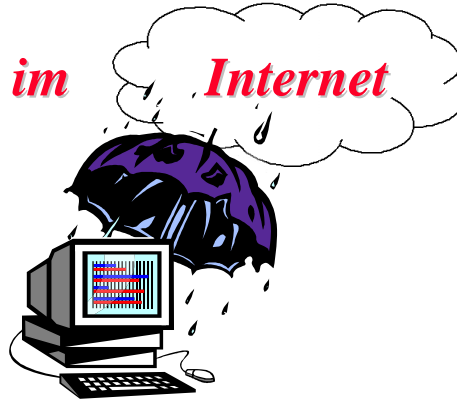




## Zur Sicherheit von Windows-PCs

im Internet



[j.meissburger@fz-juelich.de](mailto:j.meissburger@fz-juelich.de)



## Inhalt

- Teil 1: Formen der Bedrohung  
Informationsquellen
- Teil 2: Sicherung des Betriebssystems (DriveImagePro, DeployCenter)  
Nutzung systemeigener Sicherheitsfunktionen  
Sicheres Browsen im Web (Internet-Explorer)  
Verschlüsselung von Daten und Kommunikation
- Teil 3: Einrichten der Sicherheitsfunktionen von E-Mail  
(Outlook und Outlook-Express)  
Einrichten eines Virenschanners (F-Prot und NAI)
- Teil 4: Installation eines persönlichen Firewalls  
(AtGuard und Norton Personal Firewall 2002)  
Konfigurationshinweise für JuNet
- *Je nach Zeit und Bedarf:*  
Praktische Vorführung von Viren, Trojanern, Webfiltern und Firewall



## Was ist das Problem .....?

- > (Mehrere ?) 100 Millionen Rechner im Internet
- Weltweite, hochqualifizierte „Hacker“-Gemeinde (Spaß)
- Nationale Nachrichtendienste, Wirtschaftsspionage (Ernst)
- Schaden:
  - Mißbrauch von Ressourcen und Identität des Opfers (Masquerading)
  - Verändern, Kopieren (Mißbrauchen), Löschen vertraulicher Daten
  - Lahmlegen der Gesamtproduktion durch „Denial of Service“-Attacken
  - Wirtschaftlicher Nachteil durch Mehraufwand für die Abwehr
- Realität:
  - Die meisten Attacken verlaufen unbemerkt
  - Sie sind oft Benutzer-initiiert (Web, Email)



## Ein Blick in die „Szene“ ....

**HACKER NEWS NETWORK**  
<http://www.hackernews.com>

**02-10-00** Yahoo, Buy.com, Amazon, E-Bay, CNN, UUNet, Who's Next?  
 contributed by Space Rogue  
**The Day the Internet Melted**  
 Monday's Denial of Service attack on Yahoo was repeated yesterday afternoon at Buy.com and quickly followed by attacks on Amazon, E-Bay, CNN and possibly even

**HN.. THE VOICE OF REASON** - MSNBC  
 BUFFER OVERFLOW

**Chaos Computer Club e.V.**  
 KABELSALAT IST GESUND  
<http://www.ccc.de>

**Defaced Pages Archive**

**alt.2600 (653)**  
 alt.2600.crackz  
 alt.2600.hackerz  
**Newsgroups**

**INTERNET SECURITY REVIEW ONLINE**  
 e-commerce security information, documentation and news from around the globe  
<http://www.isr.net/index1.html>



## Nur ein Beispiel ...



J.Meißburger, FZI- ZAM

Seite 5



## Weshalb ist die Gefahr so groß ?

- Die Zahl der meist anonymen Internet-Nutzer und damit potentieller „Hacker“ steigt ständig
- Windows-Betriebssysteme sind wegen ihrer Verbreitung und ihrem hohen Automatisierungsgrad besonders für Angriffe beliebt, aber Unix-Systeme sind nicht sicherer („root“)
- Informationen und Werkzeuge zum „Hacken“ (Virus construction kits) sind im Internet frei verfügbar und ohne Fachwissen nutzbar
- Viele Anwender betreiben ihre Rechner ohne Schutz- und Sicherungsmaßnahmen zur Wiederherstellung
- Die meisten Betriebssysteme werden vom Hersteller mit einem Maximum an Funktionalität und einem Minimum an Sicherheit ausgeliefert
- Alle Betriebssysteme - selbst Sicherheitssoftware - enthalten Fehler!

J.Meißburger, FZI- ZAM

Seite 6



## Formen der Bedrohung

- **Physikalischer Zugriff**
  - Rechner, **Konsole**, Netze, Datenträger (Field Service !)
- **Psychologie (human/social engineering)**
  - Vertrauen, **Bequemlichkeit**, Gedankenlosigkeit, Uninformiertheit (Hoaxes)
- **Installation schädlicher Software durch den Benutzer**
  - Viren, Würmer, Logische Bomben, **Trojaner**
- **Benutzer-initiierte Ausführung aktiver Inhalte**
  - Webseiten, **E-Mails**, makrofähige (Office-) Dokumente
  - Client-Scripting, Scripting Host, Java, ActiveX
- **Angriffe von außen über das Netz (Hacker-initiiert)**
  - Paßwort-Knacken, Sniffer, Port-Scanner, **Ausnutzung von Softwarefehlern**
  - (Distributed) Denial-of-Service



## Physikalische Sicherheit

- Sensitive Systeme mit Konsolen, Druckern etc. in abgeschlossenen Räumen betreiben, Büros abschließen
- Datenträger (Backups) gegen unbefugten Zugriff physikalisch und durch Paßwortsicherung schützen (Image-Backups, ZIP-Laufwerke)
- Sensitive Information in der Hardware vor Zugriff durch Fremde (Field Service, Hardwaretausch oder Verschrottung) entfernen oder ändern
- Physikalischen Zugriff auf kritische Netzkomponenten (Switches) durch Betrieb in abgeschlossenen Räumen oder Schränken verhindern
- Bei langen Anschlußleitungen auf mögliche Übertragungswege durch Übersprechen oder Störstrahlung achten



## Computerviren

- Programme, die sich in vorhandene Dateien einschleusen oder diese ersetzen und sich selbst replizieren
- MBR (Master-Boot-Record)-Viren werden beim Booten im Hauptspeicher aktiviert und durch Datenträgeraustausch weiterverbreitet
- Dynamisch erzeugte Viren können von Virensclannern zunächst nicht erkannt werden, da ihre Signatur erst bei der ersten Ausführung entsteht (heuristische Erkennungsmethoden)
- Viren können leicht durch sog. Viren-Bausätze erstellt werden; sie können in beliebigen Programmier- oder Scriptsprachen erstellt sein (besonders beliebt: Makro-Viren und vbs-Scripts)
- Viren entstehen täglich neu; deshalb regelmäßig aktuelle Informationen und Software (Sicherheits-Patches) benutzen



## Trojaner

- Software, die unbemerkt installiert wird und u.U. weder in der Taskleiste noch im Task-Manager sichtbar ist (über 100 bekannt)
- Erlaubt über Netz den Fremdzugriff auf alle Systemressourcen wie Bildschirm, Tastatur, Dateisystem bis zur völligen Fernsteuerung des betroffenen Zielsystems
- Kann selbst im off-line-Betrieb alle Daten (wie etwa Tastaturanschläge) lokal zwischenspeichern und bei Netzbetrieb automatisch an einen Adressaten im Netz versenden
- Erlaubt das Verfolgen der Paßworteingabe und unterläuft damit selbst den Schutz von Verschlüsselungssystemen
- Diagnostizierbar nur durch geeignete Virenprogramme und/oder durch Überwachen der zulässigen IP-Verbindungen (persönliche Firewall)
- **Vorsicht:** Hacker-Software nie im Netz und nie ohne vorheriges Image-Backup „ausprobieren“; selbst Client-Software etwa von Trojanern ist schon gefährlich!



## Downloads, Hoaxes, Spam-Mail, Paßwort-Knacken

- Downloads und aktive Inhalte
  - Ausnutzung von Softwarefehlern durch dynamische Web-Seiten (Active Scripting und Scripting von ActiveX-Objekten) zum Ausführen von Programmen und Zugriff auf das Dateisystem
  - Unbemerkttes Überschreiben der Standard-Verbindung zum Internet (DFÜ) mit einer teuren 190-er Telefonnummer
- E-Mail-Bomben, Spam- oder Junk-Mail
  - Einfach löschen, keine Gegenmaßnahmen !
  - Filter einsetzen
  - Warnungen auf Hoaxes überprüfen ( <http://www.stiller.com> )
- Paßwort-Knacken
  - „gute“ Paßwörter verwenden (keine gängigen oder personenbezogene Begriffe)
  - Ablegen von Paßwörtern in Dateien wo möglich vermeiden
  - Paßwortdateien schützen
  - Paßwörter verschlüsseln



## Sniffer, Scanner

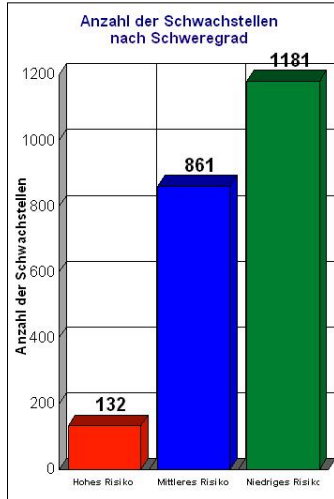
- Sniffer sind Werkzeuge, die den gesamten Verkehr am Netzwerk-Interface eines Rechners abhören („promiscuous mode“) wie etwa der Microsofts Netzwerk-Monitor
  - SNMP-Zugriff auf Netzwerkmonitor verhindern
  - Netzwerkmonitor deaktivieren
  - Sternverkabelung benutzen
- Scanner testen von außerhalb, ob ein IP-Netzdienst auf einer bestimmten IP-Portnummer aktiv ist und nutzen gegebenenfalls Implementierungsschwächen des entsprechenden Dienstes für eine gezielte Attacke
  - Nur wirklich benötigte Dienste aktivieren
  - IP-Verbindungen durch persönliche Firewall überwachen und filtern



## IP Port-Scan

- Ergebnis eines Port-Scans von 47 Unix-Workstations und PCs

und typisches Dienstangebot einer Workstation



| Service Name: | Description:                     | Port#: | Type: |
|---------------|----------------------------------|--------|-------|
| discard       | Discard                          | 9      | TCP   |
| domain        | Domain Name Server               | 53     | TCP   |
| exec          | remote process execution,        | 512    | TCP   |
| finger        | Finger                           | 79     | TCP   |
| ftp           | File Transfer [Control]          | 21     | TCP   |
| httpd         | World Wide Web HTTP              | 80     | TCP   |
| imap          | Interim Mail Access Protocol v2  | 143    | TCP   |
| irc           | irc                              | 6667   | TCP   |
| link          | any private terminal link        | 87     | TCP   |
| login         | remote login a la telnet,        | 513    | TCP   |
| pop3          | Post Office Protocol - Version 3 | 110    | TCP   |
| printer       | spooler                          | 515    | TCP   |
| RPC           | RPC                              | 135    | TCP   |
| shell         | like exec but automatic          | 514    | TCP   |
| smtp          | Simple Mail Transfer             | 25     | TCP   |
| SOCKS         | SOCKS                            | 1080   | TCP   |
| ssh           | SSH Remote Login Protocol        | 22     | TCP   |
| SSH Server    | SSH Server                       | 22     | TCP   |
| sudup         | sudup                            | 95     | TCP   |
| sunrpc        | SUN Remote Procedure Call        | 111    | TCP   |
| tcp-mux       | TCP Port Service Multiplexer     | 1      | TCP   |
| telnet        | Telnet                           | 23     | TCP   |
| uucpd         | uucpd                            | 540    | TCP   |
| X             | X                                | 6000   | TCP   |

| Banner Type   | Banner Text   |
|---------------|---|
| Trusted Hosts | ---- begin list of trusted hosts ----<br>tcoll.ha.kfa-juelich.de<br>---- end list of trusted hosts ---- |
| FTP           | 220 nam FTP server (Version 1.7.212.2 Wed Jul 14 10:24:05 GMT 1999) ready.                              |

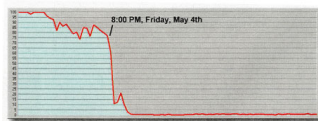
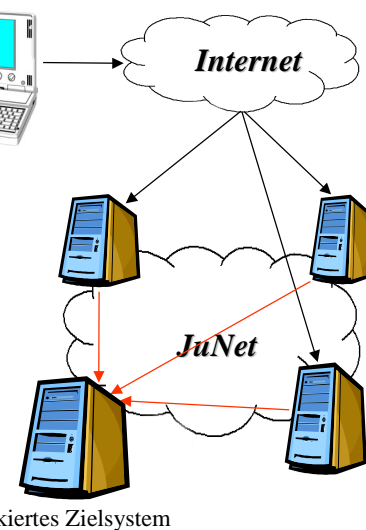
trusted hosts: Hier geht's weiter .....



## distributed Denial-of-Service-Attacke

1. Rechner im Zielnetz durch Port-Scan suchen
2. Rechner übernehmen
3. DNS-Software installieren
4. **Durch Kommando an alle übernommenen Rechner Attacke auf Zielsystem starten**

Angreifer



attackiertes Zielsystem



## Beim Surfen auf Internet-Domains achten!

- Klassische top-level-domains:
  - .mil US-Militär (Initiator des ursprünglichen, atombombensicheren Internet)
  - .gov US-Verwaltung
  - .edu US-Universitäten
  - .com Kommerz (!)
  - .org Organisationen
  - .net Internet
- Länder-Domains:
  - .de Deutschland
  - .fr Frankreich
  - .ch Schweiz
- Neue Domains der „Internet Corporation for Assigned Names and Numbers“ ICANN:
  - .name, .biz, .info, .museum, .pro, .coop, .aero



## Beispiel für Domain-Verwechslung

**whitehouse.com**

**whitehouse.gov**

**Achtung: auch Hacker-Sites benutzen häufig .com !!**



## Risiken vermeiden

- Dubiose Angebote im Netz meiden
- Vorsicht beim Ausfüllen von Formularen, vor Drücken des „OK“-Knopfes immer erst Begleittext lesen
- Mails zweifelhafter Herkunft ignorieren und ungelesen löschen
- Fremdsoftware nur von vertrauenswürdiger Quelle und nach vorheriger Überprüfung mit einem Virens Scanner installieren
- Keine automatischen Downloads und Softwareinstallationen erlauben
- Sensitive, private Informationen nicht unnötig publizieren (Mail, News, Chat)
- Vorsicht auf Fremdsystemen – andere Paßwörter und Verschlüsselung (ssh, ssl) benutzen. Vorsicht bei Hardware-Service !



## Quellen für Sicherheitsinformationen

- C(omputer) E(mergency) R(esponse) T(eam) coordination center
  - <http://www.cert.org>
  - <http://www.cert.dfn.de>
  - <http://cert.uni-stuttgart.de/ticker>
- Sicherheitsseiten von Microsoft
  - <http://www.microsoft.com/security>
  - <http://www.microsoft.com/technet/security/tools.asp>
  - <http://www.microsoft.com/germany/ms/windowsxp/security/intro.asp>
- SANS (System Administration, Networking, and Security) Institute
  - <http://www.sans.org/newlook/home.htm>



## Quellen für Sicherheitsinformationen cont.

- X-Force von Internet Security Systems
  - <https://xforce.iss.net>
- U.S. NAVY InfoSec Sicherheitsseiten
  - <https://infosec.navy.mil/>
- Computer Incident Advisory Capability (CIAC)
  - <http://www.ciac.org/ciac>
- Bundesamt für Sicherheit (BSI), Sicherheits-Handbuch- und CD
  - <http://www.bsi.de>
- ZAM-Dokumentation zum Thema Sicherheit
  - <http://www.fz-juelich.de/zam/net/security>
  - <http://www.fz-juelich.de/zam/docs/tki/tki-PC.html>
  - <news://news.kfa-juelich.de/kfa.zam.security>



## Quellen für Sicherheitsinformationen cont.

- Heise-Verlag on-line (c't, iX)
  - <http://www.heise.de/newsticker>
- Stiller Research
  - <http://www.stiller.com>
- Deutsche Trojaner-Seiten
  - <http://www.trojaner-info.de>
- Clifford Stoll „Kuckucksei“
  - ein wirklich spannender Erlebnisbericht über die Jagd nach einem deutschen Hacker in den amerikanischen Militärnetzen, Fischer-Taschenbuch, ISBN 3-596-13984-8
- Wolfram Gieseke „Das große Internet-Handbuch“, Data Becker, ISBN 3-8158-2261-0
  - <http://www.data-becker.de>



## **Grundsäulen der IT- und Systemsicherheit**

### **ZAM-TKI-0177**

- Bewußter Umgang mit den Gefahren, besonders bei E-Mail und Surfen im Internet
- Nutzung der systemeigenen Sicherheitsmechanismen
- Einsatz zusätzlicher technischer Hilfsmittel wie
  - Antiviren-Software,
  - persönliche Firewalls
  - Datenverschlüsselung
- Regelmäßige Sicherung des Betriebssystems und wichtiger Daten