

Security

Warum IT-Sicherheit?

Thomas Hildmann

`hildmann@prz.tu-berlin.de`

FSP-PV/PRZ Technische Universität Berlin

Über mich...



Object-ID	Thomas (hildi) Hildmann
Class	Mitarbeiter am PRZ TU Berlin
Security	7 Jahre Berufserfahrung/Forschung
Special Subject	RBAC, Sicherheitskonzepte, alternative Betriebssysteme
Mission	Promotion
Project	Universalverzeichnis

- Homepage: <http://www.prz.tu-berlin.de/~hildmann/>
- E-Mail: <mailto:hildmann@prz.tu-berlin.de>

Was sagt uns dieses Bild?



Was sagt uns dieses Bild?



Was sagt uns dieses Bild?



IT-Security ist ein weites Feld,
das stark in Bewegung ist.

Inhalt

- Warum überhaupt IT-Security?
- Crime vs. Cybercrime
- Die Gegner / Motivation
- Was ist IT-Sicherheit
- Identität im Cyberspace
- Werkzeuge für/gegen Cracker
- Ein Weg durch den IT-Grundschutz
- Einige Fälle und Beispiele
- Tägliche Quellen
- Lesenswertes
- Lösungsansätze für den Arbeitsalltag

Ballmer and Security Experts

“I can tell you I wish those people just would be quiet. It would be best for the world. That’s not going to happen, so we have to work in the right fashion with these security researchers,” Ballmer said at Microsoft’s Worldwide Partner Conference in New Orleans, U.S.

Patrick Gray. Why ballmer just doesn’t get it. ZDNet.com.au, October 2003.

Crime vs. Cybercrime

Die “Tricks” sind in physischer und virtueller Welt identisch.
Unterschiede sind:

- Der Angreifer kann weit vom Opfer entfernt sein.
- Es gibt gute Möglichkeiten als Angreifer seine Identität zu vertuschen oder eine fremde Identität vorzutäuschen.
- Der Angreifer kann komplexe Rechtslagen in unterschiedlichen Ländern ausnutzen.
- Die meisten Tricks kommen mit vergleichsweise wenig finanziellen Aufwand aus.
- Die Tat kann lange verdeckt bleiben bzw. fällt erst sehr viel später auf (Taschendiebstahl vs. leer räumen des gesamten Kontos).
- Es ist oft genug schwer nachzuweisen, dass man selbst das Opfer und nicht der Täter ist (z.B. bei Kreditkartenbetrug).

Mehr E-Commerce \Rightarrow mehr Computerbetrug.

Die Angreifer

- Hacker oder Cracker
- Böswillige Insider
- Industriespionage
- Presse
- Organisiertes Verbrechen
- Polizei
- Terroristen
- Nationale Geheimdienste
- Infowarriors

Massenhack und Hackerethik

21C3: Massenhack löst Welle der Empörung aus

Hacker aus dem Umfeld des Chaos Communication Congress veränderten die Homepages von rund 18.000 Websites, was das LKA auf den Plan rief und Diskussionen über die Hackerethik ausgelöst hat.

Hackerethik

- Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.
- Alle Informationen müssen frei sein.
- Mißtraue Autoritäten - fördere Dezentralisierung
- Beurteile einen Hacker nach dem, was er tut und nicht nach üblichen Kriterien wie Aussehen, Alter, Rasse, Geschlecht oder gesellschaftlicher Stellung.
- Man kann mit einem Computer Kunst und Schönheit schaffen.
- Computer können dein Leben zum Besseren verändern
- Mülle nicht in den Daten anderer Leute
- Öffentliche Daten nützen, private Daten schützen

Was ist IT-Sicherheit?

IT-Sicherheit hat die Aufgabe, Prozesse zur Wahrung der Grundwerte des Daten- und Organisations- sowie Persönlichkeitschutzes (informelle Selbstbestimmung) zu entwickeln, zu pflegen und zu überwachen.

IT-Sicherheitsprozesse müssen dabei jeweils drei Phasen umfassen:

Vorbeugung: z.B. Firewalls, Penetrationstests, Einsatz von Kryptographie

Erkennung: z.B. Intrusion Detection Systeme, Logfiles, Netzwerkmonitoring

Reaktion: z.B. Zusammenarbeit mit Strafverfolgung, Disaster-Recovery, etc.

Aus ‘Highlights 2004’

- Ein ungepatchtes Windows System überlebt nur noch 4 Minuten im Internet
- Hollywood: Trinity benutzt `nmap`
- Cisco IOS Quellcode weggekommen
- Convenience optimized patch releases
- Neues Berufsbild: Lebensstilberater für datenbank-optimiertes Leben
- Raubkopierer missbrauchen 11.800 FTP Server, haben Arbeitsteilung (Scannen, Hacken, Uploaden)
- Würmer googeln jetzt!
- Vulnerabilities in Online-Spielen
- Exploits unter Verwendung von Peripheriegeräten

Vom Passwort zur Biometrie

Probleme bei Passwörtern:

- Abhören, Mitlesen, ...
- Standardpasswörter
- Trivialpasswörter
- Wörterbuchattacken

Alternativen:

- PIN/TAN-Verfahren, Einmalpasswörter
- Speicherkarten
- Smartcards
- Biometrie

John

```
hildmann on henze: /users/prz/hildmann
henze:/tmp # john prz.passwd
Loaded 173 password hashes with 145 different salts (Traditional DES [24/32 4K])
gast          (gast)
              (marcel)
              (datouwa)
              (othman)
              (klaus)
              (ifbwo)
              (ingrid)
guesses: 7   time: 0:00:00:15 23% (2)  c/s: 528403  trying: pmc7 - chicken7
Session aborted
henze:/tmp #
```

Masterpassword

Patch beseitigt Backdoor-Passwort bei USV

APC, Hersteller von unterbrechungsfreien Stromversorgungen (USVs), hat einen Patch veröffentlicht, um ein fest einprogrammiertes Passwort (“TENmanUFactOryPOWER”) aus den optional erhältlichen Netzwerk-Management-Karte zu entfernen. Dem vorangegangen war die Veröffentlichung eines Security Advisory auf Bugtraq, in dem auf das Backdoor-Passwort hingewiesen wurde, mit dem der unautorisierte Zugriff auf das Management möglich ist.

Quelle: <http://www.heise.de/security/news/meldung/44899>

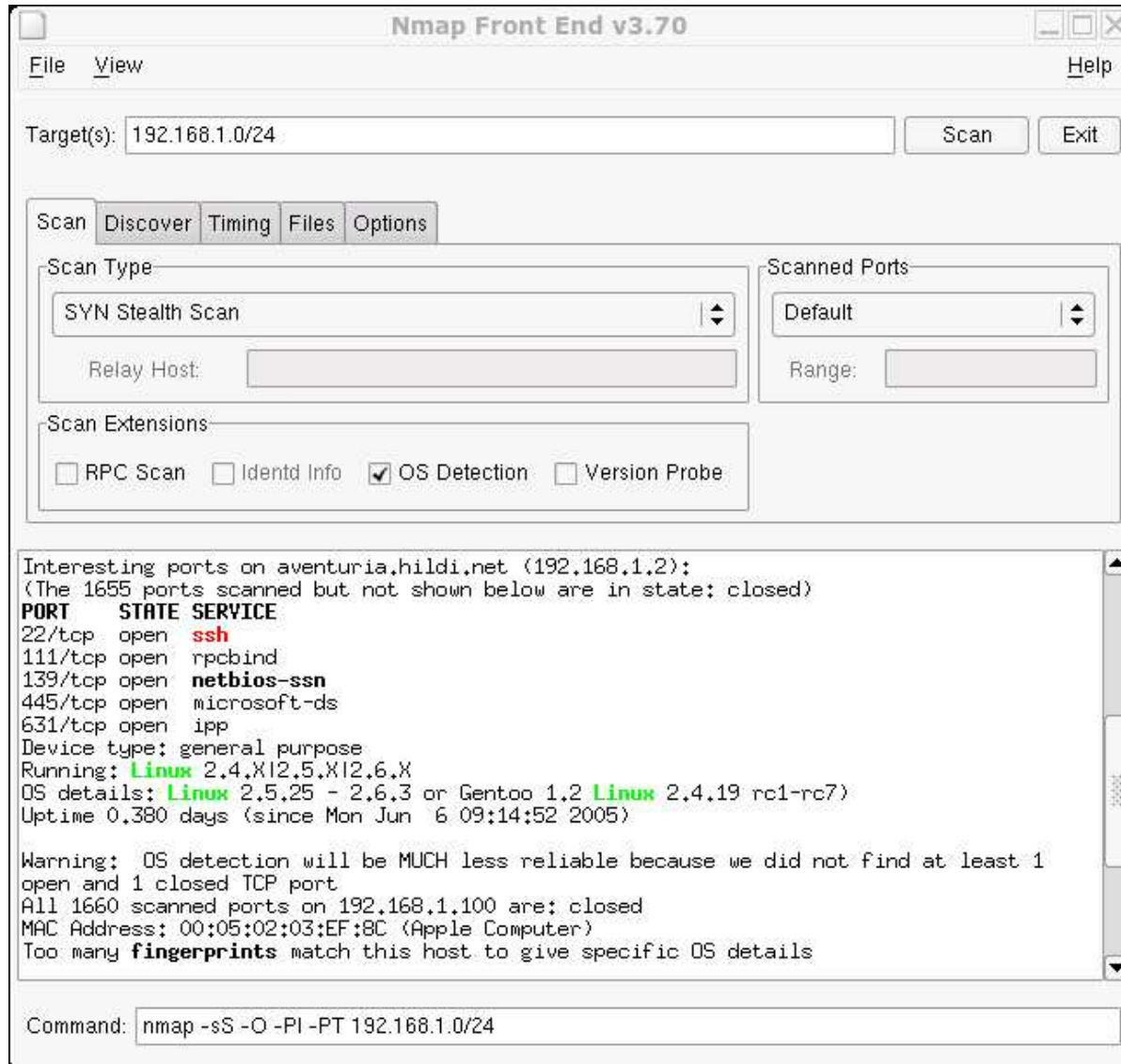
Werkzeuge

- Scanner
- Paßwort-Knacker
- Sniffer
- Firewalls
- Logging- und Audit-Tools

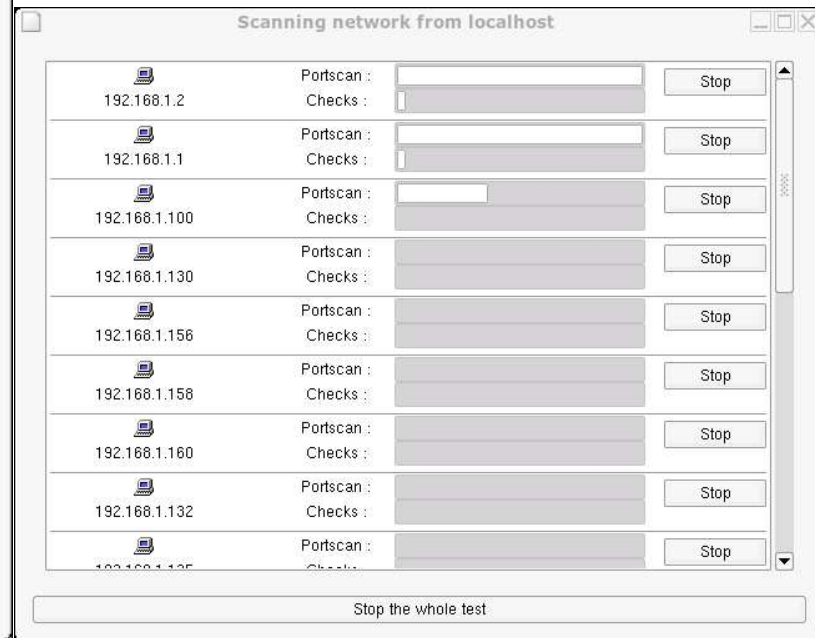
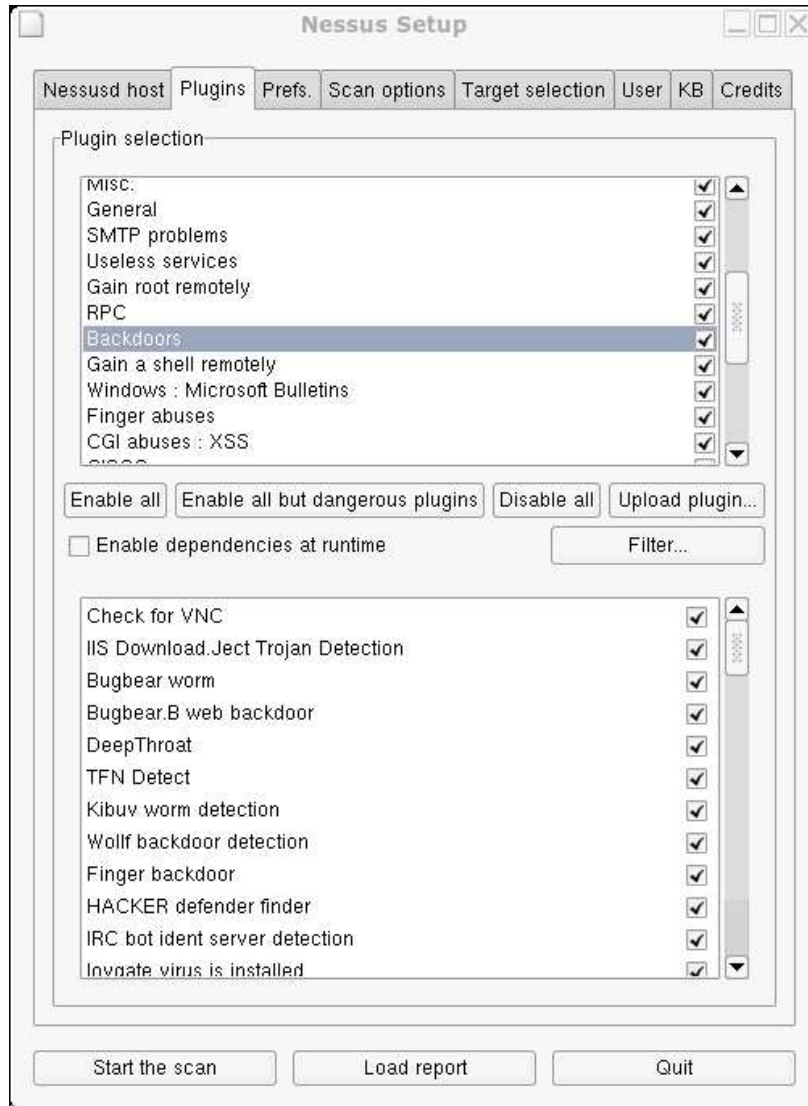
Top 75 Security Tools:

<http://www.insecure.org/tools.html>

Werkzeug: nmap



Werkzeug: nessus 1/2



Werkzeug: nessus 2/2

The screenshot shows the Nessus 'NG' Report window. The window is titled 'Nessus "NG" Report' and contains several panels:

- Subnet:** A list of subnets, with '192.168.1' selected.
- Host:** A list of hosts, with '192.168.1.2' selected.
- Port:** A list of ports and services, with 'microsoft-ds (445/tcp)' selected.
- Severity:** A list of severity levels, with 'Security Hole' selected.
- Description:** A text area containing the following information:
 - The following shares can be accessed using a NULL session :
 - IPC\$ - (readable?, writeable?)
 - Solution :** To restrict their access under WindowsNT, open the e go to the 'sharing' tab, and click on 'permissions'
 - Risk factor :** High
 - CVE :** CAN-1999-0519, CAN-1999-0520
 - BID :** 8026
- Additional Information:** A text area containing the following information:
 - . It was possible to log into the remote host using a NULL sessio
 - The concept of a NULL session is to provide a null username ar a null password, which grants the user the 'guest' access

At the bottom of the window, there are two buttons: 'Save report...' and 'Close window'.

Werkzeug: ethereal

The screenshot shows the Ethereal (Wireshark) interface with the following details:

- Filter:** (ip.addr eq 192.168.1.2 and ip.addr eq 192.168.1.1) and (t
- Packet List:**

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.2	192.168.1.1	TCP	50639 > http [SYN
2	0.000075	192.168.1.1	192.168.1.2	TCP	http > 50639 [SYN
3	0.000111	192.168.1.2	192.168.1.1	TCP	50639 > http [ACK
4	0.000148	192.168.1.2	192.168.1.1	HTTP	GET /scripts/cvsl
5	0.000185	192.168.1.1	192.168.1.2	TCP	http > 50639 [ACK
6	0.000221	192.168.1.1	192.168.1.2	HTTP	HTTP/1.0 404 Not
7	0.000258	192.168.1.2	192.168.1.1	TCP	50639 > http [ACK
8	0.000294	192.168.1.1	192.168.1.2	TCP	http > 50639 [FIN

Frame 4 (125 bytes on wire, 125 bytes captured)

- Ethernet II, Src: 00:02:e3:12:76:8d, Dst: 00:80:c8:12:12:7a
- Internet Protocol, Src Addr: 192.168.1.2 (192.168.1.2), Dst Addr: 192.168.1.1
- Transmission Control Protocol, Src Port: 50639 (50639), Dst Port: http (80)
- Hypertext Transfer Protocol

Raw Data:

```
0000  00 80 c8 12 12 7a 00 02 e3 12 76 8d 08 00 45 00  ....Z... ..v...E
0010  00 6f ad c9 40 00 40 06 09 6c c0 a8 01 02 c0 a8  .o..@.@. .l.....
0020  01 01 c5 cf 00 50 ed e0 33 27 00 61 d9 9d 50 18  ....P.. 3'.a..P
```

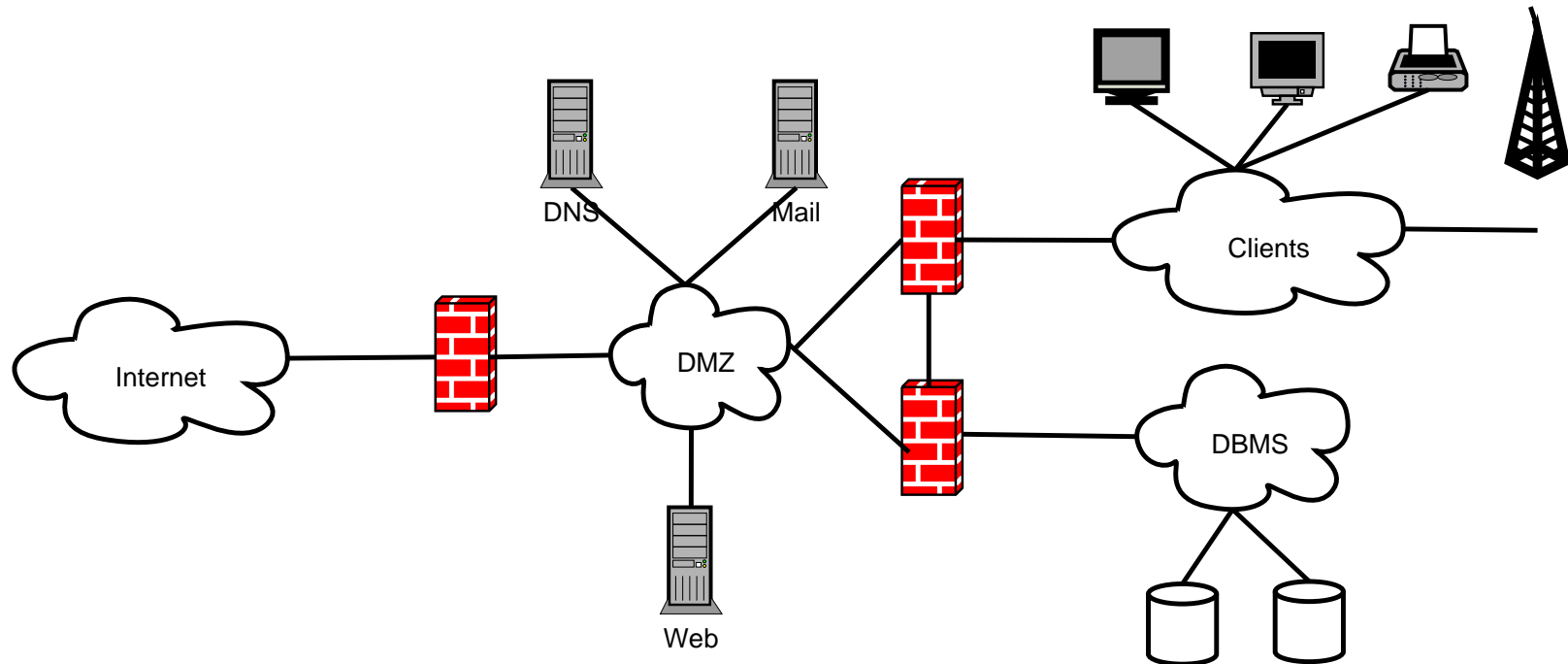
File: (Untitled) 42 KB | P: 437 D: 10 M: 0 Drops: 56

Logfileanalyse

Dictionary Attack

```
Jun  6 19:59:38 cleese sshd[16117]: Invalid user abhijit from
206.123.122.154
Jun  6 19:59:38 cleese sshd[552]: input_userauth_request: invalid
user abhijit
Jun  6 19:59:38 cleese sshd[552]: Failed password for invalid user
abhijit from 206.123.122.154 port 34222 ssh2
Jun  6 19:59:38 cleese sshd[16117]: Failed password for invalid user
abhijit from 206.123.122.154 port 34222 ssh2
Jun  6 19:59:38 cleese sshd[552]: Received disconnect from
206.123.122.154: 11: Bye Bye
Jun  6 19:59:40 cleese sshd[1380]: Invalid user abhiram from
206.123.122.154
Jun  6 19:59:40 cleese sshd[1557]: input_userauth_request: invalid
user abhiram
Jun  6 19:59:40 cleese sshd[1557]: Failed password for invalid user
abhiram from 206.123.122.154 port 34272 ssh2
```

Firewalls



Firewalls dienen der Filterung des Datenverkehrs zwischen zwei Teilnetzen mit unterschiedlichem Sicherheitsniveau.

Firewalls

- Firewalls filtern (im besten Fall)
- Personal Firewalls sind bedingt nützlich (im besten Fall)
- Lücken in Firewalls z.B. durch WLANs
- Wo mache ich das Loadbalancing?
- DBMS im Clientnetz?
- Gefahr durch Netzwerkdrucker und embedded Systems
- Backup durch die DMZ?
- Aufgabentrennung vs. Wartung der Systeme
- Firewall mit mehreren Interfaces vs. Heterogenität

Personal Firewalls

Windows Dienste abschalten: <http://dingens.org/>

Fefe zu Personal Firewalls:

<http://www.fefe.de/pffaq/halbesicherheit.txt>

Bagle schaltet PFs ab:

<http://www.heise.de/security/news/meldung/50568>

Fehler in ZoneAlarm:

<http://www.heise.de/security/news/meldung/44786>

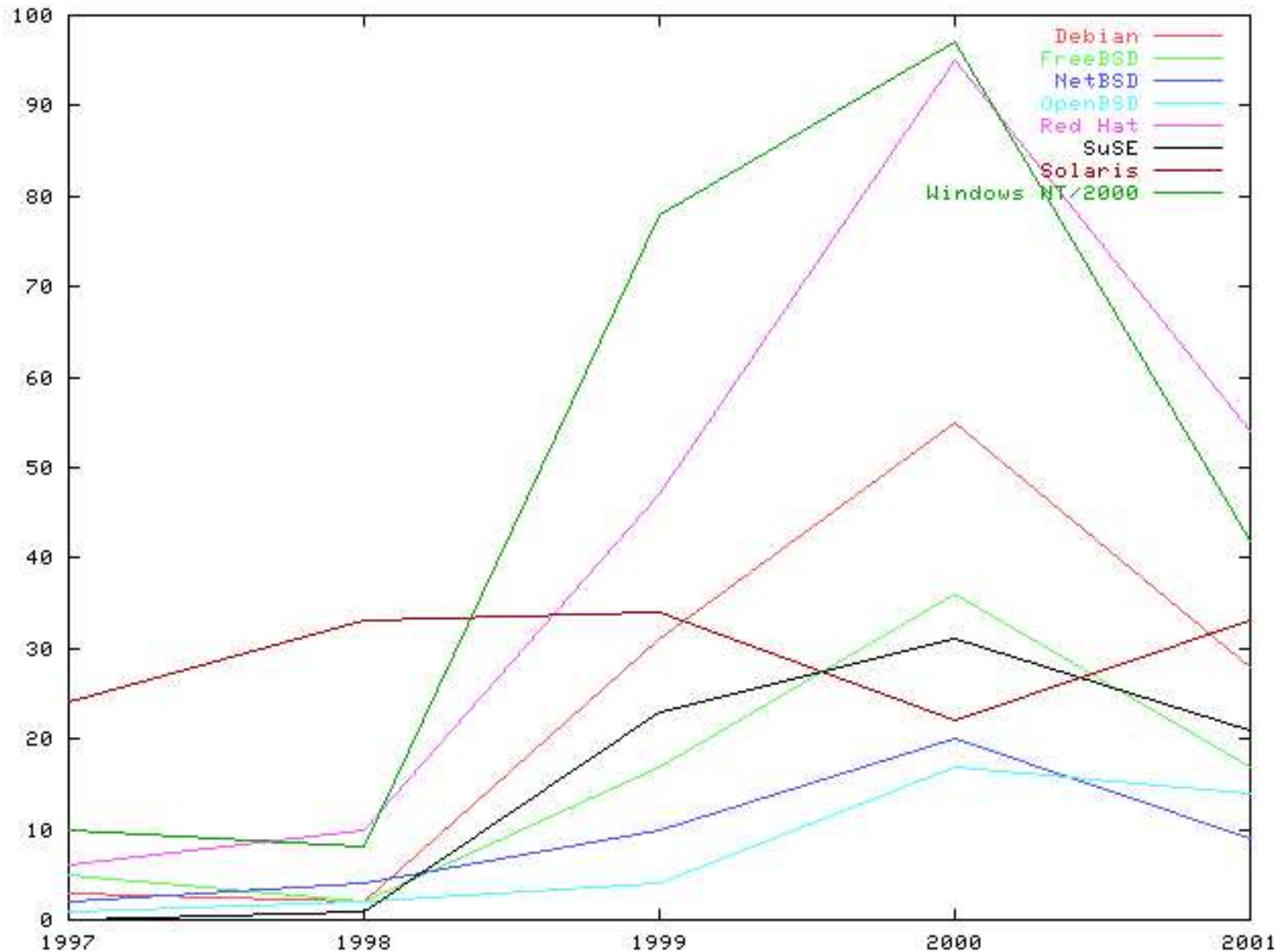
ZoneAlarm: <http://www.zonelabs.de/>

Kerio Personal Firewall: http://www.kerio.com/us/kpf_home.html

WWW-Software für Windows (32-Bit):

<http://www.tu-berlin.de/www/software/win32.shtml>

Betriebssysteme und Distributionen



Betriebssysteme und Plattformen

- Apple MacOS X
- BSD: FreeBSD, OpenBSD, NetBSD, DragonFly
- Linux: Debian, RedHat, SuSE, Knoppix, etc.
- Microsoft: Windows 2k, XP, etc.
- SUN Solaris

Unix History: <http://www.levenez.com/unix/>

Sicherheit: Grundwerte 1/2

● Datenschutz

Vertraulichkeit: Dateien dürfen nur von autorisierten Benutzern gelesen werden.

Übertragungssicherheit: Die Übertragung vom Rechner zu anderen Rechnern, Geräten oder zum Benutzer kann nicht ausgespäht werden.

Privatheit: Persönlichkeitsdaten bzw. Anonymität müssen gewahrt bleiben.

● Datensicherheit

Funktionalität: Hardware und Software soll erwartungsgemäß funktionieren.

Integrität: Software und Daten dürfen nicht unbemerkt verändert werden.

Authentizität: Überprüfbare Echtheit und Glaubwürdigkeit einer Person oder eines Dienstes

Verbindlichkeit: Urheber von Veränderungen müssen erkennbar sein und dürfen Veränderung nicht abstreiten können.

Sicherheit: Grundwerte 2/2

● Randthemen sind

Nicht-Anfechtbarkeit: Der Nachweis, dass eine Nachricht versendet und empfangen worden ist.

Zugriffssteuerung: Reglementierung des Zugriffes von außen

Verfügbarkeit: Nutzbarkeit

Quelle:

<http://de.wikipedia.org/wiki/Computersicherheit>

Einige Golem-Meldungen

AN.ON: Anonymisierungsdienst durch CCC-Server unterstützt:

<http://www.golem.de/0504/37632.html>

Taglich 24 neue Computer-Wurmer im ersten Halbjahr 2004:

<http://www.golem.de/0409/33703.html>

Trojanisches Pferd stiehlt Kontozugsdaten:

<http://www.golem.de/0406/32058.html>

Wurm gibt sich mit deutschem Text als Microsoft-Patch aus:

<http://www.golem.de/0403/30130.html>

Filenapping: Schadling erpresst Losegeld fur Dateizugriff:

<http://www.golem.de/0505/38263.html>

MP3-Killer: W32/Nopir-B macht Musikarchive platt:

<http://www.golem.de/0504/37702.html>

Gefährdungen

- Höhere Gewalt
 - Personalausfall, Ausfall des IT-Systems, Blitz, Feuer, ...
- Organisatorische Mängel
 - Fehlende oder unzureichende Regelungen, Unzureichende Kenntnisse über Regelungen, ...
- Menschliche Fehlhandlungen
 - Verlust der Datenträger beim Versand, Unbeabsichtigte Datenmanipulation, Fahrlässiges Löschen von Objekten, ...
- Technisches Versagen
 - Ausfall der Stromversorgung, Datenverlust bei erschöpftem Speichermedium, Unsichere kryptographische Algorithmen, ...
- Vorsätzliche Handlungen
 - Diebstahl, Vandalismus, Anschlag, Gebührenbetrug, Trojanische Pferde, Computer-Viren, ...

Heise-Meldungen

Trojaner verschlüsselt Daten und Dokumente:

<http://www.heise.de/security/news/meldung/59819>

Kritische Schwachstelle in Virenscannern von Computer Associates und ZoneLabs:

<http://www.heise.de/security/news/meldung/59804>

800 Server-Passwörter in Tauschbörsen:

<http://www.heise.de/security/news/meldung/59523>

Zahl bekannter Handy-Schädlinge steigt auf 71:

<http://www.heise.de/newsticker/meldung/58877>

Forscher knacken Bluetooth-PINs gekoppelter Geräte:

<http://www.heise.de/newsticker/meldung/60384>

Phishing-IQ-Test: Finde die echten und falschen Mails:

<http://www.heise.de/newsticker/meldung/60345>

Gegenmaßnahmen

- Infrastruktur
- Organisation
- Personal
- Hardware und Software
- Kommunikation
- Notfallvorsorge

Quelle: <http://www.bsi.de/gshb/index.htm>

Make or Buy?

- 24x7x364
 - Backup
 - Sicherheit
 - Skalierbarkeit
 - Monitoring
 - Ausfallsicherheit
 - Reporting
 - Statistiken
- Brauchen Sie das?
Können Sie das?
 - Seriöse Firmen gehen zum Profi
 - Ein Administrator ist kein Sicherheitsexperte

Frei nach Axel Nennker

Outsourcing

- Ihre Firmendaten in fremden Rechenzentrum?
- Outsourcing von Sicherheit: Will man das?
- Die sind doch viel zu teuer! Ich mache das mit LAMP!
- Die sind doch viel zu inflexibel... In der heutigen Zeit haben wir zwei Updates täglich / wöchentlich!

Frei nach Axel Nennker

Das BSI GSHB hat ein eigenes Kapitel zum Thema Outsourcing:

<http://www.bsi.de/gshb/deutsch/baust/03010.html>

Sicher programmieren

- Validate All Input
 - Command line
 - Environment Variables
 - File Names
- Avoid Buffer Overflow
- Structure Program Internals and Approach
 - Follow Good Software Engineering Principles...
 - Secure the Interface
 - Separate Data and Control
- Carefully Call Out to Other Resources (Libs, Syscalls, ...)
- Send Information Back Judiciously
- Secure Programming for Linux and Unix HOWTO:
<http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO.html>
- Securing Microsoft Windows:
<http://www.dwheeler.com/essays/securing-windows.html>

Elektromagnetische Emission

- Schutz von WLANs vor DoS durch Emission?
- Abhören ist nicht nur vom WLAN möglich
- RFID ist nur die logische Fortsetzung
- Neue Betätigungsfelder
 - Eisverkauf auf Parkplatz durch RFID-DoS
 - RFID-gesteuerte Anschläge auf Personen
- Konzept Tapete, LCD, Serverschrank geht auf (gemessen im TUB Trustcenter)

Bookmarks

Intrusion Detection FAQ: <http://www.sans.org/resources/idfaq/index.php>

Heise Security: <http://www.heise.de/security/>

Ins Internet - Mit Sicherheit: <http://www.bsi-fuer-buerger.de/>

Bundesamt für Sicherheit in der Informationstechnik: <http://www.bsi.bund.de/>

DFN CERT: <http://www.cert.dfn.de/>

NT-Dienste sicher konfigurieren: <http://www.ntsvcfg.de/>

GNU Privacy Guard: <http://www.gnupg.org/>

Thomas Hildmann's Bookmarks - Security:

<http://www.hildania.de/users/hildi/bookmarks/computer/security/>

NTBugtraq: <http://www.ntbugtraq.com/>

SecurityFocus: <http://www.securityfocus.com/>

Hoax-Info Service: <http://www.tu-berlin.de/www/software/hoax.shtml>

Chaos Computer Club e.V.: <http://www.ccc.de/>

Books to mark

Literatur

- [1] Bruce Schneier, *Secret & Lies – IT-Sicherheit in einer vernetzten Welt*, dpunkt.verlag GmbH, Weinheim 2001
- [2] Clifford Stoll, *Kuckucksei – Die Jagd auf die deutschen Hacker, die das Pentagon knackten*, 1989
- [3] Anonymous, *Hacker's Guide – Sicherheit im Internet und im lokalen Netz*, Markt und Technik, Haar bei München 1999
- [4] Cheswick, William R. et. al., *Firewalls und Sicherheit im Internet*, Addison-Wesley, 1996

To be continued...

Thomas Hildmann's Weblog:

<http://cleese.prz.tu-berlin.de/researchwiki/ThomasHildmannsWeblog>

Hildis privates Weblog:

<http://www.hildania.de/users/hildi/weblog/>