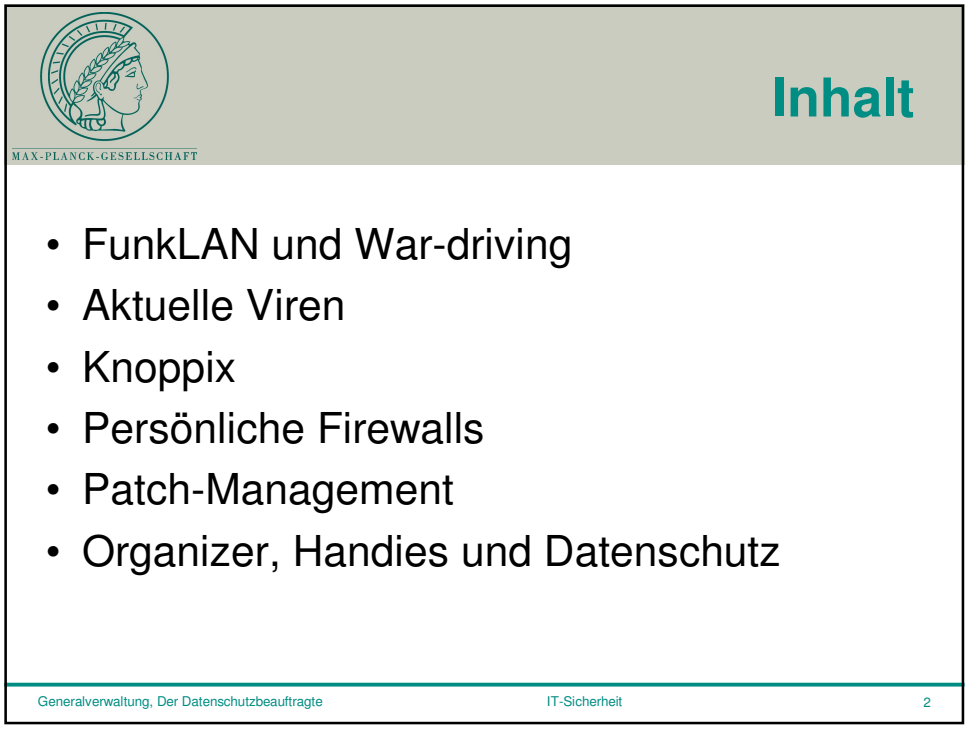


MAX-PLANCK-GESELLSCHAFT

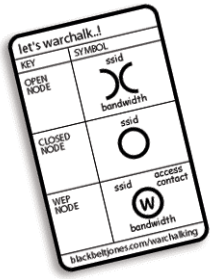
War-Driving

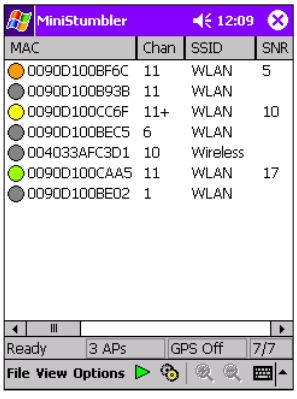
- laptop + wireless + GPS + car

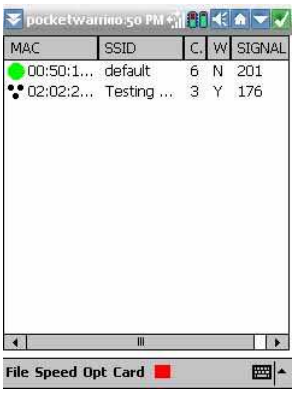
MAX-PLANCK-GESELLSCHAFT

Beispiele

- PocketPC reicht
  - Mit GPS Unterstützung







MAX-PLANCK-GESELLSCHAFT

Wardriving in München

- Moment-aufnahme Mai 2002

Dank an Studenten

Generalverwaltung, Der Datenschutzbea

MAX-PLANCK-GESELLSCHAFT

Aktueller Stand

- Durch Marketing-Aktionen der DSL-Anbieter wurden viele Wireless-DSL-Router verkauft.
  - viele FunkLAN-Karten verkauft
  - Centrino-Notebooks haben FunkLAN fest eingebaut
- FunkLAN vielfach unverschlüsselt

MAX-PLANCK-GESELLSCHAFT

Viren

- Sircam
  - Verschickt Dokumente aus „Eigene Dateien“ (Datenschutz!!)
  - Adressen z.T. aus dem Browser Cache
  - Eigene SMTP-Routine: unabhängig vom E-Mail Klienten
- Code Red
  - Greift IIS von MS über Bufferoverflow an
- Nimda
  - Greift IIS von MS über Bufferoverflow an
  - Verbreitet sich auch über E-Mail und Netzwerkfreigaben
  - Verbreitet sich über Javascript auf WWW-Seiten (readme.eml)
- Code Red und Nimda führen zu ersten Anzeichen von Instabilitäten im Internet
- BugBear

MAX-PLANCK-GESELLSCHAFT

BugBear

```
November 01, 2002, 02:03:12 PM - COM2 start to dial-up
November 01, 2002, 02:05:34 PM - Unrecognized access from 211.221.183.42:1025 to UDP port 137
November 01, 2002, 02:14:44 PM - Unrecognized access from 61.243.1.53:1124 to UDP port 137
November 01, 2002, 02:17:33 PM - Unrecognized access from 210.77.59.9:1025 to UDP port 137
November 01, 2002, 02:20:40 PM - Unrecognized access from 200.203.166.189:61158 to UDP port 137
November 01, 2002, 02:20:55 PM - Unrecognized access from 200.81.29.137:1025 to UDP port 137
November 01, 2002, 02:21:40 PM - Unrecognized access from 200.170.178.13:1024 to UDP port 137
November 01, 2002, 02:26:41 PM - Unrecognized access from 200.165.24.14:1029 to UDP port 137
November 01, 2002, 02:26:54 PM - Unrecognized access from 211.44.131.254:1027 to UDP port 137
November 01, 2002, 02:27:42 PM - Unrecognized access from 209.99.239.75:1025 to UDP port 137
November 01, 2002, 02:29:30 PM - Unrecognized access from 212.48.151.228:1030 to UDP port 137
November 01, 2002, 02:31:17 PM - Unrecognized access from 61.160.204.38:1027 to UDP port 137
November 01, 2002, 02:37:40 PM - COM2 start to hang-up

November 02, 2002, 09:26:45 AM - COM2 start to dial-up
November 02, 2002, 09:28:35 AM - Unrecognized access from 61.254.250.83:1025 to UDP port 137
November 02, 2002, 09:31:38 AM - Unrecognized access from 63.76.11.124:25783 to UDP port 137
November 02, 2002, 09:31:54 AM - Unrecognized access from 211.228.181.185:1030 to UDP port 137
November 02, 2002, 09:39:32 AM - Unrecognized access from 200.128.18.213:1027 to UDP port 137
November 02, 2002, 09:42:31 AM - Unrecognized access from 62.11.128.29:1028 to UDP port 137
November 02, 2002, 09:50:17 AM - Unrecognized access from 203.79.191.23:1029 to UDP port 137
November 02, 2002, 09:52:27 AM - Unrecognized access from 155.239.70.43:1027 to UDP port 137
November 02, 2002, 09:55:37 AM - COM2 start to hang-up
```

Aktuelle Viren/Würmer

- Anfang August: Lovsan/32.Blaster
  - rpc-Sicherheitslücke, keine Benutzerintervention
  - Mitursache Stromausfall im Nordosten der USA?
- Mitte August: Sobig.F
  - Massives E-Mail Aufkommen
- Mitte September: W32.Gibe/Swen
  - Social Engeniering auf Basis IExplorer Fehler
- Ende September: QHosts-1
  - Ändert DNS und Proxy Einstellungen
- 24.10.03: Sober
  - erster deutschsprachiger Virus

Was tun?

- Viren Scanner auf jeden Windows-Rechner!
- Signaturen täglich aktualisieren!
- Welcher ist egal, Aktualität ist wichtiger
- Privat-PCs sauber halten, denn Disketten und Datenträger (USB-Stick!!) wandern
- Zentrales Virenscannen auf dem Mailserver
  - Siehe Vortrag vom letzten Mal

MAX-PLANCK-GESELLSCHAFT

Speicher-Uhr

- Bis zu 256 MB Speicher
- Unter Windows XP/2000 ohne Treiber
- Für den Werkschutz schwierig

MAX-PLANCK-GESELLSCHAFT

KNOPPIX

- eine komplett von CD lauffähige Zusammenstellung von GNU/Linux-Software mit automatischer Hardwareerkennung und Unterstützung für viele Grafikkarten, Soundkarten, SCSI-Geräte und sonstige Peripherie.
- kann als Linux-Demo, Schulungs-CD, Rescue-System angepasst und eingesetzt werden. Es ist keinerlei Installation auf Festplatte notwendig. Auf der CD können durch transparente Dekompression bis zu 2 Gigabyte an lauffähiger Software installiert sein.

Was geht mit KNOPPIX

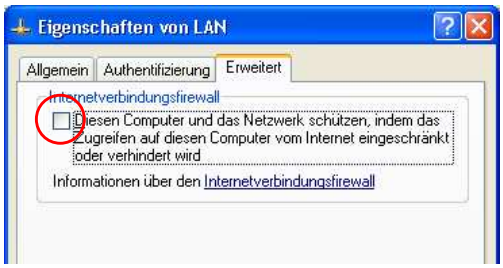
- Nach dem Booten können
  - NTFS-Partitionen gelesen und kopiert werden
  - Windows & Unix Passworte kopiert, geknackt oder geändert werden
  - Das Netzwerk abgehört werden
  - Angriffe gegen Andere gefahren werden
- KNOPPIX hinterlässt keine Spuren im Rechner oder auf der Festplatte

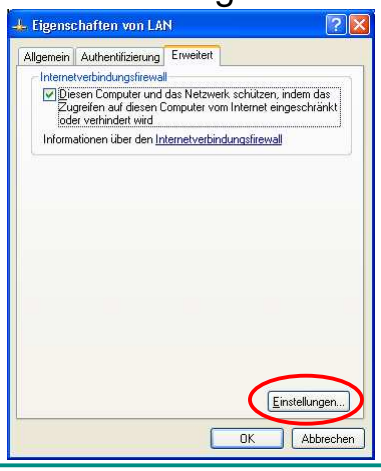
Personal Firewall

- Festplatte frei geben und dann den Zugriff per Personal Firewall sperren
  - Warum nicht die Freigabe entfernen?
- Was gibt es?
  - Unter Windows XP wird eine einfache Firewall mitgeliefert
  - Softwarefirewalls: Zonealarm, Norton .....
  - Hardware z.B. DSL-Router

XP Firewall I

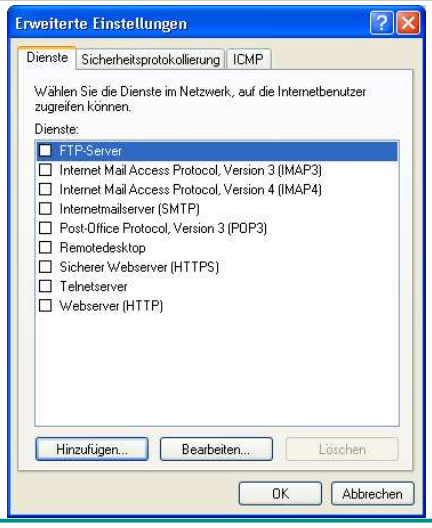
- Start->Einstellungen->Netzwerkverbindungen

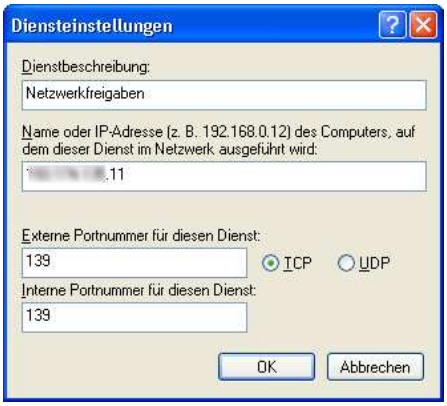




- Das Häckchen reicht, und der Rechner ist von außen nicht erreichbar

XP Firewall II





- TCP: 139,445
- UDP: 137,138,445

MAX-PLANCK-GESELLSCHAFT

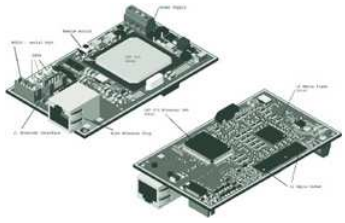
XP Firewall III

- Blockiert eingehende Verbindungen
  - Können aber frei geschaltet werden
- Beim erste Update eines frischen Windows XP mit SP1 nur mit aktivierter Firewall ins Netz
  - Schützt vor Blaster & Co.
- Ausgehende Datenverbindungen sind erlaubt
- Firewall ist UPnP fähig
  - Anwendung kann sich Ports frei schalten

MAX-PLANCK-GESELLSCHAFT

Innominate mGuard

Innominate
Security Technologies AG



- Intel IXP 425 Processor mit 533 MHz (xScale)
- 32 MB RAM, 16 MB Flash
- IPsec Protokoll
- Firewall (Stealth, statischer Router, DSL)
- Platine: ca. 56mm mal 95mm

MAX-PLANCK-GESELLSCHAFT

VPNUSB1

- Hardware Firewall
- IPsec Verschlüsselung
- Im Grunde ein kleiner Router
- Schöne Möglichkeit aus dem Netz von daheim eine VPN-Verbindung in die Firma aufzubauen
- Klein: ca. 6,4 cm x 12 cm

ftp://ftp.linksys.com/datasheet/usbvpn1_ds.pdf

MAX-PLANCK-GESELLSCHAFT

Grundregeln

- Alles was nicht verboten ist, ist erlaubt
  - d.h. unerwünschte und gefährliche Ports werden gesperrt, der Rest ist offen
  - Die Firewall erst offen betreiben und dann langsam „zudrehen“
- Alles was nicht erlaubt ist, ist verboten
  - Einige Dienste werden explizit erlaubt, dann kommt das große Deny-Satement

Firewall/Antiviren

- Microsoft Kampagne (z.Z. in Englisch)
  - http://www.microsoft.com/security/protect/
- eTrust EZ Armor von Computer Associates
  - Personal Firewall + Antivirus Programm (engl.)
  - http://www.my-etrust.com/microsoft/
  - Kostenloser Download bis 30.6.04 incl. 1 Jahr Updates

Patch-Management

- Jede Software hat offensichtlich Fehler!
- Bei sicherheitsrelevanten Fehlern muss der Fehler behoben werden
  ➔ Patch einspielen
- Das Einspielen der Patches muss zeitnah geschehen!!!!

MAX-PLANCK-GESELLSCHAFT

Beispiel: Microsoft

- Automatisches Einspielen der Updates für MS Windows und MS Office
- In einem Betrieb/einer Behörde mit MS Software-Update-Server (SUS)
- http://v4.windowsupdate.microsoft.com/de/default.asp

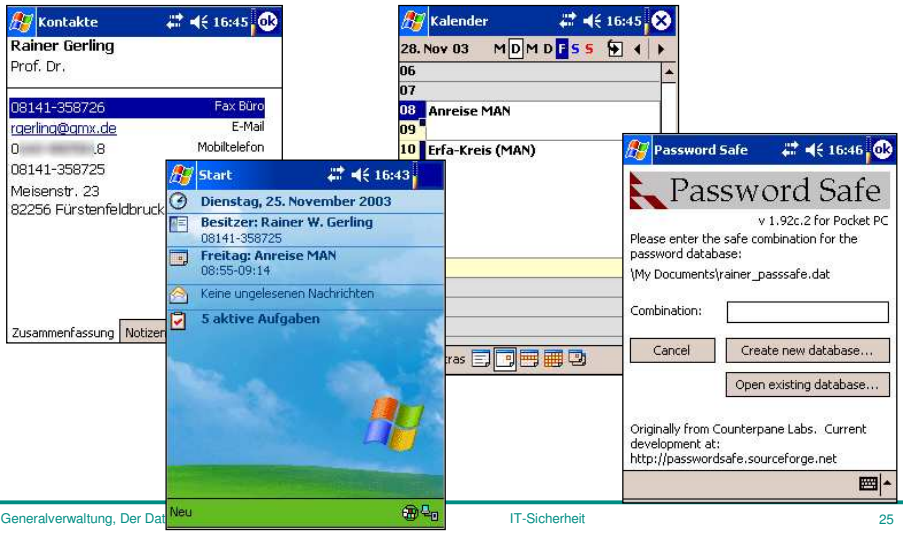
MAX-PLANCK-GESELLSCHAFT

Beispiel: OpenSSH

- Ein Bufferoverflow im OpenSSH erlaubt root-Zugriff trotz Firewall
- Angreifer installiert root-Kit „nRg/SucKIT“
- Installation über /proc/kmem
- Checksummen mit md5sum über die veränderten Dateien liefern korrekte Ergebnisse!
- Booten von Knoppix-CD und Prüfsummen berechnen!

http://www.cert.dfn.de/team/bunten/nrg.txt

Daten im Organizer



Daten im Handy

- Handies synchronisieren mit Outlook
  - Nicht nur Telefonnummern sondern auch Adressen und Termine im Handy
- PIN ist primär ein Schutz der Chipkarte
  - Informationen im Speicher des Handies

Verluste in Londoner Taxis

- 1. Halbjahr 2001
  - 1300 PDAs
  - 2900 Laptops
  - 62000 Handies
- Abgeholt wurden
  - Handies: ca. 50%
  - PDAs: ca. 85%
  - Laptops: ca. 93%

Quelle: http://news.bbc.co.uk/1/hi/uk/1518105.stm

Datenschutz

- Durchmischung privater und geschäftlicher Daten
  - Markierung als „privat“ setzt lediglich ein Flag
- Private Daten durch Synchronisierung auf Firmenserver
  - Stichwort: „Vorstellungstermin“

Betriebssysteme

- Optionaler Passwortschutz ohne Verschlüsselung
  - PalmOS (Palm)
  - WindowsCE/PocketPC (Microsoft)
  - EPOC (Symbian)
  - Blackberry
  - Linux
- Verschlüsselung durch Zusatzprodukte

Generalverwaltung, Der Datenschutzbeauftragte IT-Sicherheit 29

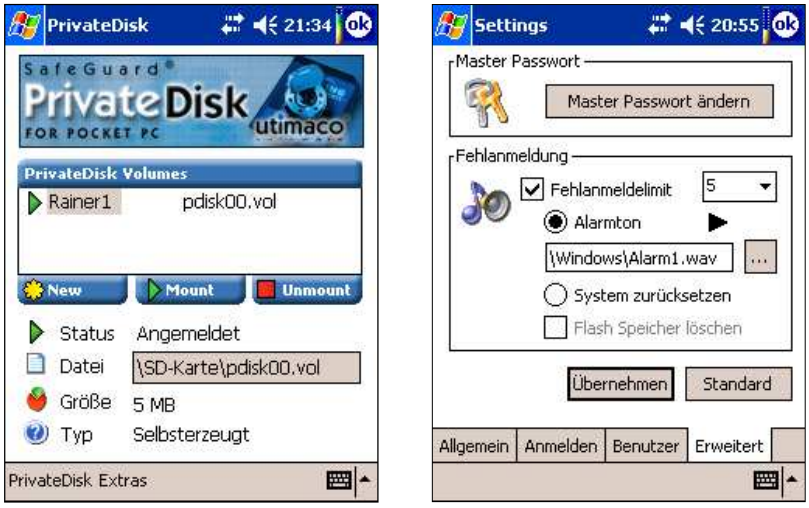
Utimaco SafeGuard PDA

- Seriöser Zugangschutz
  - Löschen des RAM nach dreimaliger Fehleingabe des Passwortes
- Dateiverschlüsselung
  - Private Crypto
  - Private Disk
- Alternativen:
  - PGP für Palm und PocketPC
  - CryptoEx für PocketPC
  - Studie im Auftrag des Innenministeriums:

http://ig.cs.tu-berlin.de/forschung/Mobile/Presseversion_BMI-Studie_mobile_Endgeraete_TU_Berlin.pdf

Generalverwaltung, Der Datenschutzbeauftragte IT-Sicherheit 30

Utimaco SafeGuard PDA



Unverzichtbarer Schutz

- Aktueller Virenscanner auf Windows/Macintosh PC
- Verschlüsselung personenbezogener und anderer vertraulicher Daten
- Firewall-Konzept
  - U.U. auch für Notebooks (Personal Firewall)
- FunkLAN Sicherheitskonzept
- Schutz der Daten in mobilen Geräten