Workshop: Unternehmenspolicy zur Mobilen Sicherheit

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

Frank Pallas – TU Berlin

Agenda

- Die Herausforderung
  - Was bedeutet „Mobile Security“?
- Die technische Sicht
  - Wege zu mehr mobiler Sicherheit
  - Grenzen technischer Ansätze
- <Pause>
- Der mögliche Ausweg
  - Security Policies im Allgemeinen
  - Beispielhaftes Erarbeiten einer „Mobile Security Policy“
- Conclusio

Worum geht es hier eigentlich?

?

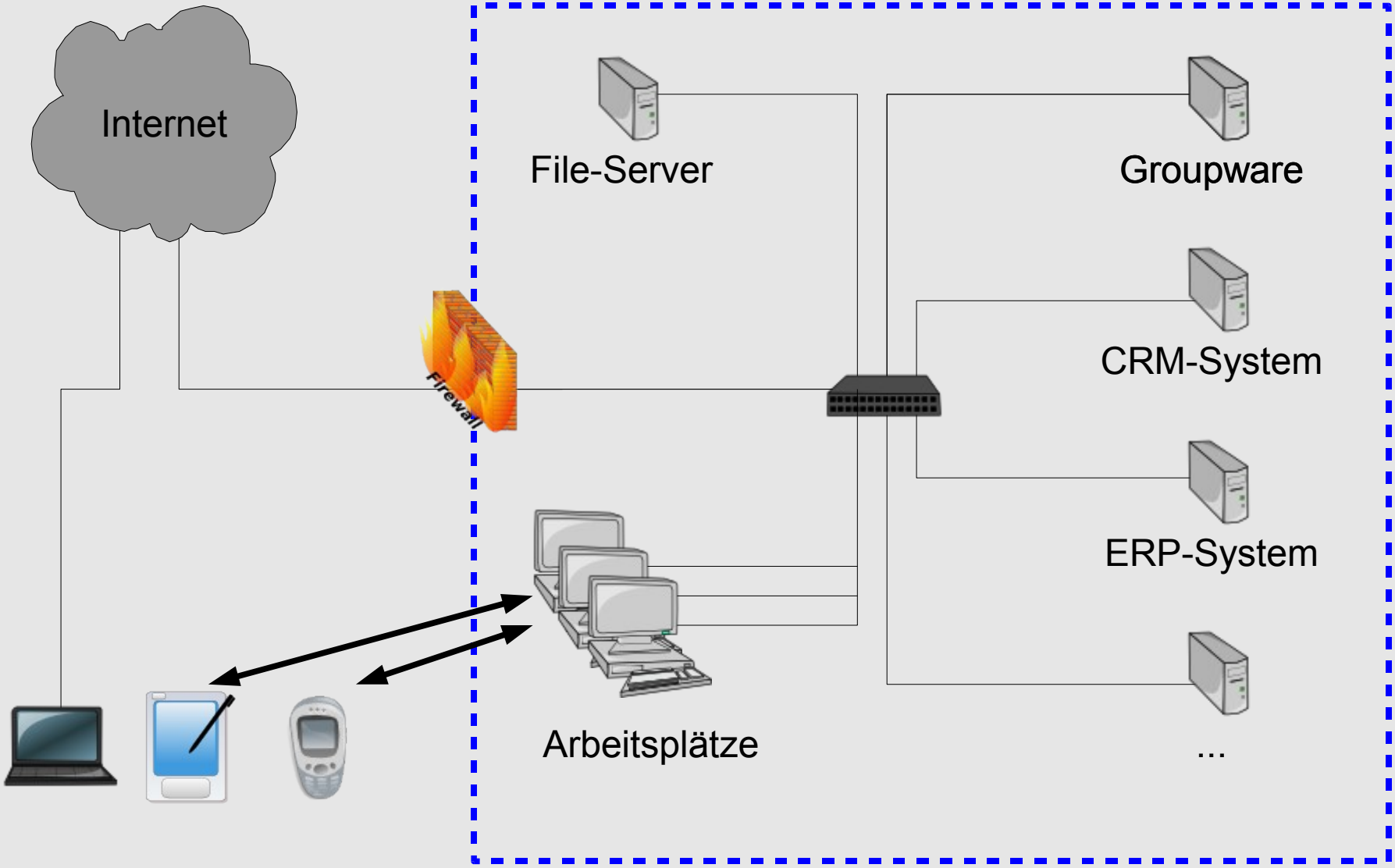
Oder geht es eher um...

?

Und nicht zu vergessen...

- BDSG
- KonTraG
- Basel II
- Sarbanes-Oxley-Act
- ...

Die Herausforderung

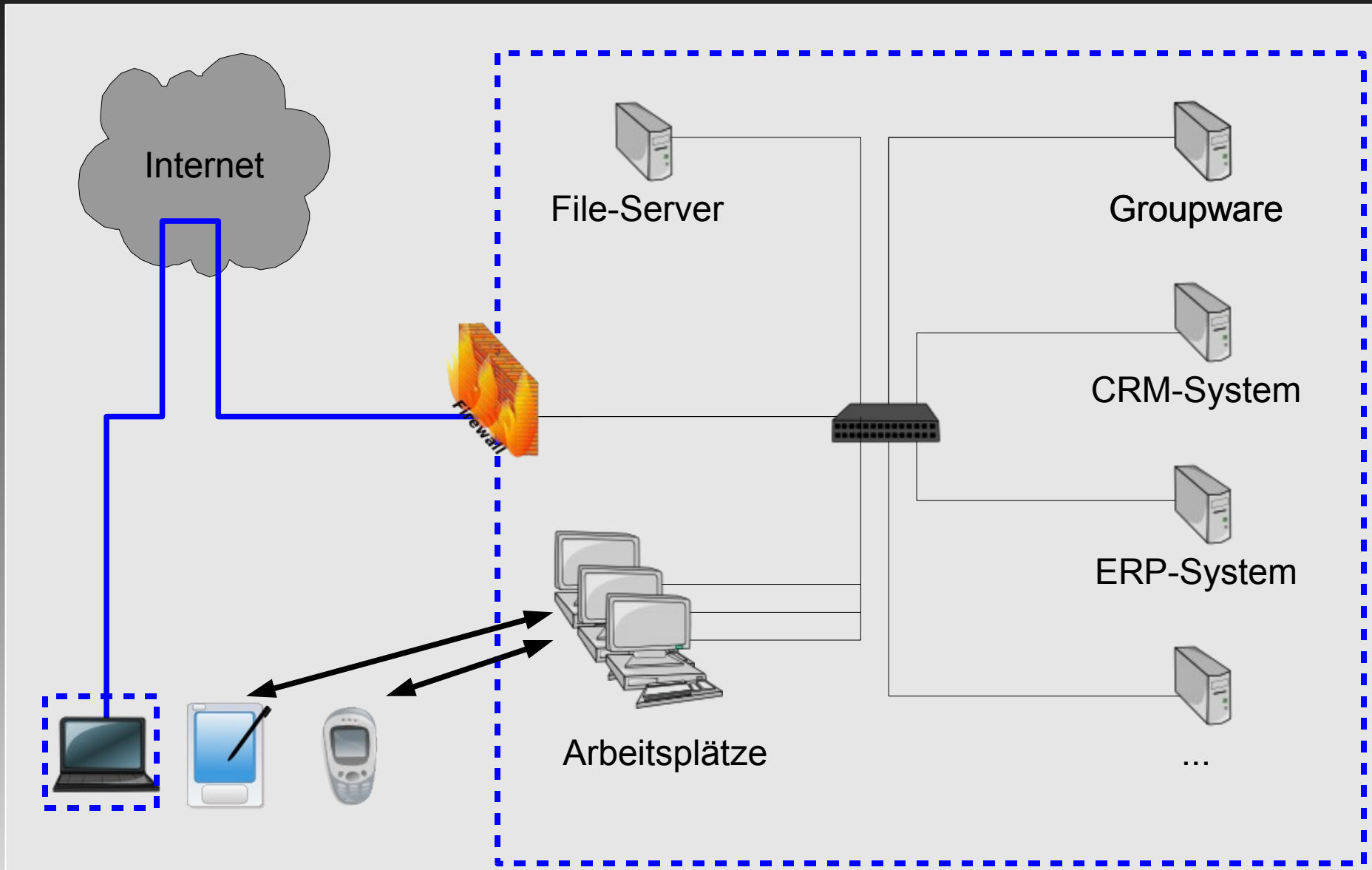


Technische Lösungsansätze

IT-Sicherheit klassisch

- Abgeschottete Netze
  - Physischer Schutz
  - Firewalls
  - ...
- Verhindern verdeckter Kanäle
  - Keine Disketten- / CD-Laufwerke
  - Überprüfen von Email-Anhängen
  - ...
- Definierte Lese- / Schreibrechte
- Protokollierung
- „Verschlüsselung“

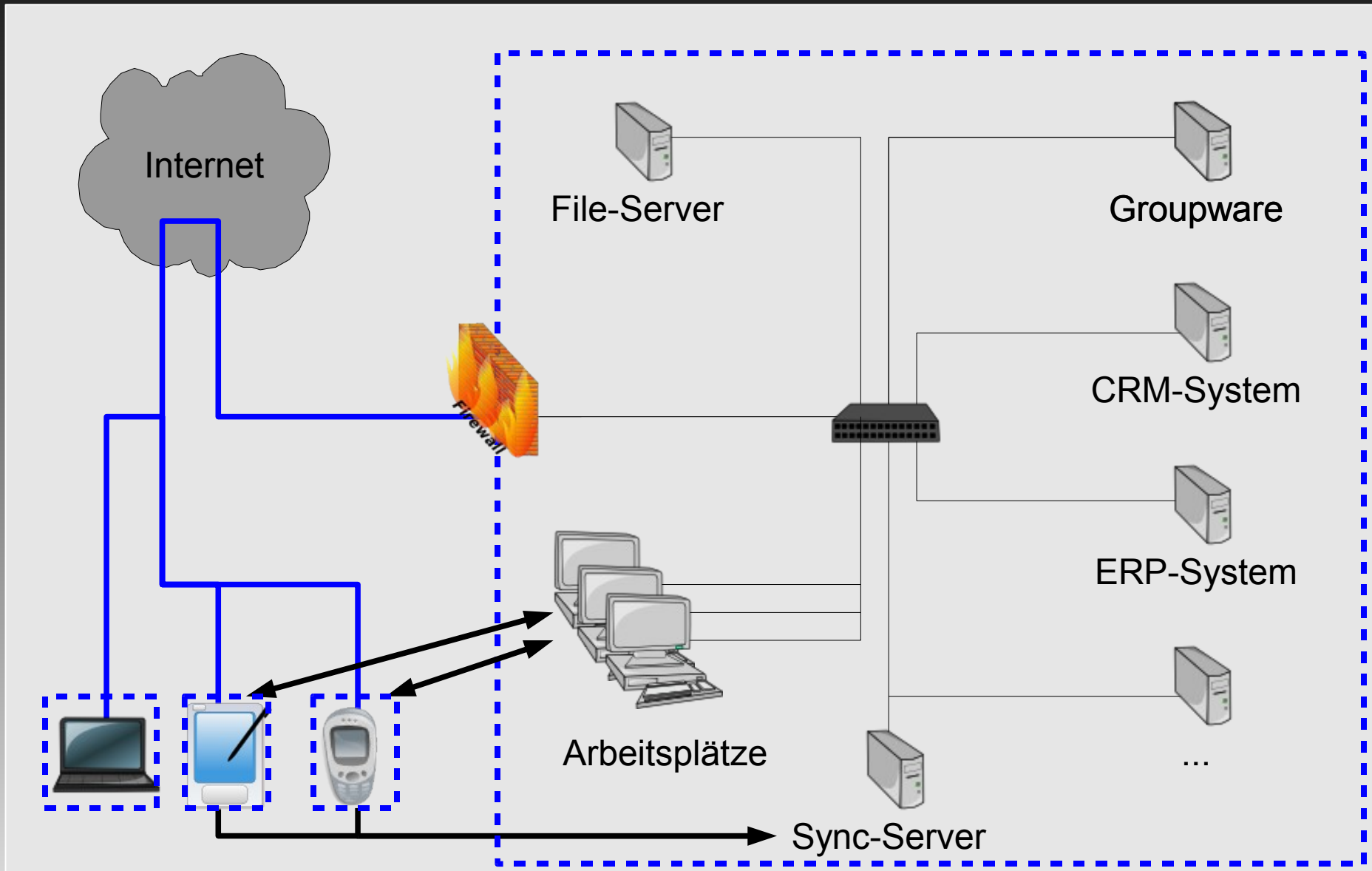
Was also tun?


Internet
File-Server
Groupware
CRM-System
ERP-System
...
Firewall
Arbeitsplätze

Technische Lösungsansätze

- Notebooks
  - VPN
  - Verschlüsselung
  - Schnittstellenreglementierung
  - Einschränkung externer Datenträger
  - Was noch?

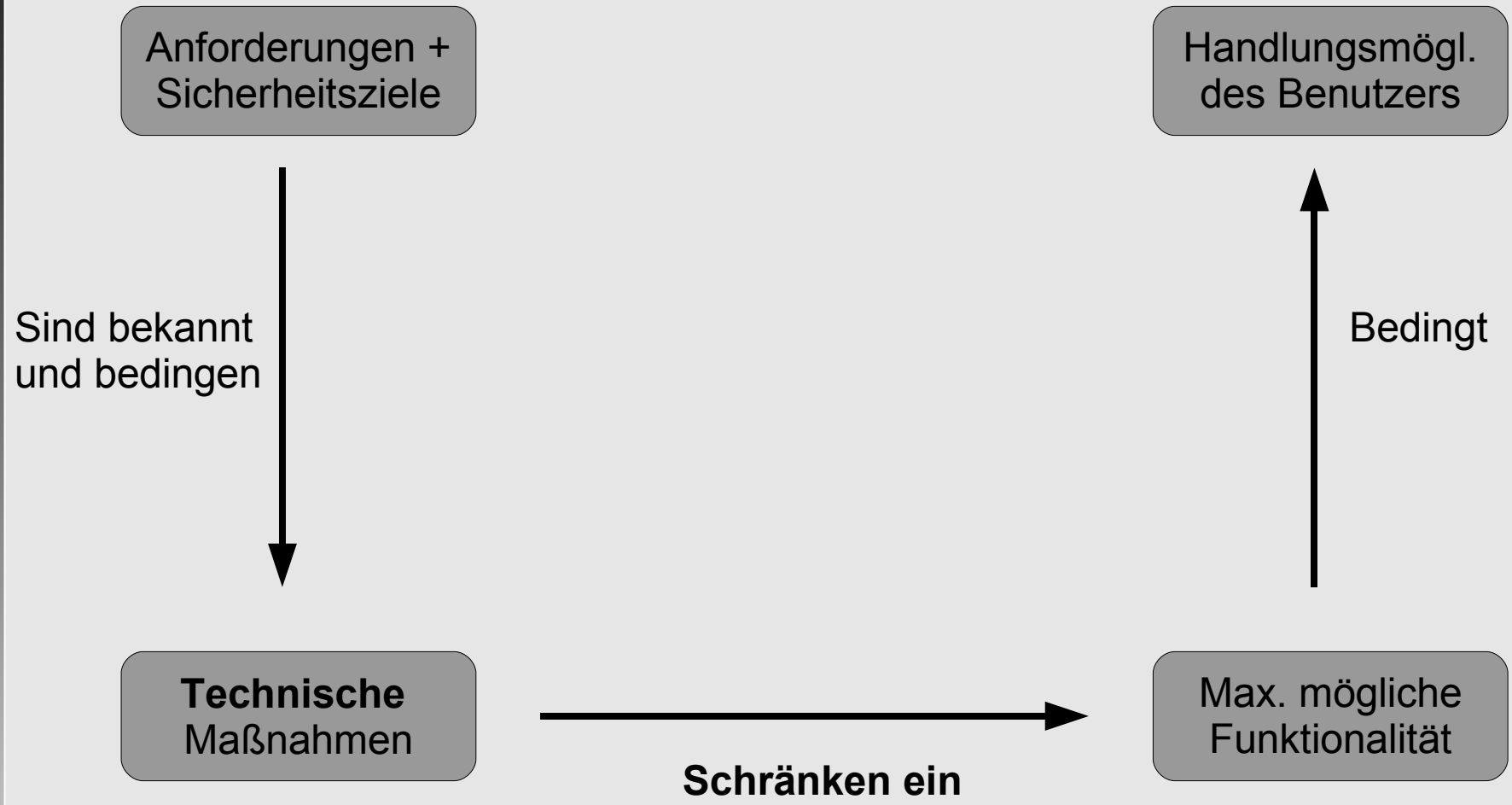
Was also tun?


Internet
File-Server
Groupware
Firewall
CRM-System
ERP-System
Arbeitsplätze
...
Sync-Server

Technische Lösungsansätze

- Notebooks
  - VPN
  - Verschlüsselung
  - Schnittstellenreglementierung
  - Einschränkung externer Datenträger
- PDAs / Smartphones
  - (VPN)
  - Verschlüsselung
  - Schnittstellenreglementierung
  - (Einschränkung externer Datenträger)
  - **Kontrollierte Synchronisation (!)**

IT-Sicherheit klassisch - Vorgehen



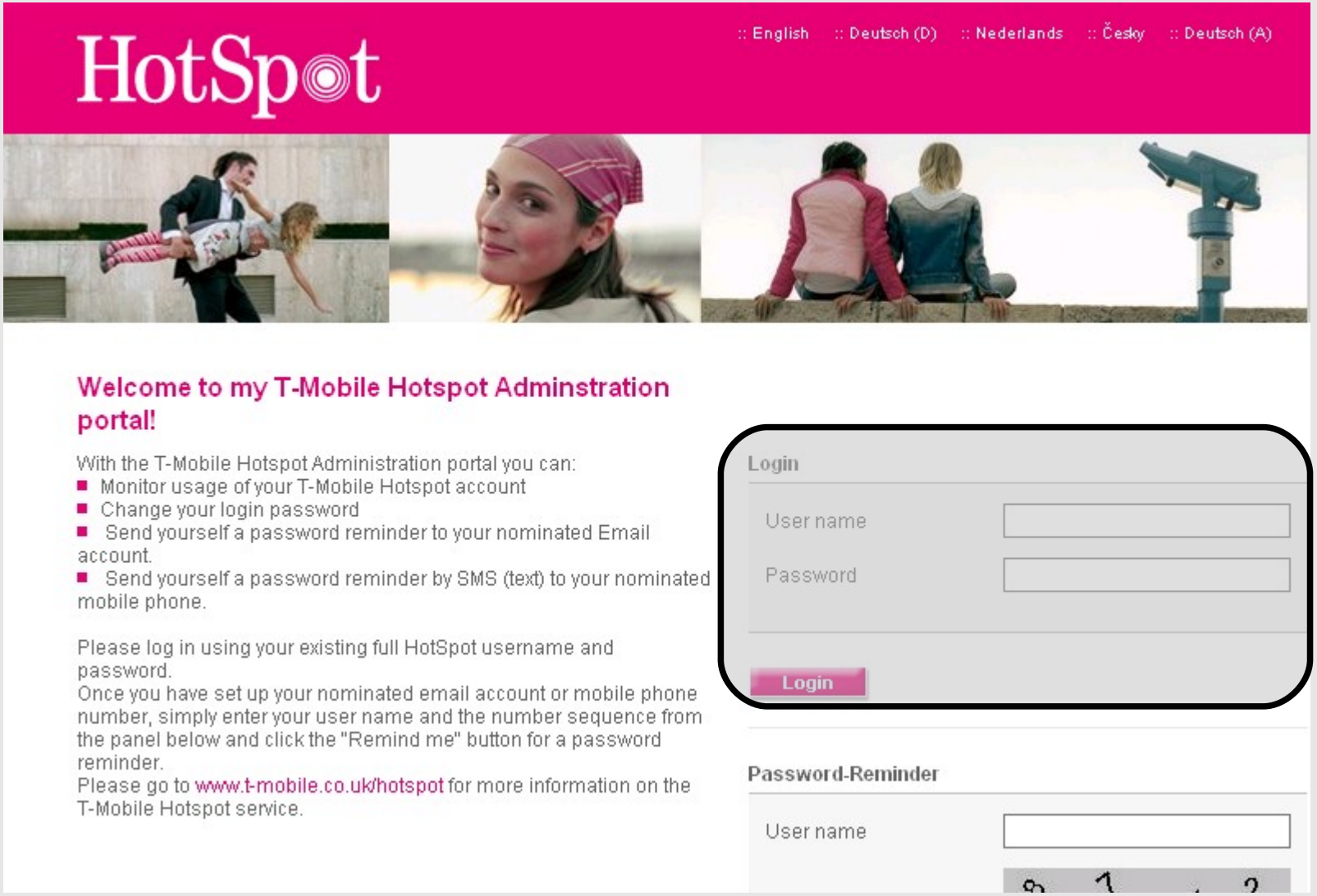
„[M]obility makes things more difficult.“

Roger Needham, Microsoft Research

Grenzen eines technischen Ansatzes

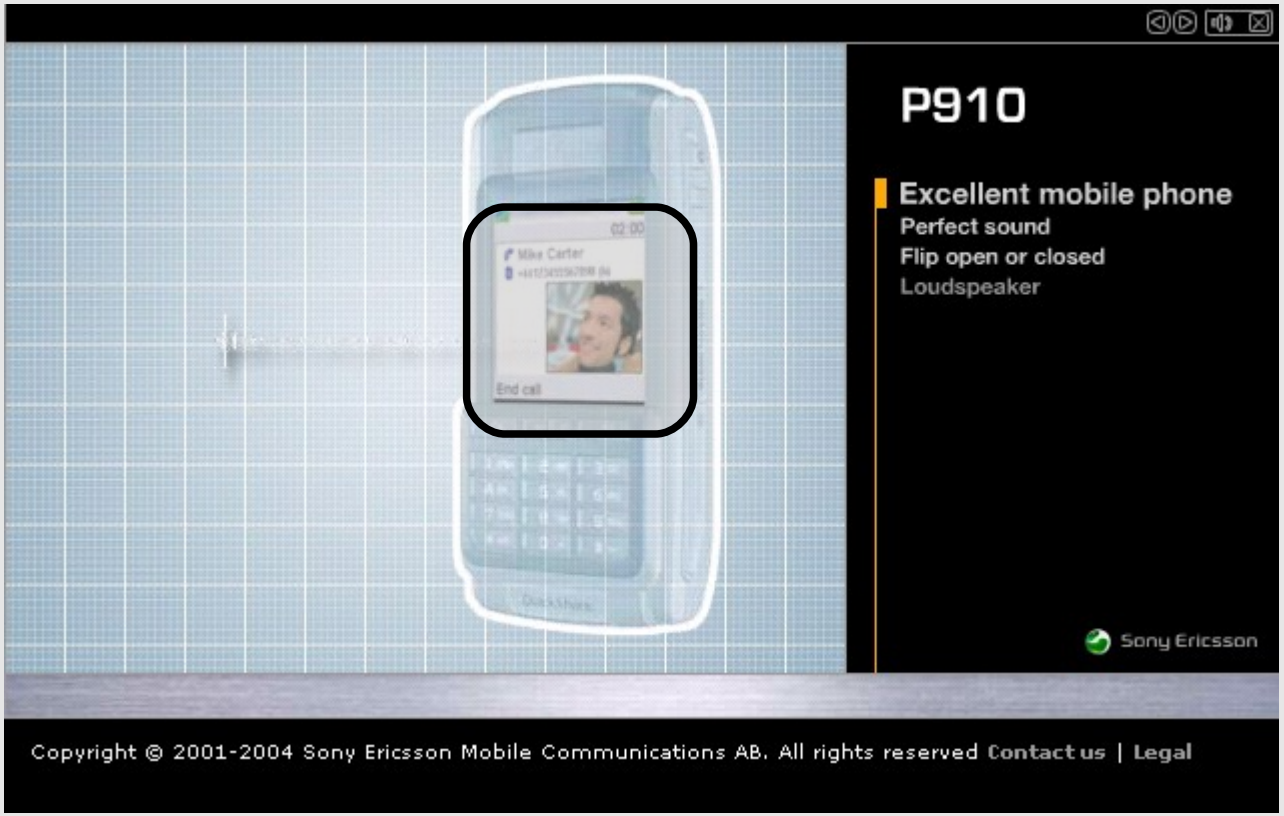
?

Widersprüche



Quelle: https://myhotspot.t-mobile.net/wlan/

Widersprüche

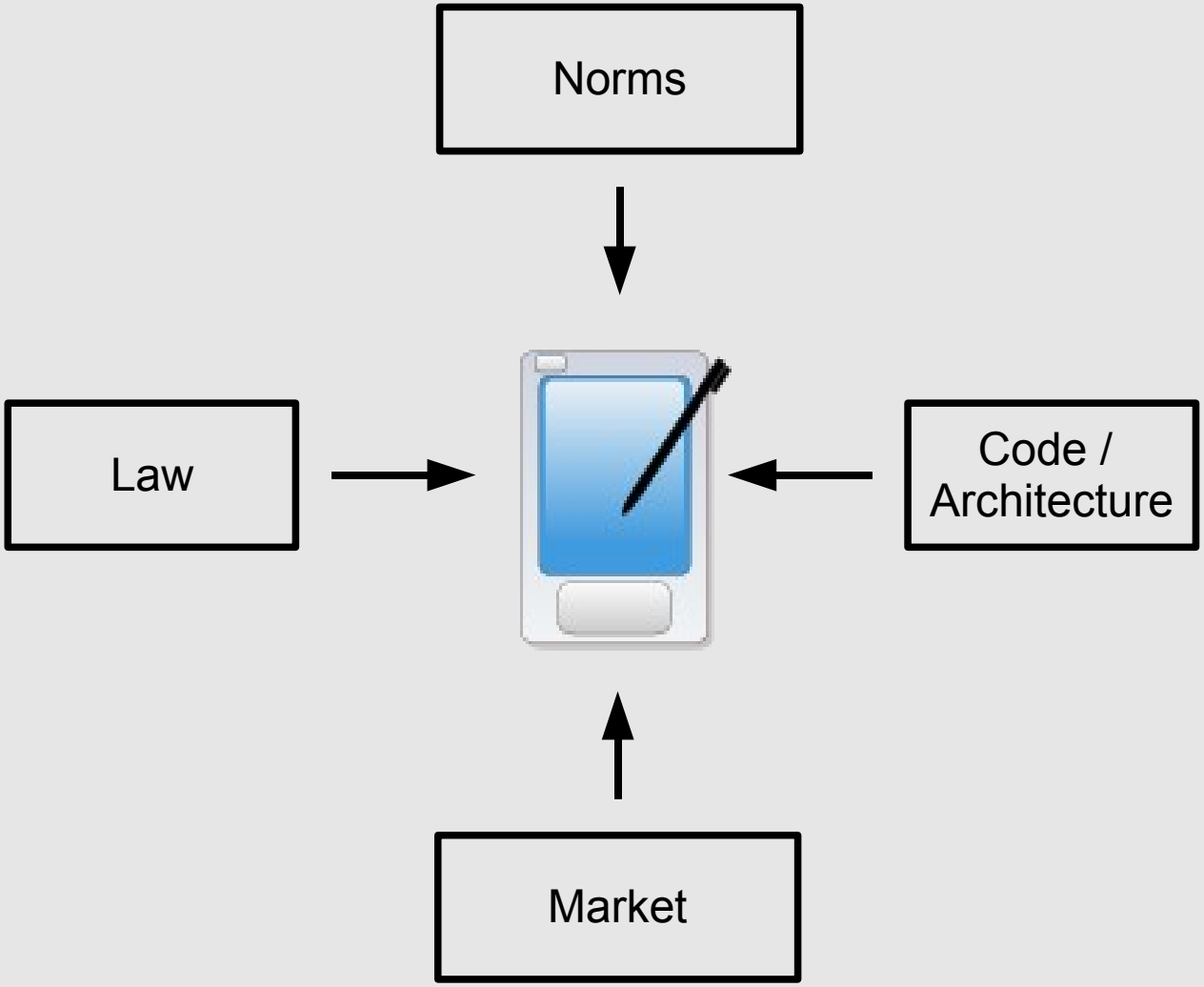


Quelle: http://www.sonyericsson.com/product/p910/

~15.20 Uhr?

<Pause>

Nicht-Technische Ansätze



Grafik nach: Lawrence Lessig (1999): Code and other laws of cyberspace

„Eine Security Policy muss her!“

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

BSI, Leitfaden IT-Grundschutz

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

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

Security Policies: 3 Grundregeln

- Betroffene beteiligen
  - „top down“ vs. „bottom up“
  - Informationsdefizite an der Spitze
- Schriftlich fixieren
  - Nach Erstellung/Änderung
  - Bei Neueinstellung
- Regelmäßig überprüfen
  - Neue Anforderungen
  - Neue Rahmenbedingungen
  - ...

Security Policies: 3 Ebenen

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

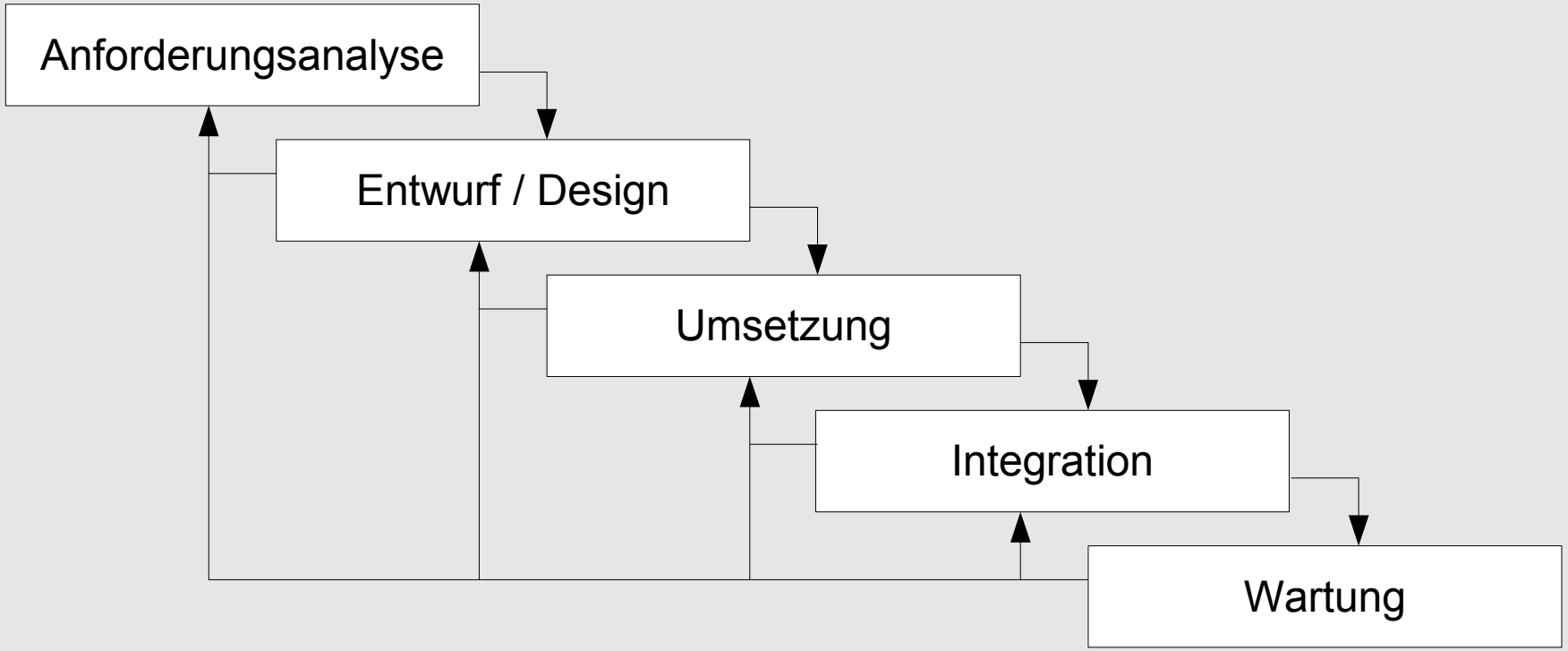
Werden genauer spezifiziert durch

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

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



Eine Beispielrichtlinie

...findet sich in einem externen Dokument

Neue Anforderungen für die Policy

- VIPs nach Weihnachten
- Erwünschte Datenübertragung von Mobilen Geräten
- Ausnahmen außerhalb der Geschäftszeiten

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

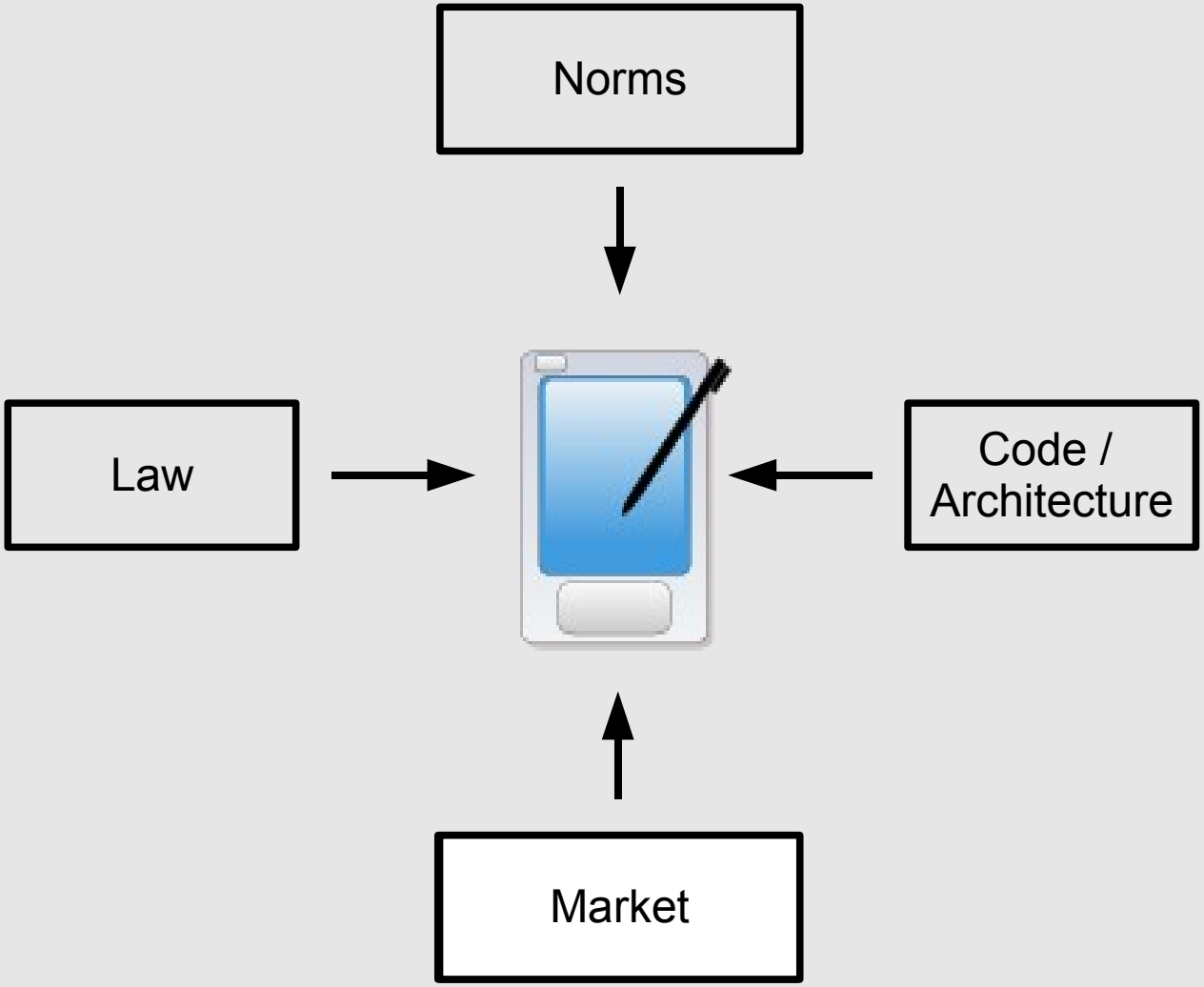
- Kommunikatives Wesen
  - Schnittstellen sichern, Ausnahmen vorsehen (technisch **und** organisatorisch)
  - Verbindungen sichern (technisch, evtl. organisatorisch)
- Kontinuierliche Aktivität (insb. PDAs)
  - Ø
  - Berücksichtigen bei obigen Maßnahmen
- Technische Unzulänglichkeiten (insb. PDAs)
 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

Zur Diskussion



Grafik nach: Lawrence Lessig (1999):
Code and other laws of cyberspace

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

Frage in eigener Sache...

Interesse an einem Gastvortrag
an der TU Berlin?

Vorstellen der Problematik aus
Unternehmenssicht im Rahmen einer
Lehrveranstaltung?

Mobile Security: 6 Herausforderungen

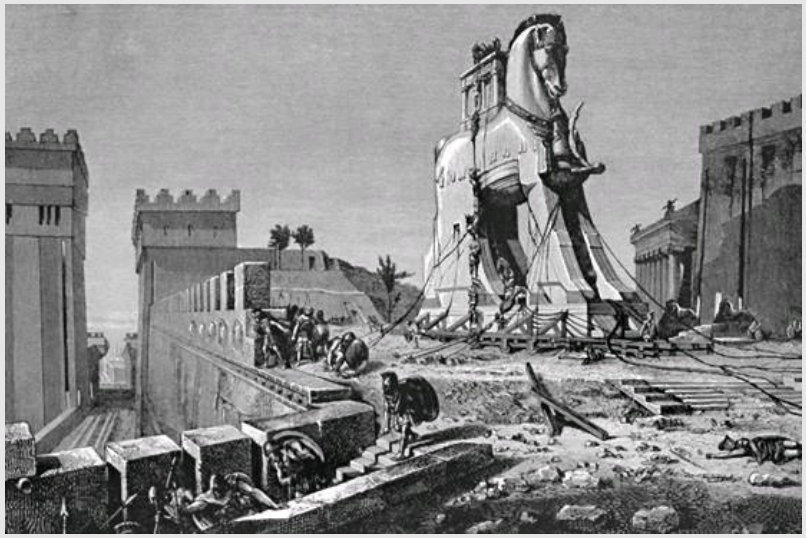
- Gerätemobilität
  - London 2005:
    >4.000 Notebooks
    >5.000 PDAs
  - Diebstahl
  - ...

➔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 Virenscannern
  - ...



➔Physisches Überwinden der Netzgrenzen

Quelle: http://commons.wikimedia.org/

Mobile Security: 6 Herausforderungen

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

➔Widerstände gegen restriktives Vorgehen

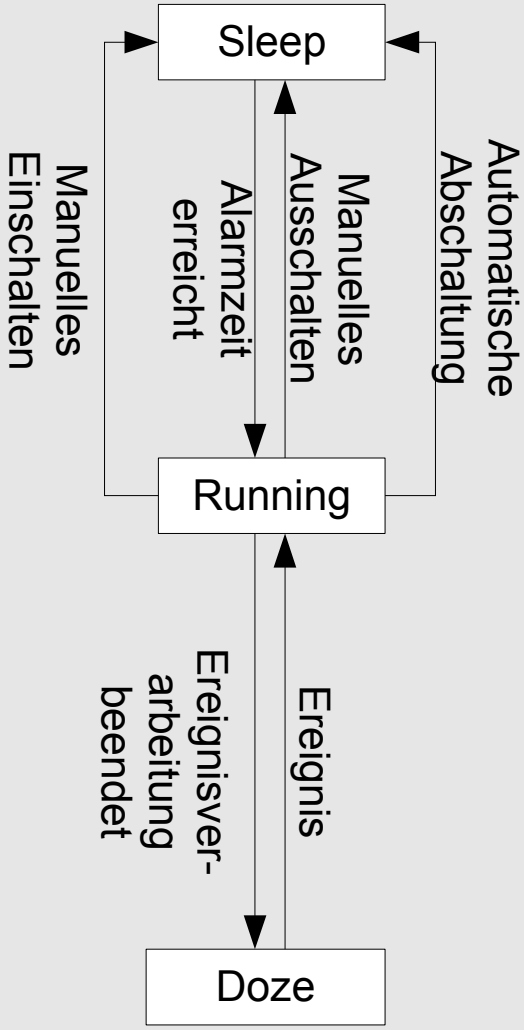
Quelle: http://commons.wikimedia.org/

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)?



Palm OS Betriebsmodi, nach:
Jörg Roth: Mobile Computing, S. 350 und
http://www.palmos.com/dev/support/docs/...

Mobile Security: 6 Herausforderungen

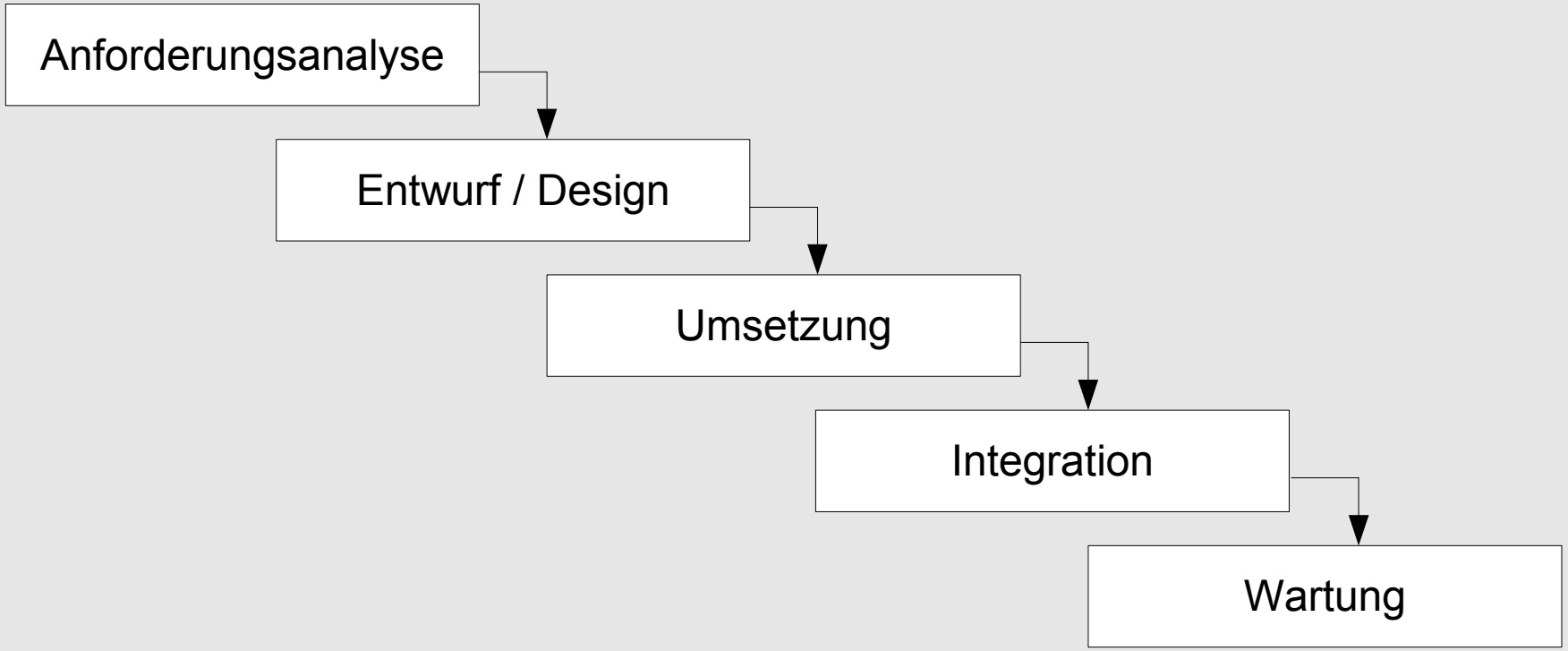
- Gerätemobilität
- Virales Verhalten
- Personengebundenheit
- Kommunikatives Wesen
- Kontinuierliche Aktivität
- Technische Unzulänglichkeiten
  - Rechteverwaltung?
  - Zentrales Management?
  - Lange Passwörter auf PDAs?

➔ Etablierte Vorgehensweisen u.U. unpassend!

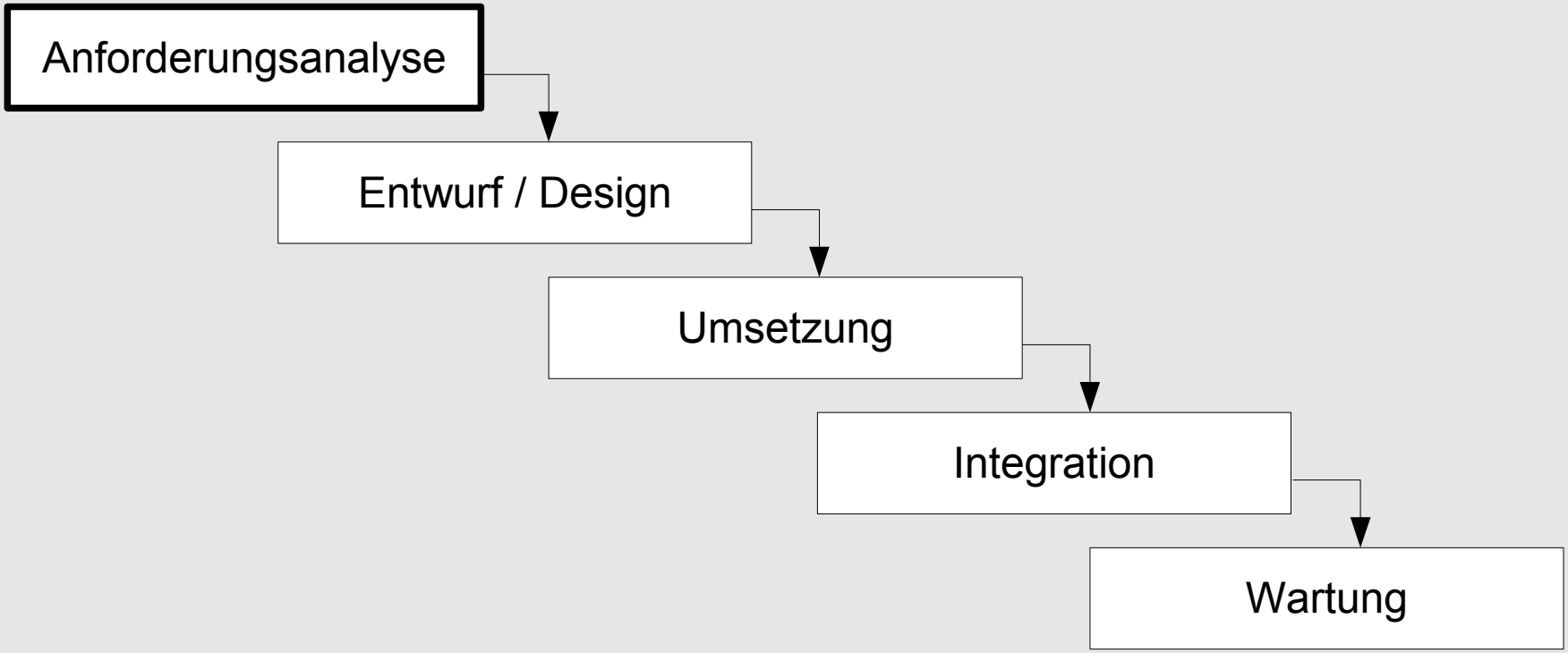
(Zwischen-) Zusammenfassend:

- 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

Entwicklung einer Security Policy



Entwicklung einer Security Policy

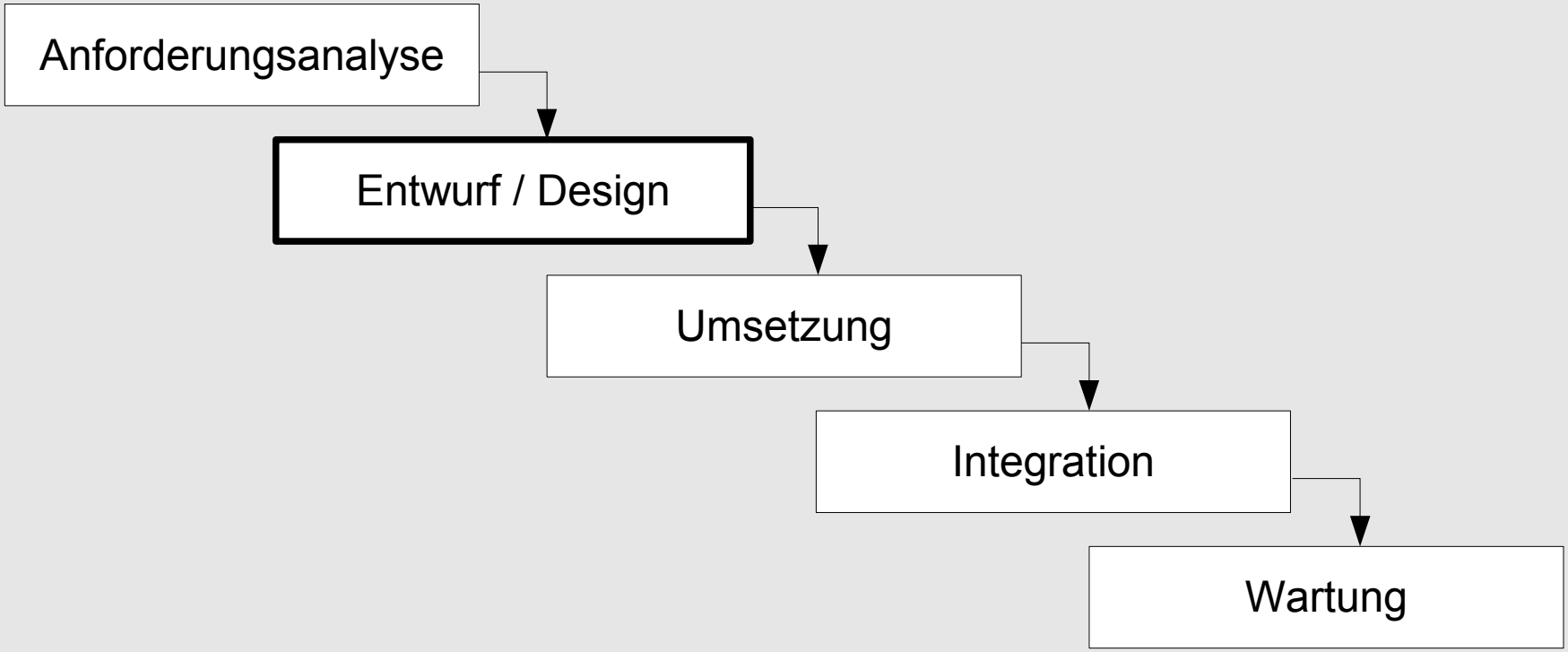


- Welche Werte sind zu schützen?
- Was sind mögliche Schadensfälle?
- Welche Rahmenbedingungen gibt es?
- **Welche Funktionalität wird benötigt?**

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?

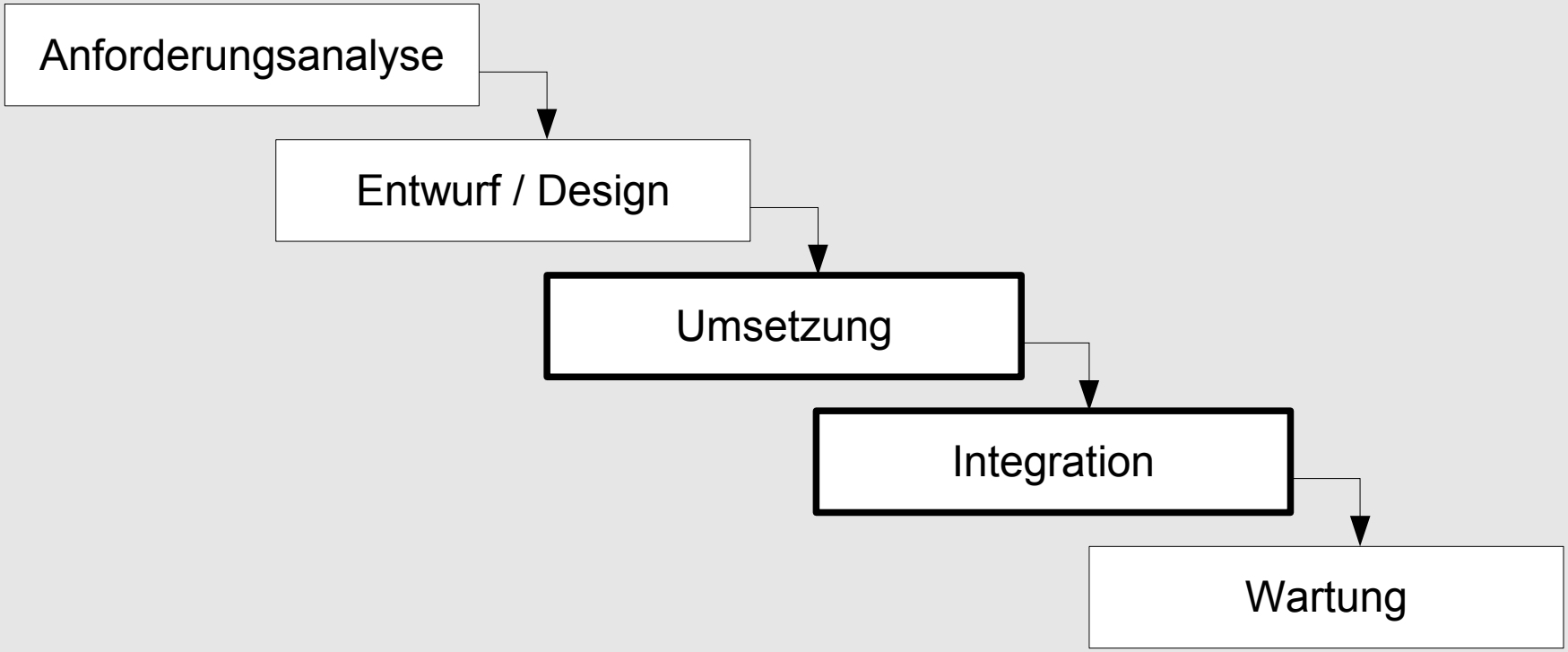
Security Policies: 2. Ebene

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

Werden genauer spezifiziert durch

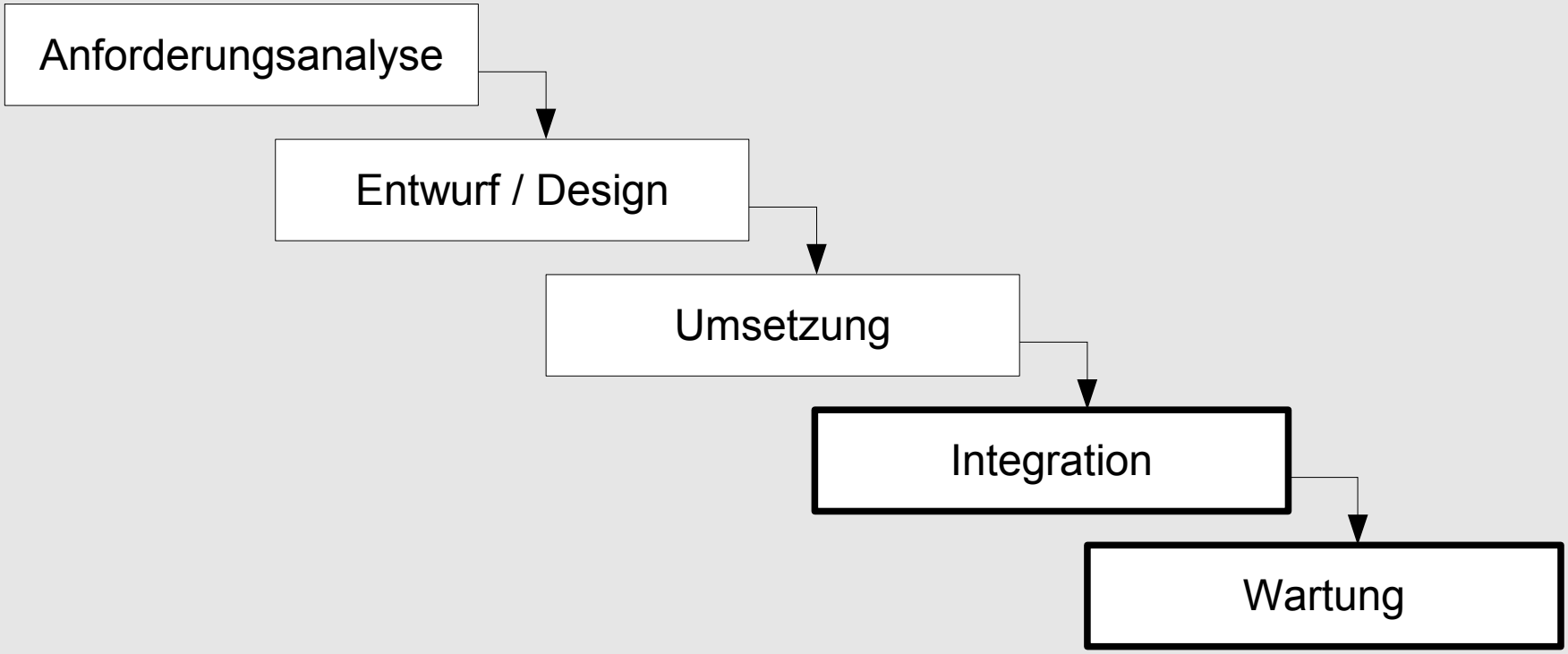
Detaillierte Sicherheitsziele
z.B. „Interne Daten dürfen nur auf mobilen Geräten gespeichert werden, wenn diese mit mindestens 128Bit-AES verschlüsselt sind.“

Entwicklung einer Security Policy



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

Entwicklung einer Security Policy



– Umsetzen
– Ständig überprüfen
– **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...