# Angriffsmöglichkeiten auf Netzwerke und Unternehmensdaten


Fraunhofer Anwendungszentrum
Logistiksystemplanung
Informationssysteme
Steffen Müller, Corina Köhler

Workshop: Sicherheit in Netzwerken


Fraunhofer Anwendungszentrum
Logistiksystemplanung
Informationssysteme

Müller, S. / Köhler, C.

# Einleitung

Hacker besuchen nicht nur Konzerne

Sicherheitslücke im Internet Explorer 5.5

IT - Sicherheit

Unterschätzte Gefahren im Netz

Notepad als Trojanisches Pferd

Angriffswelle gegen Linux-Sever

Wenn der Hacker zweimal klingelt

Quelle: Die Welt, C't



Fraunhofer IML
Anwendungszentrum
Logistiksystemplanung
Informationssysteme

Müller, S. / Köhler, C.

# Ziele des Angreifers

## Ziele:

- Vorspiegeln einer falschen Identität
- Einsehen von vertraulichen Unternehmensdaten
- Verändern und Verfälschen von Daten/Nachrichten
- Transfer von gefährlichen Programmen in das System
- Unternehmen in Misskredit bringen

## Motivation:

- Testen der eigenen Fähigkeiten und Grenzen
- Monetäre Ziele
- Rache gekündigter Mitarbeiter

# Schäden durch Angriffe auf Unternehmensnetzwerke



## Schäden:

- eingeschränkte Funktionsweise von Netzwerken und Servern
- Erleiden von materiellen Schäden
- Imageschaden
- Verlust von Firmengeheimnissen (z.B. Patente, Bilanzen)

***Wissen bedeutet Macht, aber nur solange man es für sich behält.***

# Achillesferse

## Schwachstellen:

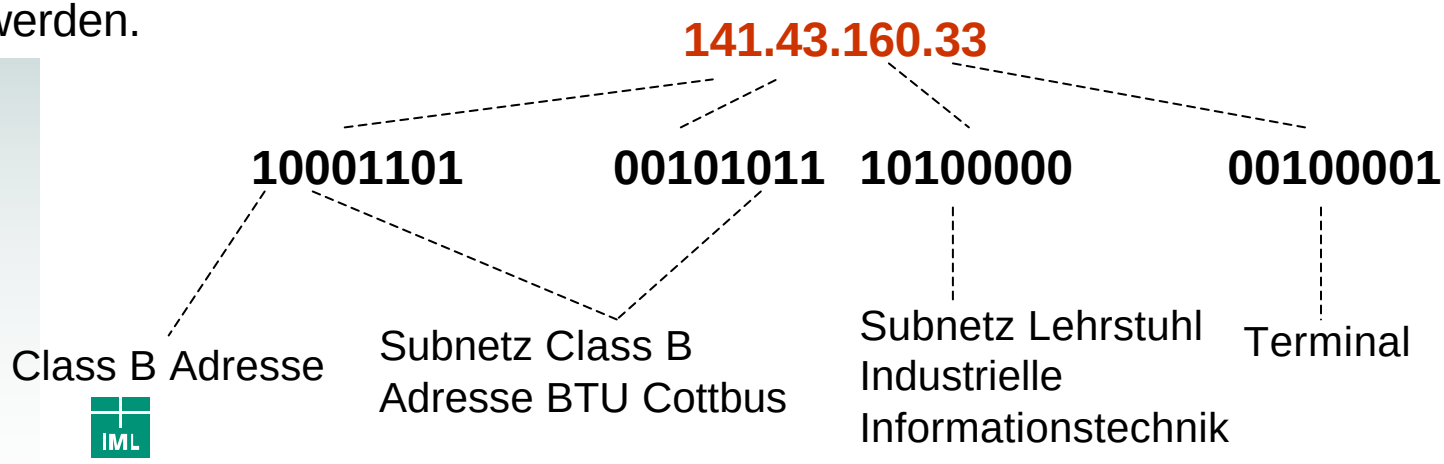
- **Ausnutzen der Unwissenheit von Anwendern**
- **Ausnutzen von Sicherheitslücken in Programmen, die auf dem angegriffenen Computer laufen (z.B. Web-Browser)**
- **Ausnutzen von z.B. fehlerhaft umgesetzten Netzwerk-Protokollen**
- **schwache Passwörter**

# Verwendung vorhandener Protokolle (1)

Das **Transport Control Protocol (TCP)** stellt eine bidirektionale, gesicherte Verbindung zwischen zwei Rechnern her. Aufgabe: Fehler- und Flusskontrolle, Zeitüberwachung und Multiplexing verschiedener Verbindungen.

Die Aufgabe des **Internet Protocols (IP)** besteht darin, Datenpakete von einem Rechner an einen anderen weiterzuleiten (Ende-zu Ende Übertragung). Funktion: Adressfunktionen, Routing zwischen den Netzwerken, Prioritätssteuerung, Paketübermittlungsdienst

Damit zwischen zwei Rechner eine Kommunikationsverbindung aufgebaut werden kann, muss jedem Rechner eine eindeutige IP-Adresse zugewiesen werden.



# Verwendung vorhandener Protokolle (2)

Damit ein Rechner gleichzeitig mehrere Verbindungen bearbeiten kann, müssen diese unterschieden werden. Dazu bedient sich das TCP der sogenannten **Ports**. Jeder Anwendung, die das TCP benutzen will, wird ein Port zugeordnet. Es gibt 65536 verschiedene Ports.

Als **Socket** wird ein Paar aus IP-Adresse und Port bezeichnet.

Auf den meisten Systemen sind die Ports über 1024 für jede Anwendung offen, während die Ports 1-1024 nur Systemprozessen (oder Anwendungen, die über entsprechende Privilegien verfügen) zur Verfügung stehen.

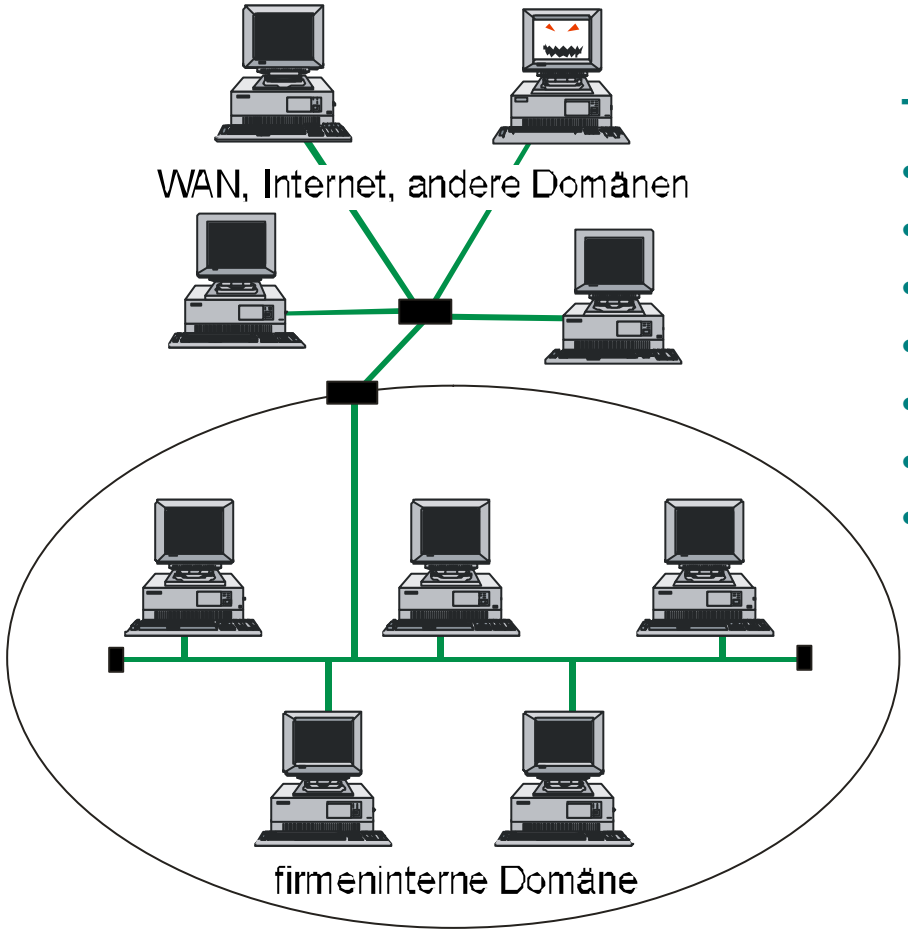
| Dienst | Port | Funktion |
|---|---|---|
| ftp-data | 20 | File Transfer [Default Data] |
| ftp | 21 | File Transfer [Control] |
| telnet | 23 | Telnet |
| smtp | 25 | Simple Mail Transfer Protocol |



Fraunhofer IML Anwendungszentrum Logistiksystemplanung Informationssysteme

Müller, S. / Köhler, C.

# Angriffsmöglichkeiten: EXTERN




**TOOLS**
- **Trojanische Pferde**
- **Würmer**
- **DoS Attacken**
- **Makro-Viren**
- **Nuker**
- **Mail-Bomber**
- **Web-Browser**



Fraunhofer Anwendungszentrum Logistiksystemplanung Informationssysteme

Müller, S. / Köhler, C.

# Trojanische Pferde

**Trojanische Pferde** waren ursprünglich Softwaretools zur Fernadministration von Rechnern (z. B. NetBus, BackOrifice, SubSeven), wurden dann aber zum ausspionieren von Rechnern umfunktioniert.

**Infektion:**
- Versteckt in einer Datei (*.exe, *.com)
- als Script (!) Datei (*.vbs, *.js, *.ps)
- Win Problem: susi.jpg.exe

**Funktionsweise:**
- meist TCP/IP Nutzung
- Client/Server Prinzip
- Client (Angreifer) bittet Server (Opfer) um Dienste (z. B. Zugriff auf Dateien)

# Trojaner Ports

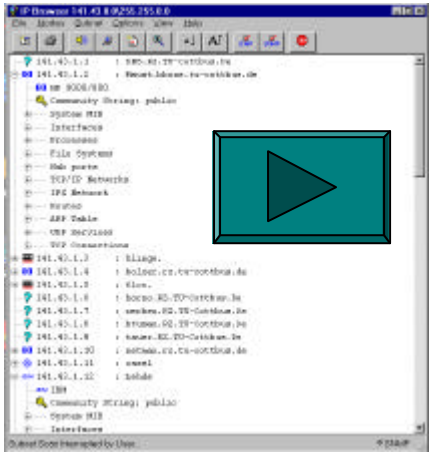
| Port | Protokoll | Bezeichnung der Trojaner |
|---|---|---|
| 12076 | TCP | GJamer |
| 12223 | TCP | Hack´99 KeyLogger |
| 12345 | TCP | GabanBus, NetBus, Pie Bill Gates, X-bill |
| 12346 | TCP | GabanBus, NetBus, X-bill |
| 20034 | TCP | NetBus 2 Pro |
| 21544 | TCP | GirlFriend |
| 22222 | TCP | Prosiak |
| 40426 | TCP | Masters Paradise |
| 47262 | UDP | Delta Source |
| 50505 | TCP | Sockets de Troie |
| 54321 | TCP | School Bus |



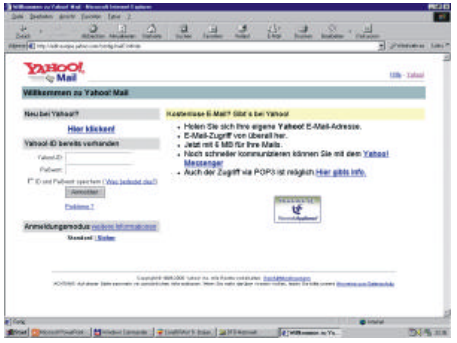
Fraunhofer IML
Anwendungszentrum
Logistiksystemplanung
Informationssysteme

Müller, S. / Köhler, C.

# ONLINE-Demo: Einschleusen von Trojanischen Pferden (1)



1. Scannen der Domäne.
2. Web-Seiten des Unternehmens nach Informationen durchsuchen.
3. E-Mail Service des Unternehmens in Anspruch nehmen.
4. Strategie festlegen – Angriff mit Trojaner.
5. Anonymen Mail-Account einrichten.



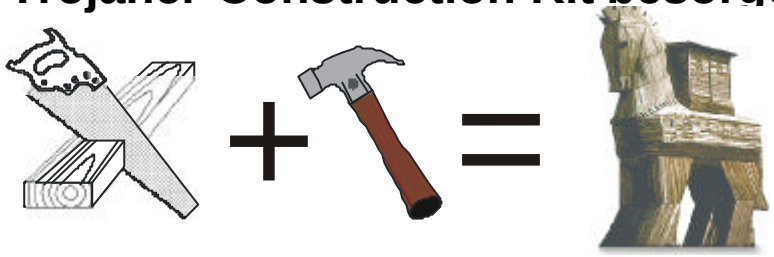


IML
Fraunhofer Anwendungszentrum Logistiksystemplanung Informationssysteme

Müller, S. / Köhler, C.

# ONLINE-Demo: Einschleusen von Trojanischen Pferden (2)

6. **Trojaner-Construction Kit besorgen.**



7. **Gag-Programme oder Anwendungsprogramme besorgen um Trojaner-Server zu tarnen.**




Moorhuhn.exe

Notepad

8. **Mittels eines Joiners das Gag-Programm und den Trojaner verschmelzen.**



EliteWarp, TopV




Fraunhofer IML Anwendungszentrum Logistiksystemplanung Informationssysteme

Müller, S. / Köhler, C.

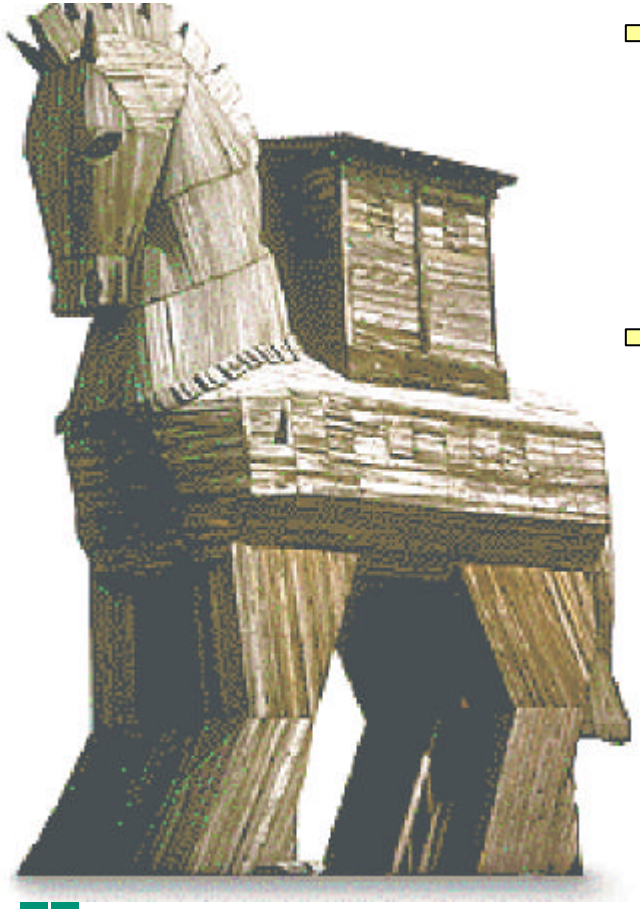
# ONLINE-Demo: Einschleusen von Trojanischen Pferden (3)

9. **Anonymen Mailserver suchen und E-Mail mit getarntem Trojaner verschicken.**

10. **Mit der per E-Mail verschickten IP-Adresse den Trojaner Server anwählen.**

11. **Eigene Spuren verschleiern (Proxy-Server, öffentlich zugängliche Computer benutzen).**

# Erkennung Trojanischer Pferde



- **Viren- oder Trojanerscanner:**
  - **TDS3, NoBackdoors,**
  - **ProtectX, Anti-Trojan**
  - **Cleaner, NetAlert**
- **Autorun-Einträge überprüfen**
  - **autostart**
  - **Win.ini**
  - **regedit**
- **Laufende Prozesse überprüfen:**
  - **Strg+Alt+Entf**
  - **„Process Viewer“**



IML
Fraunhofer Anwendungszentrum Logistiksystemplanung Informationssysteme

Müller, S. / Köhler, C.

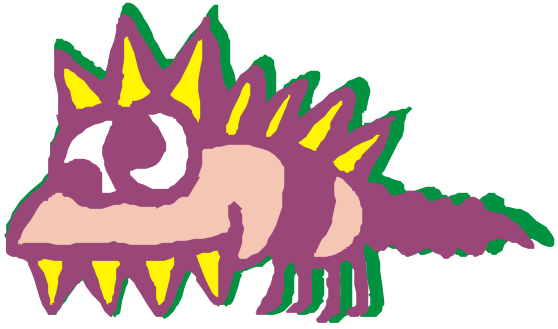
# Würmer

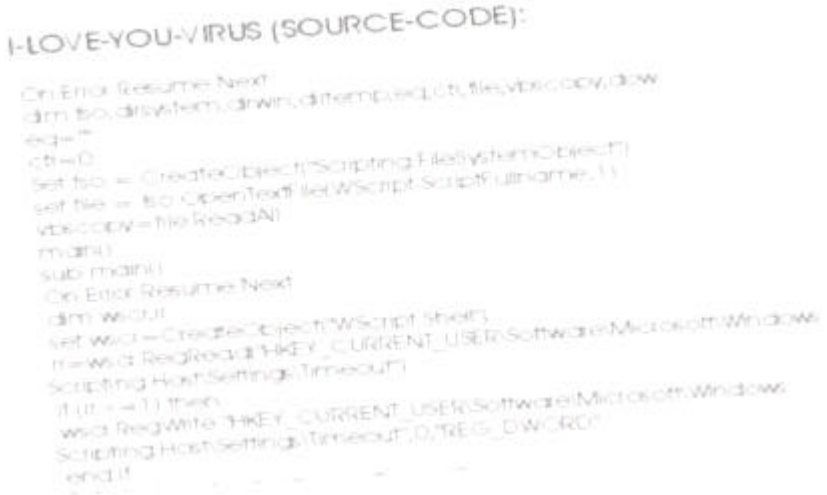
**Würmer:** Würmer sind auf Skriptsprachen basierende Computerviren, die aber kein „Wirtsprogramm“ benötigen.

**Voraussetzung:** Es müssen unterstützende Funktionen von Betriebssystemen und Anwendungsprogrammen existieren.

**Abhilfe:** Deaktivierung von Aktiv-Scripting, „sichere“ Einstellungen von Mailprogrammen.

**Beispiel:** Wurm Navidad (spanisch: Weihnachten)
Wurm I Love You





# DoS (Denial of Service) Attacken

**DoS:**

- Angreifer generiert Zufallsadressen (IP‘s)
- sehr viele IP‘s fragen gleichzeitig den gleichen Server (Dienst) an
- Server öffnet für alle IP‘s Verbindungen
- Server wartet vergeblich auf Bestätigung
- Überfüllung des connection tables, Überlastung
- seriöse Anfragen können nicht bearbeitet werden, da alle Kapazitäten gebunden sind

**Abhilfe:** Spezielle Programme für die jeweiligen Server.

**DoS-Programme:** Stacheldraht, Sonar, dndDoS, Boom

# Weitere Methoden und Tools (1)

**Makro-Viren:** Makro-Viren sind auf Skriptsprachen basierende Computerviren die mit Anwendungsprogrammen verteilt werden.

**Voraussetzung:** Es müssen unterstützende Funktionen in Betriebssystemen und Anwendungsprogrammen existieren.

**Abhilfe:** Deaktivierung von Aktiv-Scripting.

**Nuker:** Der Nuker ist ein Programm, welches andere Computer über das Netzwerk zum Absturz bringen soll.

**Voraussetzung:** Fehlerhafte Implementierung von Netzwerkprotokollen.

**Abhilfe:** Installation eines geeigneten Service-Release.

# Weitere Methoden und Tools (2)

**Mail-Bomber:** Mail-Bomber sind Programme, die massenhaft E-Mails zu ein Mail-Adresse verschicken.

**Voraussetzung:** Anonyme Mailserver -> Verschleierung der Herkunft

**Abhilfe:** Verwendung „intelligenter“ Mailserver

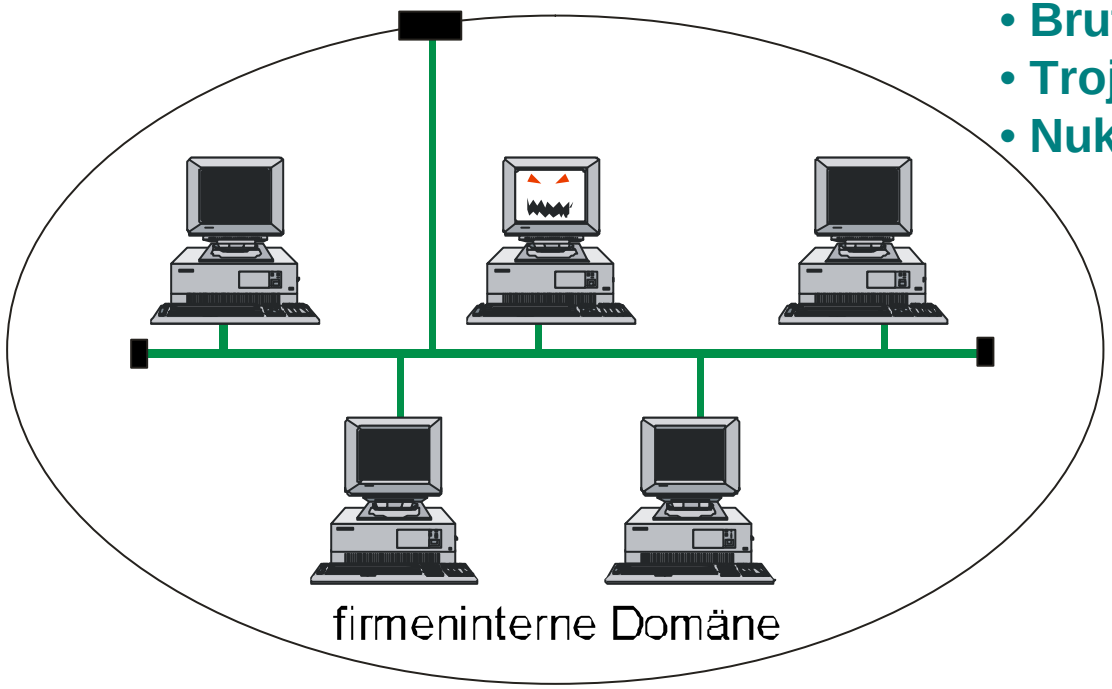
**Mail-Bomber-Programme:** BombSquad, eXtrem, Gostmail

**Web-Browser:** Internet-Explorer, Netscape Navigator usw.

**Vorraussetzung:** Besuch einer entsprechend präparierten Web-Seite

**Abhilfe:** Installation eines geeigneten Service-Release, Browser „sicher“ konfigurieren -> deaktivieren von z.B. ActivX, Jave-Script

# Angriffsmöglichkeiten: INTERN




**TOOLS:**

- **Sniffer**
- **Passwortsammler**
- **Brute Force Attacke**
- **Trojanische Pferde**
- **Nuker**

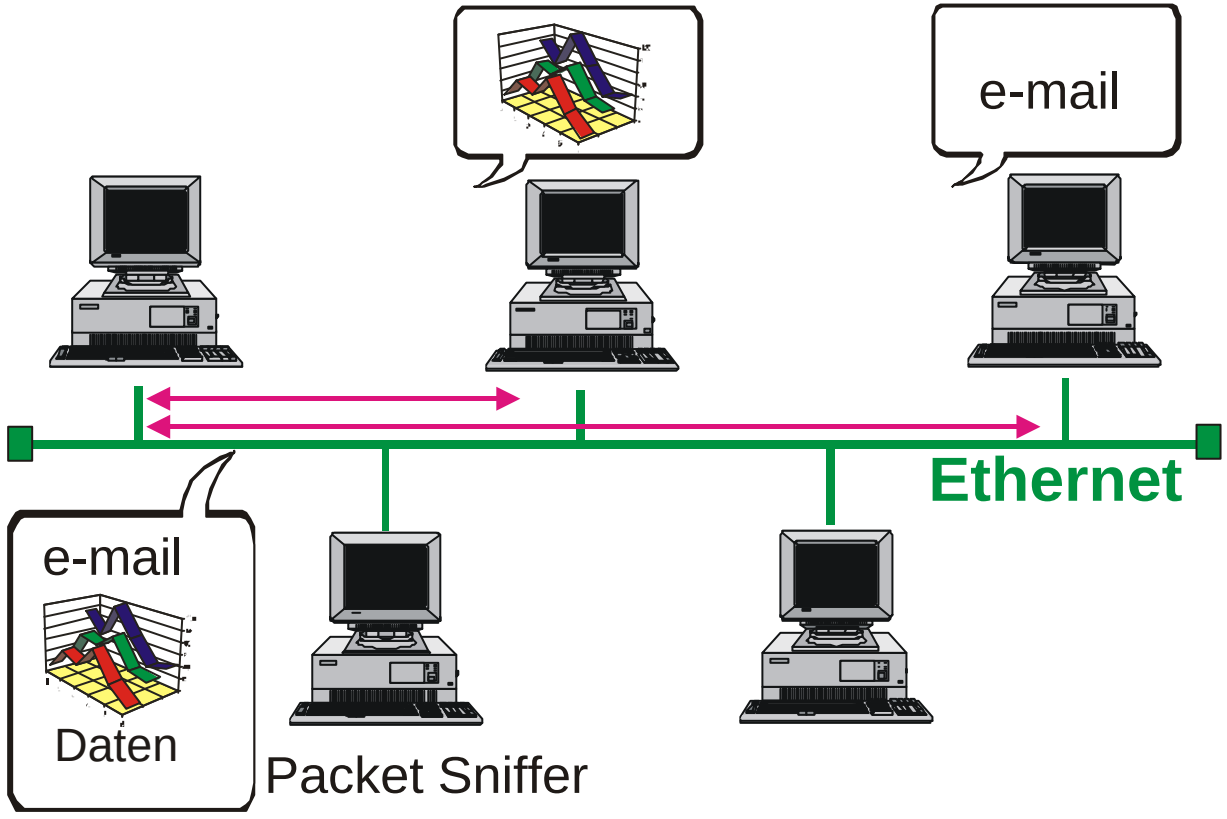


Fraunhofer IML Anwendungszentrum Logistiksystemplanung Informationssysteme

Müller, S. / Köhler, C.

# Sniffer (1)

Beim Packet Sniffing wird ein Rechner im LAN (Ethernet-Netzwerk) eingesetzt, um alle über das LAN laufende Datenpakete abzuhören. Betroffen sind alle Rechner die an einem LAN-Segment hängen.






Fraunhofer Anwendungszentrum Logistiksystemplanung Informationssysteme

Müller, S. / Köhler, C.

# Sniffer (2)

**Sniffer:** Mit Sniffern können Passwörter und alle Daten die über das Netzwerk gehen abfangen werden.

**Voraussetzung:** Sniffer müssen das jeweilige Netzwerk-protokoll beherrschen.

**Abhilfe:**
- Verwendung segmentierter Netzwerke
- Verwendung des Secure Socket Layer (SSL)
- Verwendung kryptografischer Verfahren

**Sniffer-Programme:** pptp-sniff, Buttsniff, Hcwc

# Weitere Methoden und Tools (3)

**Passwortsammler:** Programme, die alle Tastatur- und/oder Passworteingaben speichern.

**Voraussetzung:** Offener, ungeschützter Zugang zu Rechnern.

**Abhilfe:** Zugang bei Abwesenheit immer sperren.

**Brute Force Attacke:** Ist ein Verfahren, mit dem gezielt und/oder zufällig Passwörter erzeugt werden, um diese mit ausgelesenen Passwortdateien zu vergleichen.

**Abhilfe:** Vermeiden schwacher Passwörter.

# Abwehr von Angriffen auf Unternehmensnetzwerke

**Schutz vor Trojanischen Pferden**:

- Mail-Anhang genau untersuchen
- Scripting ausschalten
- spezielle Programme (NetBusScan) benutzen
- regelmäßig nach offenen Ports suchen
- Einsatz von Antiviren-Software

**Schutz vor dem Packet Sniffing**:

- Einsatz von segmentierten Netzen
- Einsatz von SSL (Secure Socket Layer)

**Andere Maßnahmen zum Abwehren von Angriffen:**

- Einsatz von Firewalls
- Verwendung sicherer Betriebssysteme
- Schulung von Mitarbeitern
- Einsatz von Watch-Dog Software
- Einsatz von kryptografischen Programmen



Fraunhofer IML Anwendungszentrum Logistiksystemplanung Informationssysteme

Müller, S. / Köhler, C.

ENDE

# SMTP (Simple Mail Transfer Protocol)

Das Simple Mail Transfer Protocol ist ein Protokoll zum senden von Mails zwischen Servern. Das senden zwischen den Servern erfolgt über Client/Server-Beziehungen. SMTP arbeitet mit POP und IMAP zusammen.

**wichtige Kommandos:**

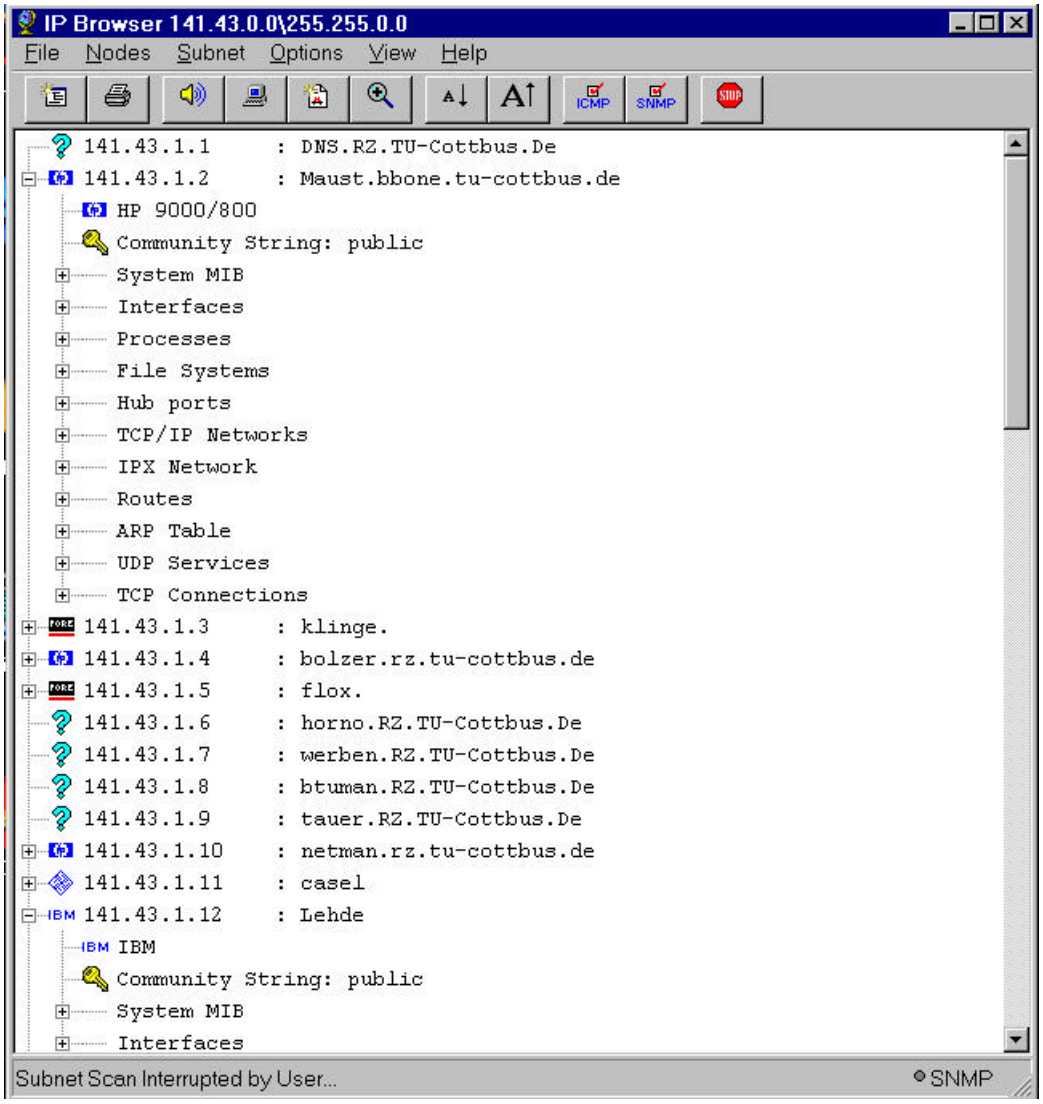
- helo — Zuordnung der Sender-Domain
- mail from: — Sender der Mail
- rcpt to: — Empfänger der Mail
- data — Textrumpf
- . *(Punkt)* — Beendet die Texteingabe/abschicken der Mail
- quit — Beenden der Anwendung

# Verwendung anonymer Mailserver - Simple Mail Transfer Protocol (SMTP)

telnet mail.horizonz.net 25
helo mueller.com
mail from: bill.gates@microsoft.com
rcpt to: opfer@opfer.com
data
Hier kann jetzt der Text eingegeben werden. Fuer das anhaengen von Programmen muessen Steuerzeichen verwendet werden.

Content-Description: filename="NOTEPAD.EXE„
Content-Disposition: inline; filename="NOTEPAD.EXE„
Content-Transfer-Encoding: base64
TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcy
.
quit

# Screenshot: IP-Browser






Fraunhofer Anwendungszentrum Logistiksystemplanung Informationssysteme

Müller, S. / Köhler, C.