abraxas INFORMATIK AG

Abraxas Kundeninformationsanlass
18. / 19. September 2002, Zürich / St. Gallen

Hacking, Cracking, Cyberwar – müssen wir wirklich reagieren?

Prof. Dr. Peter Heinzmann, Daniel Wetter
Institut für Internet-Technologien und –Anwendungen,
Fachhochschule Ostschweiz, Hochschule Rapperswil (ITA-HSR)
und cnlab Information Technology Research AG
peter.heinzmann@cnlab.ch, www.cnlab.ch, www.ita.hsr.ch

ita.hsr.ch

HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
Institut für Internet-Technologien und –Anwendungen



University of Applied Sciences Eastern Switzerland (FHO), Rapperswil (HSR)

- Electrical Engineering (195)
- Computer Science (136)
- Mechanical Engineering (103)
- Landscape Architecture (93)
- Urban Planning (68)
- Civil Engineering (65)

660 Students (44% FHO Students)

ITA-HSR: Institute for Internet-Technologies and Applications

www.cnlab.ch



- 1997 HSR spin-off
- 10 Employees
- Internet Security (PGP)
- Internet Application development
- Internet Quality Checks



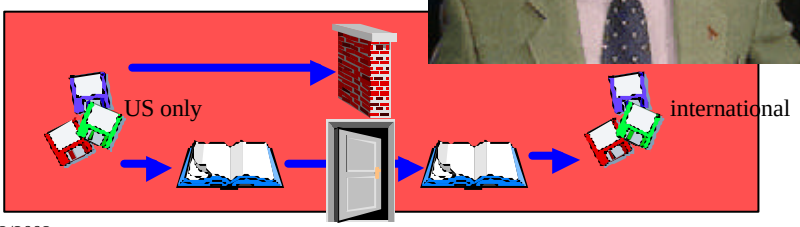


Internet Security

1998: „PGP-Deal“

- E-Mails, File, Disk encryption
- US Export Restriktionen
- **cnlab Software AG** entwickelt internationale Version für NAI



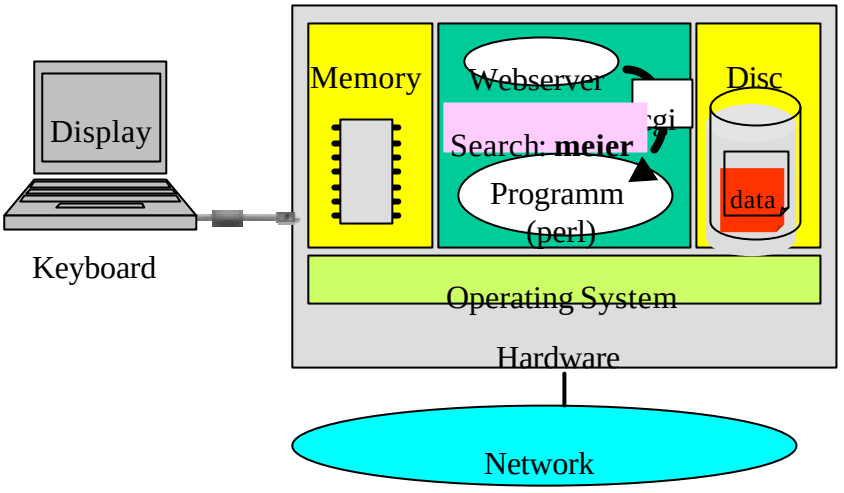


Agenda

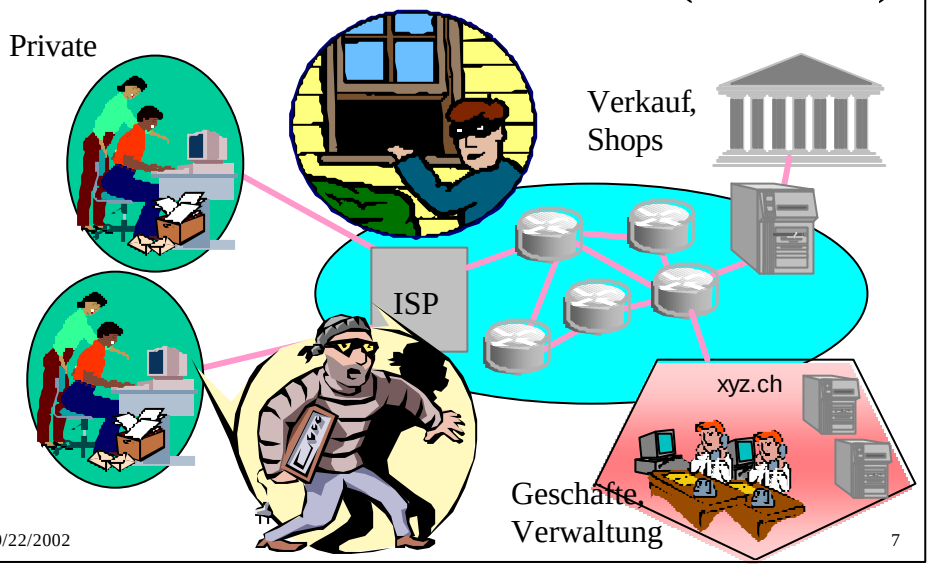
- **Werte, Bedrohungen**
  - Sie können die Security Hype beurteilen
  - Sie gehen bei Security Fragen systematischer vor
- **Hacker Cycle – Hype und Reality (inkl. Demo)**
  - Sie können mögliche Auswirkungen auf Ihr Umfeld abschätzen
  - Sie lernen neue Gefahren kennen
  - Sie erhalten Anregungen zur Risiko Abschätzung
- **Abwehrmassnahmen**
  - Perimeter- / Personal Firewall … Intrusion Detection Systems
- **Rechtslage**
  - Sie kennen Gesetze und Implikationen in Zusammenhang mit Security
- **Zusammenfassung**
  - Wer nicht hören will, muss fühlen … hören allein reicht in der Regel nicht

Was sind unsere Werte?
Welche Bedrohungen gibt es?
Sind wir verletzlich?

Was sind unsere Werte?



Internet Juli 2002:
160 Mio Hosts, 550 Mio Users (weltweit)



Wer will meine Werte?
Wer will mein System attakieren?

- Hacker mit Spieltrieb
- Bösartige Hacker (Cracker)
- Fehlerhafte Software
- Frustrierte Angestellte
- Konkurrenz
- Journalisten
- …

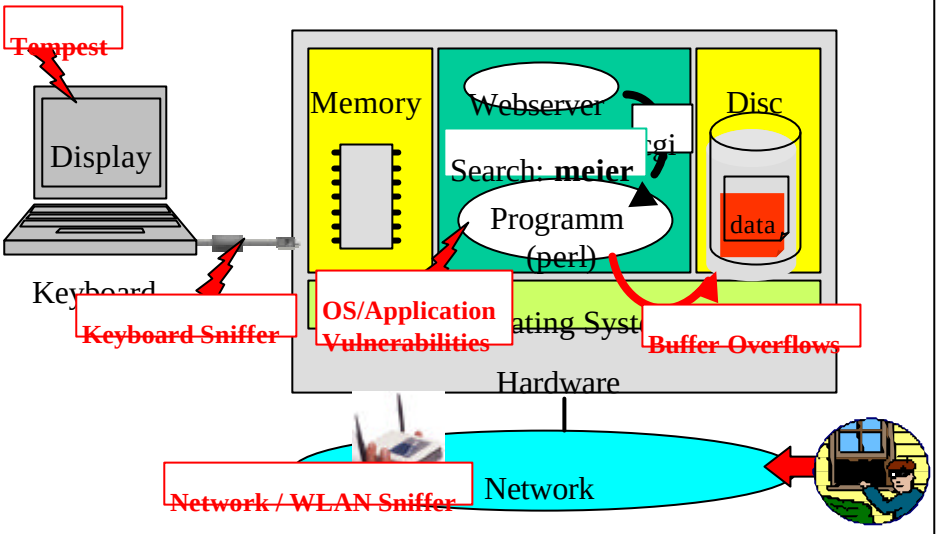
- Geheimdienste
- Staat
- Terroristen
- Natur, Wasser
- Feuer
- …

Cyberwar: Chip Location

- Spiegel TV /VOX 2000
- Cassian von Salomon, Rob Englehardt, John Scheer, **Die Zukunft der Technik "Krieg im Netz“**
  - CIA Microchip in Drucker, damit diese geortet werden können.

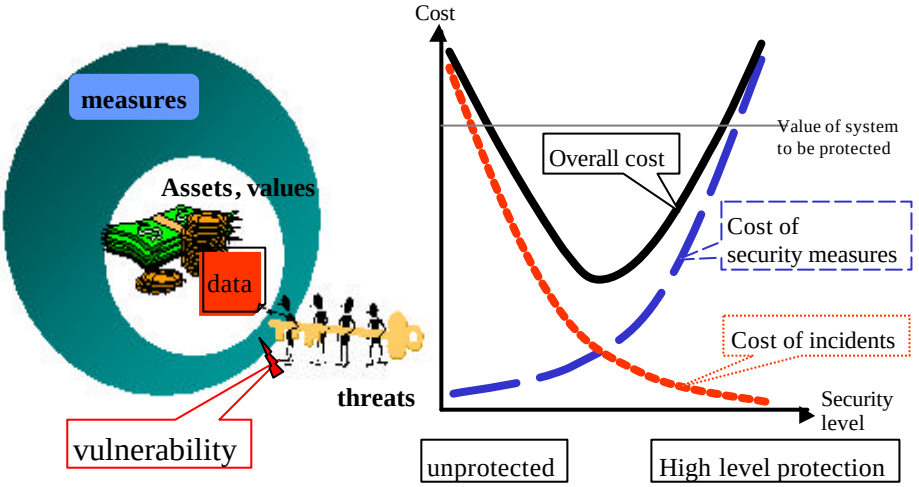


Welche Verletzlichkeiten gibt es?



Welches Risiko gehen wir ein?

"Wert, Schaden" • "Wahrscheinl. eines Zwischenfalls"



Gehe ich wirklich ein Risiko ein? (1)

NIST Statistics on Exploitable Vulnerabilities

Statistics on Remotely Exploitable Vulnerabilities				
Loss Type	**2002**	**2001**	**2000**	**1999**
Availability	164 (26%)	230 (38%)	244 (36%)	109 (31%)
Confidentiality	149 (24%)	161 (27%)	181 (27%)	102 (29%)
Integrity	72 (11%)	29 (5%)	59 (9%)	27 (8%)
Security Protection	396 (63%)	279 (46%)	291 (43%)	150 (43%)

Statistics on Locally Exploitable Vulnerabilities				
Loss Type	**2002**	**2001**	**2000**	**1999**
Availability	21 (11%)	62 (19%)	80 (19%)	39 (16%)
Confidentiality	35 (19%)	54 (16%)	75 (18%)	35 (14%)
Integrity	39 (21%)	70 (21%)	63 (15%)	31 (13%)
Security Protection	137 (73%)	209 (64%)	253 (62%)	158 (65%)

http://icat.nist.gov/icat.cfm?function=statistics

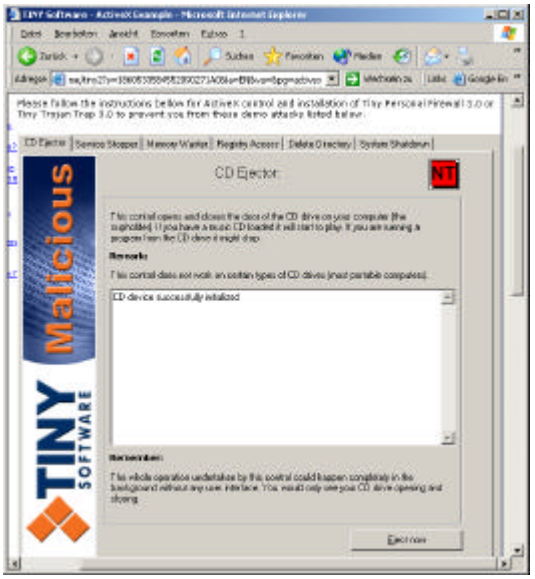
Gehe ich wirklich ein Risiko ein? (2)

Ueberprüfung Ihres privaten Systems

- www.datenschutz.ch
- Hostile ActiveX Demo (www.tinysoftware.com)
- Symantec Security Check (www.symantec.com)
- Microsoft Personal Security Advisor



Demo Hostile ActiveX (www.tinysoftware.com)



Tiger Team, White Hat Hacker, Penetration Testing, ...

- Spiegel TV /VOX 2000
- Cassian von Salomon, Rob Englehardt, John Scheer, **Die Zukunft der Technik "Krieg im Netz“**
  - 1994 Pentagon Hack
  - Pentagon Security Check
    - 8‘932 Attacken
    - 88% davon erfolgreich
    - 5% davon detektiert
    - Nur 1 of 400 Attacken offiziell weitergemeldet


Tuesday, December 31, 1996

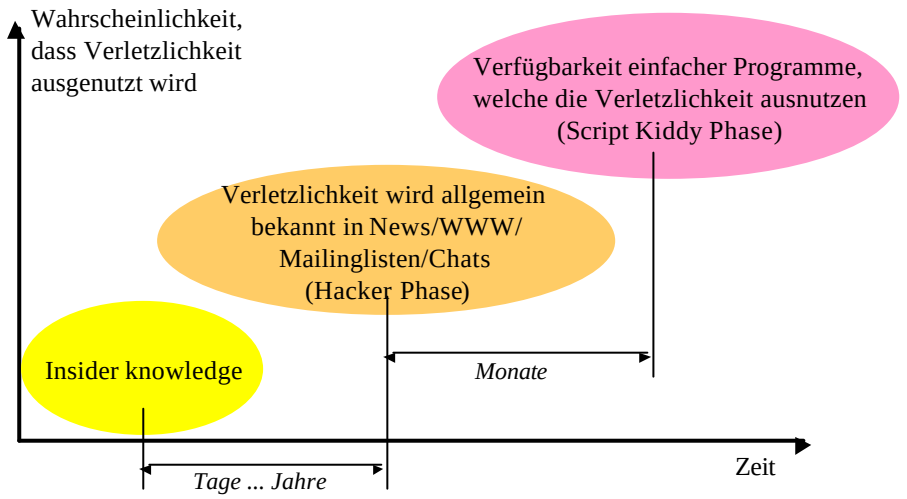
Hackers breach Pentagon on-line

Air Force home page is altered

By John Diamond

The Hacker‘s Cycle – Hype oder Realität

The „Hacker's Cycle“



Insider Knowledge

- Wer sind die „Insider“ ?
  - Aktuelle oder ehemalige Angestellte
  - Entwickler
  - Berater, externe Angestellte, ...
- Beispeile zu Insider-Wissen?
  - Debugging Funktionen in diversen Systemen
  - Versteckte Funktionen (vgl. „Easter eggs“ http://www.eeggs.com/items/8240.html)

Example: Fly The Flight Simulator on Microsoft Excel

How to Work:

1: Open a new Worksheet and Press F5.
2: Type "X97:L97" and press Enter.
3: Press the Tab key, Hold down Ctrl & Shift and left click the Chart Wizard toolbar icon.
4: Use the mouse to move around – Left button reverse thrust, Right button forward thrust.
5: Look around carefully to find the Shrine with the programmers messages and the Blue Lagoon !

http://www.eeggs.com

Veröffentlichung von Verletzlichkeiten

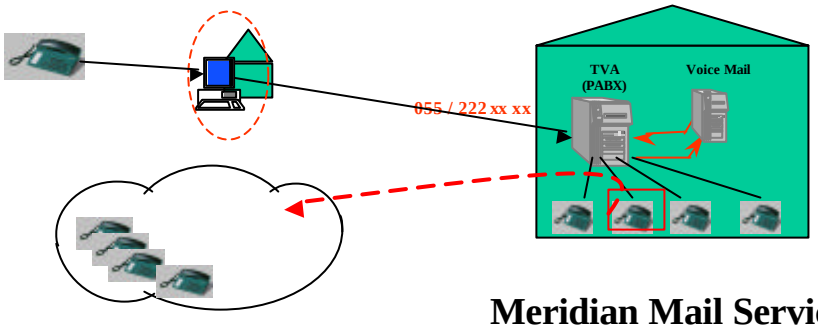


Hacking Bank of America's Home Banking System
Written By: Dark Creaper

This file explains the basics of hacking the Bank of America Home Banking System .....

To connect with the Bank's computer call your local Tymnet service and type the following:
PLEASE ENTER YOUR TERMINAL IDENTIFIER:
APLEASE
7LOGIN: HOME ....

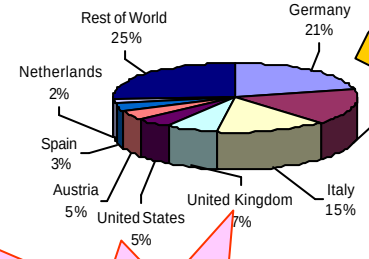
Example: Meridian Mail PABX



Meridian Mail Services

- Call back function
- Call forward function
- ...

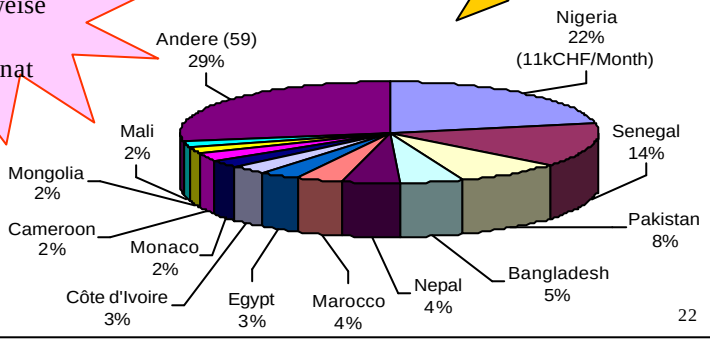
Normale Destinationen(in 1'000 Taxminuten, Juli 2000)



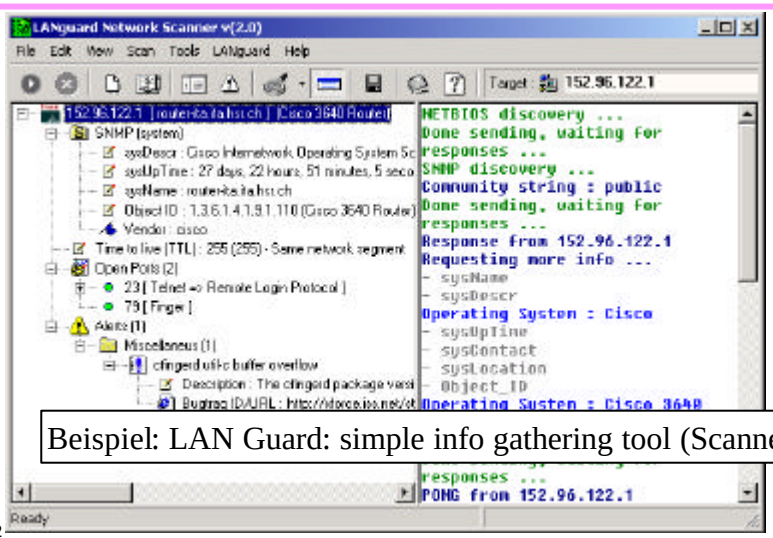
http://google.com/bin/query?p=PBX+hacking+Voice+system+Meridian

Destinationen nach PABX-Voicemail-Fraud
(in 1'000 Taxminuren, Umsatz > Fr. 1'000.00)

Schaden teilweise über 100kFr/Monat



Einfache “public domain” Hacking-Programme (Script Kiddy Tools)

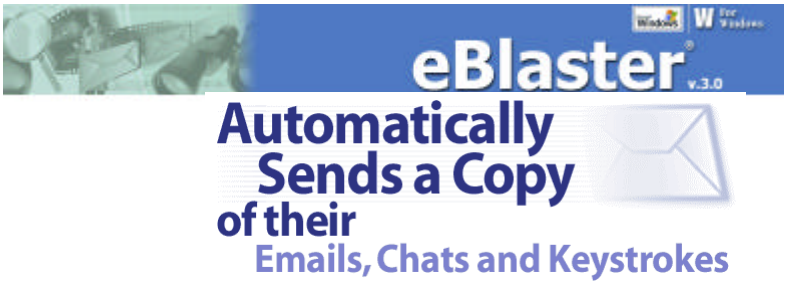


Beispiel: LAN Guard: simple info gathering tool (Scanner)



1998 Pentagon Hacker
Ehud Tenebaum

Demo: Spyware (eBlaster)

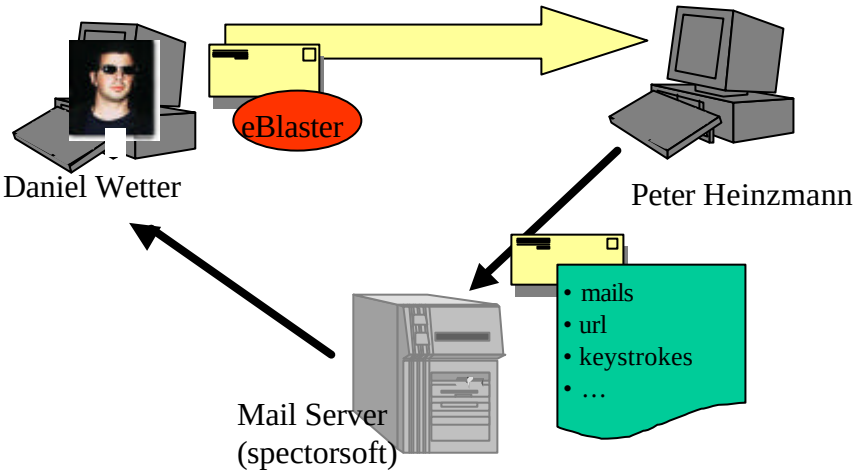


- Überwachungssoftware: Meldet Benutzereingaben an Überwachungsstelle
  - Abgeschickte E-Mail
  - Besuchte Webseiten
  - alle Tastatureingaben (SW Keystroke Sniffer)
  - Meldeintervall, Meldestelle etc. konfigurierbar



Daniel Wetter, cnlab

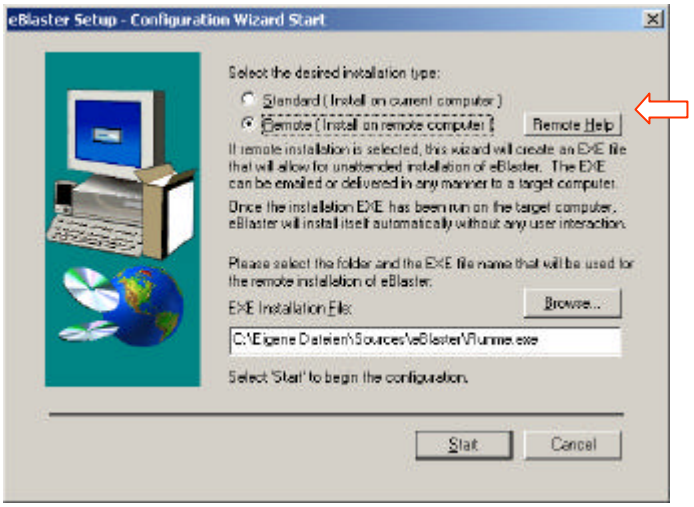
Demo Aufbau (Strategie)





Daniel Wetter, cnlab

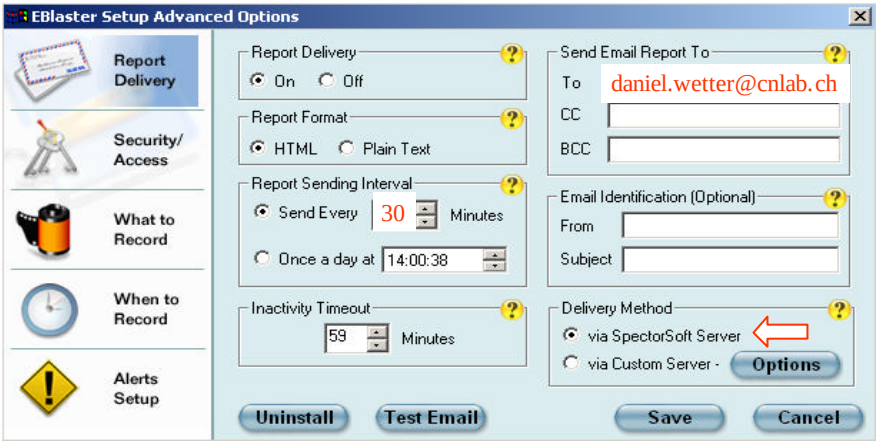
1: eBlaster (SW-Keystroke Sniffer) lokal oder remote installieren





Daniel Wetter, cnlab

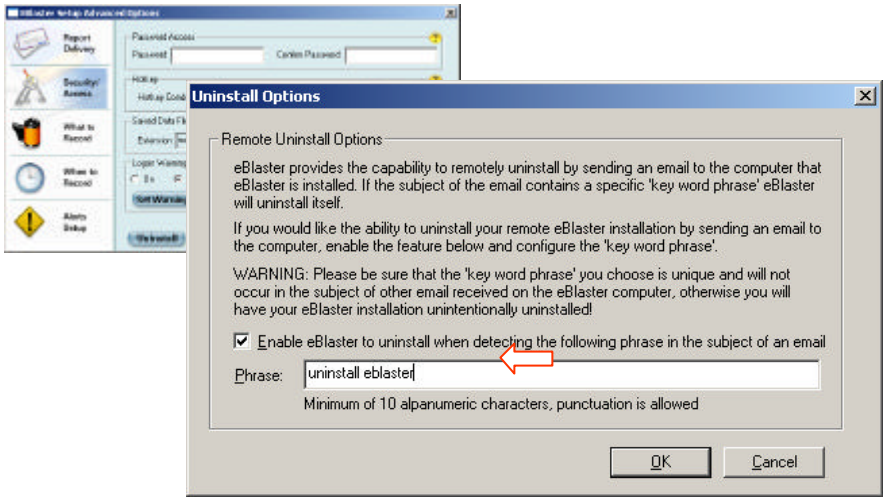
2a: Infizierte exe-Datei erzeugen und konfigurieren: Meldestelle





Daniel Wetter, cnlab

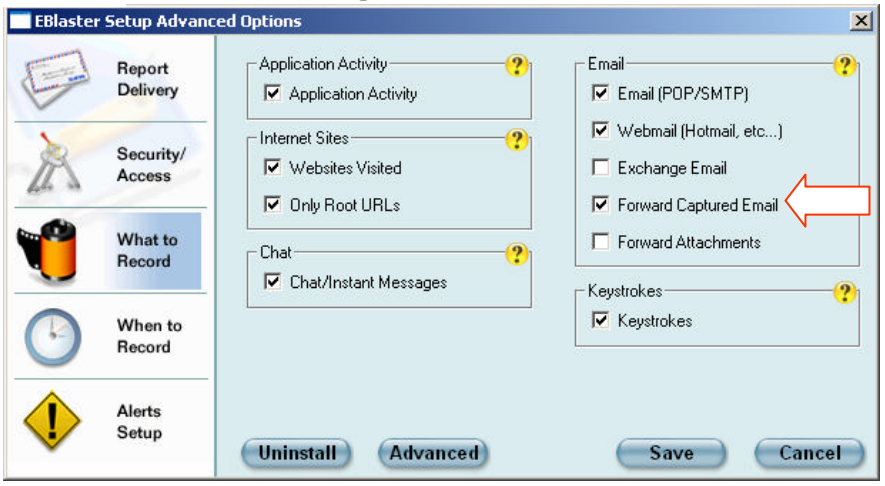
2b: Infizierte exe-Datei erzeugen und konfigurieren: Deinstallation





Daniel Wetter, cnlab

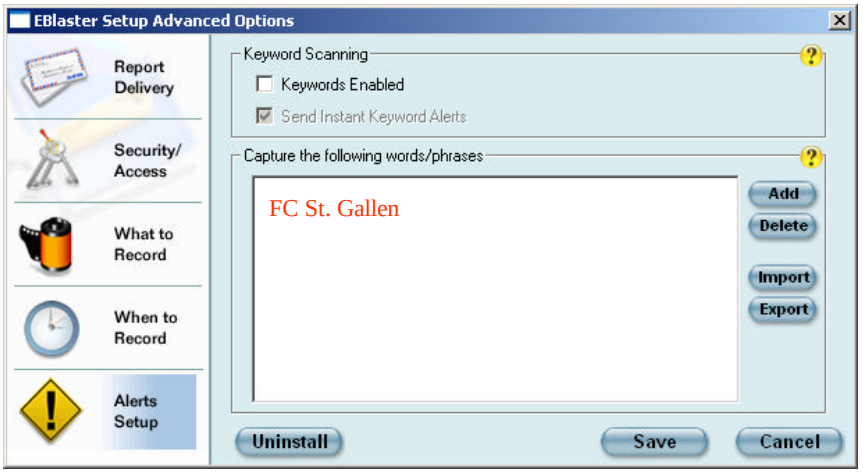
2c: Infizierte exe-Datei erzeugen und konfigurieren: e-Mail Forward





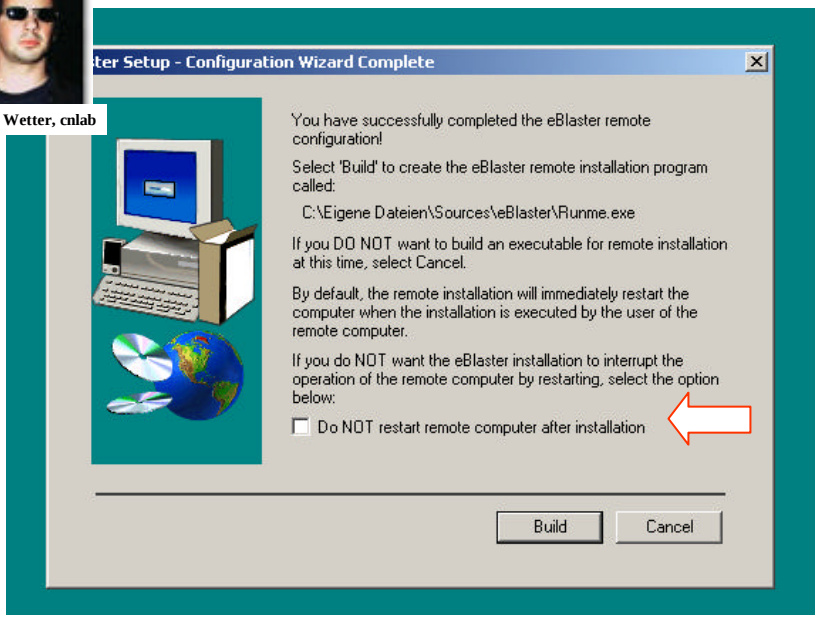
Daniel Wetter, cnlab

2d: Infizierte exe-Datei erzeugen und konfigurieren: Wort-Trigger





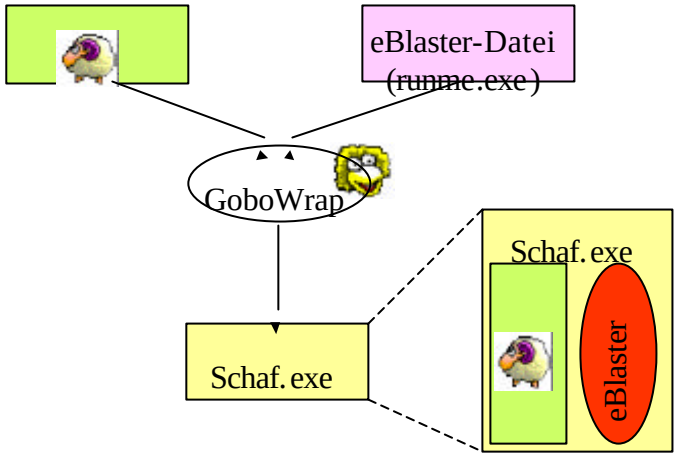
Daniel Wetter, cnlab





Daniel Wetter, cnlab

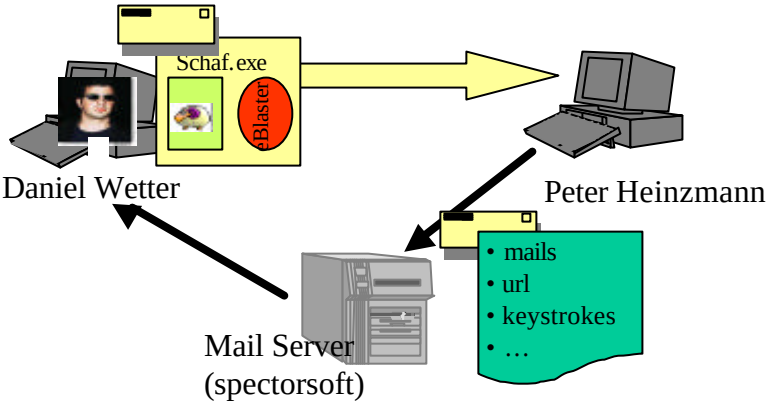
3: Verpacken von eBlaster in andere Programme





Daniel Wetter, cnlab

4: E-Mail mit Attachment verschicken

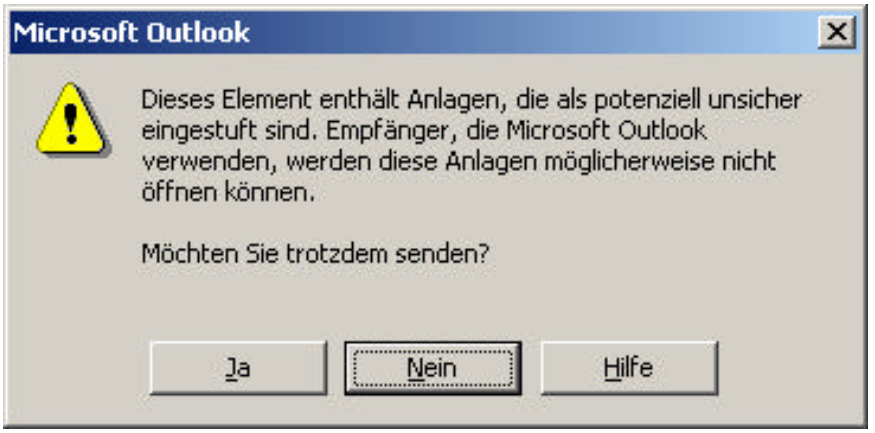


... und auf Resultate warten ☺



Daniel Wetter, cnlab

E-Mail Empfänger



Rechtslage

Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992



Art. 7 Datensicherheit

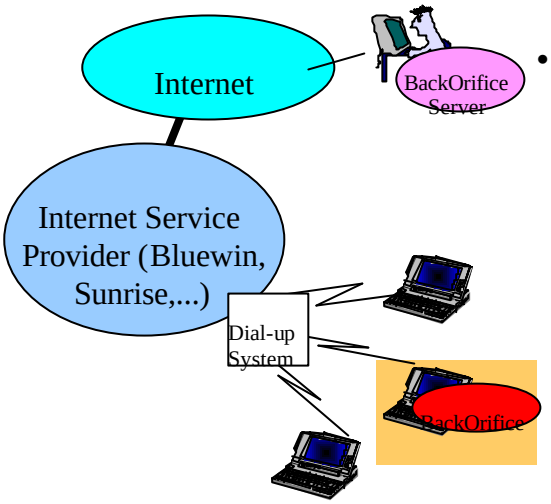
[1] Personendaten müssen durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.

Beispiel: Verletzlichkeit des privaten Rechners (z.B. eines Arztes)



1) Die momentane IP-Adresse Ihres Rechners lautet:
   193.66.123.10
2) Ihr Rechner ist unter folgenden Namen bekannt:
   CHEF0
   Server0
3) Auf Ihrem Rechner sind folgende Ressourcen (Laufwerke, Verzeichnisse, etc.) sichtbar.
   C$
   Kunden

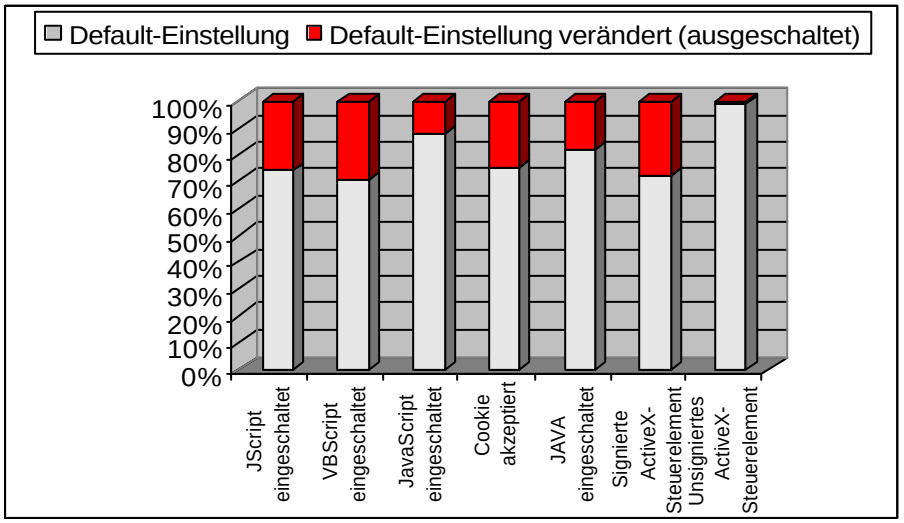
Trojans (BackOrifice, Netbus)



- Remote Control Programme
  - absolute Kontrolle des Rechners
  - Kopieren von Daten
  - Aufbau von Verbindungen zu 906-Nummern
  - …

Typische Browser Konfiguration

(Bänziger/Heinzmann, Rechte für Fremde auf Ihrem Rechner, digma, Okt. 2001, Statistik 1Q2001, vgl. auch http://www.lfd.niedersachsen.de)



Strafgesetzbuch Art. 143: Unbefugte Datenbeschaffung („Hacking-Tatbestand“)

Art. 143

1 Wer in der **Absicht, sich oder einen andern unrechtmässig zu bereichern**, sich oder einem andern elektronisch oder in vergleichbarer Weise **gespeicherte oder übermittelte Daten beschafft**, die **nicht für ihn bestimmt** und gegen seinen unbefugten Zugriff **besonders gesichert** sind, wird mit Zuchthaus bis zu fünf Jahren oder mit Gefängnis bestraft.

2 Die unbefugte Datenbeschaffung zum Nachteil eines Angehörigen oder Familiengenossen wird nur auf Antrag verfolgt.

Art. 143 bis

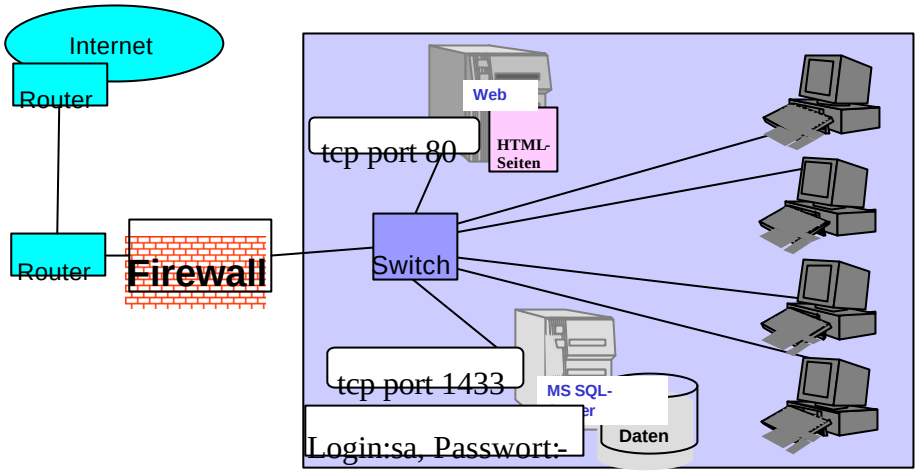
Wer **ohne Bereicherungsabsicht** auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein **fremdes**, gegen seinen Zugriff **besonders gesichertes** Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.

http://www.admin.ch/ch/d/sr/311_0/

Februar 2001: World Economic Forum's Davos Teilnehmer Daten

- Crackers accessed the **forum's registration database** in Davos, which stored data on "about 3,000 forum big shots," who had attended the World Economic Forum (WEF) over the last three years. They were able to **copy all the records** on that server.
- "They got **credit card numbers**, **addresses**, **e-mail addresses**, **home** and **cell phone numbers** and **passport numbers** ".
- Former U.S. president Bill Clinton and his secretary of state, Madeleine Albright were reportedly on the hackers' **list of 27,000 people**, including Microsoft Chairman Bill Gates, and top officials from South Africa, China and other countries.

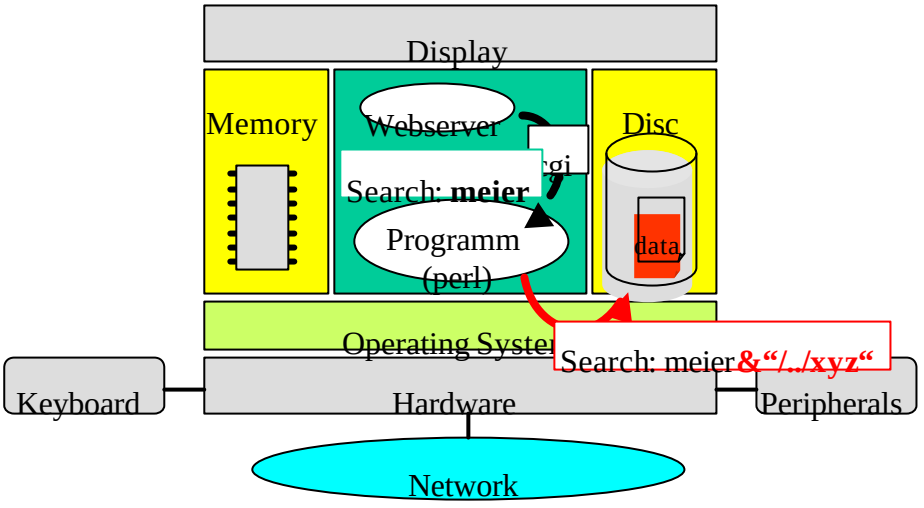
MS SQL Hack



Juli 2001: 250 000 E-Mail-Konten offen

- CD-Rom mit E-Mail-Kontenangaben und Passwort von 185 000 ISP-Kunden
- Betroffen vom Datenloch sind viele Prominente wie der ehemalige Ski-Olympiasieger Bernhard Russi und Tele 24-Chef Roger Schawinski
- Es ist möglich, dass Hacker seit Monaten alle E-Mails, die auf sensible Konten geschickt wurden, in das eigene Postfach weiterleiteten

cgi Hack und clear password file



Strafgesetzbuch Art 144bis: Datenbeschädigung („Virentatbestand“)

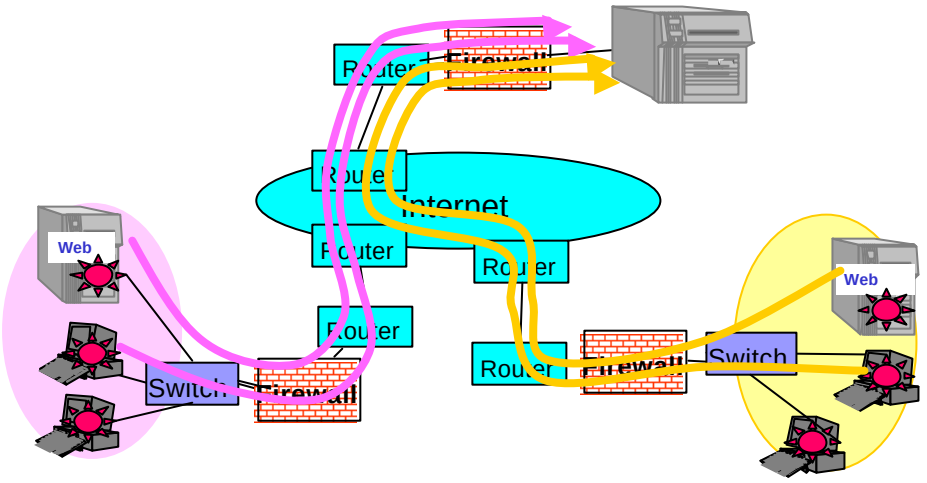
Art. 144bis
Datenbeschädigung
1. Wer unbefugt elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte **Daten verändert, löscht oder unbrauchbar macht**, wird, **auf Antrag**, mit Gefängnis oder mit Busse bestraft.
   Hat der Täter einen **grossen Schaden verursacht**, so kann auf Zuchthaus bis zu fünf Jahren erkannt werden. Die **Tat wird von Amtes wegen verfolgt**.
2. Wer **Programme**, von denen er weiss oder annehmen muss, dass sie **zu den in Ziffer 1 genannten Zwecken verwendet** werden sollen, **herstellt, einführt, in Verkehr bringt, anpreist, anbietet oder sonstwie zugänglich macht** oder zu ihrer Herstellung Anleitung gibt, wird mit Gefängnis oder mit Busse bestraft.
   Handelt der Täter gewerbsmässig so kann auf Zuchthaus bis zu fünf Jahren erkannt werden.

http://www.admin.ch/ch/d/sr/311_0/

Feb. 2000: Denial of Service Attacken

- Einige der am häufigsten besuchten amerikanischen Sites wurden durch Denial-of-Service-Attacken lahmgelegt.
- Betroffen waren CNN, Ebay, Buy.com, Yahoo und Amazon. Alle Sites waren während mehrerer Stunden nicht erreichbar.
- Hacker hatten synchron aus verschiedenen IP-Adressen Anfragen auf die Sites der Anbieter geschossen. Bei Buy.com zum Beispiel prasselten 800 Mbit pro Sekunde auf die Server ein. Das war achtmal mehr, als dieser hätte verarbeiten können.

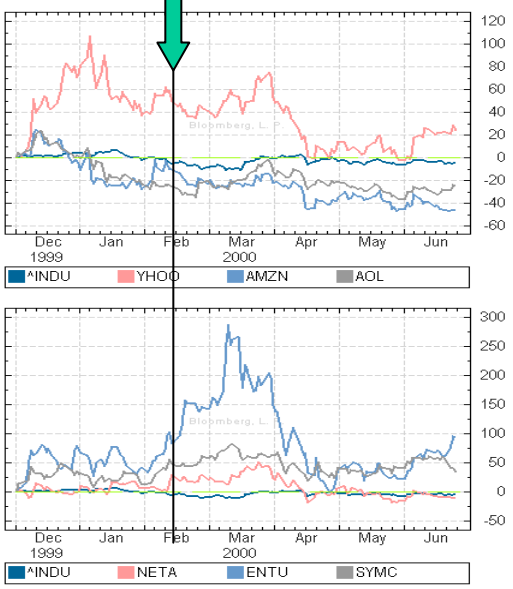
Distributed Denial of Service (DDoS) Attacke



DDoS Tools

- Trinoo / Trin00 (Juni/Juli 1999)
- TFN (Tribe Floot Network) (Juli/August 1999)
- Stacheldraht (Sommer 1999)
- Trinity (Herbst 1999)
- Shaft (November 1999)
- TFN2K (Dezember 1999)
- mstream (April 2000)
- ...

Denial-of-Service Attacks, 7.2.2000



16.9.2002: Linux Worm Hits the Network

A new worm called *Linux.Slapper* is targeting Linux Web servers and creating a network of tens of thousands of drone machines that can be used in a distributed denial-of-service (DDoS) attack. The worm can be used to remotely scan for and recover email addresses on contaminated servers. The Slapper worm had already spread to 11,249 servers running the Apache Web server software on Monday morning, according to F-Secure, which infiltrated the network with a dummy machine. Code Red, one of the most damaging viruses to date, had infected only a few hundred computers in a similar time frame.

Slapper uses a vulnerability discovered only in August, and works only on Apache Linux machines with OpenSSL technology. An upgrade has been made available since the flaw was discovered.

http://www.wired.com/news/linux/0,1411,55172,00.html

Strafgesetzbuch Art. 144bis: Datenbeschädigung („Virentatbestand“)

Art. 144bis
Datenbeschädigung

1. Wer unbefugt elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte **Daten verändert, löscht oder unbrauchbar macht**, wird, auf Antrag, mit Gefängnis oder mit Busse bestraft.
   Hat der Täter einen grossen Schaden verursacht, so kann auf Zuchthaus bis zu fünf Jahren erkannt werden. Die Tat wird von Amtes wegen verfolgt.
2. Wer **Programme**, von denen er weiss oder annehmen muss, dass sie **zu den in Ziffer 1 genannten Zwecken verwendet** werden sollen, **herstellt, einführt, in Verkehr bringt, anpreist, anbietet oder sonstwie zugänglich macht** oder zu ihrer Herstellung Anleitung gibt, wird mit Gefängnis oder mit Busse bestraft.
   Handelt der Täter gewerbsmässig so kann auf Zuchthaus bis zu fünf Jahren erkannt werden.

http://www.admin.ch/ch/d/sr/311_0/

Feb 2002: Strafe für Viren-CD-ROM

- Das Zürcher Obergericht hat einen 30-jährigen EDV-Experten für den Vertrieb einer CD-ROM mit Quellcodes für Computerviren zu zwei Monaten Gefängnis und 5000 Franken Busse verurteilt.
  Die erste Instanz gab nur 300 Franken

Ref: (IPD-074044-A) 25.02.01

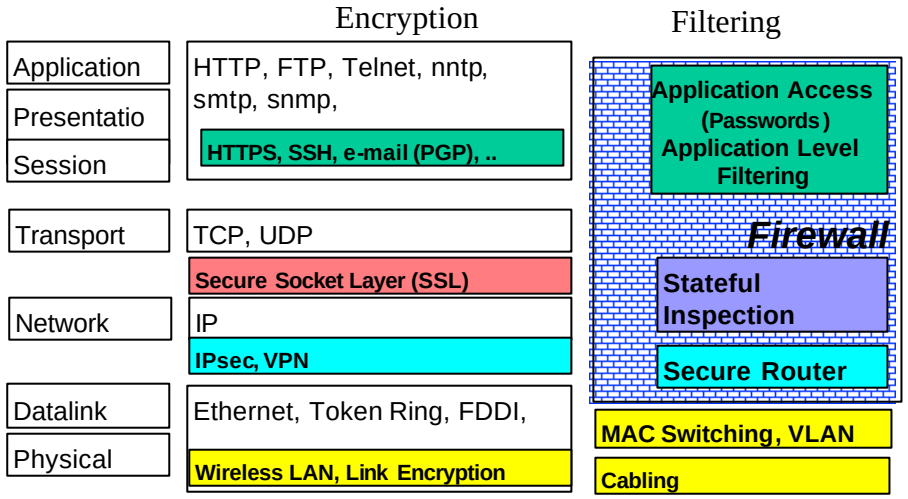
Abwehrmassnahmen

Massnahmen (1)

- Schwächste Stellen identifizieren
  - Technische, organisatorische und betriebliche Aspekte beachten
  - Verschiedene Sicherheitsmassnahmen kombinieren
- Zugang einschränken, Verkehr filtern
  - Physischer Zugang, Firewall, ..., Passworte
- Daten verschlüsseln
  - Auf Speichermedien, in Mail, in Datenpaketen
- Überwachen (Attacken detektieren)
  - Intrusion Detection
  - Vulnerability Testing
- Reagieren
  - Löcher stopfen ... Abschalten
  - Wiederherstellungsprozeduren (Backup ... Informationspolitik)

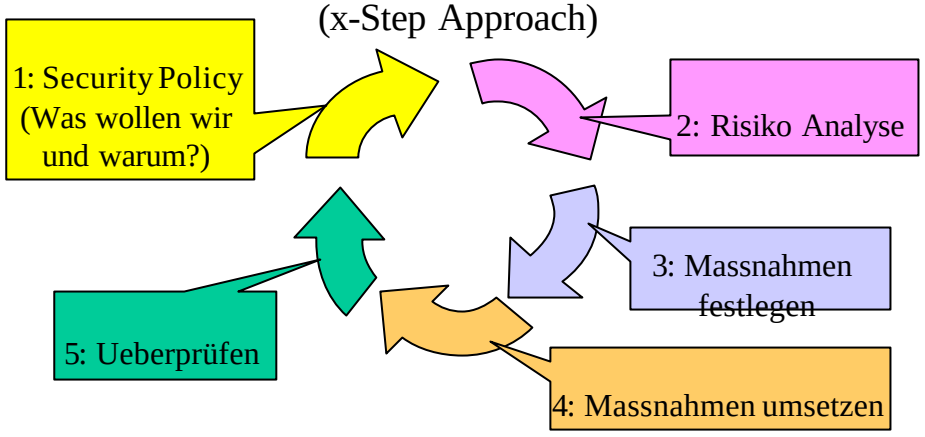
Massnahmen (2)

Verschlüsselung und Filtern im ISO-OSI-Modell



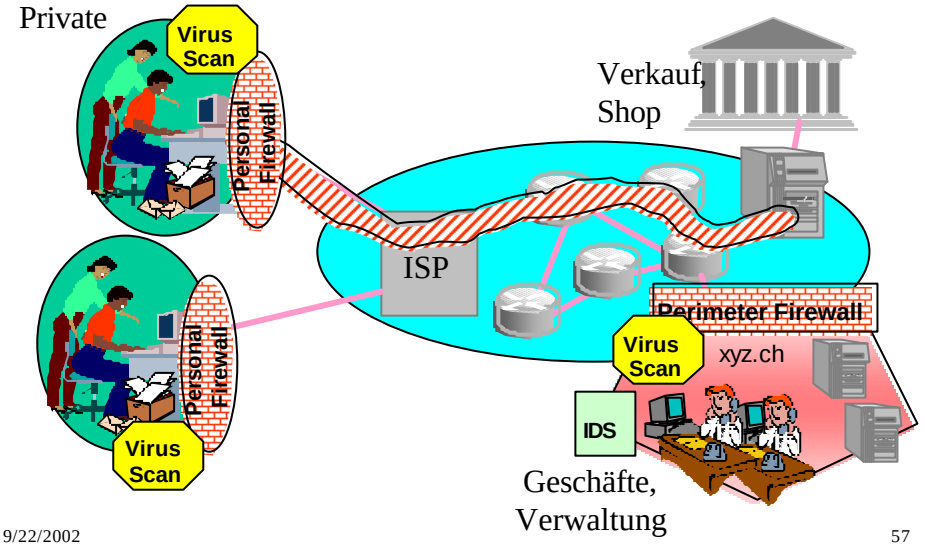
Organisation: Security „Life Cycle“

(x-Step Approach)

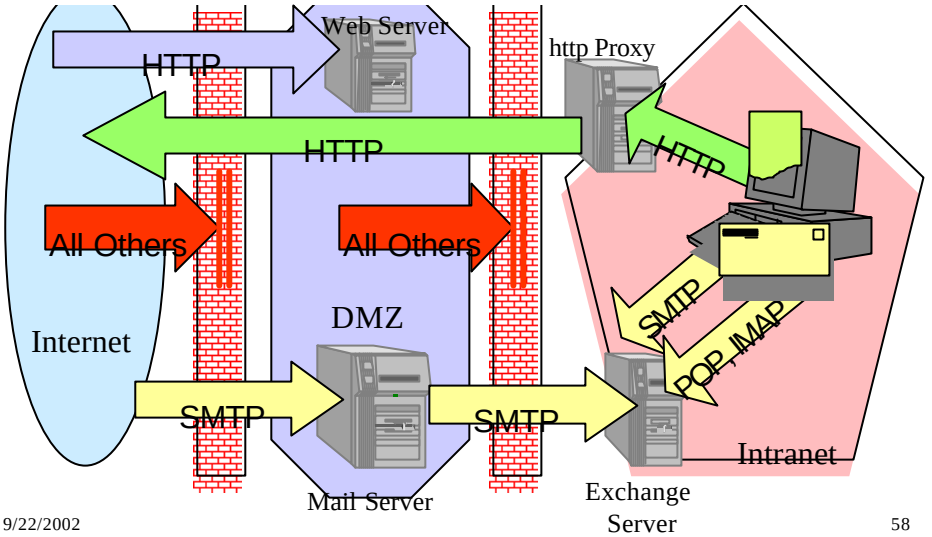


- Bundesamt für Sicherheit in der Informationstechnik (BSI) IT-Grundschutzhandbuch (www.bsi.de)
- DoD Orange Book (http://www.dynamoo.com/orange/summary.htm)
- British Standard 7799 (www.bsi-global.com)

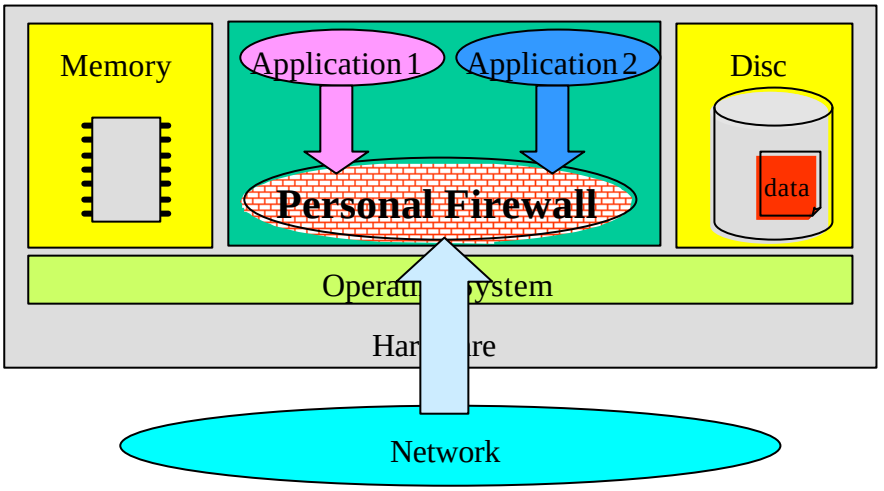
Internet Countermeasures



Typische Perimeter Firewall Konfiguration



Personal Firewall Architektur



Verschlüsselung: PGP Flop



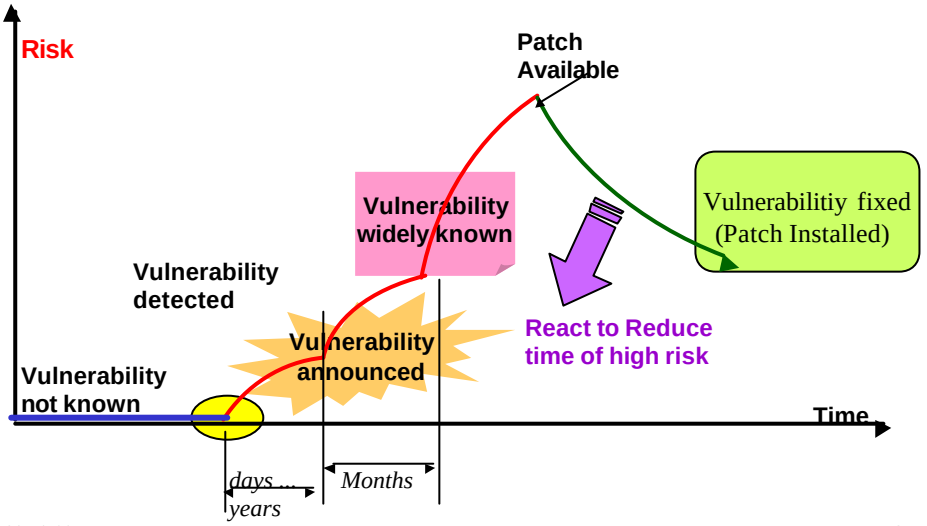
(Gartner Flash, 12 March 2002)

On 7 March 2002, Network Associates (NAI) has discontinued sales of PGP for encrypting e-mail at the desktop

Failure of commercial PGP results from:

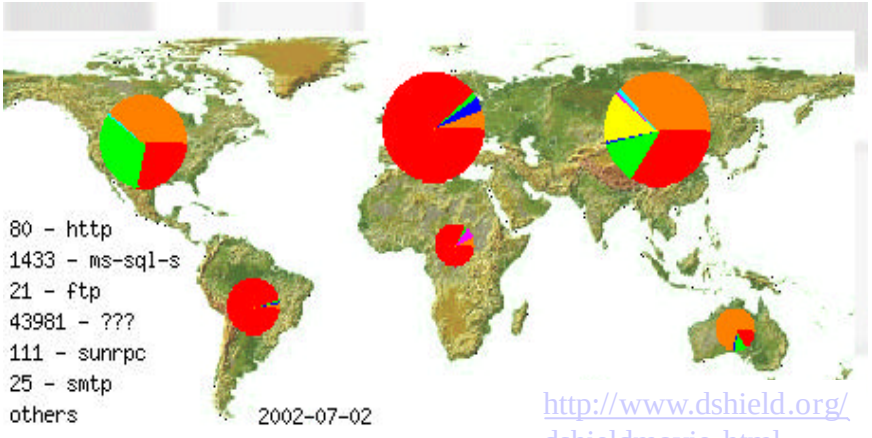
- NAI past organizational problems
- Lack of demand for secure e-mail
- Failure to make PGP easier to use and manage

Minimiere die kritische Zeit im Hacker's Cycle



Frühzeitig Attacken kenne lernen

(dshield.org – Online Attacken Monitor)



http://www.dshield.org/dshieldmovie.html

Wer sind die Treiber für Sicherheit?

	BU‘s View of Security	Security Budget	Operations Management	BU Risk Management
1	• No perception • No awareness	No identified dedicated budget	Deployment	-
2	Seen as technical requirement	100% for infrastructure (from IT budget)	Monitoring and Problem resolution	Infrastructure security, Cyber-incident response team (CIRT)
3	• Business activity damage potential • Need for business transaction security	25% for transaction security (from business budget) 75% for infrastructure security (from IT budget)	Configuration and change management	Security architecture, proactive risk analysis
4	As a quality of the IT environment that can provide competitive advantage	70% for transaction security (from business budget) 30% for infrastructure security (from IT budget)	Transaction incidence management	Transaction risk management

In 2001 appr. 40% of companies are at stage 1 and 50% at stage 2, only 5% of companies are at stage 3 (at stage 3 are mainly financial, defence, health care companies).

In 2003 appr. 30% of companies will be at stage 3.

Source: Gartner Group 2002

10 Punkte zur besseren Sicherheit

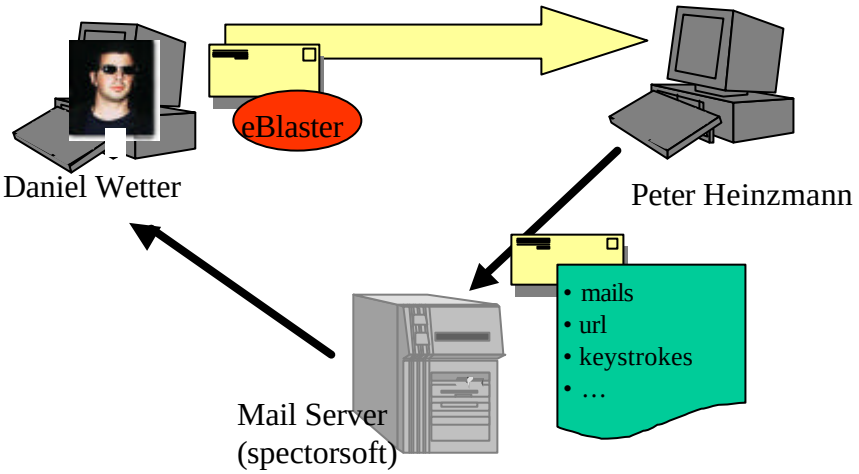
(auf Client und *Server* Seite)

1. Bewusstseinsbildung, Organisation (Betreiber, Anwender, Management)
2. Kontinuierliche Aktualisierung von Anwendungen und Plattformen (Patches, Updates)
3. Aktualisierter, durchgängiger Virenschutz
4. Gute Passwörter (Codesequenzen)
5. *Perimeter Firewall*
6. Personal Firewall
7. Verschlüsselung (Transport, File)
8. *Program Input Checking (cgi, Buffer Overflow)*
9. *Intrusion Detection*
10. Überprüfung



Daniel Wetter, cnlab

Demo: Resultate Sypware





Daniel Wetter, cnlab

Kann man sich gegen eBlaster schützen?

- eBlaster gilt nicht als Virus und wird daher auch nicht als solcher von aktuellen Virenscannern erkannt
  - Norton AV 2002
  - McAfee
- Verkehr an Default eBlaster Destinations-Domain sperren
  - V19170DC0-7597-11D.COM (sofern smtp Server von eBlaster verwendet wird)
- Anti Spy Software wie Nitrouse
  - Die Wirkung solcher Anti Spy Software ist aber noch immer zufriedenstellend



Daniel Wetter, cnlab

Spyware-Verbreitungsarten

- Attachement von Email
- Download von Webseite
- Tauschbörsen (z.B. KaZaA)
- CD Rom mit Autostart









Zusammenfassung
… „so what?“

Müssen wir uns schützen?
… depends …

1. Rechtssituation kann Schutz verlangen
2. Risiko-Abschätzung (Werte, Schäden und Aufwände vergleichen) kann Schutz empfehlen
3. Grundsätzliche Überlegungen können Schutz vorschreiben

Können wir uns schützen?
… ja, aber …

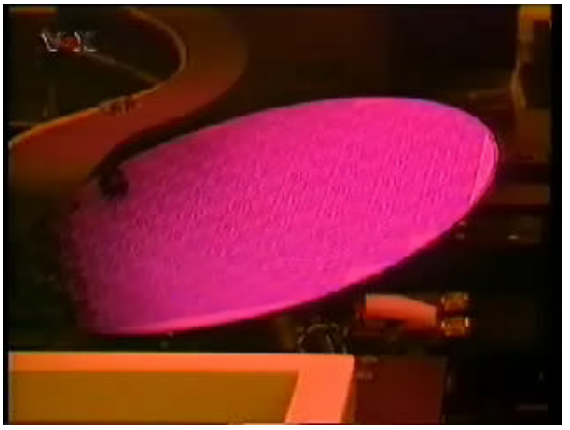
1. Organisatorische, technische und betriebliche Massnahmen ergreifen
2. Schutz bewusst auf „Gegner“ ausrichten
3. Regelmässig den „Schutzgrad“ überprüfen

… aber „there is no free lunch“

… und manche Gegner sind sehr stark …

Biologische Computerviren

- Spiegel TV /VOX 2000
- Cassian von Salomon, Rob Englehardt, John Scheer, **Die Zukunft der Technik "Krieg im Netz“**
  - SiliconViren, Chippen



Wie schützen wir uns gegen Spyware wie beispielsweise eBlaster?

- Organisatorische Massnahmen
  - Problem „Spyware“ thematisieren (Firmen- und Privat- Nutzer sensibilisieren)
  - Gefahr von ausführbaren Programmen allen bewusst machen
  - Nur sehr selektiv Installation von Programmen erlauben (Administratorenrechte einschränken)
- Technische Massnahmen
  - .exe-Dateien aus E-Mail filtern
  - Verbindung zur „eBlaster Domain“ *V19170DC0-7597-11D.COM* sperren
  - Sobald als Virus erkennbar, Virenscanner updaten
  - Spezielle Sypware Detection Programme einsetzen


BRINGING CIVILIZATION TO ITS KNEES...
Goths
HACK
HACK
HACK
Vandals
HACK
HACK
HACK
Huns
HACK
HACK
KEVIN SIERS ©2000 THE CHARLOTTE OBSERVER
Geeks
HACK
HACK
HACK
HACK