

IT-Sicherheit



MAX-PLANCK-GESellschaft

Aktuelle Entwicklungen der IT-Sicherheit

Rainer W. Gerling
Max-Planck-Gesellschaft

Generalverwaltung, Der Datenschutzbeauftragte

IT-Sicherheit

1



MAX-PLANCK-GESellschaft

Inhalt

- FunkLAN und War-driving
- Aktuelle Viren
- Knoppix
- Persönliche Firewalls
- Patch-Management
- Organizer, Handies und Datenschutz

Generalverwaltung, Der Datenschutzbeauftragte

IT-Sicherheit

2


**War-Driving**

MAX-PLANCK-GESELLSCHAFT

- laptop + wireless + GPS + car

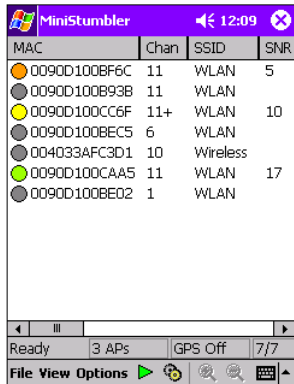
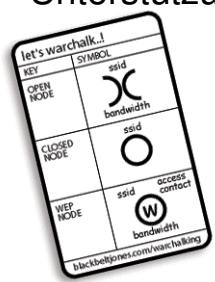


Generalverwaltung, Der Datenschutzbeauftragte IT-Sicherheit 3

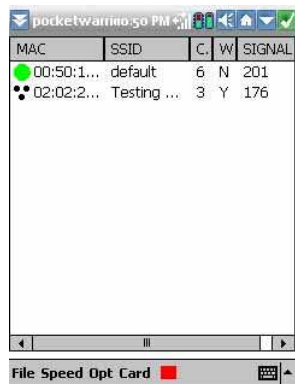
**Beispiele**

MAX-PLANCK-GESELLSCHAFT

- PocketPC reicht
– Mit GPS Unterstützung



MAC	Chan	SSID	SNR
0090D100BF6C	11	WLAN	5
0090D100B93B	11	WLAN	
0090D100CC6F	11+	WLAN	10
0090D100BEC5	6	WLAN	
004033AFC3D1	10	Wireless	
0090D100CAA5	11	WLAN	17
0090D100BE02	1	WLAN	




MAC	SSID	C	W	SIGNAL
00:50:1...	default	6	N	201
02:02:2...	Testing ...	3	Y	176

Generalverwaltung, Der Datenschutzbeauftragte IT-Sicherheit 4


MAX-PLANCK-GESELLSCHAFT

Wardriving in München


- Momentaufnahme
Mai 2002



Dank an Studenten

Generalverwaltung, Der Datenschutzbeauftragte

© 2003 Microsoft Corporation. Alle Rechte vorbehalten.


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

Generalverwaltung, Der Datenschutzbeauftragte

IT-Sicherheit

6

IT-Sicherheit




Viren

MAX-PLANCK-GESELLSCHAFT

- 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

Generalverwaltung, Der Datenschutzbeauftragte IT-Sicherheit 7



BugBear

MAX-PLANCK-GESELLSCHAFT

```
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 209.128.18.213:1027 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
```

Generalverwaltung, Der Datenschutzbeauftragte IT-Sicherheit 8



MAX-PLANCK-GESELLSCHAFT

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 Engineering auf Basis Explorer Fehler
- Ende September: QHosts-1
 - Ändert DNS und Proxy Einstellungen
- 24.10.03: Sober
 - erster deutschsprachiger Virus

Generalverwaltung, Der Datenschutzbeauftragte

IT-Sicherheit

9



MAX-PLANCK-GESELLSCHAFT

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 Virenschannen auf dem Mailserver
 - Siehe Vortrag vom letzten Mal

Generalverwaltung, Der Datenschutzbeauftragte

IT-Sicherheit

10



Speicher-Uhr



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

LAKS Memory saves your

- Files
- Pictures
- Movies
- Password
- MP3 Sounds

Active Mode
USB 1.0 connected to personal computer

Generalverwaltung, Der DatenschutzbeauftragteIT-Sicherheit11



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.

Generalverwaltung, Der DatenschutzbeauftragteIT-Sicherheit12



MAX-PLANCK-GESELLSCHAFT

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

Generalverwaltung, Der Datenschutzbeauftragte

IT-Sicherheit

13



MAX-PLANCK-GESELLSCHAFT


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

Generalverwaltung, Der Datenschutzbeauftragte

IT-Sicherheit


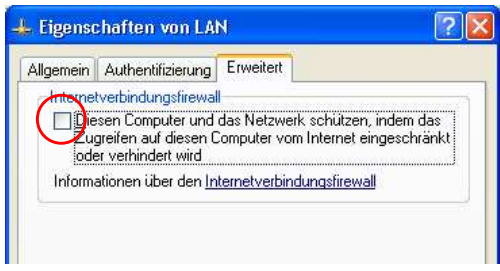
14



XP Firewall I


MAX-PLANCK-GESELLSCHAFT

- Start->Einstellungen->Netzwerkverbindungen



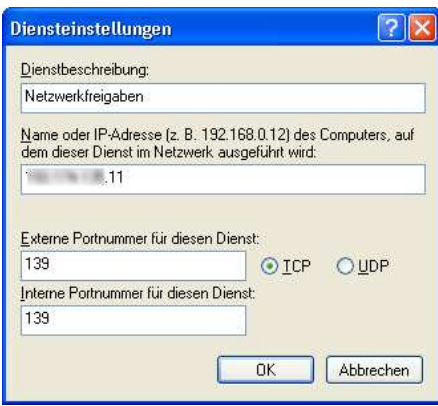
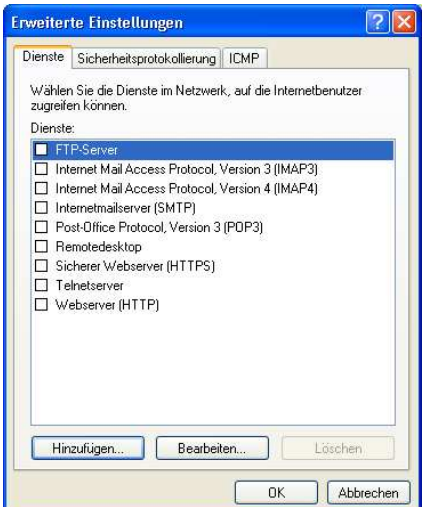
- Das Häkchen reicht, und der Rechner ist von außen nicht erreichbar

Generalverwaltung, Der DatenschutzbeauftragteIT-Sicherheit15



XP Firewall II

MAX-PLANCK-GESELLSCHAFT



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

Generalverwaltung, Der DatenschutzbeauftragteIT-Sicherheit16



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

Generalverwaltung, Der Datenschutzbeauftragte

IT-Sicherheit

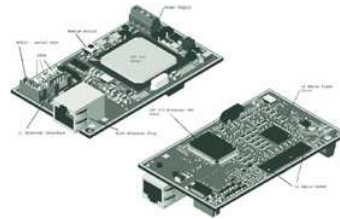
17



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

Generalverwaltung, Der Datenschutzbeauftragte

IT-Sicherheit


18

IT-Sicherheit




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

Generalverwaltung, Der Datenschutzbeauftragte IT-Sicherheit 19



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

Generalverwaltung, Der Datenschutzbeauftragte IT-Sicherheit 20



MAX-PLANCK-GESELLSCHAFT

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



MAX-PLANCK-GESELLSCHAFT

Patch-Management

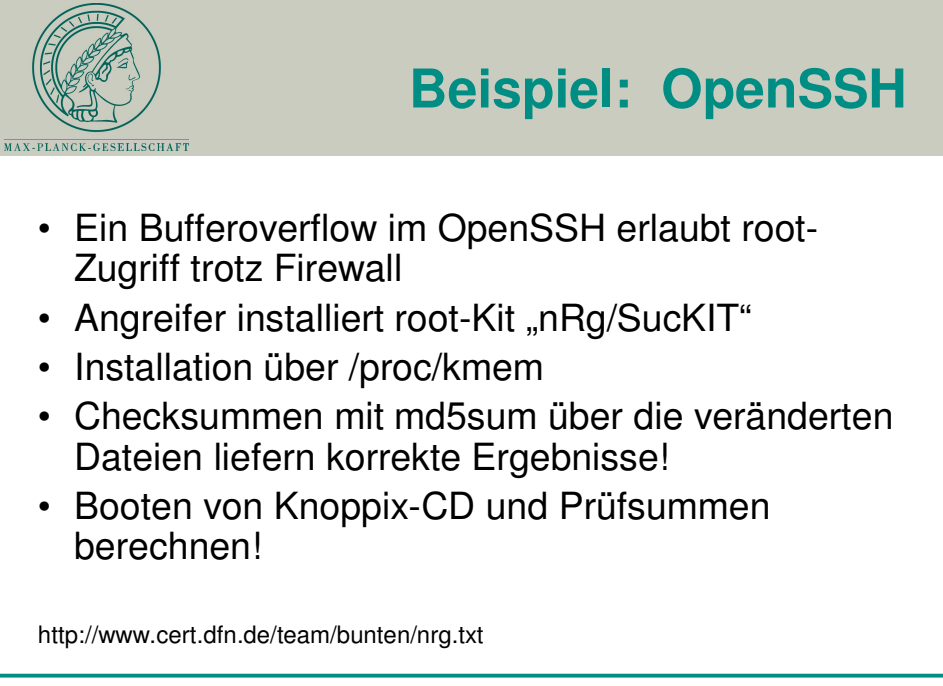
- Jede Software hat offensichtlich Fehler!
- Bei sicherheitsrelevanten Fehlern muss der Fehler behoben werden
 - ➔ Patch einspielen
- Das Einspielen der Patches muss zeitnah geschehen!!!!



The screenshot shows the Microsoft Windows Update website. At the top left is the Max-Planck-Gesellschaft logo. The main header features the Microsoft logo and the text 'Windows Update'. Below the header, there is a navigation bar with links for 'Startseite', 'Windows-Katalog', 'Windows-Familie', 'Office-Update', and 'Windows Update - Weltweit'. The main content area is divided into two columns. The left column contains a sidebar with a 'Windows Update' section, including options like 'Willkommen', 'Updates auswählen', 'Wichtige Updates und Service Packs (0)', 'Windows XP (11)', 'Treiberupdates (1)', and 'Updates überprüfen und installieren'. Below this is a 'Weitere Optionen' section with checkboxes for 'Installationsverlauf anzeigen' and 'Windows Update anpassen'. The right column has a 'Willkommen' section with a welcome message and a 'Updates suchen' button. A 'Hinweis' section below it states that Windows Update does not collect private information. On the far right, there is a small box with the text 'Schützen Sie Ihren Computer Drei Schritte zum Schutz Ihres Computers'. At the bottom of the screenshot, there is a footer with the text '© 2003 Microsoft Corporation. Alle Rechte vorbehalten. Nutzungsbedingungen'.

- 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>

Generalverwaltung, Der Datenschutzbeauftragte IT-Sicherheit 23




The slide features the Max-Planck-Gesellschaft logo at the top left. The main heading is 'Beispiel: OpenSSH'. Below the heading is a list of five bullet points describing a security vulnerability in OpenSSH. At the bottom of the slide, there is a URL: <http://www.cert.dfn.de/team/bunten/nrg.txt>. The footer contains the text 'Generalverwaltung, Der Datenschutzbeauftragte IT-Sicherheit 24'.

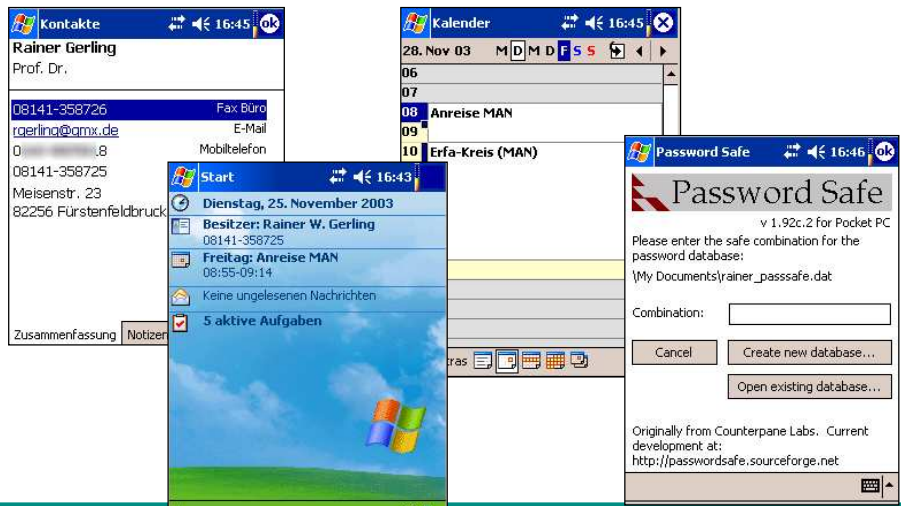
- Ein Bufferoverflow im OpenSSH erlaubt root-Zugriff trotz Firewall
- Angreifer installiert root-Kit „nRg/SucKIT“
- Installation über /proc/kmem
- Checksummen mit md5sum über die veränderten Dateien liefern korrekte Ergebnisse!
- Booten von Knoppix-CD und Prüfsummen berechnen!

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

Generalverwaltung, Der Datenschutzbeauftragte IT-Sicherheit 24

**Daten im Organizer**

MAX-PLANCK-GESELLSCHAFT



The screenshot displays a Windows XP desktop environment. On the left, the Outlook 'Kontakte' (Contacts) window is open, showing contact information for Rainer Gerling, including phone numbers and email addresses. In the center, the 'Start' menu is open, showing the date 'Dienstag, 25. November 2003' and a list of tasks and activities. On the right, the Outlook 'Kalender' (Calendar) window is open, showing a weekly view with a highlighted event 'Anreise MAN' on November 9th. Overlaid on the bottom right is a 'Password Safe' dialog box, which prompts the user to enter a safe combination for a password database. The dialog box includes fields for 'Combination', buttons for 'Cancel', 'Create new database...', and 'Open existing database...', and a footer with the software's origin and development information.

Generalverwaltung, Der Datenschutzbeauftragte

IT-Sicherheit

25

**Daten im Handy**

MAX-PLANCK-GESELLSCHAFT

- 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



The image shows four different models of mobile phones (feature phones) arranged horizontally. From left to right: a black phone with a small screen and a full keypad; a silver phone with a larger screen and a full keypad; a silver flip phone with its screen open; and a black phone with a small screen and a full keypad.

Generalverwaltung, Der Datenschutzbeauftragte

IT-Sicherheit

26



MAX-PLANCK-GESELLSCHAFT

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>

Generalverwaltung, Der Datenschutzbeauftragte

IT-Sicherheit

27



MAX-PLANCK-GESELLSCHAFT


Datenschutz

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

Generalverwaltung, Der Datenschutzbeauftragte

IT-Sicherheit


28




Betriebssysteme

MAX-PLANCK-GESELLSCHAFT

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




Generalverwaltung, Der DatenschutzbeauftragteIT-Sicherheit29



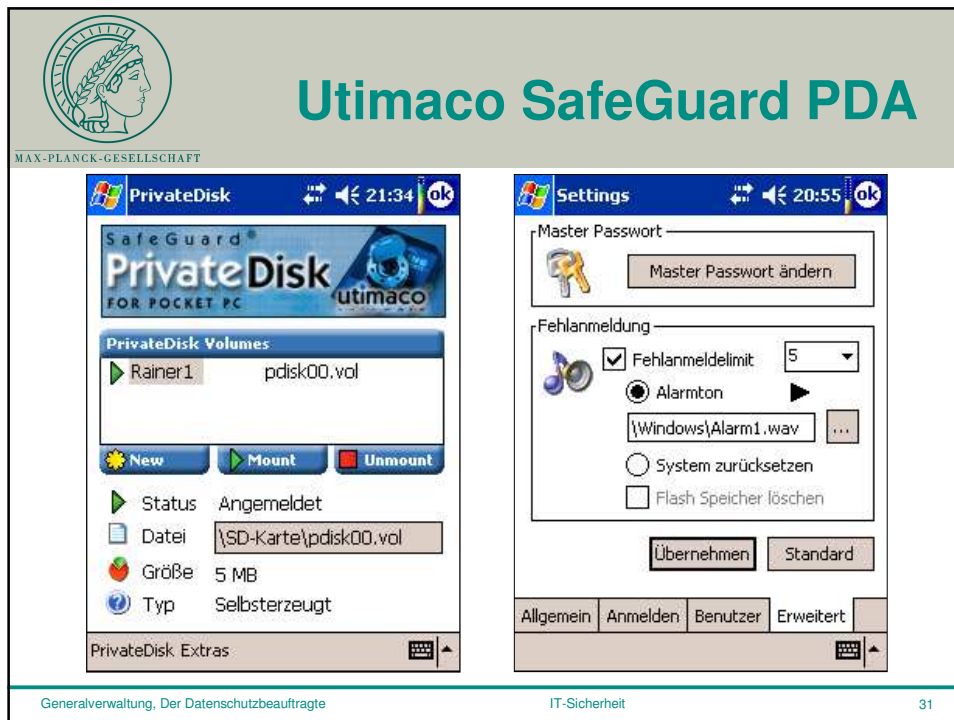
Utimaco SafeGuard PDA

MAX-PLANCK-GESELLSCHAFT

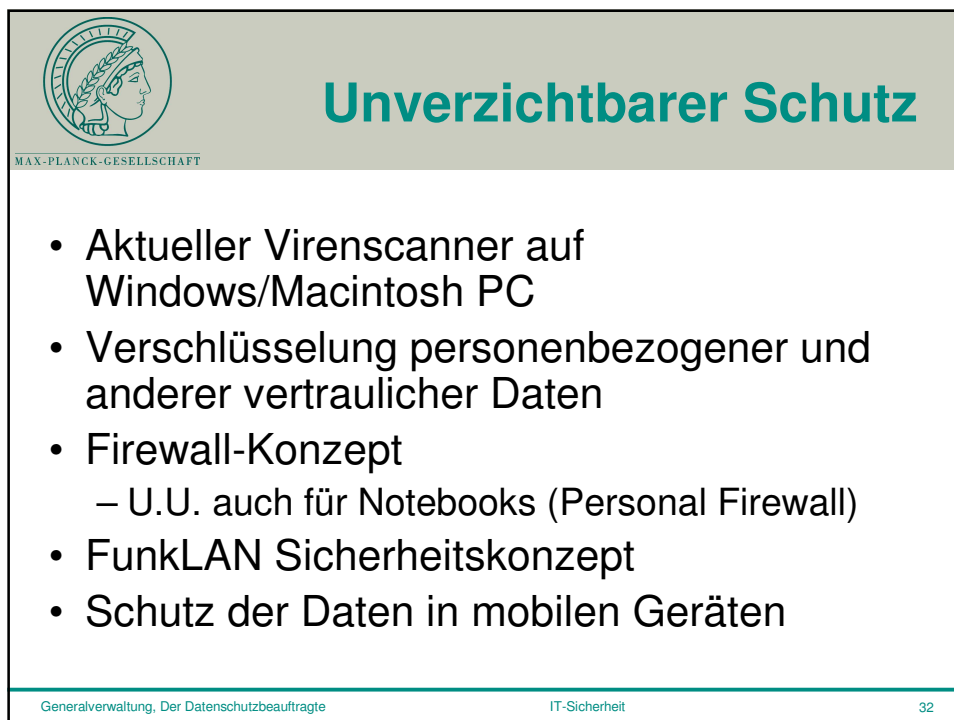
- **Seriöser Zugangschutz**
 - Löschen des RAM nach dreimaliger Fehleingabe des Passwortes
- **Dateiverschlüsselung**
 - Private Crypto
 - Private Disk
- **Alternativen:**
 - PGP für Palm und PocketPC
 - CryptoEx für PocketPC
 - Studie im Auftrag des Innenministeriums:



http://ig.cs.tu-berlin.de/forschung/Mobile/Presseversion_BMI-Studie_mobile_Endgeraete_TU_Berlin.pdfGeneralverwaltung, Der DatenschutzbeauftragteIT-Sicherheit30



The screenshot displays two screens from the Utimaco SafeGuard PDA interface. The left screen, titled 'PrivateDisk', shows the 'PrivateDisk Volumes' section with a volume named 'Rainer1' (pdisk00.vol) mounted on an SD card. It includes buttons for 'New', 'Mount', and 'Unmount', and displays details such as 'Status: Angemeldet', 'Datei: \SD-Karte\pdisk00.vol', 'Größe: 5 MB', and 'Typ: Selbsterzeugt'. The right screen, titled 'Settings', shows the 'Master Passwort' section with a 'Master Passwort ändern' button, and the 'Fehlalarmmeldung' section with options for 'Fehlalarmlimit' (set to 5), 'Alarmton' (set to \Windows\Alarm1.wav), 'System zurücksetzen', and 'Flash Speicher löschen'. At the bottom, there are tabs for 'Allgemein', 'Anmelden', 'Benutzer', and 'Erweitert'. The footer of the slide contains the text 'Generalverwaltung, Der Datenschutzbeauftragte', 'IT-Sicherheit', and the page number '31'.



Unverzichtbarer Schutz

- Aktueller Virenschanner 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

The footer of the slide contains the text 'Generalverwaltung, Der Datenschutzbeauftragte', 'IT-Sicherheit', and the page number '32'.