

**Sicher ist sicher?**

—

# **Risiken beim Einsatz von Virensclannern**

Stephan Eckner  
stephan@codeblau.de

13. Juni 2002

# Überblick

- **Begriffsdefinitionen**
- Virens Scanner im Netzwerk
- Welche Probleme werden durch den Einsatz von Virens Scannern gelöst?
- Welche Probleme werden durch den Einsatz von Virens Scannern nicht gelöst?
- Welche Probleme werden durch den Einsatz von Virens Scannern erzeugt?
- Wie können Risiken minimiert werden?
- Virenresistente Anwendersoftware
- Links und Literatur
- Diskussion

# Virus

- BSI-Definition: “Ein Computer-Virus ist eine nicht selbständige Programm-routine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt.”
- attackiert Anwenderprogramme
- Programm, das vom Benutzer (unabsichtlich) ausgeführt wird
  - automatic macro-execution on startup
- Verbreitet sich via E-Mail oder Disketten/CDROM
  - wegen der Überlastung von Mailservern Ausbreitungsgeschwindigkeit geringer als bei Würmern
- Man unterscheidet File-, Boot- und Macro-Viren
- Beispiel: LOVEBUG

# Wurm

- attackiert Serverprogramme (Web/Mailserver)
- selbständiges Suchen nach und Ausnutzen von Schwachstellen
- selbständige Replikation
- verbreitet sich schneller, da nicht von User-Input abhängig
  - “How to Own the Internet in your spare time”
- Beispiel: nimda, Code Red

# Trojanisches Pferd

- oft auch einfach nur 'Trojaner' genannt
- Werkzeug zur Fernadministration
- Beispiel: Sub Seven, Back Orifice
- Mischformen (s. Vortrag über 'Blended Threads')

# Überblick

- Begriffsdefinitionen
- **Virens Scanner im Netzwerk**
- Welche Probleme werden durch den Einsatz von Virens Scannern gelöst?
- Welche Probleme werden durch den Einsatz von Virens Scannern nicht gelöst?
- Welche Probleme werden durch den Einsatz von Virens Scannern erzeugt?
- Wie können Risiken minimiert werden?
- Virenresistente Anwendersoftware
- Links und Literatur
- Diskussion

# Virens Scanner im Netzwerk

- Zentraler Virens Scanner
  - als Plug-In in Firewall/Mail-Server/WWW-Proxy
    - \* scannt ein/ausgehende Mails
    - \* scannt FTP/HTTP Traffic (Download von Viren)
  - auf dem zentralen Fileserver
    - \* scannt Dateien, die auf dem 'Netzlaufwerk' gespeichert werden
- dezentraler Virens Scanner
  - Installation auf jeder Workstation
  - scannt Dateien, die auf dem 'lokalen Laufwerk' gespeichert/ausgeführt werden

# Überblick

- Begriffsdefinitionen
- Virens Scanner im Netzwerk
- **Welche Probleme werden durch den Einsatz von Virens Scannern gelöst?**
- Welche Probleme werden durch den Einsatz von Virens Scannern nicht gelöst?
- Welche Probleme werden durch den Einsatz von Virens Scannern erzeugt?
- Wie können Risiken minimiert werden?
- Virenresistente Anwendersoftware
- Links und Literatur

# Welche Probleme werden von Virenscannern gelöst?

- Virenscanner bieten Schutz gegen
  - Viren, die zum Zeitpunkt des letzten Pattern-Updates bekannt waren

# Überblick

- Begriffsdefinitionen
- Virens Scanner im Netzwerk
- Welche Probleme werden durch den Einsatz von Virens Scannern gelöst?
- **Welche Probleme werden durch den Einsatz von Virens Scannern nicht gelöst?**
- Welche Probleme werden durch den Einsatz von Virens Scannern erzeugt?
- Wie können Risiken minimiert werden?
- Virenresistente Anwendersoftware
- Links und Literatur
- Diskussion

# Welche Probleme werden von Virenscannern nicht gelöst?

- Virenscanner bieten keinen Schutz gegen
  - Viren, die vom aktuell installierten Pattern-File nicht erkannt werden
- insbesondere
  - Kein Schutz gegen gezielten Angriff mit speziell erzeugtem Virus (s. späterer Vortrag über Virengeneratoren)
  - 'Window of Vulnerability' zwischen Auftreten des Virus, Analyse, Bereitstellung und Download des neuen Pattern-Files
  - automatisierter Download, Gefahren:
    - \* gehackter DNS-Server lenkt ftp.antiviruspattern.net auf ftp.evilhacker.com um
    - \* DoS-Attacke legt ftp.antiviruspattern.net lahm
    - \* ftp.antiviruspattern.net wird gehackt, das nächste Pattern- File ist korrupt

# Welche Probleme werden von Virenscannern nicht gelöst?

- zentrale Virenscanner, die Mails/HTTP-Traffic scannen, bieten zusätzlich keinen Schutz gegen
  - Viren, die über SSL heruntergeladen werden
  - Viren, die Teil einer verschlüsselten Mail sind
    - \* ... und trauen sie ja keiner E-Mail-Verschlüsselungstechnologie, die zentrales Scannen der verschlüsselten Mails ermöglicht
- Virenscanner bieten keinen Schutz gegen Angriffe des Benutzers auf sein eigenes System
  - sulfnbk.exe
  - “Diesen supertollen Bildschirmschoner müssen Sie unbedingt ausprobieren ...”
  - Benutzer, die den Virenscanner deaktivieren

# Überblick

- Begriffsdefinitionen
- Virens Scanner im Netzwerk
- Welche Probleme werden durch den Einsatz von Virens Scannern gelöst?
- Welche Probleme werden durch den Einsatz von Virens Scannern nicht gelöst?
- **Welche Probleme werden durch den Einsatz von Virens Scannern erzeugt?**
- Wie können Risiken minimiert werden?
- Virenresistente Anwendersoftware
- Links und Literatur

# Virens Scanner erhöhen die Komplexität der Systeme

- zusätzliche Fehlerquelle
- Sicherheitslücken in Antivirus-Programmen
  - z.B. “Buffer Overrun in NAI WebShield SMTP v4.5.44 Management Tool”
- DoS Angriffe auf Virens Scanner
  - werden z.B. auch Mails an nicht vorhandene Benutzer gescannt?
- Virens Scanner kosten CPU-Zeit
- Stabilitätsprobleme
  - z.B. “McAfee pattern 4.0.4102. bringt Windows zum Absturz”
- Konflikte mit anderen Programmen
  - “Wenn Sie unser Programm installieren wollen, deaktivieren Sie bitte vorher eventuell laufende Virens Scanner...”

# Gefahr durch falsches Gefühl von Sicherheit

- Mails mit Subject: Hi! [Virus checked]
- Magic Lantern
  - Wieviel Vertrauen kann nicht-quelloffenen Programmen entgegengebracht werden?
- Wie sicher ist ein automatisches Pattern-Update?

# Überblick

- Begriffsdefinitionen
- Virens Scanner im Netzwerk
- Welche Probleme werden durch den Einsatz von Virens Scannern gelöst?
- Welche Probleme werden durch den Einsatz von Virens Scannern nicht gelöst?
- Welche Probleme werden durch den Einsatz von Virens Scannern erzeugt?
- **Wie können Risiken minimiert werden?**
- Virenresistente Anwendersoftware
- Links und Literatur
- Diskussion

# Minimierung von Risiken

- Schulung von Anwendern
  - keine aus nicht vertrauenswürdigen Quellen stammenden Programme ausführen oder installieren
    - \* md5-Checksummen, PGP-Signatures prüfen
  - Java, JavaScript, ActiveX deaktivieren
  - E-Mails als Text verschicken, nicht als HTML oder sogar MSWord
  - Dokumente als pdf-Dateien verschicken
- Systemkonfiguration
  - System klein halten, keine unnötige Software installieren
  - Patches einspielen
  - Principle of least Privilege

# Minimierung von Risiken – Windows

- kein Windows benutzen
- Wenn Windows, dann kein Outlook und kein Office benutzen
- eventuell Worddokumente mit Wordpad/Wordview betrachten
  - Vorsicht: Beides sind Programme von Microsoft
- Wenn Outlook, dann HTML, Java, Javaskript und ActiveX deaktivieren
- Attachements nicht automatisch öffnen
- Wenn Office, dann Macros deaktivieren

# Minimierung von Risiken – Unix

- `/home` und `/tmp` als `noexec` mounten
- Mails an `root` an normalen User-Account umleiten
- Vorsicht bei postscript-Dokumenten
  - `gs` immer mit `-dSAFER` Option aufrufen
- Anzahl der `suid-root` Programme minimieren
  - `find / -user root -perm "-u+s"`

# Überblick

- Begriffsdefinitionen
- Virens Scanner im Netzwerk
- Welche Probleme werden durch den Einsatz von Virens Scannern gelöst?
- Welche Probleme werden durch den Einsatz von Virens Scannern nicht gelöst?
- Welche Probleme werden durch den Einsatz von Virens Scannern erzeugt?
- Wie können Risiken minimiert werden?
- **Virenresistente Anwendersoftware**
- Links und Literatur
- Diskussion

# Virenresistente Anwendersoftware

- Der Microsoft–Effekt: *“Virenresistente Software?! Das soll gehen?!?”*
- Grundsätze sicheren Designs
  - Prinzip des geringsten Privilegs (least privilege)
  - modular programmieren, Privilegien separieren
  - grundsätzlich Input-Daten validieren
  - Trennung von Daten und Programmroutinen
- Die vier Microsoft Sünden:
  1. Vermischung von Daten und Programmroutinen (z.B. Word-Macros) – Es reicht, die Dateien zu 'öffnen'
  2. Word-Makros haben Zugriff auf System-Ebene – 'Principle of least Privilege' verletzt
  3. Keine/Ungenügende Trennung von User und Administrator – 'Principle of least Privilege' verletzt
  4. Softwareinstallation per Doppelklick

# Überblick

- Begriffsdefinitionen
- Virens Scanner im Netzwerk
- Welche Probleme werden durch den Einsatz von Virens Scannern gelöst?
- Welche Probleme werden durch den Einsatz von Virens Scannern nicht gelöst?
- Welche Probleme werden durch den Einsatz von Virens Scannern erzeugt?
- Wie können Risiken minimiert werden?
- Virenresistente Anwendersoftware
- **Links und Literatur**
- Diskussion

## Links und Literatur

- “How to Own the Internet in your spare time”  
<http://www.icir.org/vern/papers/cdc-usenix-sec02/>
  - Analyse der Ausbreitungsgeschwindigkeit von Würmern
- “Buffer Overrun in NAI WebShield SMTP v4.5.44 Management Tool”  
<http://online.securityfocus.com/advisories/2288>
- “McAfee pattern 4.0.4102. bringt Windows zum Absturz”  
<http://www.heise.de/newsticker/data/pab-03.11.00-000/>
- “BSI warnt vor dem Einsatz von JavaScript”  
<http://www.bsi.de/fachthem/sinet/java99.htm>
- “Ausführbare Inhalte - Sicherheitsrisiken und Lösungen”  
<http://www.bsi.de/taskforce/literatur/aktivinh.htm>
  - Konfigurationshinweise für Windows

# Links

- “How to Think About Security”

<http://www.counterpane.com/crypto-gram-0204.html#1>

- “Secure Programming for Linux and Unix HOWTO”

<http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/index.html>

- Sicher ist sicher? – Risiken beim Einsatz von Virenschannern

<http://www.codeblau.de/antivir.pdf>

– Folien zu diesem Vortrag :-)

# Überblick

- Begriffsdefinitionen
- Zentraler versus dezentraler Virens Scanner
- Welche Probleme werden durch den Einsatz von Virenscannern gelöst?
- Welche Probleme werden durch den Einsatz von Virenscannern nicht gelöst?
- Welche Probleme werden durch den Einsatz von Virenscannern erzeugt?
- Wie können Risiken minimiert werden?
- Virenresistente Anwendersoftware
- Links und Literatur
- **Diskussion**