

# **Fachfrühstück Sicherheit von mobilen Lösungen**



**Wettbewerbsvorteil durch Mobilität.  
Wir begleiten Sie.**

## Sicherheit, ein wachsendes Thema

**McAfee®**

Februar 2007

[...] the number of mobile security incidents in 2006 increased by 500 percent and that 83 percent of mobile operators had been hit by mobile infections.

**Microsoft**

September 2006

Nach einer Umfrage der Sicherheitssoftwarefirma CREDANT Technologies unter IT-Experten in den USA verschlüsseln weniger als 20 Prozent aller Unternehmen ihre Daten auf mobilen Geräten. **Die Verwendung von Kennwörtern ist zwar weiter verbreitet (Schätzungen belaufen sich auf 50 Prozent), aber auch diese Zahl ist alarmierend niedrig.**

**COMPUTERWOCHE.de**

21.11.07

**Sicherheitsvorfälle auf mobilen Endgeräten verdoppelt**

[...] so sind die Sicherheitsvorfälle durch mobile Endgeräte in kleinen und mittelgroßen Firmen in den letzten vier Jahren sprunghaft angestiegen. In Unternehmen mit mehr als 500 Mitarbeitern hat sich die Anzahl an Sicherheitsvorfällen beim Einsatz von Handhelds gemäß einer aktuellen Studie im Vergleich zum Vorjahr sogar verdoppelt.

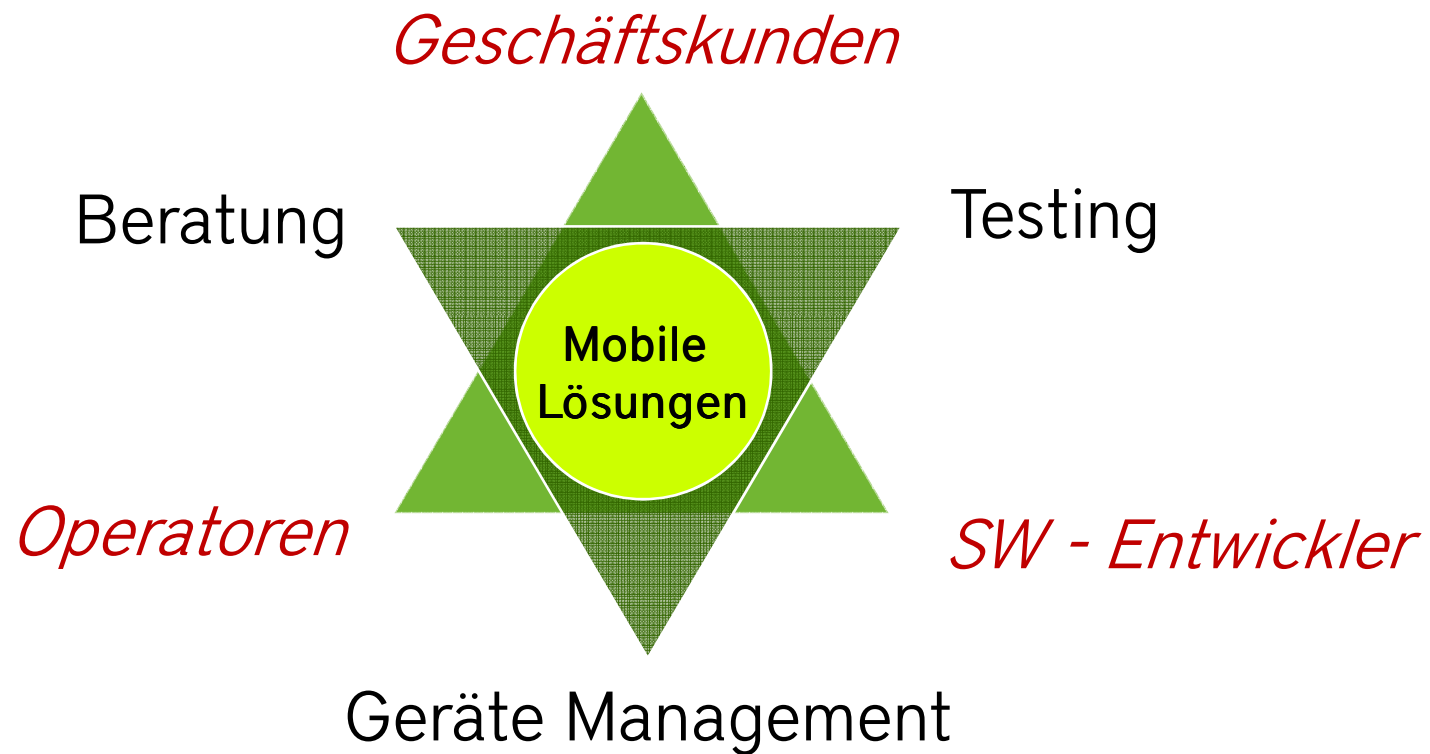
---

# Inhalt

- 1 Vorstellung go4mobile ag
- 2 Gefahren und Anforderungen
- 3 Lösungsansatz
- 4 Live Demo
- 5 Ausblick und Fazit



## go4mobile ag, Bern



**go4mobile, DER Spezialist für mobile Lösungen.**

# Inhalt

- 1 Vorstellung go4mobile ag
- 2 Gefahren und Anforderungen
- 3 Lösungsansatz
- 4 Live Demo
- 5 Ausblick und Fazit



## Ist die Bedrohung relevant?

- Stark wachsende Nutzerzahlen im Mobilfunk
- Schnelles mobiles Internet (HSPA bis 7.2Mbps Downlink / 1.4Mbps Uplink)
- Leistungsfähige Geräte -> werden sehr PC ähnlich
- Starke Zunahme von Mobilisierungen von Applikationen
- Sensitive Daten lokal auf den Geräten, z.B. via Mailsync
- Professionalisierung der Wirtschaftskriminalität

# Gefahrengruppen

## Umfeld

- Beeinträchtigung durch wechselnde Einsatzumgebung

## Organisatorische Mängel

- Fehlende oder unzureichende Regelungen
- Unzureichende Kontrolle der IT-Sicherheitsmaßnahmen
- Ungesicherter Akten- und Datenträgertransport
- Ungeeignete Entsorgung der Datenträger und Dokumente

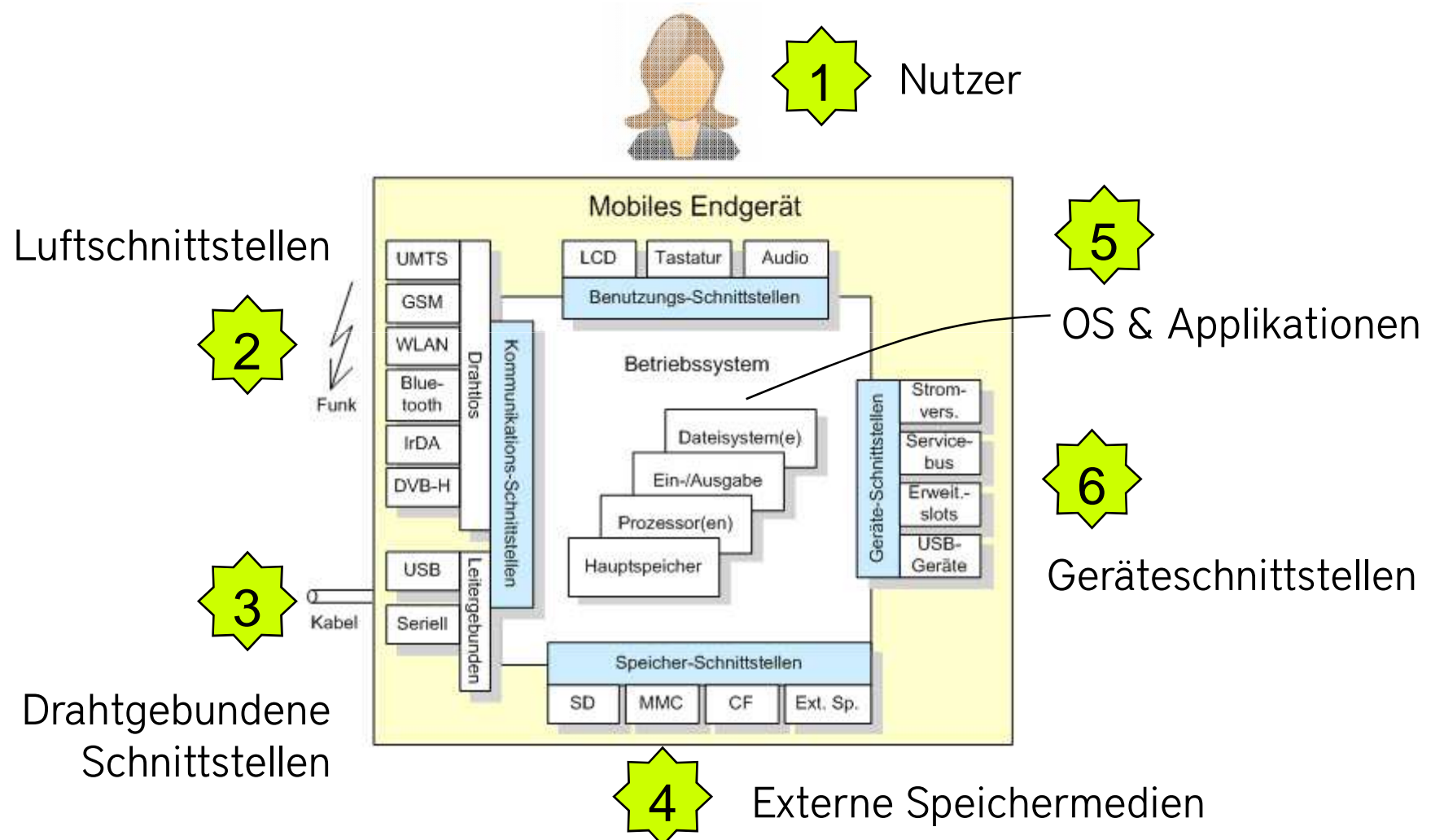
## Menschliche Fehler

- Nichtbeachtung von IT-Sicherheitsmaßnahmen
- Ungeeigneter Umgang mit Passwörtern
- Sorglosigkeit im Umgang mit Informationen

## Vorsätzliche Handlungen

- Manipulation/Zerstörung von IT-Geräten oder Zubehör
- Manipulation an Daten oder Software
- Diebstahl und Veröffentlichung von Daten und Informationen
- Vertraulichkeitsverlust schützenswerter Informationen

# Übersicht über das Gesamtsystem "Natel"



# Konkrete Gefahren

## 1 Nutzer

- Geräteverlust
- Datendiebstahl
- Manipulation der Geräteeinstellungen
- Einbringen von Malware

## 2 Luftschnittstellen

(unterschiedlich gefährlich: WLAN, BT, IrDa, GSM, UMTS, DVBH)

- Man in the middle (Mithören)
- Spoofing (Emulation einer Basisstation)
- DoS
- IP-orientierte Attacken
- Aufzeichnung von Bewegungsprofilen

## 3 Drahtgebundene Schnittstellen

- I.d.R. ist der Datenaustausch via USB Kabel nicht PIN geschützt

## 4 Externe Speichermedien

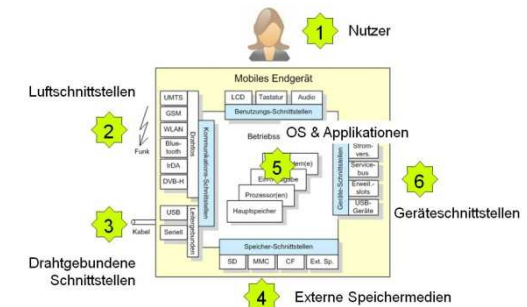
- Selbstausführende .cab / .exe Files
- Schadhafte Software
- Datendiebstahl
- Liegengelassen, verloren

## 5 OS & Applikationen

- Viren, Würmer, Trojaner, Backdoors

## 6 Geräteschnittstellen

- Strichcodeleser etc. – kaum Gefährdung
- SIM – Kosten für Gespräche & Daten



# Sicherheitsbezogene Anforderungen

| Der IT(-Sicherheit)                                                                                                                                                                                                                                                                                                                                                                                                                              | Der Nutzer                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| E2E Sicherheit des Gesamtsystems                                                                                                                                                                                                                                                                                                                                                                                                                 | Einfache Nutzung                                                                                                                                                                                                                                                                                                     |
| <ul style="list-style-type: none"> <li>• Nicht manipulierbar</li> <li>• Zentral gemanagt</li> <li>• Tiefe Fehlerwahrscheinlichkeit mit kleiner Auswirkung und hohe Entdeckungswahrscheinlichkeit.</li> <li>• Kostengünstig in Beschaffung und Betrieb</li> <li>• Kann schnell auf neue Bedrohungen reagieren</li> <li>• Adaptiv anwendbare Sicherheitsprofile auf verschiedene Risikogruppen</li> <li>• Gerät ist immer in Firmen-LAN</li> </ul> | <ul style="list-style-type: none"> <li>• Passwort nicht "zu kompliziert"</li> <li>• Geräte noch schnell genug</li> <li>• Gewünschte Funktionen noch verfügbar</li> <li>• Datentransfer soweit gewünscht und nötig noch möglich (ab Speichermedien)</li> <li>• Lange Nutzung ohne Akku nachladen zu müssen</li> </ul> |

# Inhalt

- 1 Vorstellung go4mobile ag
- 2 Gefahren und Anforderungen
- 3 Lösungsansatz**
- 4 Live Demo
- 5 Ausblick und Fazit



# Grundsatz für Massnahmen



Gefahr vermeiden



Gefahrenherd isolieren



Objekt schützen

# Lösungsebenen

Prozesse

Passwortanfrage

Nutzer  
Identifikation

Passwort-  
vergabe

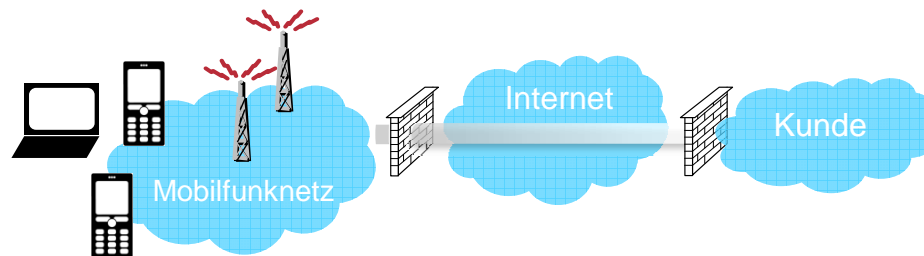
Gerät



+



Netz



# Angriff / Massnahmen Prozesse und Netz

| Angriffspunkt Proz.                           | Massnahme                                                                                                                     | Hilfsmittel                                                                                                                             |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Menschliche Fehler, Herausgabe von Passwörter | <ul style="list-style-type: none"> <li>• Klare Authentifizierungsabläufe im Support</li> </ul>                                | <ul style="list-style-type: none"> <li>• Informieren und Schulen</li> </ul>                                                             |
| Geräteverlust                                 | <ul style="list-style-type: none"> <li>• Inventur mit Natelnummer, IMEI, Nutzer damit Sperre ausgelöst werden kann</li> </ul> | <ul style="list-style-type: none"> <li>• MobiControl von SOTI</li> <li>• SCMDM von Microsoft</li> <li>• Inventurdatensysteme</li> </ul> |

| Angriffspunkt Netz                                                                                                                                                        | Massnahme                                                                                                                                                                                                                                                                                                                                        | Hilfsmittel                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mobile Operator Netzwerk <ul style="list-style-type: none"> <li>• Man in the Middle</li> <li>• Spoofing</li> <li>• DoS</li> </ul>                                         | <ul style="list-style-type: none"> <li>• Operatornetzwerk ist ein privates überwachtes Netzwerk, welches Anomalien erkennt und verhindert.</li> <li>• Die zur Zeit stärkste Mobilfunkverschlüsselung verwenden</li> </ul>                                                                                                                        | <ul style="list-style-type: none"> <li>• Endgeräte fix auf UMTS umschalten</li> </ul>                                                                         |
| Datenverbindung zwischen Mobile Operator und Firmeninfrastruktur <ul style="list-style-type: none"> <li>• Man in the Middle</li> <li>• Spoofing</li> <li>• DoS</li> </ul> | <ul style="list-style-type: none"> <li>• Datenkommunikation end2end mit Mobile VPN verschlüsseln</li> <li>• Firmenlan kontrolliert am mobile Operatornetzwerk anbinden</li> <li>• Applikationsdatenkommunikation mit SSL/TLS verschlüsseln</li> <li>• Firmenfirewall akzeptiert nur Datenverbindungen aus dem Mobile Operatornetzwerk</li> </ul> | <ul style="list-style-type: none"> <li>• SCMDM</li> <li>• CNA mit VPN Tunnel / CNA over IPSS</li> <li>• Firewall Konfiguration spezifisch anpassen</li> </ul> |

# Angriffe / Massnahmen am Gerät

| Angriffspunkt                                          | Massnahme                                                                                                                                                                                                       |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Datendiebstahl                                         | <ul style="list-style-type: none"> <li>• Verschlüsselung der Speicher- und Gerätedaten,</li> <li>• Passwortzugriffschutz aktivieren</li> </ul>                                                                  |
| Geräteverlust                                          | <ul style="list-style-type: none"> <li>• Passwortzugriffschutz aktivieren,</li> <li>• Remote Wipe des Gerätes auslösen</li> <li>• SIM Karten PIN aktivieren</li> <li>• SIM Karte sperren lassen</li> </ul>      |
| Selbstaufführende Installation von Software verhindern | <ul style="list-style-type: none"> <li>• Sperren der Autostart, Autoexecution ab Speicherkarten (.cab/ .exe)</li> <li>• Verwendung von Speicherkarten sperren</li> </ul>                                        |
| Einbringen von Malware                                 | <ul style="list-style-type: none"> <li>• Virenschutz verwenden im Gerät und Backend</li> <li>• Schnittstellen sperren BT, IR, WLAN, USB</li> <li>• Internet Browsing über Firmenproxyserver erlauben</li> </ul> |
| Manipulation von Geräteeinstellungen                   | <ul style="list-style-type: none"> <li>• Gerätepolicies zentral definieren und anwenden</li> <li>• Black/ Whitelists von Applikationen</li> <li>• Kiosk verwenden</li> </ul>                                    |
| Aktivierung betriebsfremder Geräte verhindern          | <ul style="list-style-type: none"> <li>• Inbetriebnahme erfolgt mit Gerätezertifikaten</li> </ul>                                                                                                               |

| Hilfsmittel                                                                                                                                                                                                  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Geräte Management Lösungen</b> <ul style="list-style-type: none"> <li>• MobiControl von SOTI</li> <li>• SCMDM von Microsoft</li> <li>• Afaria von Sybase</li> <li>• (Exchange 2007 Enterprise)</li> </ul> |
| <b>Malware Schutz</b> <ul style="list-style-type: none"> <li>• F-Secure</li> <li>• Trend Micro</li> </ul>                                                                                                    |
| <b>Sicherheitssoftware</b> <ul style="list-style-type: none"> <li>• Safeguard PDA von Utimaco</li> </ul>                                                                                                     |
| <b>Gesamtlösung</b> <ul style="list-style-type: none"> <li>• Blackberry</li> </ul>                                                                                                                           |

# Inhalt

- 1 Vorstellung go4mobile ag
- 2 Gefahren und Anforderungen
- 3 Lösungsansatz
- 4 Live Demo
- 5 Ausblick und Fazit



## Live-Demo

### Verbindung zu PC sperren

- Geräteschnittstellen blockieren, Autoinstallation von Applikationen sperren, Zugriffsschutz aktivieren, Mobile VPN oder Corporate Network Access

### Gestohlenes Gerät löschen

- Gerät wird mittels einem Wipe Befehl unbrauchbar gemacht. Wipe kann über Datenverbindung, SMS ausgelöst werden.

# Inhalt

- 1 Vorstellung go4mobile ag
- 2 Gefahren und Anforderungen
- 3 Lösungsansatz
- 4 Live Demo
- 5** Ausblick und Fazit



# Ausblick

## Prozesse

- Umsetzung ITIL V3.0 in der Mobilität
- Natel = Werkzeug -> Durchsetzung

## Gerät


- CPU Leistung steigt:  
Virenschutz, VPN-Applikationen
- Gerätemanagement-Lösungen
- Biometrik
- SmartCard auf SIM

## Netz

- GSM A5/1 -> A5/3
- UMTS Abdeckung nimmt zu

## Fazit

- Effizienzsteigerung -> sensitive Daten auf Natels
- Natels ... sind voll internetfähig
  - ... haben keine Admin/Nutzer Trennung
  - ... müssen auch privaten Ansprüchen genügen

- 
- "Gefahr vermeiden" ist oft schwierig oder unerwünscht  
=> isolieren & schützen
  - Diverse Sicherheitskomponenten sind verfügbar, müssen aber sorgfältig abgestimmt und eingesetzt werden

# Besten Dank für Ihre Aufmerksamkeit!



go4mobile ag  
Felsenastrasse 17  
3004 Bern  
[www.go4mobile.ch](http://www.go4mobile.ch)

Telefon: +41 (0) 31 914 18 18  
Fax: +41 (0) 31 914 18 19  
[info@go4mobile.ch](mailto:info@go4mobile.ch)

# Normen & Gesetze

## Normen

- FIPS 140-x (<http://www.nist.gov/>)
- ISO/IEC 27001, Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung, und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems
- ISO/IEC 27011: Telecommunications  
ISO/IEC 27012: Finance  
ISO/IEC 27013: Manufacturing
- Payment Card Industry Data Security Standard

## Gesetze (Bsp.)

- CH: Art 47 BankG: Bankgeheimnis
- USA: Sarbanes Oxley Act (SOX)

## **Einfache Sicherheitstips**

- PIN Schutz aktivieren
  - Infrarot Schnittstelle deaktivieren
  - Speicherkarte verschlüsseln
  - Bluetooth nur einschalten wenn nötig und nur geschützte Verbindungen zulassen
  - UMTS anstelle von GSM nutzen
  - Vor Weitergabe der Geräte: Hard Reset
  - Verluste sofort dem Admin melden -> SIM und Firmenzugänge sperren
-