



Angriffe im Netz

Monika Tavas



Übersicht

- Einführung
- Angriffe im Netz
- Schwachstellen und Bedrohungen von IT-Systemen
- Trends und Entwicklungen bei IT-Bedrohungen

Abhängigkeit von der Informationstechnik

- Informationsverarbeitung
- IT-Verbreitung und Durchdringung
- Steigender Vernetzungsgrad
- Verschwinden der Netzgrenzen



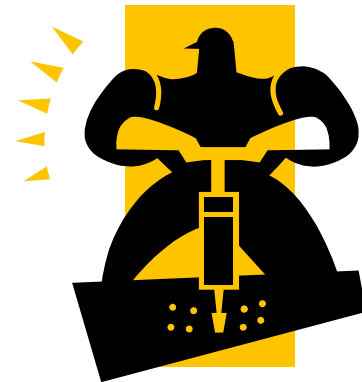
Fazit:

Angriffe kommen schneller



Schäden durch die IT-Fehlfunktionen

- Verlust der Verfügbarkeit
- Verlust der Vertraulichkeit von Daten
- Verlust der Integrität
 - Verlust der Authentizität



Verschiedene Gefahrenbereiche in deutschen Unternehmen(2004)

Gefahrenbereich	Bedeutung heute		Prognose		Schäden	
	Rang	Priorität	Rang	Priorität	Rang	ja, bei
Irrtum und Nachlässigkeit eigener Mitarbeiter	1	1,50	2	1,70	2	51 %
Malware (Viren, Würmer, Trojanische Pferde usw.)	2	1,34	1	2,80	1	54 %
unbefugte Kenntnisnahme, Informationsdiebstahl, Wirtschaftsspionage	3	0,60	4	1,14	8	9 %
Softwareängel/-defekte	4	0,57	5	0,96	3	43 %
Hacking (Vandalismus, Probing, Missbrauch usw.)	5	0,48	3	1,26	5	9 %
Hardwareängel/-defekte	6	0,40	8	0,32	4	38 %
unbeabsichtigte Fehler von Externen	7	0,30	9	0,26	7	15 %

Quelle: kes/Microsoft

Angriffe im Netz

Manipulation

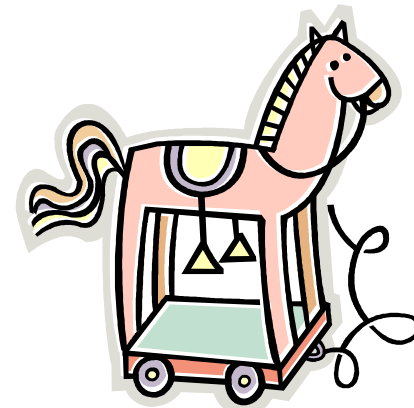
„Manipulation ist jede vorsätzliche Änderung oder Gestaltung eines Objekts für die gilt:

Ist ≠ Soll „

Objekte der Manipulation:

- Programme
- Programm-Generatoren
- Daten
- Rechner und deren Peripherie
- Versorgungseinrichtungen und Infrastruktur
- Netze und Netzkomponenten
- Bauteile oder Baugruppen

Berühmteste Manipulation der Geschichte
– trojanisches Pferd

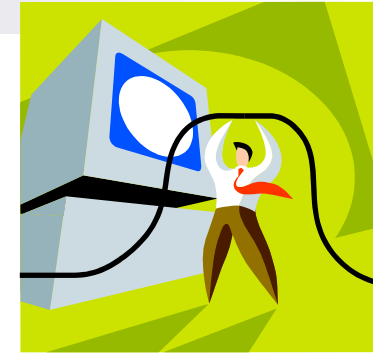




Programmanomalien und -manipulationen

Bezeichnung	Erklärung
Fehler <i>Bugs</i>	Programm (code) mit nicht den Anforderungen entsprechenden Wirkungen
Trojanisches Pferd <i>Trojan horse</i>	Programm (code) mit verdeckten Wirkungen oder Nebenwirkungen
Verschleierungsprogramm <i>spoofing program</i>	Eine Art der <i>trojanischen Pferde</i>
Logische Bombe <i>logic bomb</i>	Programm (code) mit zerstörerischer Wirkung und Zeitzünder oder Auslöser

Programmanomalien und -manipulationen



Bezeichnung	Erklärung
Hintertür, Falltür <i>trap door</i>	Programm (code) mit Nebenein- oder -ausgängen
Wurm <i>worm</i>	Selbstreproduzierendes Programm, das in einem System selbständig abläuft
Virus <i>Virus</i>	Selbstreproduzierender Programm, der über ein Wirtsprogramm abläuft

Fehler



Definition:

„Fehler (engl. bugs) ist ein Programm oder ein Programmteil mit Wirkungen, die nicht den Anforderungen entsprechen.“

- Manipulation unterscheiden sich vom einfachen Fehler durch *ausdrücklich gewollte* Programmänderungen.
- Verursacher von Fehler kann ein Mensch sein, oder auch ein Programm (Programmgenerator, Compiler,...)

Trojanische Pferde



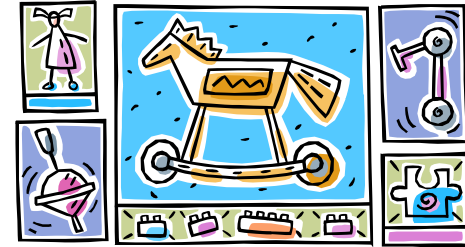
Definition:

Trojanisches Pferd (engl. trojan horse) ist ein Programm oder ein Programmteil mit verdeckten Wirkungen (oder Nebenwirkungen).

Es wird unterschieden:

- *Träger-trojanisches Pferd*, der eine Schadfunktion überträgt (z. B. Systemfunktion, Spiel, Utility...)
- und die Schadfunktion selbst

Wirkung



- Daten ausspionieren (Passwörtern, Kto. Nr., Kreditkarten Nr.)
- Überwachung von Home-Banking-Programmen (Daten werden weiter geschickt)
- Server-Programme (Hacker bekommt volle Zugriff auf das Rechner)



Trojaner Unterteilung (Beispiele)

- Backdoor - Trojaner-utility der remote - Administrierung
- Trojan – PSW (Password-Stealing-Ware) : Passwort-Diebstahl
- Trojan - Clicker : Internet-Klicker
- Trojan - Downloader : Zustellung anderer Schadprogramme
- Trojan - Dropper : Installateur anderer Schadprogramme

Beispiele



- Syphilis (Backdoor Trojaner)
 - ermöglicht voller Zugriff auf das System. Der Trojaner hat mehr Nutzer-Rechte, als der eigentliche User vor dem entsprechenden System

- Eclipse 2000
 - ermöglicht Zugriff von außen auf:
 - Ausführen von Anwendungen
 - Aufzeichnung von Tastatureingaben
 - Systeminformationen

Trojaner (Futz)

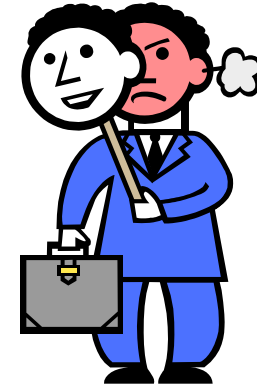




Schutz

- der Verzicht auf die Benutzung von Programmen aus unbekanntem oder unsicheren Quellen
- Antivirenprogramme
- Personal Firewalls

Verschleierungsprogramm



Definition:

Verschleierungsprogramm ,Schwindelprogramm (engl. *spoofing program*) ist ein Programm oder Programmteil, das die Oberfläche oder das Verhalten einer bekannten (System) - Funktion vorspiegelt.

- Eine Art von trojanischen Pferden

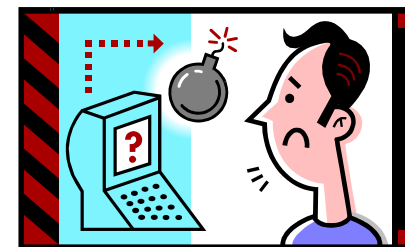
Beispiel: LOGON-Prozedur

Logische Bomben, Zeitbomben

Definition:

Logische Bombe, Zeitbombe (engl. logic bomb) ist ein Programm oder ein Programmteil, das seine versteckte zerstörerische Wirkung erst nach Eintreten eines bestimmten Ereignisses (Auslöser) entfaltet.

- Auslöser können unterscheiden werden nach:
 - Interne Auslöser
 - Datums- und Zeitangabe
 - Zähler
 - Interne Ereignisse

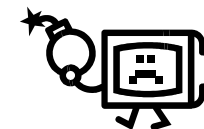


Logische Bomben, Zeitbomben

- Beispiel: Datum oder Zeitabfrage

```
Subroutine AUSLÖSER ::=  
  {if Datum > 3.7.2006 then 'true'  
   otherwise 'false'}
```

- Externe Auslöser
 - Schlüssel- oder Passwörter
 - Externe Ereignisse, Transaktionen
 - Ausblenden von Ereignissen („Toter - Mann - Knopf“)



Hintertüren, Falltüren

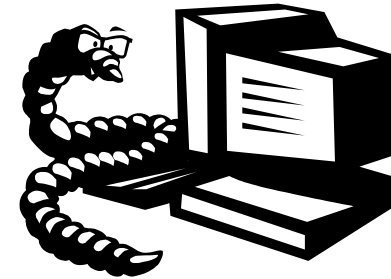


Definition:

Hintertür, Falltür (engl. trap door) ist ein Programm oder eine Programmteil mit verdeckten oder unbekanntem Nebenein- oder Nebenausgängen.

- Hintertüren sind alle Befehle, Anweisungen, Programmteile, Systemkomponenten, die für den ordnungsmäßigen Betrieb des Systems nicht benötigt werden und für z. B. „sonder“ Aufgaben benutzt werden

Würmer



Definition:

Wurm (engl. worm) ist ein selbstreproduzierendes Programm, das in einem System selbständig abläuft.

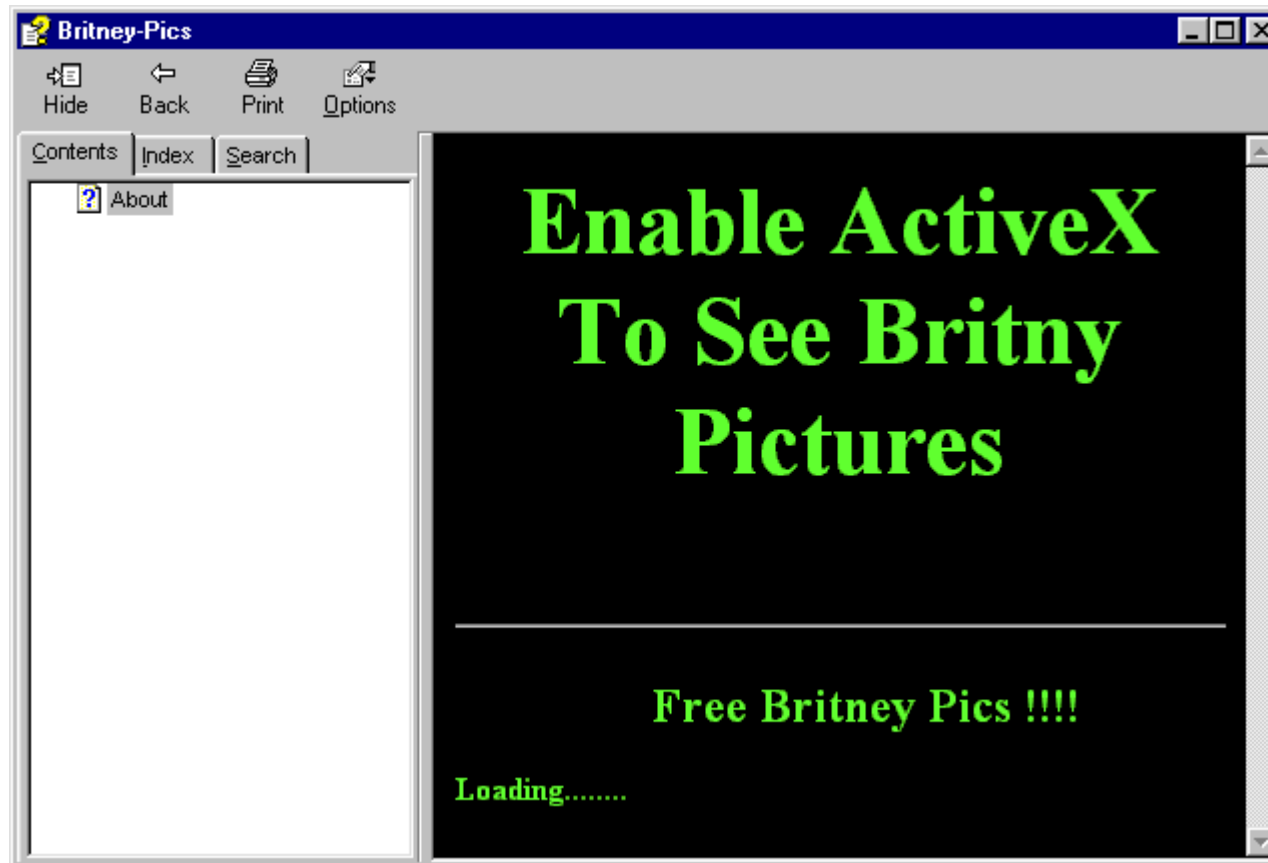
- verbreitet sich über Computernetzwerke
- es besteht aus verschiedenen Segmenten, die sich auf unterschiedlichen Systemen versuchen zu installieren und miteinander zu kommunizieren

Kategorien



- Email worms- Postwürmer
 - Instant Messaging (ICQ und MSN) Worms
 - IRC Worms - Würmer in den IRC-Kanälen
- Internet Worms - andere Netzwürmer
 - File-sharing Networks oder P2P Worms - Würmer für Datei-Austausch-Netze
- Handywürmer
- seit 2006 erste Wurm für RFID-Funkchips

Ein Mass - Mailing - Wurm (VBS/Britney-A)





Schutz

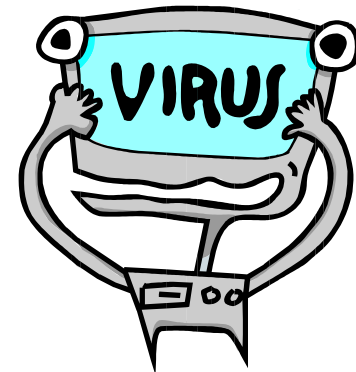
- Software (Betriebssystem, E-Mail-Software) immer auf dem neuesten stabilen Stand halten
- Personal - Firewalls einsetzen
- Paketfiltern einsetzen
- Virens Scanner
- Keine unbekannte E-Mails öffnen

Viren

Definition:

Virus (engl. virus) ist nicht-selbständiges Programmcode mit der Eigenschaft: Infektion. Er reproduziert Code und manipuliert ein Wirtsprogramm (oder dessen Umgebung) so, dass mit dessen Nutzung auch das Virusprogramm abläuft.

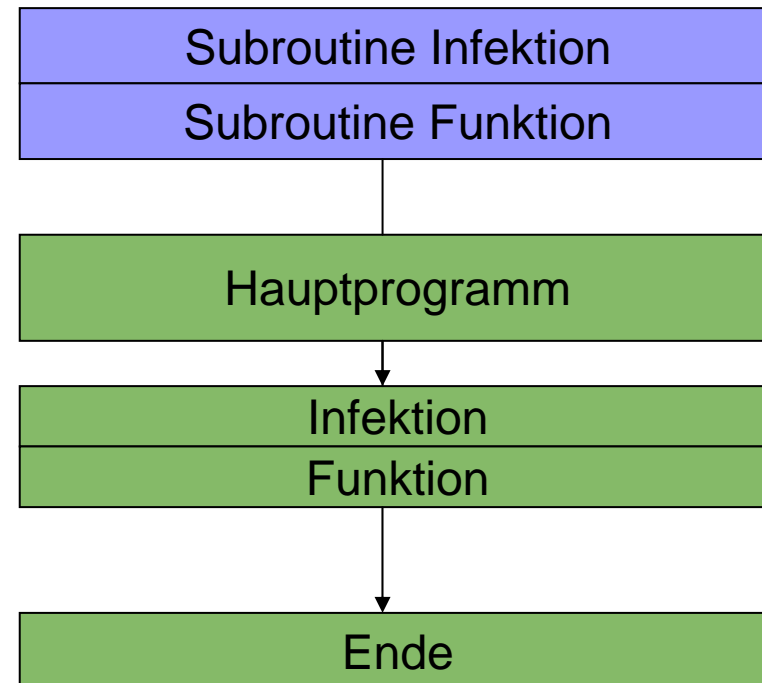
- Aufbau eines Comuter-Virus:
 - Reproduktionsteil
 - Erkennungsteil
 - Schadensteil
 - Bedingungsteil
 - Tarnungsteil



Struktur eines Virus

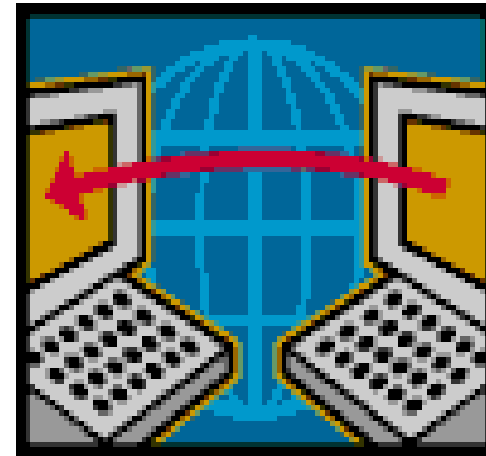
```
Programm V ::=  
subroutine INFEKTION ::=  
  {schleife:  
   datei:= hole-exec-datei;  
   infiziere;}  
subroutine FUNKTION ::=  
  {führe eine bestimmte Funktion  
   aus}  
Hauptprogramm ::=  
  {INFEKTION;  
   FUNKTION;  
   goto weiter;}  
Weiter}
```

VIRUS V



Vermehrung und Ausbreitung

- **Infektion durch:**
 - Reproduktion
 - Manipulation
- **Infektionsarten:**
 - Direkte Infektion
 - Indirekte Infektion
- **Ziel der Vermehrung:**
 - Jeder Programmaufruf verursacht ein Viruscodeablauf



Direkte Infektion



- **Direkte Manipulation-** die Teile des Viruscodes sind in Programmen integriert
- **Virustypen:**
 - Nicht -überschreibende Viren (Viruscode ist vor, mittig oder hinter den Wirt angehängt)
 - Überschreibende Viren (Wirt wird nicht verlängert)

Indirekte Infektion



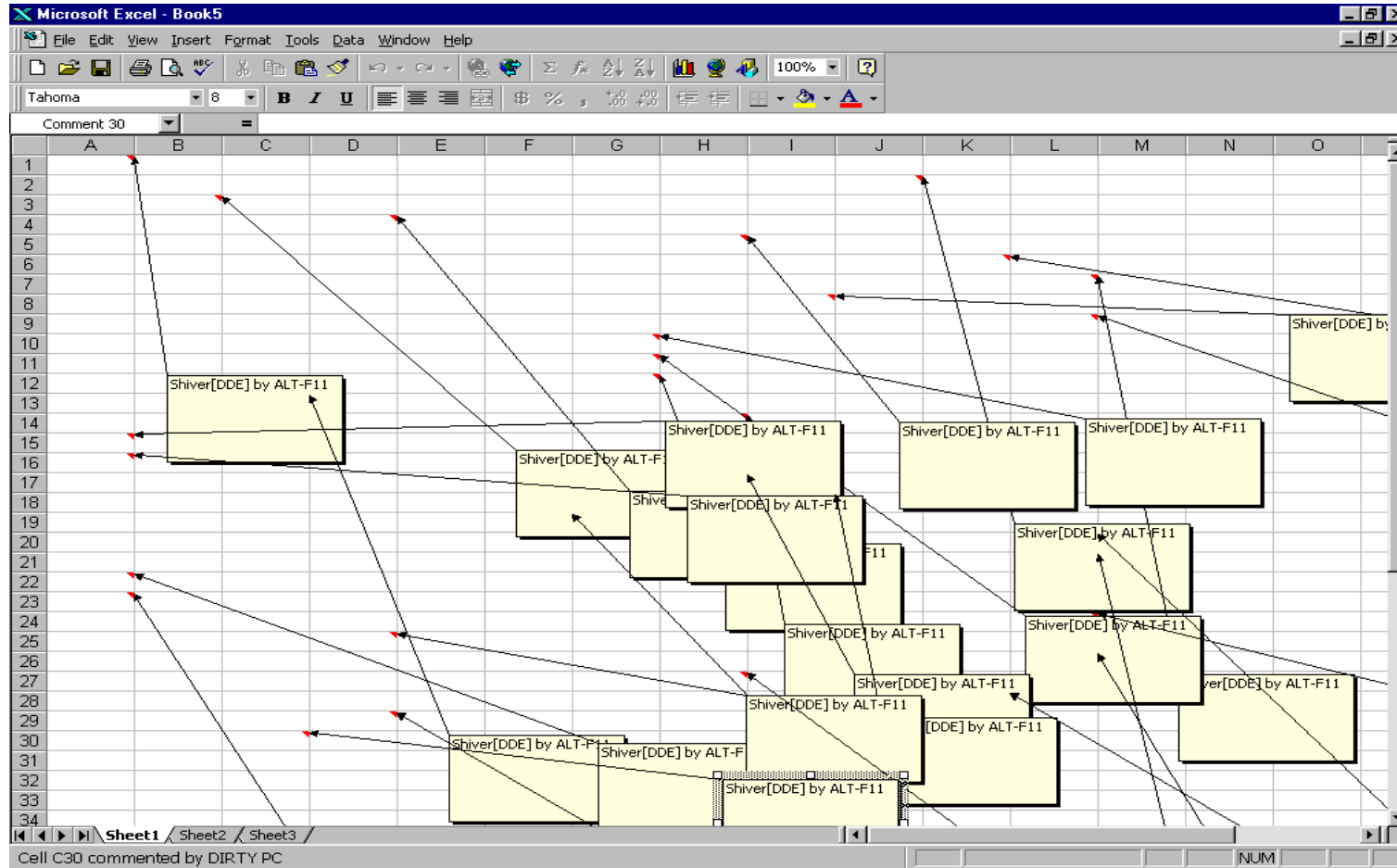
- **Indirekte Manipulation-**

Teile des Wirtssystems werden mit Hilfe der reproduzierten Teilen des Viruscodes so verändert, dass mit jedem Programm auch der Viruscode abläuft.

- **Beispiel:**

- Boot-Sektor-Viren (der Startsektor des Betriebssystems wird verändert)
- Andere Viren: Makroviren, Mischformen, usw.

Ein Microsoft-Office-Makrovirus (OF97/Shiver-N)



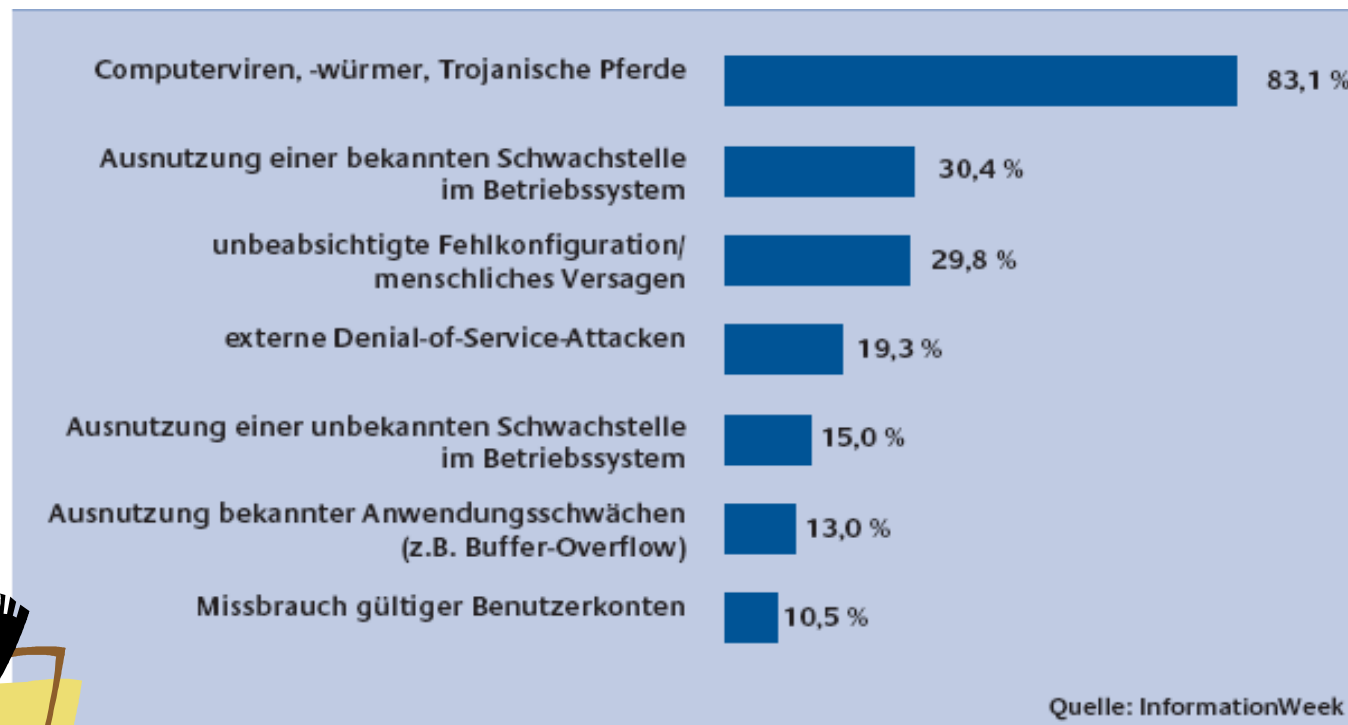


Schutz

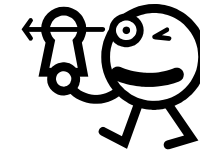
- Virens Scanner, Firewalls
- Umbenennen von wichtigen Dateien (FORMAT.com, FDISK.EXE, DEBUG.EXE,...)
- Sicherheitskopie von Dateien, die man nicht verlieren möchte
- bei Microsoft-Betriebssystemen:
 - niemals unbekannte Dateien oder Programme öffnen
 - Service Packs, Patches/Hotfixes und Updates regelmäßig installieren

Schwachstellen und Bedrohungen von IT-Systemen

Angriffsmethoden(2004):

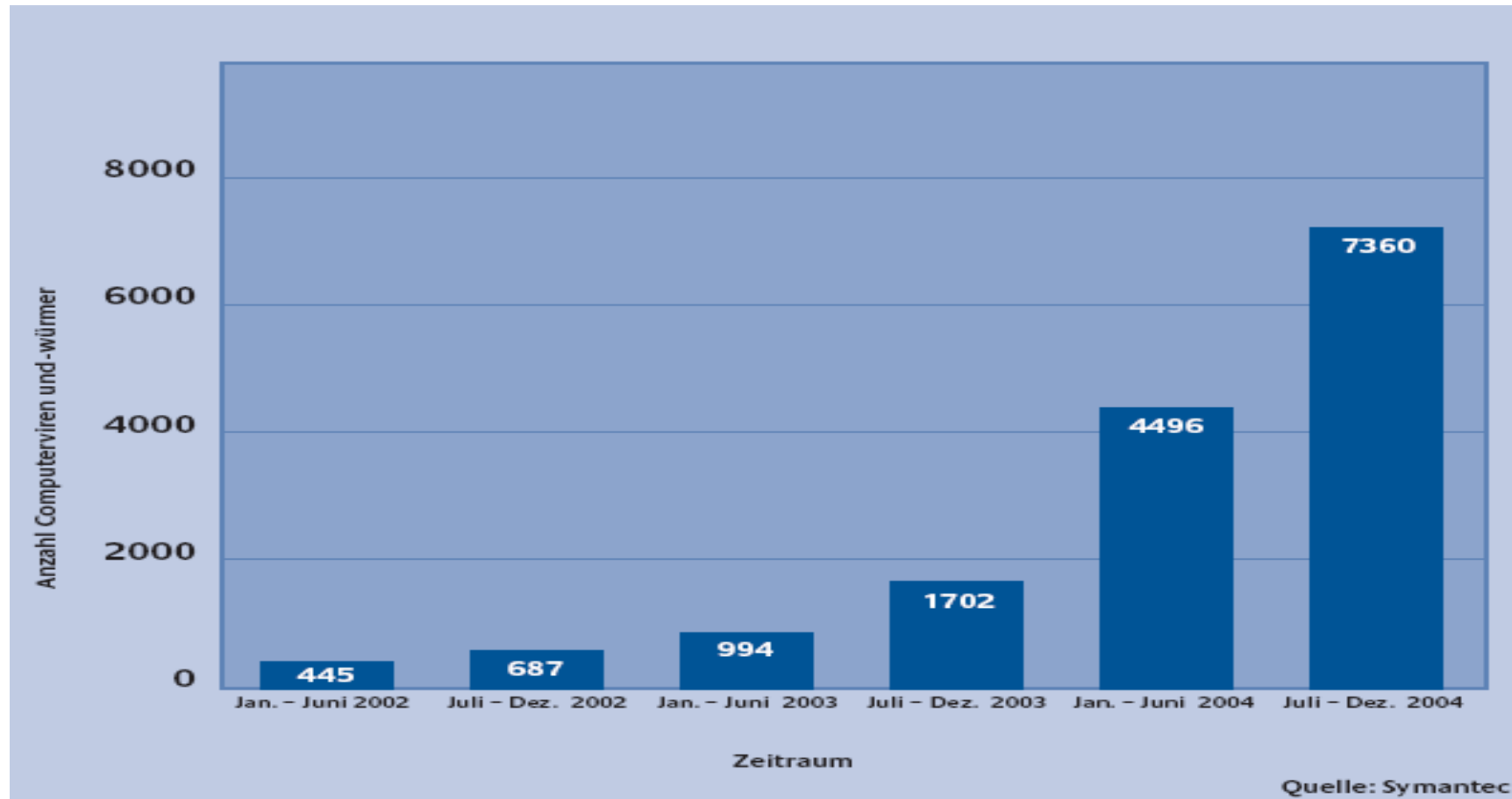


Schadprogramme



- Werden immer effektiver programmiert
- Es wird versucht den Computer unter Kontrolle zu bringen, anstatt Schaden anzurichten (Dos-Angriffe)
- Problem der Spionagesoftware
 - Spyware- greifen nach persönlichen Daten
 - Adware- zeichnen Nutzungsgewohnheiten des Anwenders

Zuwachs der Computerviren und Würmer weltweit



DoS - Angriffe



- DoS (Denial of Service) Attack, wo der Server mit sinnlosen Paketen überflutet wird.
- DDoS Angriffe - Verteilte Angriffe gegen Internetserver, wo:
 - Die Angreifer verschaffen sich die Ausführungsrechte auf mehreren ungeschützten Computer der Dritten
 - Installieren darauf die DDoS (Distributed Denial-of-Service-Attacken) Software
 - Starten durch die infizierte Rechner die Angriffe, um das System zu überlasten (z. B. durch überfluten den Server mit sinnlosen Paketen)

Spam

- Verursachen Überlastung technischer Komponenten, Kosten für den unerwünschten Datenverkehr, usw.
- Verbreiten sich durch die Massenmailerwürmer

Zur Kenntnisnahme

Zum Verbleib

Nein, ich habe Ihnen keinen
Virus/Wurm/Spam geschickt!

Mit Bitte um Rückruf

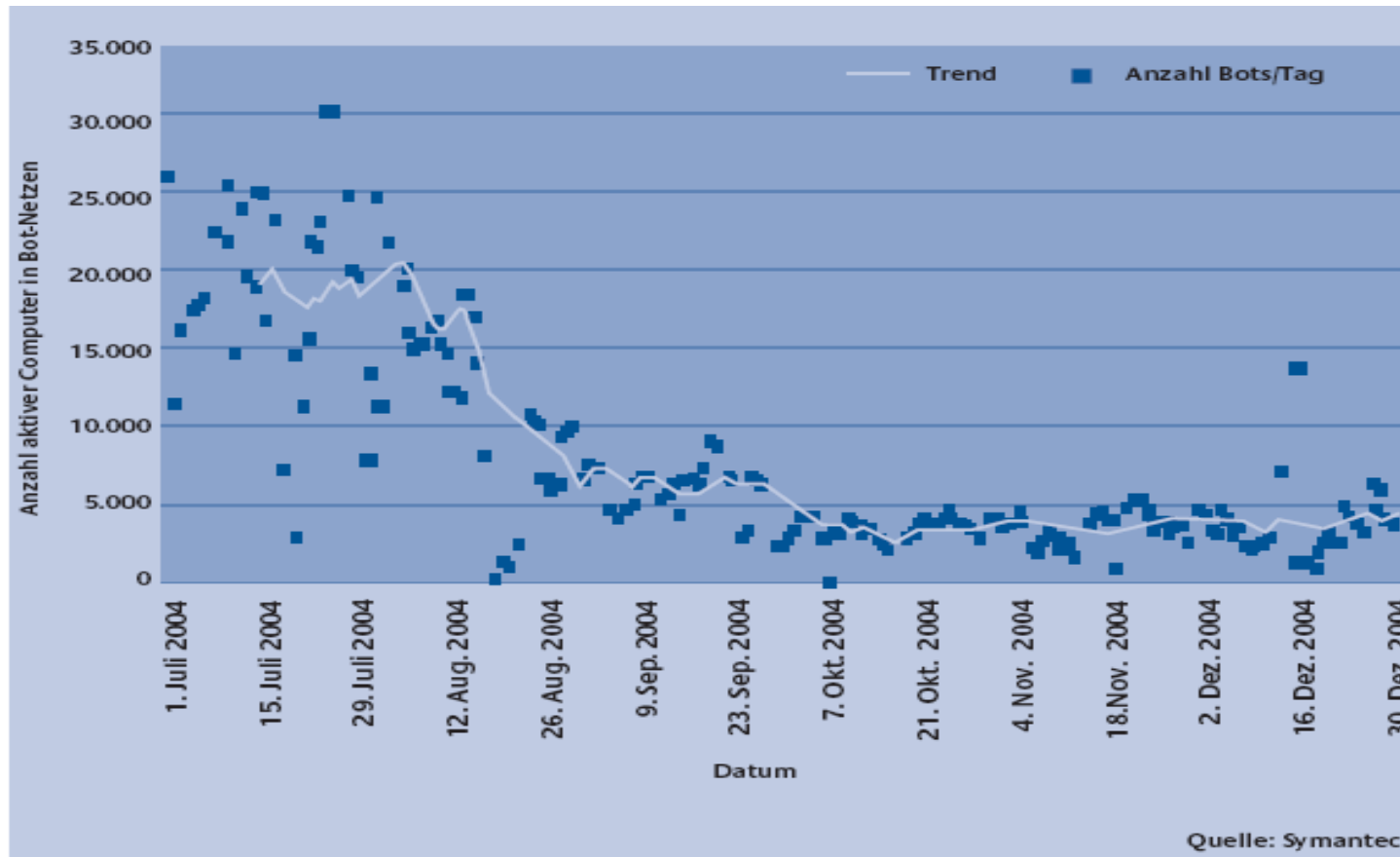
Bitte unterschrieben zurück

Bot-Netze

- Sind von einem Angreifer aus durch eine Vielzahl von Systemen z. B. mittels netzwerkbasierender Würmer kompromittiert und meist durch eine Trojaner Komponente nachgeladen, die es dem Angreifer ermöglicht, das System fernzusteuern.
- Benutzt für Massenmails und DDos-Attaken



Anzahl und Größe von Bot-Netzen weltweit



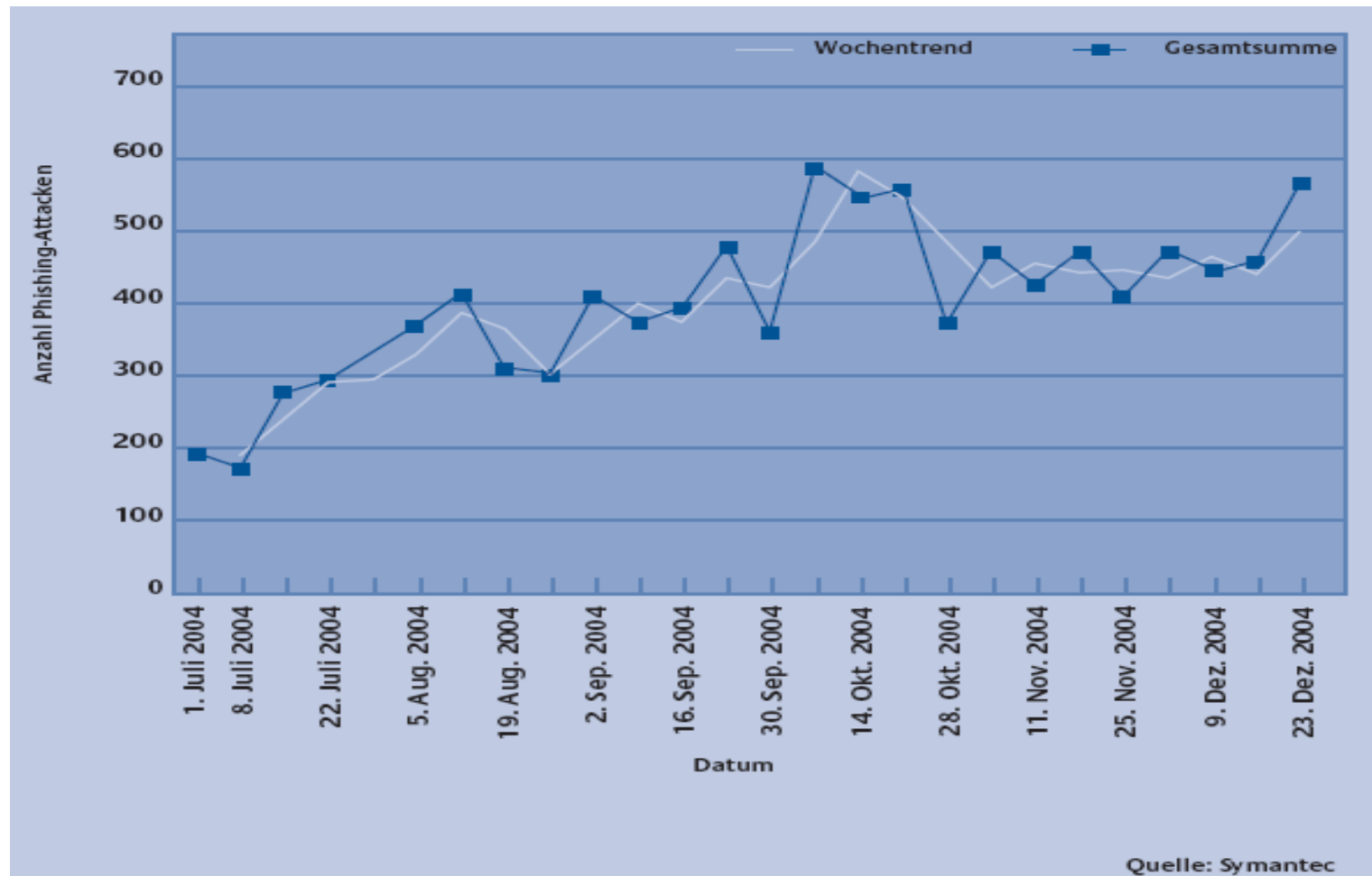
Phishing



Gefälschte E-Mails

- sind mit gefälschter Absenderadresse versehen (z.B. bekannte Unternehmen)
- enthalten ein Link, das zu einer nachempfundener Webseite des Unternehmens führt
- Dorthin versuchen die Betrüger die persönliche Daten auszuspionieren (Passwörter, Kreditkartennummer, usw.)

Anzahl von Phishing-Mails weltweit



Trends bei IT - Bedrohungen

- Sicherheitslücken
- Wirtschaftsspionage
- Angriffe gegen Infrastrukturen
- Angriffe gegen Unternehmen
- Kriminalisierung
- Regionalisierung von Schadensprogrammen





Danke für Ihre Aufmerksamkeit.

Wer schreibt Virusprogramme?

- Cyber-Vandalismus - Stufe 1
- Cyber-Vandalismus - Stufe 2
- Professionelle Virenautoren
- Virusforscher: die Autoren von 'Proof-of-Concept'-Malware

