Privacy by design (Pbd)

Von der Theorie zur Praxis

DB Mobility Logistics AG

Thomas Biedorf

CDM

07.03.2015

Warum Pbd?

- Menschenrecht, formuliert u.a. in Artikel 8 der europ. Menschenrechtskonvention

  Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.

- Artikel 23 DSGVO-EU: Datenschutz durch Technik und ds-freundliche Voreinstellungen
- Immense Fortschritte bei CPU-Rechenpower, Kosten für Speicherplatz etc. (Big Data)
- Abhängigkeit von vetrauenswürdiger Verarbeitung personenbez. Daten wird immer größer
- Unklare Verantwortlichkeiten, mangelnde Transparenz

Cloud

Wearables

„Social Web“

„always on“

PET

- Schon 1980 Einführung des Begriffs "PET" (Privacy Enhanced Technology)
- PET wurde eigener Bereich in den Computerwissenschaften, der Kryptologie
- Aktuelles Beispiel: Apple Pay

PET

- PET betrachtet nur einzelne Komponenten
- Das Zusammenführen von PET führt nicht zu einem sicheren Gesamtsystem!
- Aktuelles Beispiel: Apple Pay

03.03.2015 13:40

Betrügereien mit Apple Pay: Banken wollen Lücken schließen

Apple Pay im Einsatz: Apple sichert Transaktionen per Fingerabdruck ab.

Zu laxe Kontrollen bei den ausgebenden Instituten sollen in den USA dazu geführt haben, dass Diebe gestohlene Kreditkarten bei Apples NFC-Bezahldienst hinterlegen konnten. Auch in den Läden des iPhone-Herstellers haben sie damit offenbar eingekauft.

Kein Mensch kennt Pbd

- Es gibt Unmengen an Publikationen zum Thema, aber dies ist bei Entwicklern (noch) nicht angekommen
- Nur wenige Programmiertools unterstützen bei diesem Ansatz

IT-Sicherheit

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Datenschutz

- Unverkettbarkeit
- Transparenz
- Widerspruchsmöglichkeit / Intervention

Privacy by design = „vorbildlicher Datenschutz“

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Unverkettbarkeit
- Transparenz
- Widerspruchsmöglichkeit / Intervention

Wie beginnen? PIA

- PIAs oder “data protection impact assessment”
- Aus Pbd-Sicht 5 Schritte
  - Identifizierung der Projektbeteiligten und deren Einbeziehung
  - Identifizierung der Risiken -> Risikoanalyse
  - Identifizierung von Lösungen und der Formalisierung der Empfehlungen
  - Implementierung der Empfehlungen
  - Review und Audits der Implementierung

Wie beginnen? PIA - “data protection impact assessment”

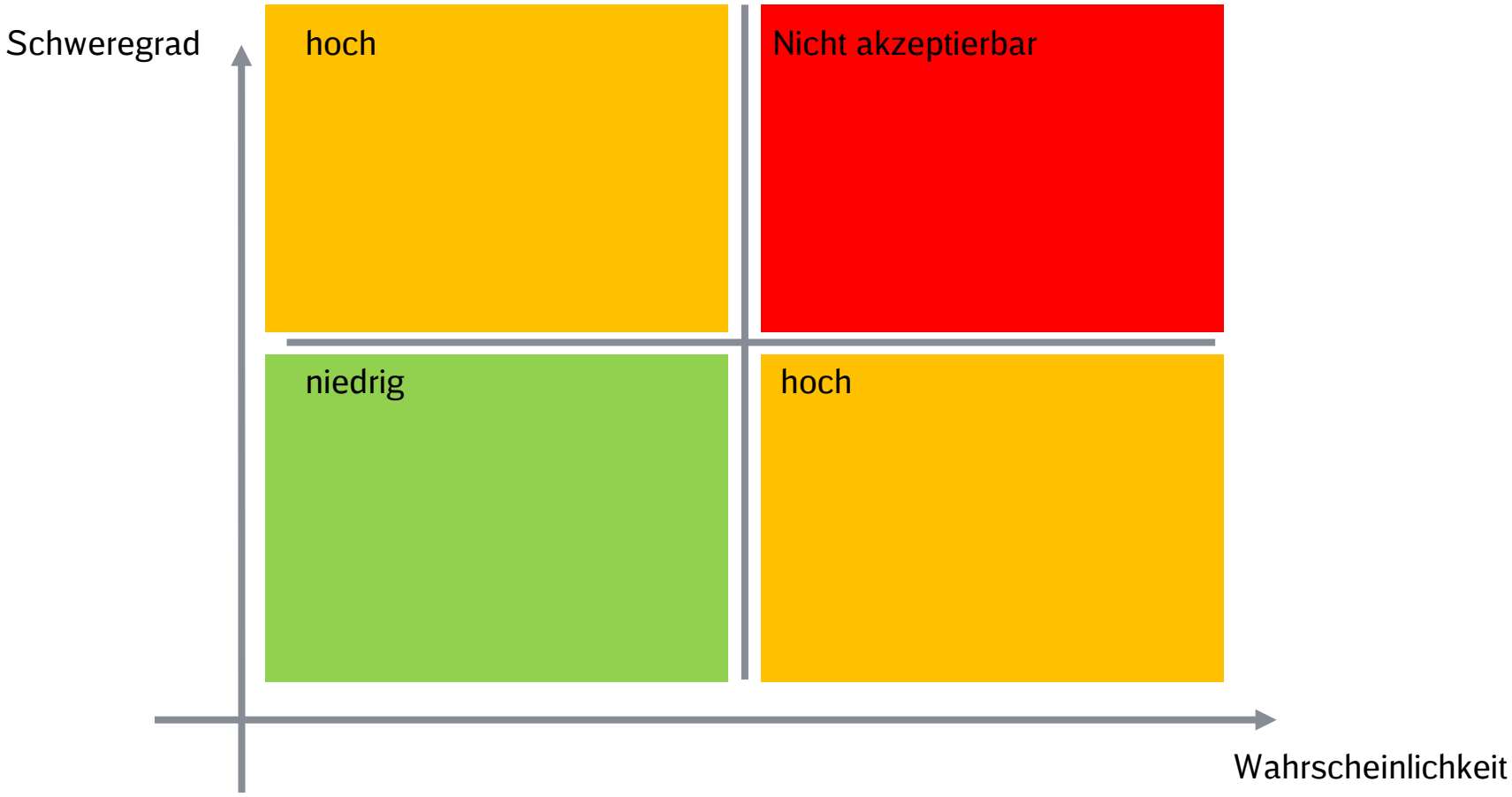
- Identifizierung der Risiken -> Risikoanalyse und
- Identifizierung von Lösungen und der Formalisierung der Empfehlungen
    - … gehen als Input in „Implementierung der Empfehlungen“ mit hinein

- "Privacy by design" ist eine Hülle, die sich um alle 5 Schritte schließt
- PIA in verschiedenen Stadien
- Risikoanalyse ist wichtigster Schritt am Anfang der Entwicklung/des Prozesses

Risikoanalyse

- Erkennen von
  - gefürchteten Ereignissen
  - deren Auslöser
- „Gefürchtete Ereignisse“:
  - wie leicht kann eine Person identifiziert werden?
  - welcher (finanzielle) Schaden entsteht?
- „Auslöser“:
  - welchen Wert hat ein personenbezogenes Datum
  - finanzielle Ausstattung eines Angreifers (Zeit, Wissen, Geld, Motivation etc.)

Risikoanalyse



Risikoanalyse

- Ergebnis sollte sein:
  - Feststellung der Rahmenbedingungen
    - Inkl. externe Parameter
    - Annahmen über eventuelle Angreifer/Angriffe und deren Möglichkeiten
  - Präzise Festlegung und Identifizierung aller datenschutzrelevanten Dinge im System
  - ggfs. Empfehlungen zu den einzusetzenden Methoden (PET)
- Immer ganz am Anfang der Entwicklung durchzuführen

Methoden vor der Entwicklung

- Große Herausforderung an Entwicklung, die richtigen Protokolle / PET zu finden
- Oft Konflikte zwischen angestrebten Schutz und anderer Vorgaben
  - Userinterface / Bedienung
  - Funktionale Vorgaben
- Großes Spektrum an PET vorhanden, welches ist das richtige?

Methoden vor der Entwicklung – Vertraulichkeit festlegen

- Verschiedene Arten von Vertraulichkeit
  - Blindes Vertrauen
    - stärkste Art von Vertrauen
    - führt im Zweifelsfall zur unsichersten Implementierung!
  - Verifizierbares Vertrauen
  - Verifiziertes Vertrauen

Methoden vor der Entwicklung – Userinteraktion festlegen

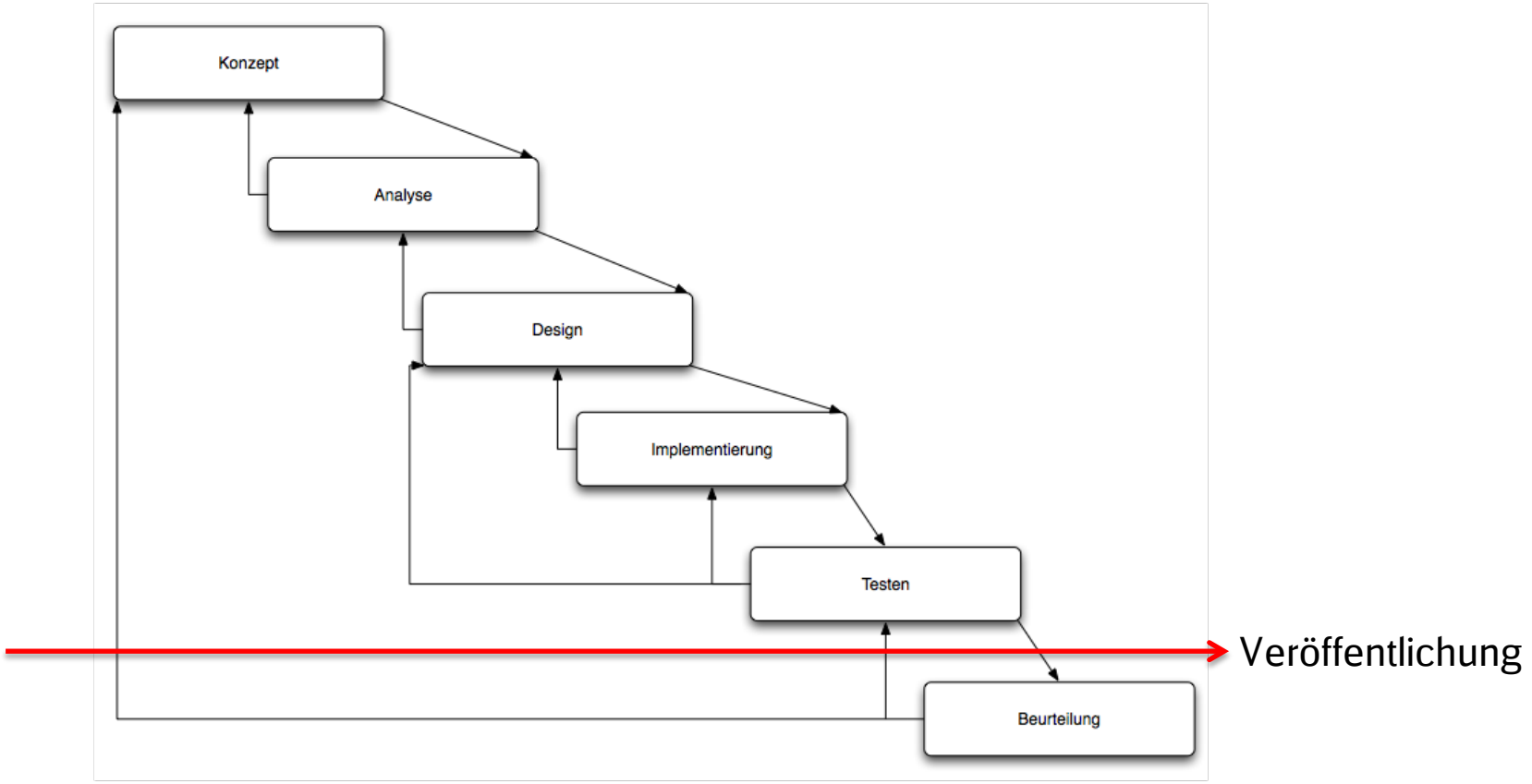
- Verschiedene Arten von Userinteraktion
  - Keine Interaktion
    - Smart Meter und dgl.
    - Einverständnis muss ggfs. auf anderen Wegen eingeholt werden
  - Interaktion zur Grundrechtswahrnehmung
    - was soll wie kommuniziert werden?
    - welche Eingriffsmöglichkeiten muss der User bekommen?
    - wie spiegelt sich das im Nutzerinterface wieder?

Bewertungshilfsmittel für den Nutzer

- Es gibt keine Sicherheit, dass ein System allen Pbd-Vorgaben entspricht
- Entscheidungshilfen für den Nutzer:
  - Das Vorliegen aller Dokumente
  - Transparenz der Abläufe
  - Gelebte Praxis
  - ggfs. Datenschutz-Siegel
    - Problem: Wer ist der Aussteller? Vertrauen? Ziel der Zertifizierung?
    - Standards der Prüfung und deren Kommunikation an den Nutzer
    - Gefahr einer „Illusion von Datenschutz“

Pbd Strategien – Design und Technologien

- Verschiedene Software-Entwicklungsmethoden existieren
  - z.B. das Wasserfall-Modell, bestehend aus 6 Phasen



Pbd Strategien – Design und Technologien

- Software wird nie in einem „Durchlauf“ entwickelt
- Verschieden Iterationen sind zu durchlaufen
  - auch nach der Veröffentlichung der ersten Version
- „Kreisbewegung“

Pbd Strategien – Design und Technologien

- „Design patterns“ (Entwurfsmuster) sind bewährte Lösungswege
- Standards für wiederkehrende Designprobleme in der Softwareentwicklung
- Aber: Keine patterns für Pbd!

„Ein gutes Muster sollte ein oder mehrere Probleme lösen,
ein erprobtes Konzept bieten, auf realen Designs basieren,
über das rein Offensichtliche hinausgehen,
den Benutzer in den Entwurfsprozess einbinden, Beziehungen aufzeigen,
die tiefergehende Strukturen und Mechanismen eines Systems umfassen.“

Wikipedia

Pbd Strategien – Design und Technologien

- 8 Pbd-Strategien
  - **MINIMISE**
    - Datensparsamkeit als oberstes Ziel
    - „Was macht Amazon in der Zukunft mit den Empfehlungen?“

Pbd Strategien – Design und Technologien

- 8 Pbd-Strategien
  - **HIDE**
    - Vermeidet Missbrauch
    - In der Vergangenheit oft übersehen (z.B. RFID-Tags)
    - Hilft bei der Unverkettbarkeit: pb-Daten getrennt von anderen Daten
    - „Was wird in Zukunft aus Facebooks Voreinstellungen?“

Pbd Strategien – Design und Technologien

- 8 Pbd-Strategien
  - **SEPARATE**
    - Pb-Daten aufteilen und in verschiedenen „Containern“ ablegen
    - Daten aus verschiedenen Quellen in verschiedenen, nicht verbundenen Datenbanken ablegen
    - Vermeidet Profilbildung
    - „Was macht Google demnächst mit dem generischen Account für alles?“

Pbd Strategien – Design und Technologien

- 8 Pbd-Strategien
  - **AGGREGATE**
    - „Sammele so viel wie möglich über eine Gruppe von Individuen…“
    - „… mit den gerade noch notwendigen Details“
    - Anonymität in der Masse, Beschränkung der Details, Gültigkeit für viele
    - „Was wird in Zukunft aus medizinischen Studien?“

Pbd Strategien – Design und Technologien

- 8 Pbd-Strategien
  - **INFORM**
    - Herzstück der Transparenz
    - Information über die 4 Ws:
      - Welche Daten sollen verarbeitet werden?
      - Welcher Zweck wird dabei verfolgt?
      - Welche Technologie wird dabei eingesetzt?
      - Wie werden die Daten gesichert?
    - „Wer liest in Zukunft 10-seitige Datenschutzerklärungen?“

Pbd Strategien – Design und Technologien

- 8 Pbd-Strategien
  - **CONTROL**
    - Der Nutzer bleibt Herr seiner Daten
    - Nur er darf festlegen, was damit gemacht werden soll
    - „Was wird aus den Nutzungsrechten bei Diensten wie Instagram?“

Pbd Strategien – Design und Technologien

- 8 Pbd-Strategien
  - **ENFORCE**
    - Eine (mind.) gesetzeskonforme Datenschutzerklärung ist vorhanden und wird auch durchgesetzt
    - sowohl auf technischer als auch auf organisatorischer Seite
    - „Werden in Firmen in Zukunft ausreichende Prozesse implementiert?“

Pbd Strategien – Design und Technologien

- **Authentifizierung**
  - Attributbasiertes Anmelden
    - Zentralisiert über einen „Identity Provider (IdP)“
    - Ähnlich Single-Sign-On
    - Bei Zugriff auf einen Service, Umleitung auf IdP, dort Login, dann zurück
    - Ein sog. Token übergibt dann **nur die benötigten Daten**
    - Zentralisiertes System führt zu Problemen
      - Kompromittiert?
      - Was kann alles geloggt werden?

Pbd Strategien – Design und Technologien

- **Sichere Kommunikation, Verschlüsselung**
  - Netzwerke sind ein schlechter Garant für Vertraulichkeit und Datenschutz
  - Mit WLAN wird das ganze noch schlimmer
  - Verschlüsselung ist das Gebot der Stunde, nicht nur nach Snowden

Pbd Strategien – Design und Technologien

- **Sichere Kommunikation, Verschlüsselung**
  - TLS 1.2
    - Öffentliche Schlüsselverwaltung
    - Zertifikatsinfrastruktur muss da sein (kann kompromittiert werden!)
    - Verschiedene Zertifikatsstellen können theoretisch für ein und dieselbe Domain verschiedene Zertifikate ausstellen -> Problem!

Pbd Strategien – Design und Technologien

- **Sichere Kommunikation, Verschlüsselung**
  - Ende-zu-Ende Verschlüsselung
    - PGP und S/MIME
    - OTR (Off The Record) für Messaging-Dienste
    - TextSecure, Crypto Phone, Red Phone etc.
  - Hinterlässt Meta-Daten: wer spricht mit wem

Pbd Strategien – Design und Technologien

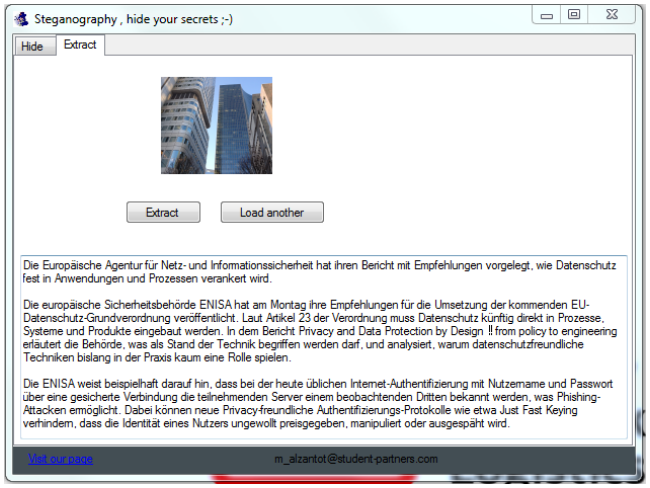
- **Sichere Kommunikation, Verschlüsselung**
  - Meta-Daten verbergen ist schwierig, einige Lösungsansätze existieren
  - = Anonyme Kommunikation
    - Proxy und VPN
      - Ein Betreiber, Traffic-Beobachtung kann de-anonymisieren
      - Betreiber weiß immer, wer gerade kommuniziert
    - „Onion Routing“
      - Verteilen auf viele Betreiber, Angreifer muss mehrere Systeme beobachten (z.B. TOR-Netzwerk)

Pbd Strategien – Design und Technologien

- **Sichere Kommunikation, Verschlüsselung**
  - Broadcasting
    - Senden einer Nachricht an alle („Flooding“)
    - Jeder muss mit seinem Key versuchen, die Nachricht zu entschlüsseln
    - Teuer bei vielen Teilnehmern

Pbd Strategien – Design und Technologien

- **Sichere Kommunikation, Verschlüsselung**
  - Steganographie
    - Vortäuschen eines anderen Protokolls / Formats
    - Verstecken der Kommunikation



Privacy by design - Limitierungen

- **Fragilität**: Verbinden mehrerer Komponenten kann zu unerwarteten Ergebnissen führen
- **Datenschutzmetriken**: Bisher keine Lösungen bekannt (soziale Komponenten!), Metriken bisher nur für Angriffsvektoren und dgl.
- Steigende **Komplexität**
- **Implementierungshemmnisse**: Datenschutz ist kein „Erfolgsmodell“ für Anbieter.
- Unklar, was PbD ist, **zu enge Auslegung**

Privacy by design - Ausblick

- **Artikel 23 DSGVO-EU wird den Datenschutz radikal verändern**
- **Pbd wird vermutlich gesetzliche Vorgabe**
  - Datensparsamkeit und Zweckbindung als oberstes Gebot
  - Regelt nicht nur, wie mit bereits erhobenen Daten umgegangen werden soll, sondern auch schon das „Davor“
- Es fehlen z.Zt. noch best-practices – es gibt einfach **zu wenige Umsetzungen**
- **Es fehlen Tools** für Entwickler, die durchgängiges Pbd ermöglichen.

Privacy by design – Links zum Thema

Enisa-Paper
***Privacy and Data Protection by Design – from policy to engineering*: http://www.enisa.europa.eu**

- **Design patterns I:** http://de.wikipedia.org/wiki/Entwurfsmuster
- **Design patterns II:** http://www.philipphauer.de/study/se/design-pattern.php
- **Attributbasiertes Anmelden:** https://abc4trust.eu
- **Bruce Schneier:** https://www.schneier.com/
- **Matthew Green:** http://blog.cryptographyengineering.com/

Privacy by design – Von der Theorie zur Praxis

V i e l e n D a n k !

Thomas.Biedorf@deutschebahn.com