

# **T.I.S.P. Community Meeting 2010**

**Köln, 03./04.11.2010**

**Jörg Völker**

**Secorvo Security Consulting GmbH**

## **iPhone Security**

**Harmloses Gadget oder Sicherheitstrauma**

# Business Tool oder Gadget

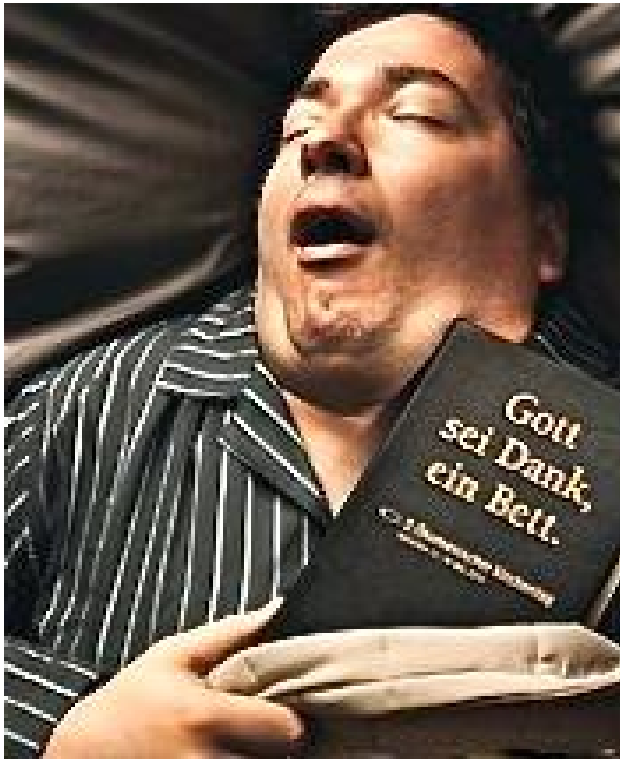
## ◆ iPhone hat den Markt mobiler Endgeräte „revolutioniert“

- Schickes Design
- Multifunktionaler Alles-Könnner
- Ultrakomfortable Bedienung
- Hunderttausende von Apps

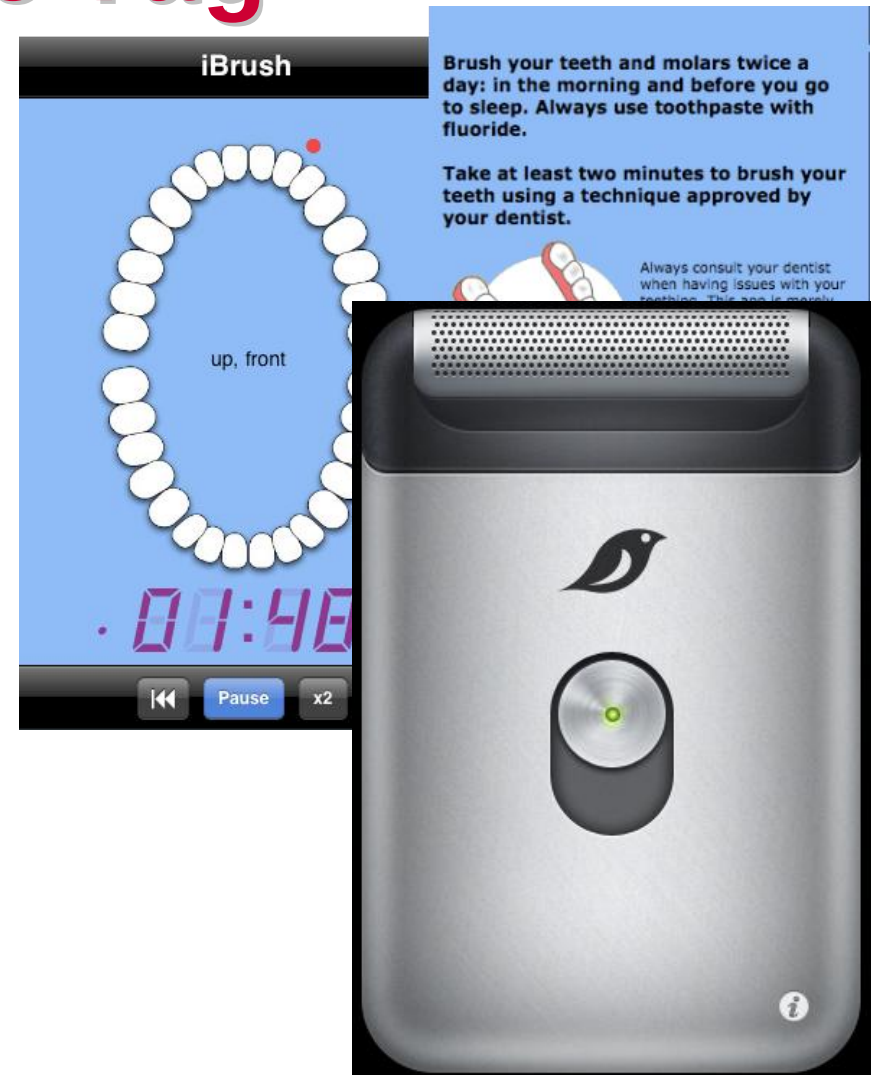


## ◆ Kurz: Ein Begleiter für alle Lebenslagen gestresster Manager

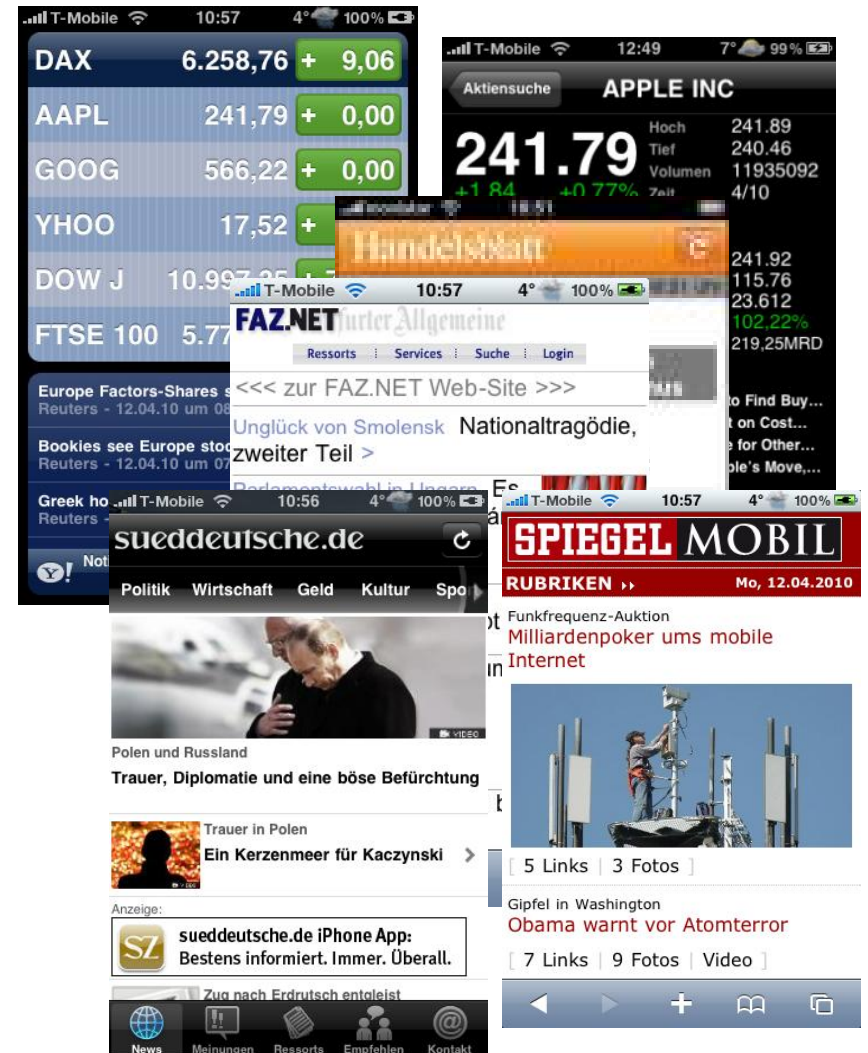
# Managers iPhone Tag



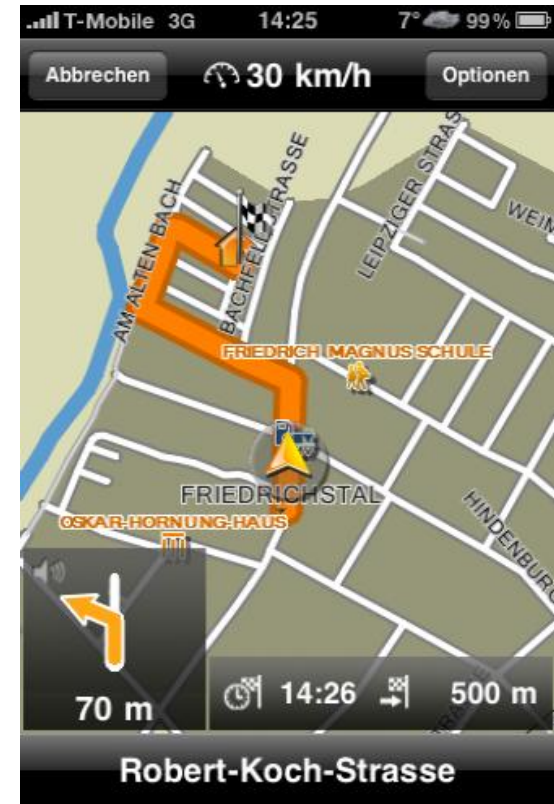
# Managers iPhone Tag



# Managers iPhone Tag



# Managers iPhone Tag



# Managers iPhone Tag



# Managers iPhone Tag

◆ Und zwischendurch natürlich



# Managers iPhone Tag



# Managers iPhone Tag



# ...also Business Tool !



**Datensafe iPhone**

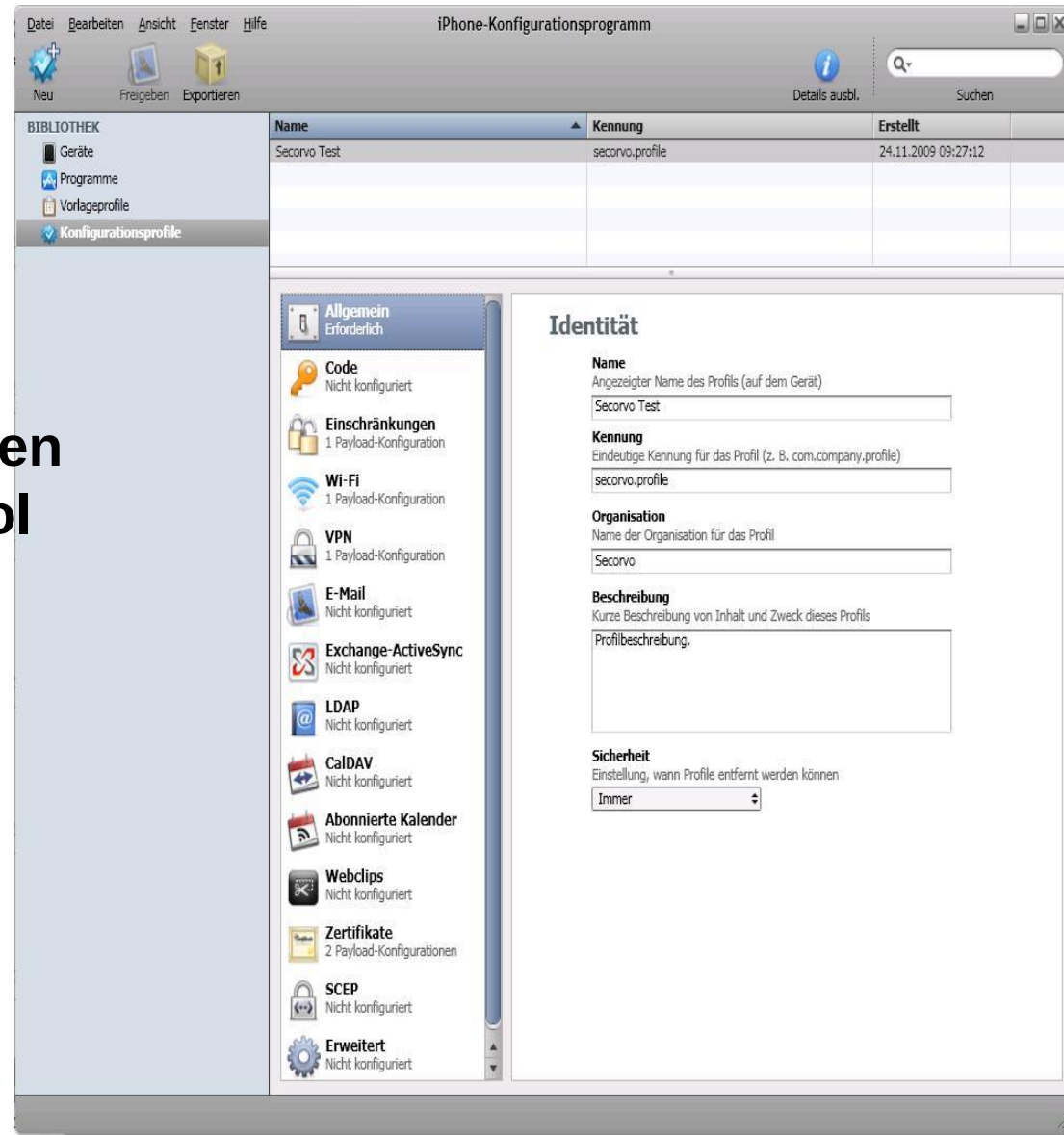


# Datensafe iPhone

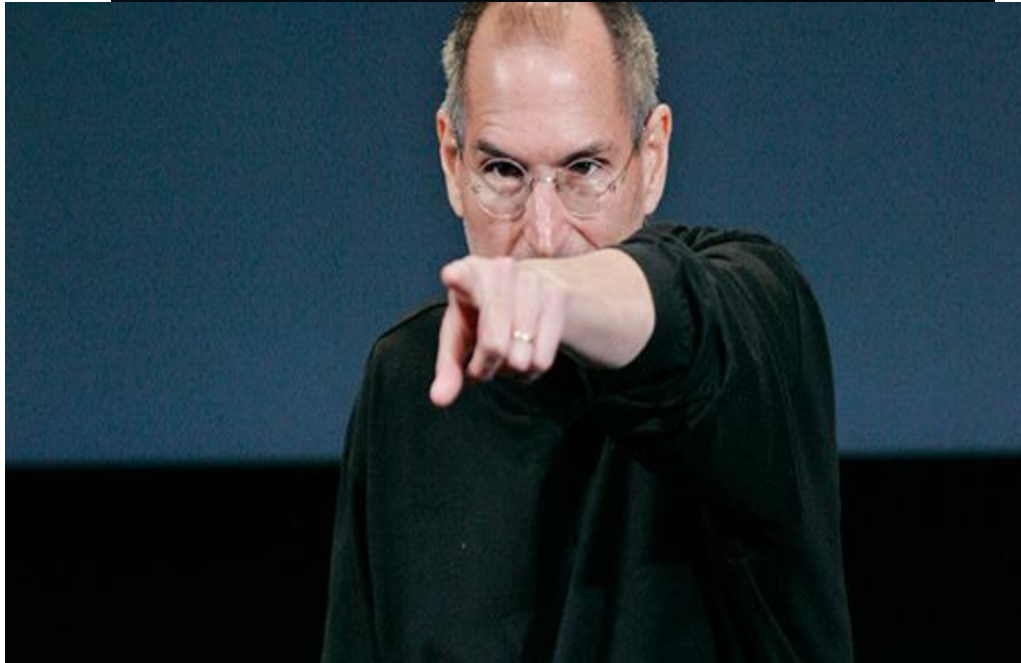
- ◆ Pin-Schutz, Automatische Sperre
- ◆ Hardwareverschlüsselung
- ◆ Verschlüsselte Backups
- ◆ Local Wipe, Remote Wipe
- ◆ WPA/WPA2, VPN Unterstützung, X.509 Zertifikate, RSA SecureID, ...
- ◆ Runtime Protection (Sand-Box für Apps)
- ◆ Code Signing
- ◆ ...

# Datensafe iPhone

- ◆ **Security Features müssen manuell aktiviert werden (Passcode, Local Wipe, automatische Sperre)**
- ◆ **Einige Einstellungen können nur über ein separates Tool von Apple adäquat angepasst werden**



# Und Steve sprach...



# ...oder vielleicht doch nicht?

# Datenkrake iPhone

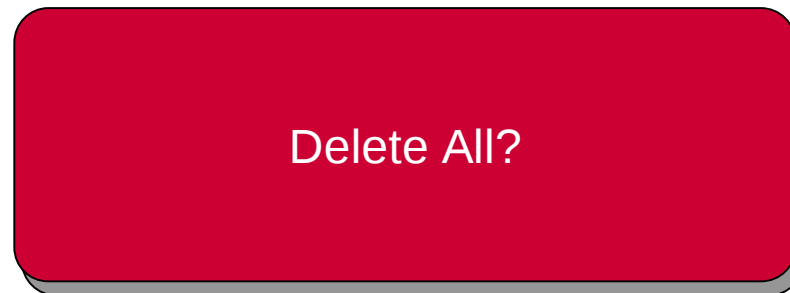


# Datenkrake iPhone

- SMS
- E-Mails
- Adressen
- Bilder
- Anruferlisten (letzte 100 Anrufe)
- Besuchte Webseiten (Browser Cache)
- Kartenausschnitte Google Maps (inkl. GPS-Daten)
  - Screenshots von Apps
  - Tastatur-Cache
- Pairing Informationen (Bluetooth)

# Datenkrake iPhone

- ◆ Viele dieser Informationen werden für unbestimmte Zeit auf dem Gerät vorgehalten
- ◆ Selbst wenn der Benutzer davon ausgeht, diese gelöscht zu haben



- ◆ Das Verhalten kann durch den Benutzer auch nicht direkt beeinflusst werden



# Datenloch iPhone

- ◆ **Trotz dieser Sicherheitsvorkehrungen muss man das iPhone derzeit als „unsicher“ betrachten**
- ◆ **Die wichtigsten Sicherheitsmechanismen lassen sich umgehen**
  - Code Signing
  - Pin-Schutz
  - Hardwareverschlüsselung
- ◆ **Alle iDevices betroffen**
  - iPod touch 1G/2G/3G/4G, iPhone 2G/3G/3GS/4, iPad und AppleTV
  - Abhängig von Firmware, Baseband und Boot Loader
  - Details: <http://www.jailbreakmatrix.com/iPhone-iTouch-Jailbreak>

# Datenloch iPhone

## ◆ Code Signing

### ➔ Jailbreak

- Aufhebung der iPhone Beschränkungen
- Ermöglicht Nutzung vieler i.d.R. deaktivierter OS Funktionen (SSH Server, Shell, etc.)
- Installation beliebiger Apps, manuell oder über andere AppStore Quelle (z.B. Cydia)
- Diese Apps durchlaufen natürlich keine „Qualitätsprüfung“ bei Apple

## ◆ Somit können Anwender Unternehmensvorgaben umgehen

# Datenloch iPhone



limera1n



greenpois0n

# Datenloch iPhone

## ◆ Pin-Schutz zum 1.

### ➔ Notruf Weakness

- Gesperrtes iPhone erlaubt nur Notrufe
- Durch Eingabe von „####“ und flinker Tastenkombination „Hörer abnehmen“ und Standby lässt Pin-Schutz umgehen

## ◆ Unberechtigter Zugriff auf Kontaktdaten und Telefon möglich



# Datenloch iPhone

## ◆ Pin-Schutz zum 2.

### ➔ Pairing Weakness

- Gesperrtes iPhone verweigert die Kommunikation mit Gegenstellen, die es noch nicht kennt
- Wenn das iPhone im entsperrtem Zustand ausgeschaltet wird, ist es beim Neustart aber für kurze Zeit „offen“
- Dieser Zeitraum reicht aus, um sich bspw. mit unbekanntem iTunes zu verbinden
- Danach kann Zugriff auf gespeicherte Daten erfolgen, bspw. durch Backup

## ◆ Unberechtigter Zugriff auf Daten möglich



# Datenloch iPhone

## ◆ Pin-Schutz zum 3.

### ➔ Jailbreak und Löschen des Pin-Schutzes

- Erstellen einer modifizierten Firmware
- Aufspielen der modifizierten Firmware auf das iPhone
- Alle Benutzerdaten und -einstellungen bleiben dabei erhalten, auch der Sperrcode
- Deaktivieren des Pin-Schutzes

## ◆ Vollzugriff auf iPhone für jeden, der das Gerät besitzt



# Datenloch iPhone

## ◆ Hardwareverschlüsselung

- Lässt sich ebenfalls ähnlich einfach umgehen wie Passcode
- Modifizierte Firmware erstellen
- Per SSH auf iPhone aufschalten
- DiskDump der Raw Disk erstellen
- Per Forensic Tool analysieren



## ◆ Vollzugriff auf alle Daten (auch bereits gelöschte) für jeden, der das Gerät besitzt

Umgehung aller Schutzfunktionen  
in wenigen Minuten...



X-Ways Forensics - [rdisk0s2] 15.4.5R-11

Datei Bearbeiten Suchen Position Ansicht Extras Specialist Optionen Fenster Hilfe

Falldaten rdisk0s2 7 Dateien, 26 Verz.

Neuer Fall

rdisk0s2

| Name                         | Typ | Größe | Erzeugung           | Änderung            | Zugriff             | Attr.     | 1. Sektor | Berichtsta | Kommentar |
|------------------------------|-----|-------|---------------------|---------------------|---------------------|-----------|-----------|------------|-----------|
| .HFS+ Private Data           |     |       | 11.12.2009 09:02:42 | 11.12.2009 09:02:42 | 11.12.2009 09:02:42 | -----     |           |            |           |
| .HFS+ Private Directory Data |     |       | 11.12.2009 09:02:42 | 11.12.2009 09:02:42 | 11.12.2009 09:02:42 | r-xr-xr-t |           |            |           |
| backups                      |     |       | 11.12.2009 09:24:46 | 11.12.2009 09:24:46 | 11.12.2009 09:24:46 | rw-rw-r-x |           |            |           |
| cache                        |     |       | 11.12.2009 09:24:46 | 11.12.2009 09:24:46 | 11.12.2009 09:24:46 | rw-rw-r-x |           |            |           |
| CommCenter                   |     |       | 11.12.2009 09:09:38 | 11.12.2009 09:09:38 | 11.12.2009 09:09:38 | rwk-----  |           |            |           |
| db                           |     |       | 28.09.2009 00:46:23 | 11.12.2009 09:09:04 | 28.09.2009 01:06:55 | rw-rw-r-x |           |            |           |
| ea                           |     |       | 26.09.2009 08:04:10 | 26.09.2009 08:04:10 | 28.09.2009 01:06:55 | rw-rw-r-x |           |            |           |
| empty                        |     |       | 26.09.2009 08:04:07 | 26.09.2009 08:04:07 | 28.09.2009 01:06:55 | rw-rw-r-x |           |            |           |
| folders                      |     |       | 26.09.2009 08:04:07 | 26.09.2009 08:04:07 | 28.09.2009 01:06:55 | rw-rw-r-x |           |            |           |
| Keychains                    |     |       | 26.09.2009 08:04:11 | 20.03.2010 17:55:12 | 28.09.2009 01:06:55 | rw-rw-r-x |           |            |           |
| lib                          |     |       | 11.12.2009 09:24:46 | 11.12.2009 09:24:46 | 11.12.2009 09:24:46 | rw-rw-r-x |           |            |           |
| local                        |     |       | 11.12.2009 09:24:46 | 11.12.2009 09:24:46 | 11.12.2009 09:24:46 | rw-rw-r-x |           |            |           |
| lock                         |     |       | 11.12.2009 09:24:46 | 11.12.2009 09:24:46 | 11.12.2009 09:24:46 | rw-rw-r-x |           |            |           |
| log                          |     |       | 28.09.2009 00:46:23 | 11.12.2009 09:24:46 | 28.09.2009 01:06:55 | rw-rw-r-x |           |            |           |
| logs                         |     |       | 28.09.2009 00:05:14 | 20.03.2010 22:07:48 | 28.09.2009 01:06:55 | rw-rw-r-x |           |            |           |
| Managed Preferences          |     |       | 26.09.2009 08:04:11 | 26.09.2009 08:04:11 | 28.09.2009 01:06:55 | rw-rw-r-x |           |            |           |
| mobile                       |     |       | 28.09.2009 00:36:54 | 22.12.2009 13:06:05 | 28.09.2009 01:06:55 | rw-rw-r-x |           |            |           |
| MobileDevice                 |     |       | 26.09.2009 08:04:11 | 11.12.2009 09:10:08 | 28.09.2009 01:06:55 | rw-rw-r-x |           |            |           |
| msgs                         |     |       | 26.09.2009 08:04:08 | 26.09.2009 08:04:08 | 28.09.2009 01:06:55 | rw-rw-r-x |           |            |           |
| preferences                  |     |       | 26.09.2009 08:04:11 | 23.03.2010 12:32:49 | 28.09.2009 01:06:55 | rw-rw-r-x |           |            |           |
| root                         |     |       | 26.09.2009 07:53:48 | 11.12.2009 09:31:37 | 28.09.2009 01:06:55 | rw-rw-r-x |           |            |           |
| run                          |     |       | 26.09.2009 08:04:08 | 15.03.2010 14:28:52 | 28.09.2009 01:06:55 | rw-rw-r-x |           |            |           |
| spool                        |     |       | 11.12.2009 09:24:46 | 11.12.2009 09:24:46 | 11.12.2009 09:24:46 | rw-rw-r-x |           |            |           |
| stash                        |     |       | 11.12.2009 09:24:46 | 08.01.2010 09:01:52 | 11.12.2009 09:24:46 | rw-rw-r-x |           |            |           |
| tmp                          |     |       | 26.09.2009 07:54:17 | 23.03.2010 14:01:27 | 28.09.2009 01:06:55 | rw-rw-r-x |           |            |           |

Volume Datei Vorschau Details Galerie Kalender Legende Sync

| Offset   | 0  | 1  | 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | A  | B  | C  | D  | E  | F  |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 00000000 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000010 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000020 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000030 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000040 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000050 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000060 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000070 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000080 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000090 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 000000A0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 000000B0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 000000C0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 000000D0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 000000E0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 000000F0 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000100 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000110 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000120 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000130 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000140 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000150 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000160 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000170 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |
| 00000180 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 |

Sektor 0 von 1973186 Offset: 0 = 0 Block: / Größe:

[rdisk0s2.dd] 90% frei  
Dateisystem: HFS+  
[Schreibschutz-Modus]  
Inhalt der Sektorenansicht:  
Block: 0  
Volume Header Area  
Datei-Überblick von vor 0 Min.  
Genutzter Speicher: 2,8 GB  
3.000.107.008 Bytes  
Freier Speicher: 26,5 GB  
28.487.417.856 Bytes  
Gesamtkapazität: 0,9 GB  
1.010.271.232 Bytes  
Bytes pro Cluster: 8.192  
Freie Cluster: 3.477.468  
Cluster insgesamt: 3.843.692  
Bytes pro Sektor: 512  
Sektoren: Daten-Dolmets...

8 Bit (±): 0  
16 Bit (±): 0  
32 Bit (±): 0

# WiFi-Bewegungsprofil

[Web](#) [Bilder](#) [Videos](#) **Maps** [News](#) [Shopping](#) [E-Mail](#) [Mehr](#) ▼

Google maps  
Deutschland

50.1065851,8.6620563

Maps-Suche

[Suchoptionen anzeigen](#)

[Route berechnen](#) [Meine Karten](#)



## Am Hauptbahnhof 1

60329 Frankfurt am Main, Deutschland

[Routenplaner](#) [In der Nähe suchen](#) [Speichern](#) [Mehr](#) ▼

[Erkunden Sie dieses Gebiet »](#)

### Fotos

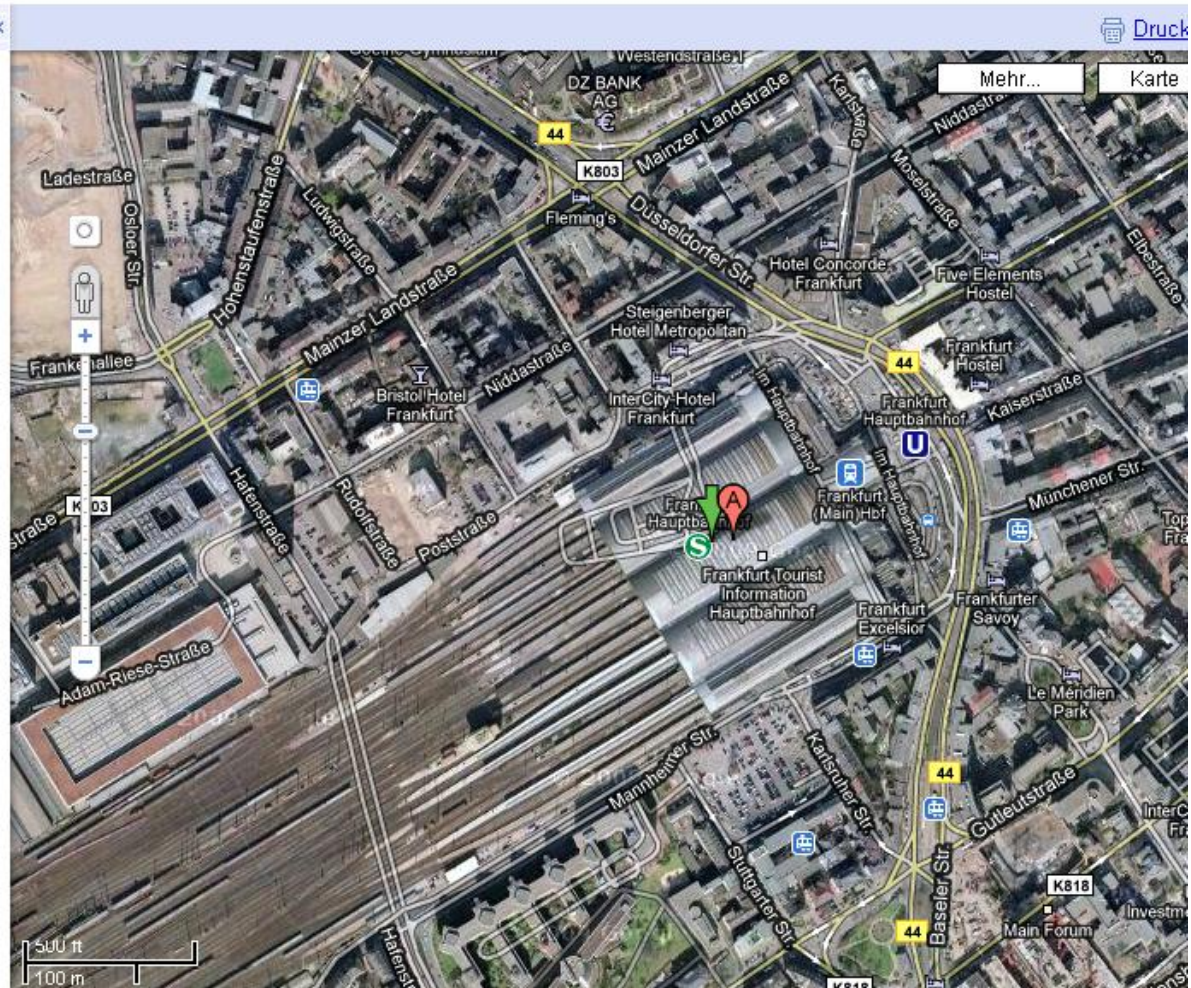


### Orte

[Frankfurt Hauptbahnhof](#)

[Frankfurt Hauptbahnhof tief](#)

[Am Hauptbahnhof](#)



# Datenloch iPhone

- ◆ **Passwort-Recovery Tools für verschlüsselte iPhone Backups**
- ◆ **Schlecht programmierte oder vorsätzlich manipulierte Apps (insbesondere, wenn Apps nicht über Apples App Store installiert werden)**
- ◆ **Viele Apps leiten Benutzerinformationen an die Firma Pinchmedia weiter (ähnlich wie Google Analytics), ohne dass dies dem Benutzer transparent ist**
- ◆ **Spezielle Überwachungssoftware für Mobile Phones auch für iPhone verfügbar**
  - **z.B. FlexiSpy: Mithören von Gesprächen, Fernbedienung per SMS, Ausführliches Weblog über Nutzung des iPhones**

Und jetzt!?



# Und jetzt!?

- ◆ iPhone erfreut sich zunehmender Beliebtheit im Management
- ◆ Nutzen und Komfort überwiegen potentiellen Gefährdungen, sofern diese den Anwendern überhaupt bekannt/bewusst sind
- ◆ Letztendlich lässt sich die Einführung im Unternehmen kaum verhindern

# Und jetzt!?

- ◆ **Über bestehende Gefährdungen aufklären**
- ◆ **Festlegen, welche Datenarten auf dem iPhone mitgeführt/bearbeitet werden dürfen (auch aus Datenschutzaspekt)**
- ◆ **Prüfen, ob der Einsatz zusätzlicher Sicherheitssoftware (z.B. Sybase iAnywhere Mobile Office, Good Technology ...) möglich ist**
- ◆ **Gerätekonfigurationen zentral managen und entsprechende Policy zu verabschieden**

# Fragen?

- ◆ Gerne jetzt oder später bei einem kleinen...





[www.secorvo.de](http://www.secorvo.de)