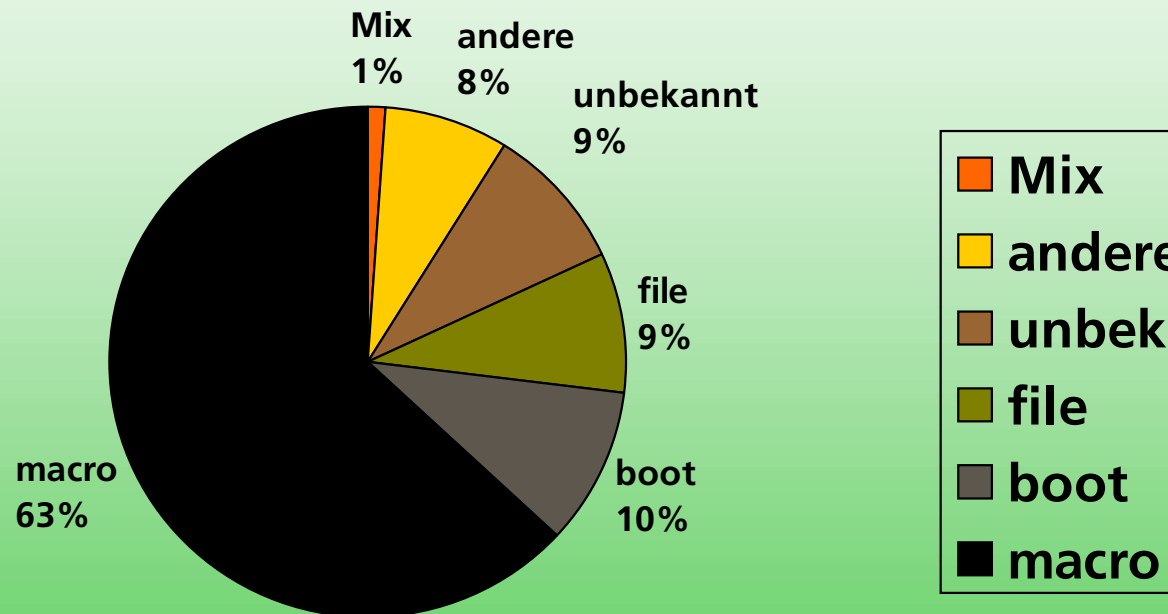


Verbreitungsarten von Viren





Klassen von Viren





3.9 Viren, Würmer, Trojanische Pferde (7 von ...)

(3) Typen von Viren (1 von ...)

Viren werden entweder nach dem funktionellen Teil des Computer-Systems, das sie befallen klassifiziert oder nach der Strategie zur Vermeidung ihrer Entdeckung

→ **Boot-Viren:**

Boot-Viren befallen den für den Systemstart verantwortliche Dateibereich

- bei DOS-Systemen ist das der *DOS-Boot-Sektor* oder der *Master Boot Record* – *MBR* von Festplatten
- **Beispiele:** Brain, Stones, Empire, Azusa, Michelangelo, ...



3.9 Viren, Würmer, Trojanische Pferde (8 von ...)

(3) Typen von Viren (2 von ...)

→ System-Viren bzw. Cluster-Viren:

Filesystem- oder Cluster-Viren modifizieren Dateiverzeichnis-Einträge -File Allocation Tables -, so daß Virus noch vor dem betreffenden Programm geladen wird

- **Beispiel:** Dir-II

→ Programm-Viren:

Programmviren – klassischer Virentyp - besteht aus Miniaturprogramm, das in einer ausführbaren Datei verborgen ist und bei Start der betreffenden Anwendung zur Ausführung kommt. Benutzer bemerkt zunächst nichts. Virusaktivität wird erst nach Beendigung des Wirtsprogramms bzw. nach Neustart sichtbar



3.9 Viren, Würmer, Trojanische Pferde (9 von ...)

(3) Typen von Viren (3 von ...)

→ Polymorphe Viren:

Polymorphe Viren können unterschiedliche Kopien von sich selbst generieren und so gegenüber verschiedenen Antivirenprogrammen Resistenz entwickeln.

- **Methode (1):** Benutzung unterschiedlicher Verschlüsselungsmethoden für den Virus-Code zur Erschwerung der Suche nach bestimmten Code-Mustern

Beispiel: Whale-Virus



3.9 Viren, Würmer, Trojanische Pferde (10 von ...)

(3) Typen von Viren (4 von ...)

→ Polymorphe Viren (2 von ...):

- **Methode (2):** Veränderung von Befehlssequenzen des Viren-Codes oder zufällige Einfügung von Pseudo-Befehlen

Beispiel: V2P6-Virus

- **Methode (3):** Die berühmte **Mutation Engine** des bulgarischen Viren-Designers Dark Avenger erzeugt bei Aufruf aus jedem Virus eine zufallsgeneratorgesteuert modifizierte polymorphe Variante



3.9 Viren, Würmer, Trojanische Pferde (10 von ...)

(3) Typen von Viren (4 von ...)

→ **Stealth-Viren:**

Stealth-Viren sind in der Lage, die durch sie bewirkten Veränderungen im Boot- oder Dateibereich mit Hilfe von Manipulationen der Systemprogramme zu tarnen.

- Veränderung der Ergebnisse von Funktionen wie Lesen von Dateien oder Sektoren, so daß Werte für Dateigrößen oder vorhandenen Speicherplatz so ausgegeben werden, als ob Virus nicht vorhanden ist

Ziel: Täuschung von Antivirenprogrammen



3.9 Viren, Würmer, Trojanische Pferde (11 von ...)

(3) Typen von Viren (5 von ...)

→ **Retroviren:**

Retroviren sind besonders bösartige Viren, die gezielt Antivirenprogramme beschädigen oder löschen. Beispiele:

- **CPW-Virusfamilie:**

CPW-Viren löscht die Antivirenprogramme:

TOOLKIT, GUARE, CHKVIRUS, SCAN, CLEAN, CPAV und VSAFE

- **Firefly:**

Firefly enthält Endlosschleife, um F-PROTR zu Täuschen und löscht die Dateien:

IM, VIRX, PCRX, VIRSTOP, MSAV, NAV, SCAN, CLEAN, TBAV, TBCSCAN, TBCLEAN, TBCHECK, TBMEM, TBSCANX, TBFILE, VC und VCHECK



3.9 Viren, Würmer, Trojanische Pferde (12 von ...)

(3) Typen von Viren (6 von ...)

→ Daten-Viren (1 von ...):

- jüngste Generation von Viren sind Daten-Viren
- Daten-Viren nutzen die in vielen Anwendungen enthaltenen Makrobefehle oder die Befehlsstruktur von Dokumentenbeschreibungssprachen, wie z.B. Postscript.
- **Beispiele (1): Winword.Concept** und **Word.-Marco.Nuklea** und Hunderte von abgeleiteten Varianten

Methode: Nutzung der im MS-Office-Paket verfügbaren Word-Makros.

Ist Autostart-Option für Word-Makros aktiviert, so starten beim

Aufruf von infizierten Dokumenten die betreffenden Viren-Makros.



3.9 Viren, Würmer, Trojanische Pferde (13 von ...)

(3) Typen von Viren (7 von ...)

→ Daten-Viren (2 von ...):

- Datei-Viren arbeiten ausschließlich mit Visual Basic-Befehlen, so daß sie plattformunabhängig sind
- **Schäden:** Selbstvermehrung, Zerstörung von Systemdateien, Verunstaltung von Ausdrucken,...

Abwehr: Einsatz von **Antiviren-Dokumenten**

● **Beispiel (2): JPEG-Virus**

Methode: versteckt sich im Kommentarfeld von JPEG-Bilddaten und gelangt beim in-den-Videospeicher-Laden der JPEG-Datei in den Shadow-ROM-Speicher



3.9 Viren, Würmer, Trojanische Pferde (14 von ...)

(3) Typen von Viren (8 von ...)

→ Trojanische Pferde (1 von ...):

- Trojanische Pferde sind Programme, bei denen sich Ist-Funktion und Soll-Funktionen für den Nutzer nicht wahrnehmbar unterscheiden. Sie täuschen z.B. Paßwort- oder Login-Eingabedialoge vor und zeichnen dabei Tastatureingaben auf
- Trojanische Pferde vermehren sich auf dem infizierten System nicht, einige zerstören sich sogar nach Erfüllung ihres Auftrages



3.9 Viren, Würmer, Trojanische Pferde (15 von ...)

(3) Typen von Viren (9 von ...)

→ Trojanische Pferde (2 von ...):

- die meisten Trojanischen Pferde werden über das Internet mittels E-Mail verteilt oder versteckt in Spielen oder Demoprogrammen
- **Beispiele: BackOrifice, NetBus**
Methode: erlauben als komplexe Client-Server-Anwendung die komplette Fernsteuerung des befallenen Rechners über das Netzwerk



3.9 Viren, Würmer, Trojanische Pferde (16 von ...)

(3) Typen von Viren (10 von ...)

→ **Würmer** (1 von ...):

- Würmer sind lauffähige Programme , die sich über Datennetze hinweg vervielfältigen
- **Beispiele (1): Internet-Wurmprogramm** von Robert Morris
Schaden: wurde 1988 im Internet ausgesetzt und hat innerhalb weniger Stunden mehr als 6.000 Host infiziert
- **Beispiele (2): Milnet**
Schaden: hat 1988 Datennetz der nichtvertraulichen Daten des US-Verteidigungsministeriums verseucht
- spezielle Würmer haben das Ziel, durch Infektion Computer-Systeme für einen späteren Angriff vorzubereiten und Systeme mit Sicherheitslücken zu selektieren



3.9 Viren, Würmer, Trojanische Pferde (17 von ...)

(4) Viren-Fabriken

- der berüchtigte Virenprogramm „Dark Avenger“ (Dark Avenger, V2000, V2100, Phoenix, Diamond, Nomenklatura etc.) betreibt Mailbox „Virus eXchange“ zum Virentausch. Da man in deren Virenbereich nur gelangt, wenn man einen eigenen Virus anbietet, hat die Sammlung schon einen beträchtlichen Umfang ... „**Viren-Fabrik**“
- inzwischen existieren im Computeruntergrund mehrere Viren-Fabriken, die permanent neue Viren produzieren



3.9 Viren, Würmer, Trojanische Pferde (18 von ...)

(5) Antiviren-Management (1 von ...)

- In den IT-Sicherheitsrichtlinien für den Umgang mit Hard- und Software muß gewährleistet sein, daß die Infizierung durch Viren möglichst ausgeschlossen bleibt
- Durchführung entsprechender Benutzerschulungen
- Erstellung eines **Viren-Aktionsplans**, der systematisch Maßnahmen sowohl zur Prävention als auch zur Reaktion beschreibt. Ein besonderes Augenmerk gilt den verschiedenen Zugangswegen:
 - Datenfernverbindungen (Internetzugänge, DialBack-Leitungen usw.)
 - Software-Quellen
 - Gastzugänge für Besucher und Geschäftspartner



3.9 Viren, Würmer, Trojanische Pferde (19 von ...)

(5) Antiviren-Management (2 von ...)

Viren-Prävention:

- insbesondere potentiell gefährdete Systeme - z.B. Systeme mit Internetzugang oder mit häufig wechselnden Benutzern - müssen besonders abgesichert werden:
 - durch den Einsatz von Antiviren-Software immunisieren
 - Erstellung spezieller Backup-Pläne
- Einsatz von Viren-Scannern
 - Viren-Scanner bei jedem Systemstart standardmäßig starten
 - Internetzugänge besonders absichern
- ➔ Ernennung eines Viren-Verantwortlichen



3.9 Viren, Würmer, Trojanische Pferde (20 von ...)

(5) Antiviren-Management (3 von ...)

Viren-Reaktionsplan (1 von ...):

- Sofort nach Feststellung einer Infektion tritt Viren-Reaktionsplan in Kraft
- **Ziel:**
restlose Entfernung aller Viren, Würmer und Trojanischen Pferde
- **Methode** (1 von ...):
 - falls akzeptabel, gesamten Datenbestand vernichten und befallenen Systeme physikalisch löschen (Formatierung der Festplatten).
Dann System vollständig neu konfigurieren



3.9 Viren, Würmer, Trojanische Pferde (21 von ...)

(5) Antiviren-Management (4 von ...)

Viren-Reaktionsplan (2 von ...):

→ Methode (2 von ...):

- Analyse des Virenbefalls und Ursachenforschung - 90% der befallenen Systeme werden innerhalb von 3 Monaten auf den selben/ähnlichen Wegen erneut infiziert
- Kann Vireneintrittspforte nicht lokalisiert werden, ist regelmäßige Immunisierung und Untersuchung der Speicherbereiche notwendig



3.9 Viren, Würmer, Trojanische Pferde (22 von ...)

(5) Antiviren-Management (5 von ...)

Antiviren-Beratung (1 von ...):

Internet-Informationsserver zur Virenproblematik:

- Viren-Test-Centrum - VTC - der Uni Hamburg:
<http://agn-www.informatik.uni-hamburg.de/vtc/eng.htm>
- Eddy Willems, belgischer Virenspezialist <http://gallery.uunet.be/ewillems>
- Joe Wells and andere Anti-Viren-Spezialisten
<http://www.virusbtn.com/WildLists>
- Virenlabor der International Computer Security Association - ICSA
<http://www.icsa.net/html/communities/antivirus/index.shtml>



3.9 Viren, Würmer, Trojanische Pferde (23 von ...)

(6) Antivirus-Software (1 von ...)

Software zur Verhinderung bzw. Beseitigung von Virenbefall - sogenannte **Antivirus-Software** - basiert auf den folgenden Techniken:

- Signatur-Suche
- Aktivitätsfilter
- Veränderungsüberwachung



3.9 Viren, Würmer, Trojanische Pferde (24 von ...)

(6) Antivirus-Software (2 von ...)

→ Signatur-Suche:

bei der Signatur-Suche werden alle Dateien nach Programmsequenzen durchsucht, die für den jeweiligen Virus charakteristisch sind

- alle Text- und Binärdateien sowie Applikations- und Systemdateien werden gescannt und mit der Signaturbibliothek der Antivirus-Software verglichen



3.9 Viren, Würmer, Trojanische Pferde (25 von ...)

(6) Antivirus-Software (3 von ...)

→ **Aktivitätsfilter:**

Aktivitätsfilter beobachten das Computer-System auf verdächtige, für Virenbefall typische Verhaltensweisen und schließen indirekt auf eine mögliche Virusinfektion

→ **Veränderungsüberwachung:**

Erkennung verdächtiger Veränderungen bei den Parametern wichtiger Systemdateien (Größe, Quersumme, usw.) durch regelmäßige Überwachung



3.9 Viren, Würmer, Trojanische Pferde (26 von ...)

(6) Antivirus-Software (4 von ...)

Informationen über Antivirus-Programme:

- Antivirus-Software ist von sehr unterschiedlicher Qualität und Aktualität
- ohne stete Aktualisierung der eingesetzten Antivirus-Software ist kein ausreichender Schutz gewährleistet
- vor einem Einsatz der Software sollten Tests der Virenlabore beachten
- Informationen über die leistungsfähigsten Antivirus-Programme im Internet:
 - **Tucows Software-Archiv:** <http://tucows.com>
 - **Uni Hamburg:** <http://agn-www.informatik.uni-hamburg.de/pub>
 - **Antivirus Online von IBM:** <http://www.av.ibm.com/current/FrontPage>