

Mobile Security Policies

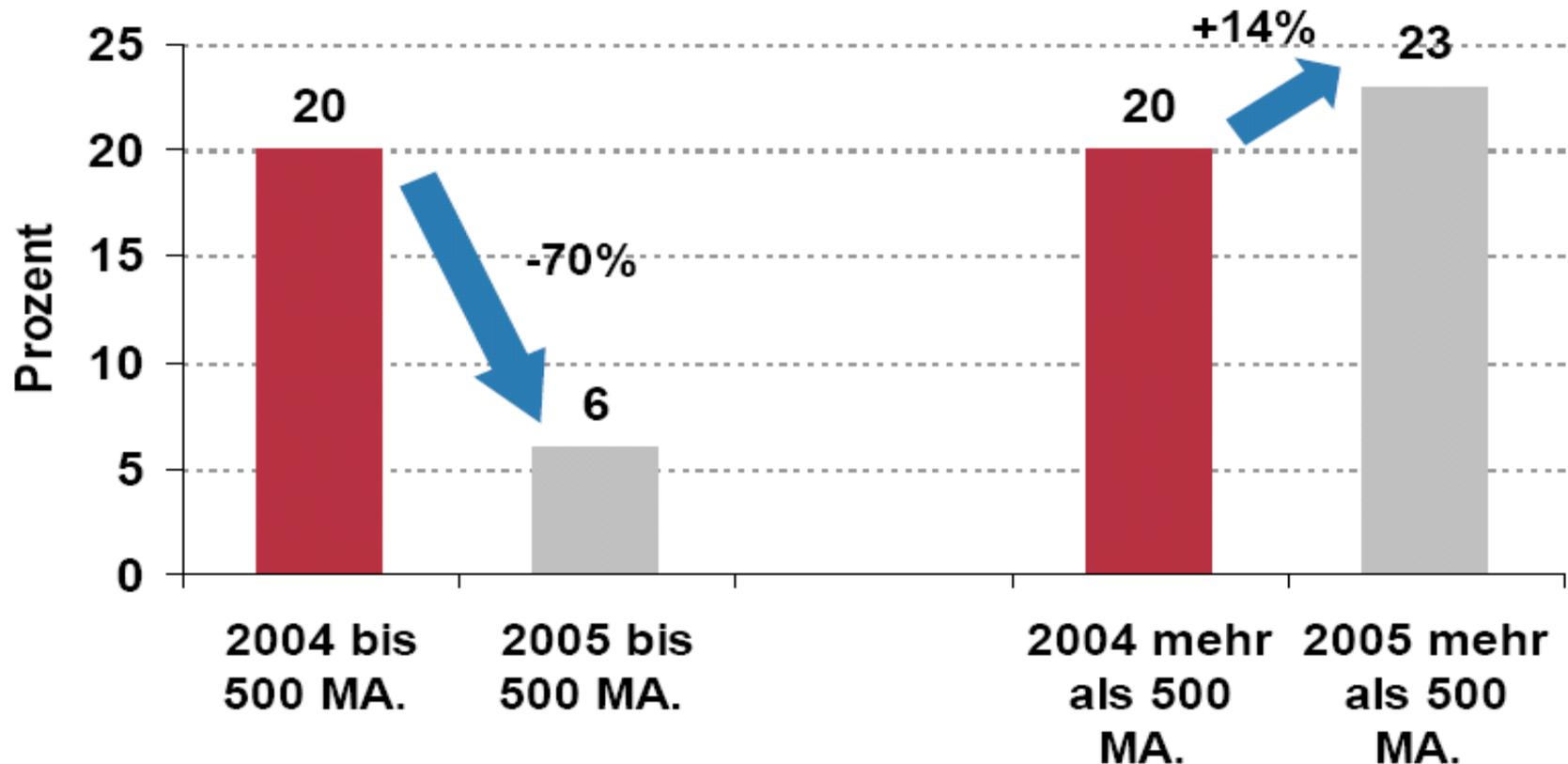
IQPC Kongress „Mobile Security“
FF/M - 30.01. - 01.02.2006

Frank Pallas – TU Berlin

Zur Einstimmung

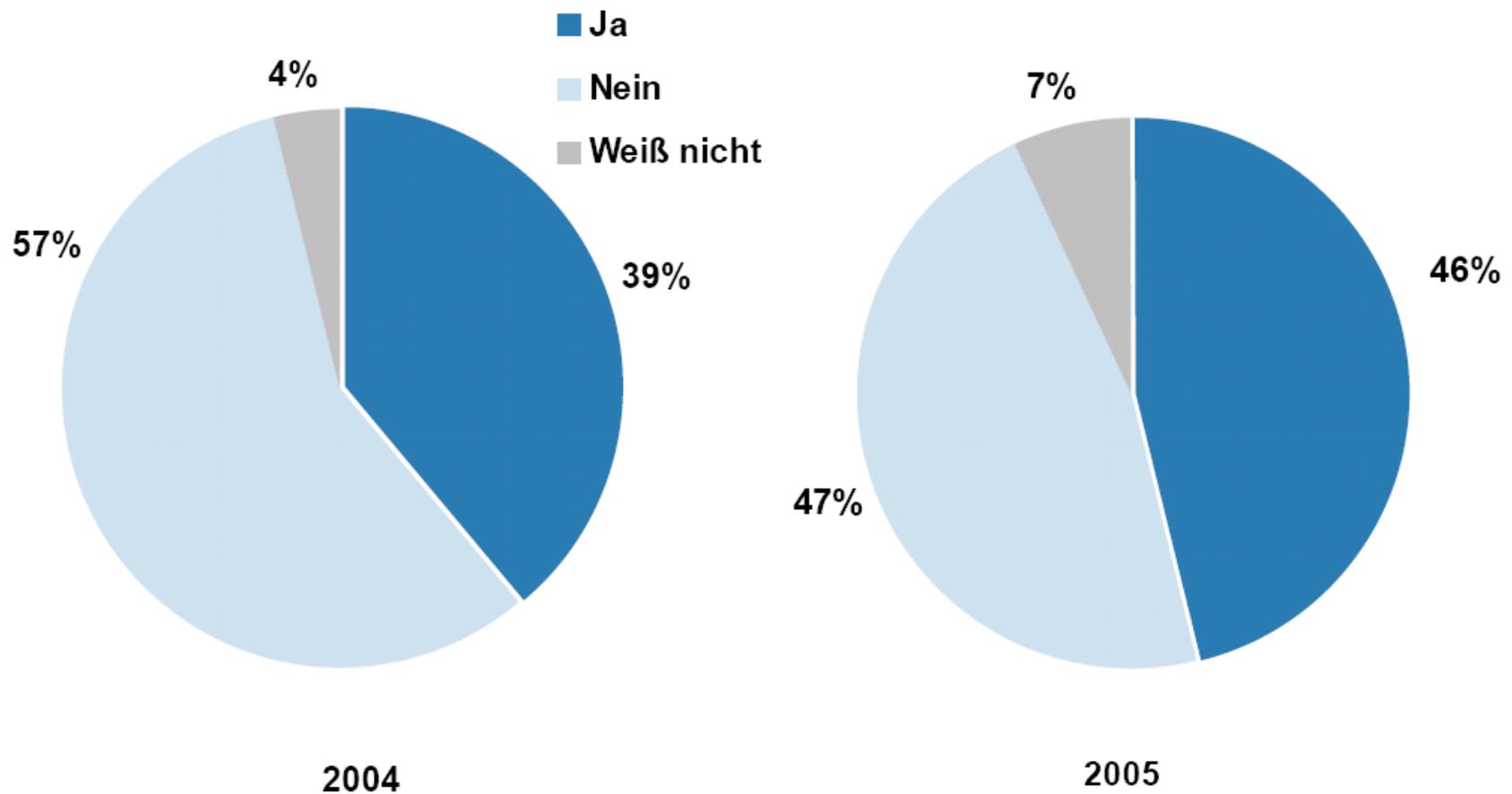
Ubitexx/Informationweek: PDA Security Studie 2005

Auftreten schwerer Sicherheitsvorfälle bei PDAs



Zur Einstimmung

„Existiert eine einheitliche Security Policy?“



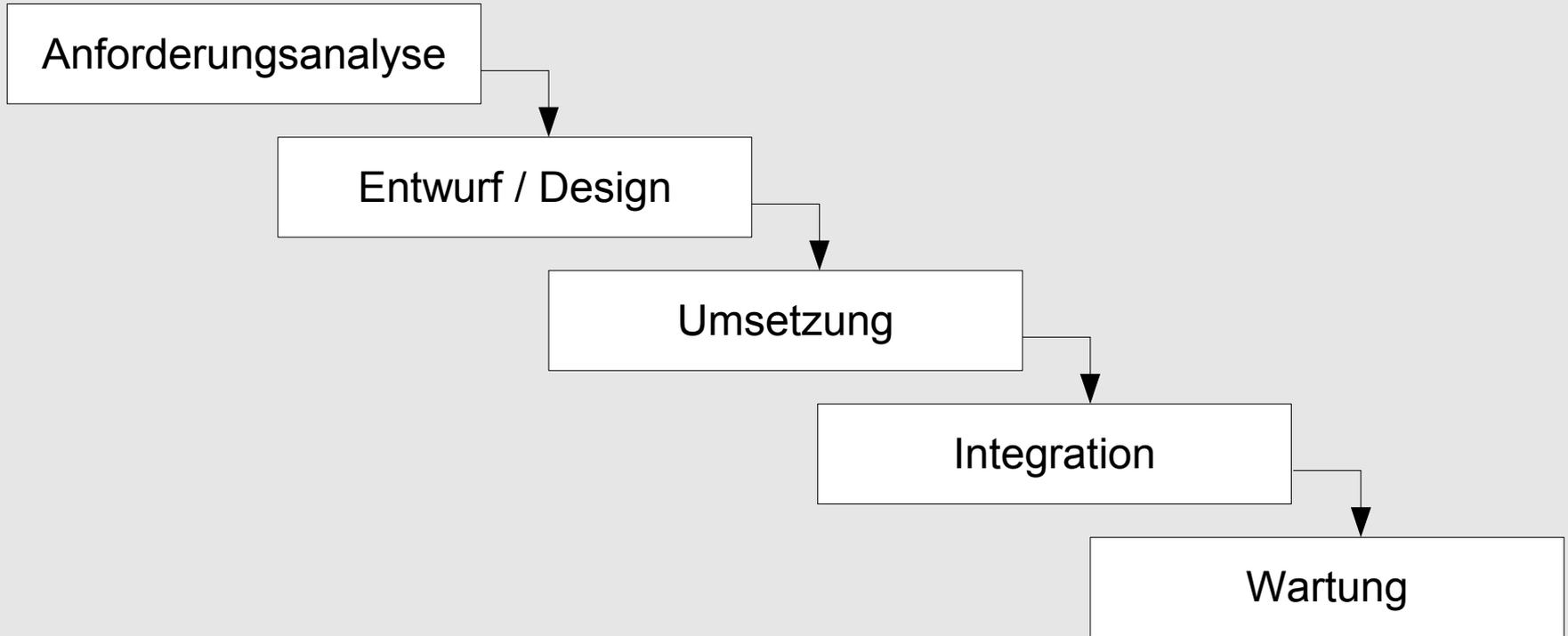
„Eine Sicherheitspolitik [...] definiert
Richtungen und Ziele [...] Die Politik
ist der Teil, der alles miteinander
verknüpft.“

Bruce Schneier: Secrets & Lies, S. 279f.

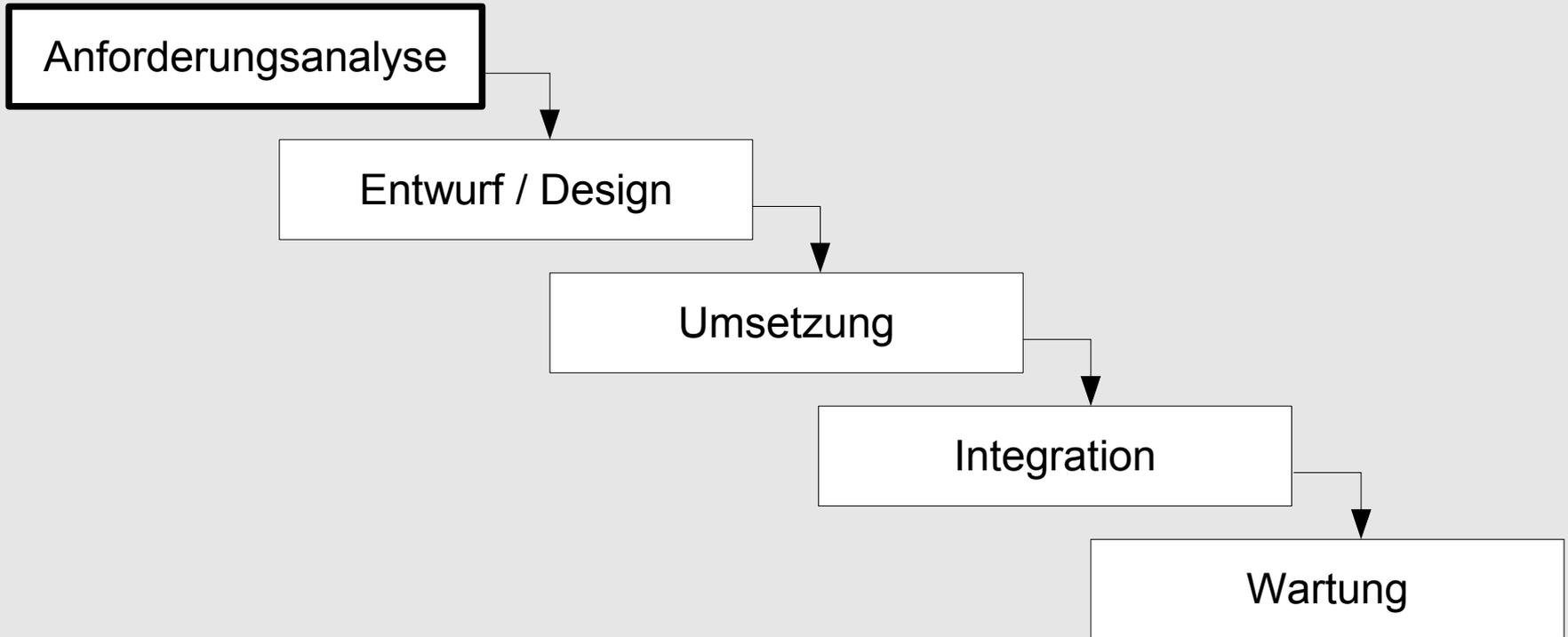
„In einer Sicherheitsrichtlinie werden
Schutzziele und allgemeine
Sicherheitsmaßnahmen im Sinne
offizieller Vorgaben [...] formuliert.“

BSI, Leitfaden IT-Grundschutz

Entwicklung einer Security Policy



Entwicklung einer Security Policy



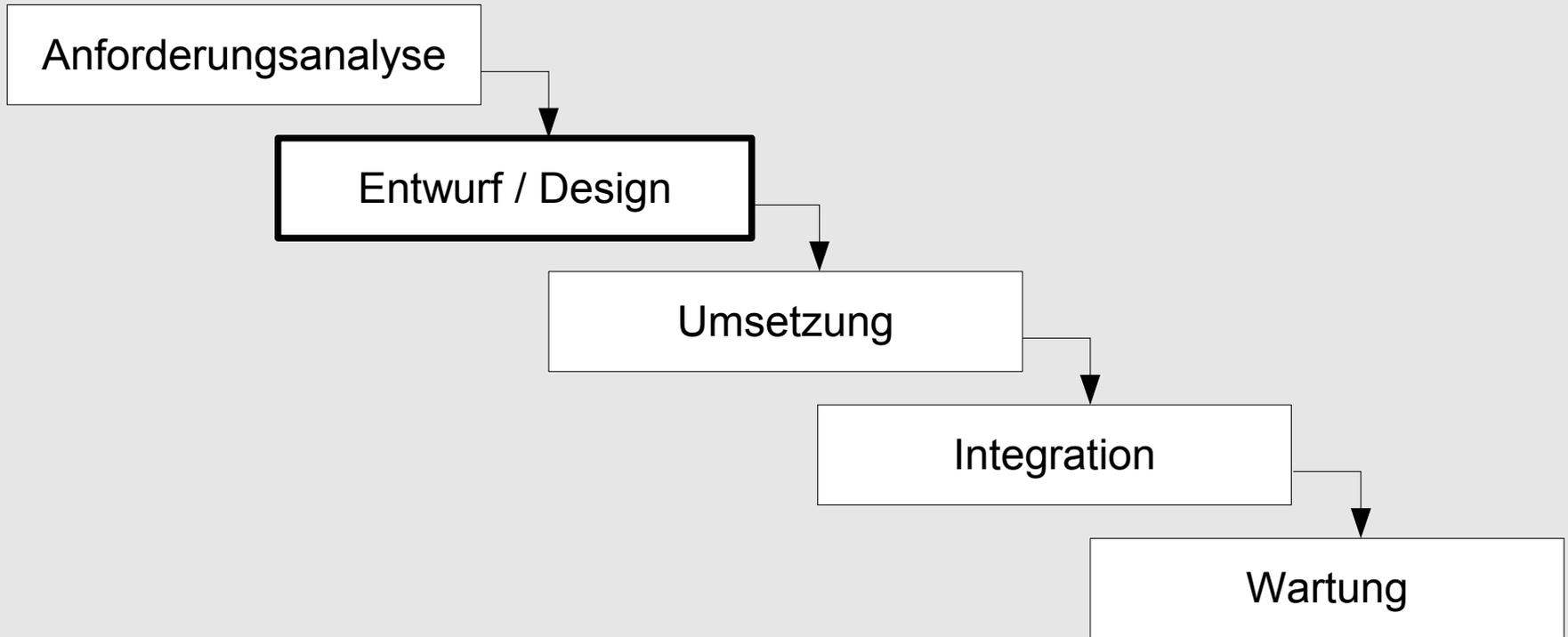
- Welche Werte sind zu schützen?
- Was sind mögliche Schadensfälle?
- Welche Rahmenbedingungen gibt es?
- **Welche Funktionalität wird benötigt?**

Security Policies: 1. Ebene

Allgemeine Sicherheitsziele

z.B. „Interne Daten werden auch bei mobiler Nutzung adäquat geschützt.“

Entwicklung einer Security Policy



- Wie lassen sich die Ziele erreichen?
- Welche Vorgehensweise (techn./org.)?
- Wie sind die Mechanismen miteinander vereinbar?

Security Policies: 2. Ebene

Allgemeine Sicherheitsziele

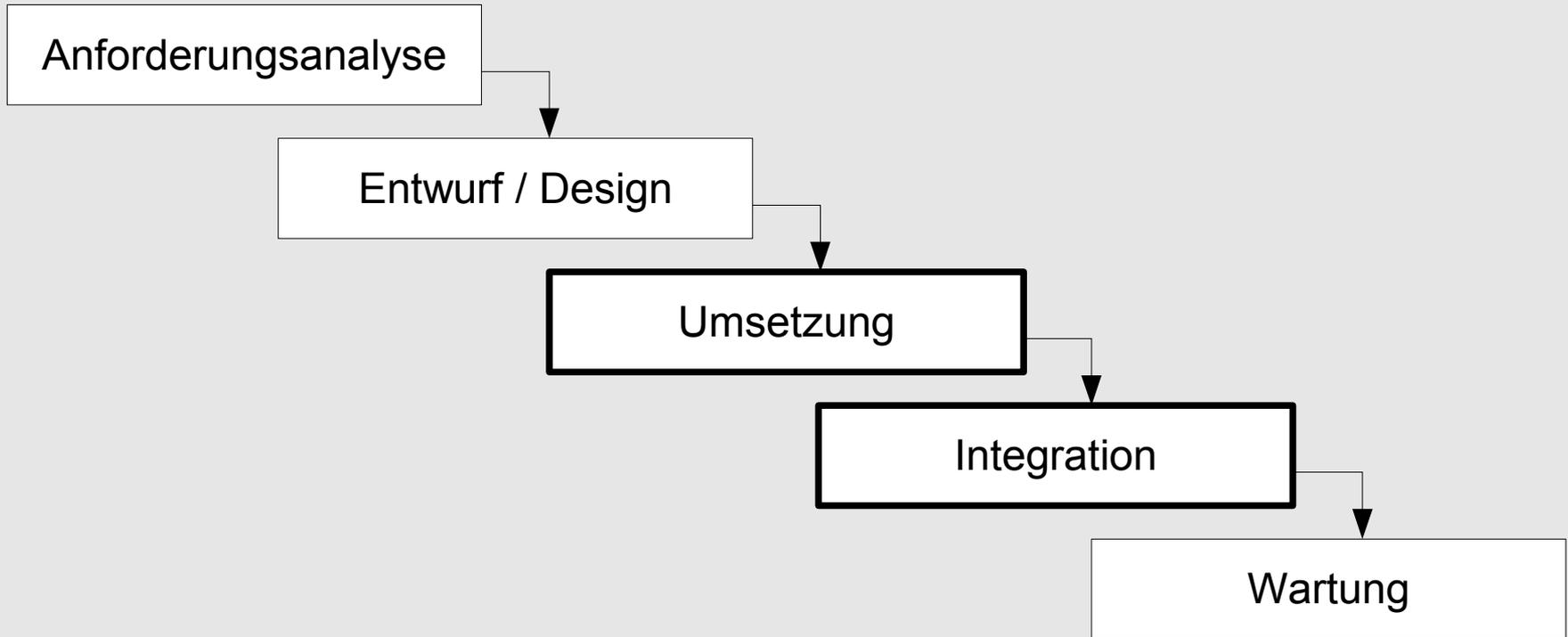
z.B. „Interne Daten werden auch bei mobiler Nutzung adäquat geschützt.“

Werden genauer spezifiziert durch

Detaillierte Sicherheitsziele

z.B. „Interne Daten dürfen nur auf mobilen Geräten gespeichert werden, wenn diese mit mindestens 128Bit-AES verschlüsselt sind.“

Entwicklung einer Security Policy



- Welche Produkte sind verfügbar?
- Wie müssen diese konfiguriert werden?
- Wie werden org. Regelungen umgesetzt?
- **Formale Anerkennung durch alle Beteiligten**

Security Policies: 3. Ebene

Allgemeine Sicherheitsziele

z.B. „Interne Daten werden auch bei mobiler Nutzung adäquat geschützt.“

Werden genauer spezifiziert durch

Detaillierte Sicherheitsziele

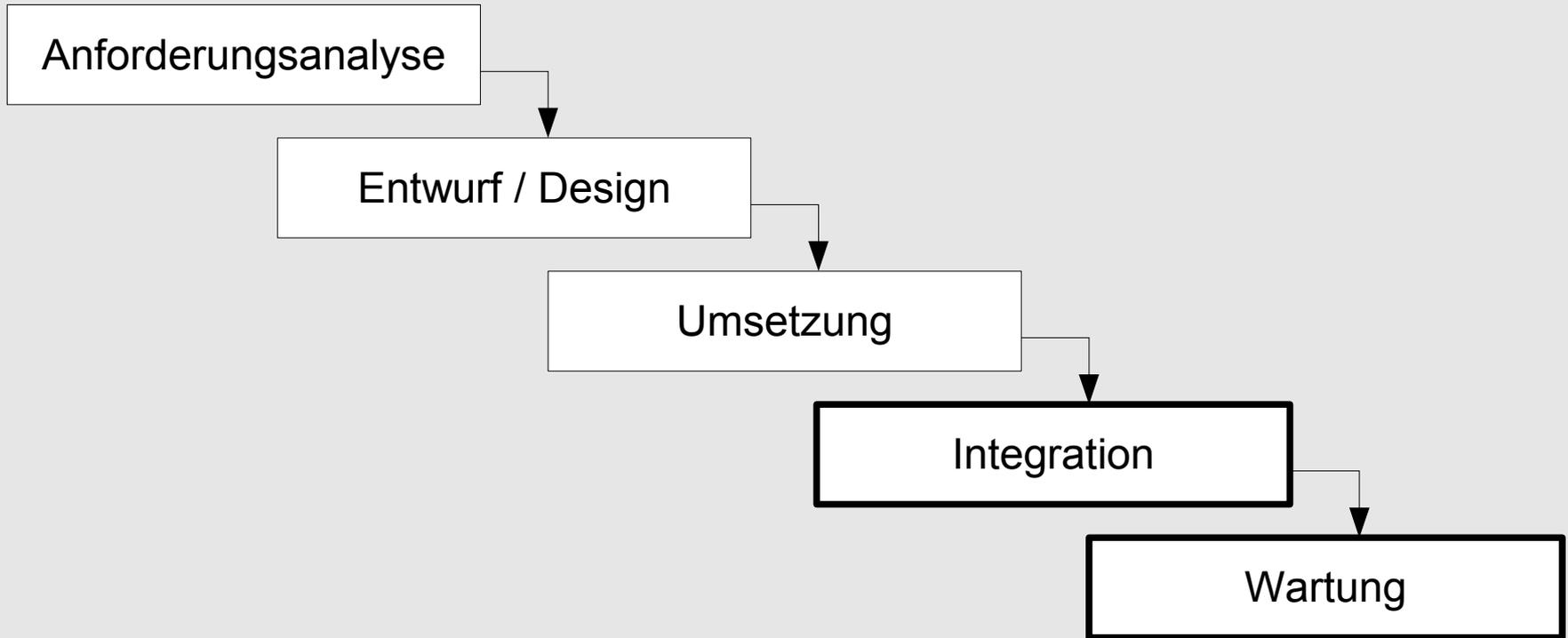
z.B. „Interne Daten dürfen nur auf mobilen Geräten gespeichert werden, wenn diese mit mindestens 128Bit-AES verschlüsselt sind.“

Werden konkret umgesetzt durch

Konkrete Maßnahmen

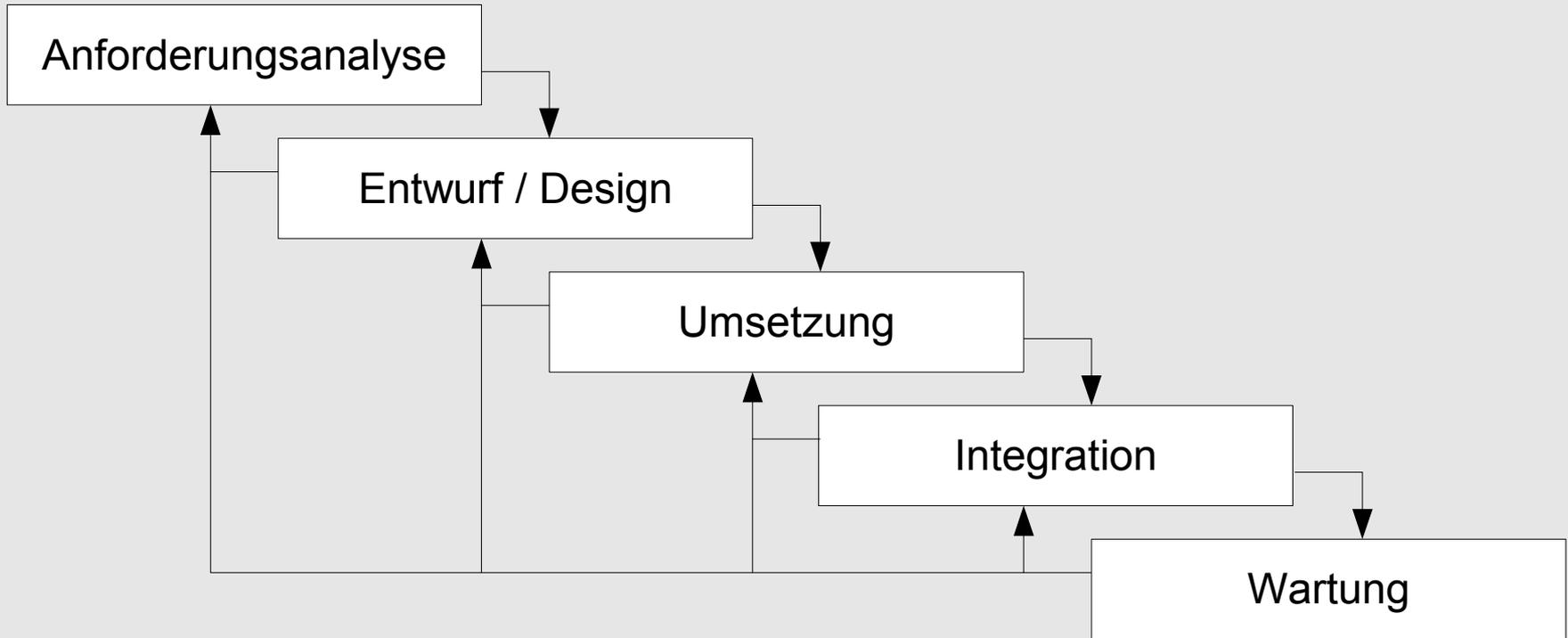
z.B. „Zur Sicherung von Notebooks kommt <xyz> in der Version <123> zum Einsatz. [...] <xyz> wird so konfiguriert, dass die Geräte mit 128Bit-AES verschlüsselt werden.“

Entwicklung einer Security Policy



- Umsetzen
- Ständig überprüfen
- **Wenn nötig: Nachsteuern, Ändern, Erweitern, ...**

Entwicklung einer Security Policy



– Wenn nötig: Nachsteuern, Ändern, Erweitern, ...

Security Policies: 3 Ebenen

Allgemeine Sicherheitsziele

z.B. „Interne Daten werden auch bei mobiler Nutzung adäquat geschützt.“

Werden genauer spezifiziert durch

Detaillierte Sicherheitsziele

z.B. „Interne Daten dürfen nur auf mobilen Geräten gespeichert werden, wenn diese mit mindestens 128Bit-AES verschlüsselt sind.
Passwörter haben eine Länge von mindestens 8 Zeichen.“

Werden konkret umgesetzt durch

Konkrete Maßnahmen

z.B. „Zur Sicherung von Notebooks kommt <xyz> in der Version <123> zum Einsatz. [...] <xyz> wird so konfiguriert, dass die Geräte mit 128Bit-AES verschlüsselt werden **und dass die minimale Passwortlänge von 8 Zeichen erzwungen wird.**“

Zusammenfassend:

- Sicherheitspolicies werden in mehreren Schritten erstellt
- Sicherheitspolicies existieren in mindestens 3 Ebenen
- Sicherheitspolicies unterliegen ständigen Anpassungen

So weit nichts neues...

„[M]obility makes things more
difficult.“

Roger Needham, Microsoft Research

Mobile Security: 6 Herausforderungen

- Gerätemobilität

- London 2005:
 - >4.000 Notebooks
 - >5.000 PDAs
- Diebstahl
- ...



→ Kein physischer Schutz

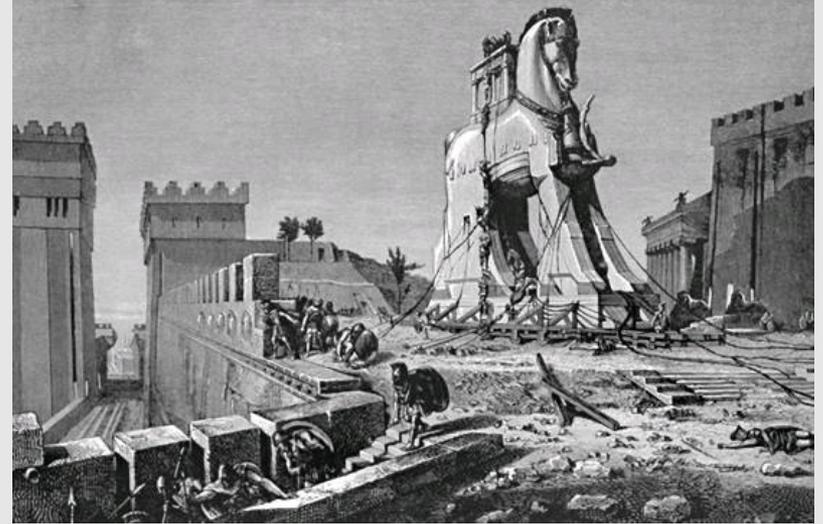
Quellen:

<http://www.england2004.afewbytes.com>

http://www.theregister.co.uk/2005/01/25/taxi_survey/

Mobile Security: 6 Herausforderungen

- Gerätemobilität
- Virales Verhalten
 - Umgehen von Firewalls
 - Umgehen von Virensclannern
 - ...



➔ Physisches Überwinden der Netzgrenzen

Mobile Security: 6 Herausforderungen

- Gerätemobilität
- Virales Verhalten
- Personengebundenheit
 - Direkte Zuweisung
 - Private Geräte
 - Individuelle Anpassung
 - V.I.P.s



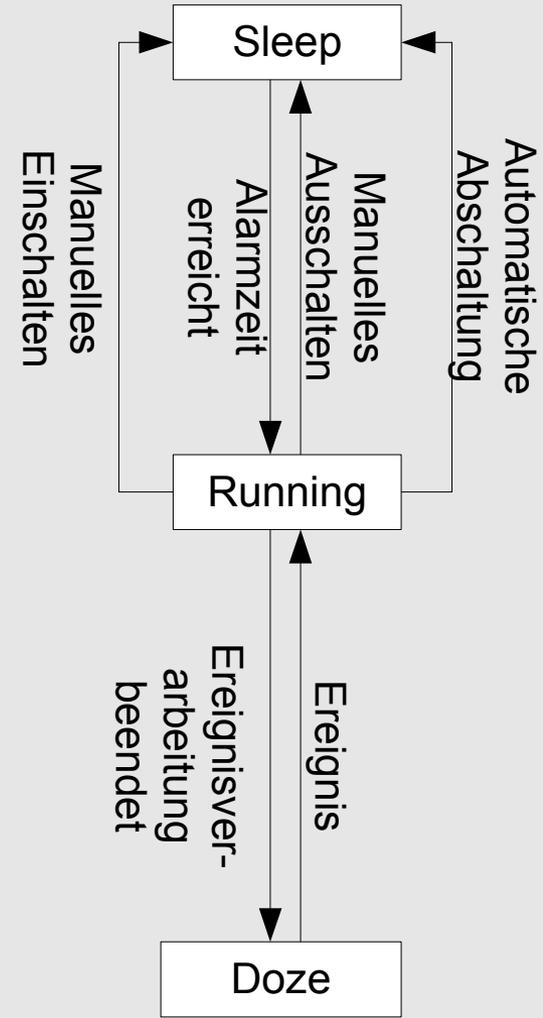
➔ Widerstände gegen restriktives Vorgehen

Mobile Security: 6 Herausforderungen

- Gerätemobilität
- Virales Verhalten
- Personengebundenheit
- Kommunikatives Wesen
 - Bluetooth, IrDA, LAN, WLAN
 - GSM, GPRS, UMTS
 - CD, DVD (Brenner?)
 - SD-, MMC-, PC-Cards, USB-Sticks
 - ...

Mobile Security: 6 Herausforderungen

- Gerätemobilität
- Virales Verhalten
- Personengebundenheit
- Kommunikatives Wesen
- Kontinuierliche Aktivität
 - PDAs/Smartphones: durchgehend an
 - Notebooks: Suspend-to-(Disk|RAM)?



Mobile Security: 6 Herausforderungen

- Gerätemobilität
 - Virales Verhalten
 - Personengebundenheit
 - Kommunikatives Wesen
 - Kontinuierliche Aktivität
 - Technische Unzulänglichkeiten
 - Rechteverwaltung?
 - Zentrales Management?
 - Lange Passwörter auf PDAs?
- Etablierte Vorgehensweisen u.U. unpassend!

Widersprüche

:: English :: Deutsch (D) :: Nederlands :: Česky :: Deutsch (A)



Welcome to my T-Mobile Hotspot Administration portal!

With the T-Mobile Hotspot Administration portal you can:

- Monitor usage of your T-Mobile Hotspot account
- Change your login password
- Send yourself a password reminder to your nominated Email account.
- Send yourself a password reminder by SMS (text) to your nominated mobile phone.

Please log in using your existing full HotSpot username and password.

Once you have set up your nominated email account or mobile phone number, simply enter your user name and the number sequence from the panel below and click the "Remind me" button for a password reminder.

Please go to www.t-mobile.co.uk/hotspot for more information on the T-Mobile Hotspot service.

Login

User name

Password

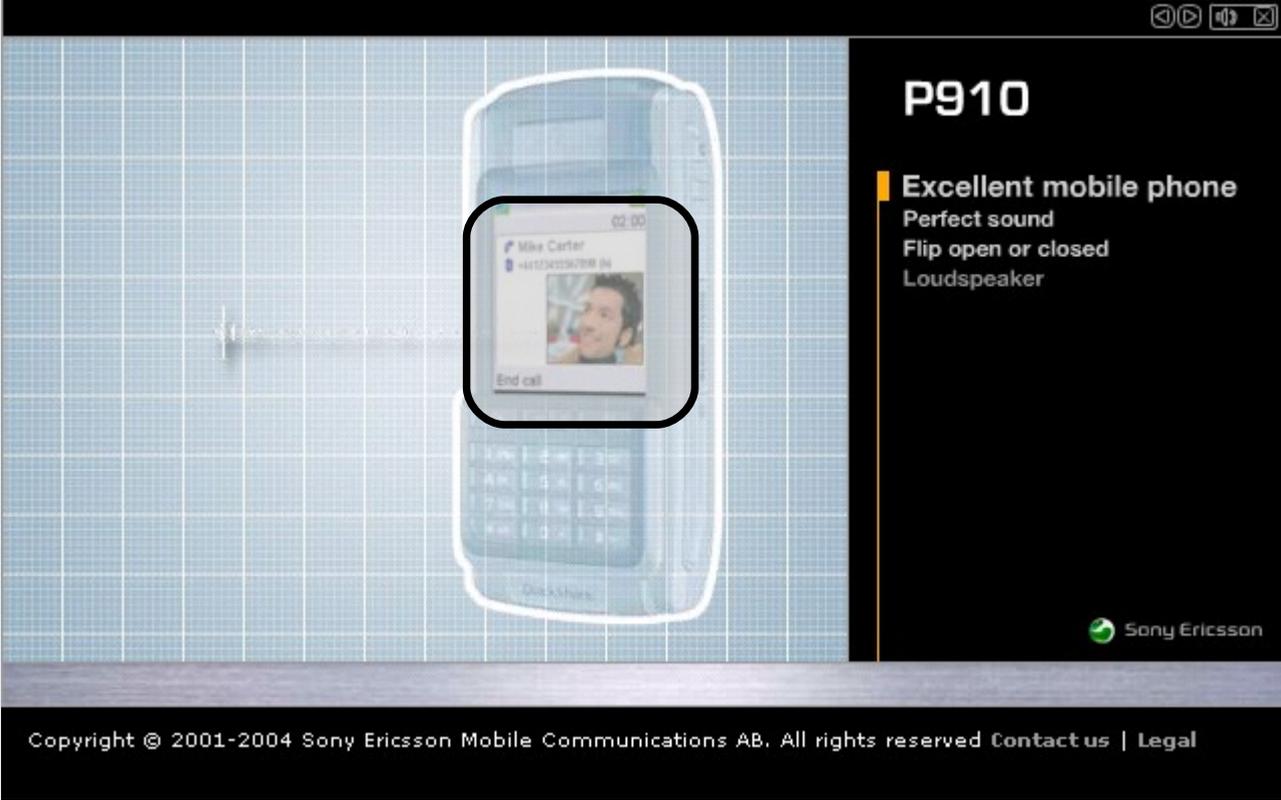
Login

Password-Reminder

User name

8 1 . 2

Widersprüche



P910

Excellent mobile phone
Perfect sound
Flip open or closed
Loudspeaker

Sony Ericsson

Copyright © 2001-2004 Sony Ericsson Mobile Communications AB. All rights reserved Contact us | Legal

Zusammenfassend:

- Smartphones und PDAs sind besonders heikel
- Mobiler Nutzen und IT-Sicherheit widersprechen sich oftmals
- Security Police muss mobile Geräte explizit berücksichtigen
 - Alle 3 Ebenen
 - Technische **und** organisatorische Maßnahmen
 - **Mindestens** 6 besondere Eigenschaften

Mobile Security Policy: Ein Anfang

- **Gerätemobilität:**
 - Datenmenge klein halten
(technisch, organisatorisch)
 - Geräte verschlüsseln
(technisch)
- **Virales Verhalten**
 - Nur kontrollierte Synchronisation
(technisch)
- **Personengebundenheit**
 - Private Geräte verbieten, Individualisierung einschränken
(technisch **und** organisatorisch)

Mobile Security Policy: Ein Anfang

- **Kommunikatives Wesen**
 - Schnittstellen sichern, Ausnahmen vorsehen (technisch **und** organisatorisch)
 - Verbindungen sichern (technisch, evtl. organisatorisch)
- **Kontinuierliche Aktivität (insb. PDAs)**
 - ∅
 - Berücksichtigen bei obigen Maßnahmen
- **Technische Unzulänglichkeiten (insb. PDAs)**
 - Zentrales Management einführen (technisch)
 - Berücksichtigen bei obigen Maßnahmen

„As soon as you have distributed systems, you have people responsible for security in all sorts of places,

and they have to apply rules which in general terms they don't understand.“

Roger Needham, Microsoft Research

Weitere Anlaufstellen

- BSI Grundschutzleitfaden:
<http://www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf>
- BSI Grundschutzhandbuch (insb. Kap. 5.3 + 8.7)
<http://www.bsi.de/gshb/deutsch/download/GSHB2004.pdf>
- The SANS Security Policy Project:
<http://www.sans.org/resources/policies/>
- Homepage des Referenten:
<http://ig.cs.tu-berlin.de/ma/fp>