mHealth im Licht des Standard-Datenschutzmodells

Martin Rost

TMF

10. Februar 2015, Berlin

Gliederung

1. Was meint „Datenschutz“?
2. Der Regelungskern des Datenschutzrechts
3. mHealth - Vision
4. Schutzziele des Datenschutzes und
   das Standard-Datenschutzmodell (SDM)
5. Merkmale von Mobilgerätschaften

Datenschutz?

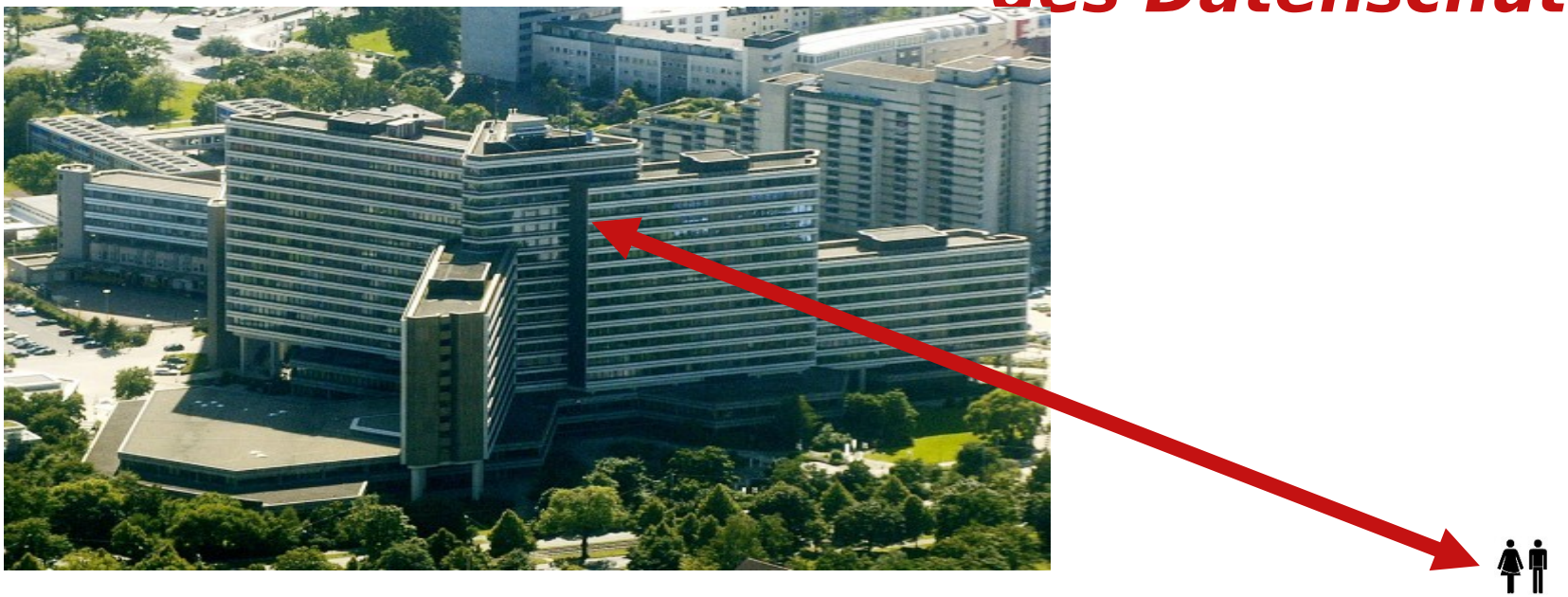
... ist nicht mit *Datenschutzrecht* gleichzusetzen.
=> juristischer Kurzschluss

… ist nicht mit *IT-Sicherheit* gleichzusetzen.
=> technizistischer Kurzschluss

… ist nicht mit einem *privaten Bedürfnis nach Privatheit* gleichzusetzen.
=> psychologistischer Kurzschluss

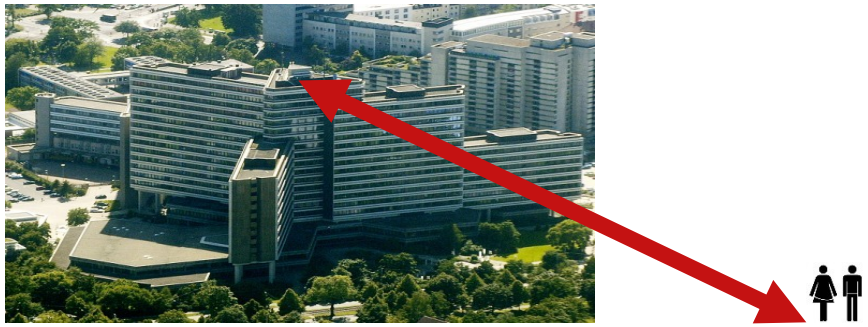
Was ist „Datenschutz“?

Objektbereich des Datenschutzes



Datenschutz beobachtet, beurteilt und gestaltet die **asymmetrischen Machtbeziehungen** zwischen Organisationen und Personen.

Objektbereich des Datenschutzes



Strukturelle Machtasymmetrien werden im Rechtsstaat unter Bedingungen gestellt...

- durch **gesetzliche Vorgaben** (Grundrechte, Spezialgesetze, Datenschutzgesetze)

  Grundrechte sind Abwehrrechte von Bürgern gegenüber Organisationen, insbesondere dem Staat.

- und durch **Beratungs-, Prüf- und Sanktionsinstanzen** kontrolliert.

DER datenschutzrechtliche Regelungskern

Es dürfen keine personenbezogene Daten verarbeitet werden PUNKT

Eine Ausnahme von diesem Grundsatz ist zulässig, wenn ein Gesetz die Verarbeitung regelt oder eine Einwilligung durch den Betroffenen vorliegt.

„Das Verbot mit Erlaubnisvorbehalt“

(§ 4 Abs. (1), BDSG)

Grundrecht Datenschutz

Artikel 1 Grundgesetz

(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

(2) Das Deutsche Volk bekennt sich darum zu unverletzlichen und unveräußerlichen Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt.

(3) Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.

Artikel 2

(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

(2) Jeder hat das Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.

„Volkszählungs-urteil“ des BVerfG. von 1983

Zentrale Datenschutz-Figur: „Recht auf **informationelle Selbstbestimmung**“

(BVerfGE 65, 1 - Volkszählung (http://www.servat.unibe.ch/dfr/bv065001.html))

1. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen *Persönlichkeitsrecht des Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG* umfaßt. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

2. Einschränkungen dieses Rechts auf "*informationelle Selbstbestimmung*" sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer *verfassungsgemäßen gesetzlichen Grundlage*, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.

Datenschutz
Aktuell geltende Normen

Bundesdatenschutzgesetz (BDSG) erstreckt sich auf Privatpersonen, Privatwirtschaft und Bundesbehörden

Landesdatenschutzgesetze erstrecken sich auf öffentliche Verwaltung in Land und Kommunen

- speziell in SH: **DS-Verordnung**

EU: Europäische Grundrechte-Charta

- **Datenschutz-Richtlinie** Wirkung über Import in deutsche Gesetze
- Entwurf: **EU-DS-Verordnung**, die BDSG/LDSGe ersetzen wird!

Spezialgesetze (haben Vorrang):

- Telemedien-Gesetz, T-Kommunik-Gesetz,
- SGB, AO, LandesMeldeGes, LVerwGesetz/ PolizeiGes, PassGes, PersonalausweisGes, AufenthaltsGes., ...

- Rechtmäßigkeit der Datenverarbeitung
  - Gesetzliche Rechtsgrundlagen
  - Einwilligung
- Grundsatz der Zweckbindung
- Grundsatz der Erforderlichkeit
- Grundsatz der Datenvermeidung und Datensparsamkeit
- Grundsatz der Transparenz
- Grundsatz der klaren Verantwortlichkeit
- Grundsatz der Kontrolle
- Grundsatz der Gewährleistung der Betroffenenrechte
  - Verbot der Profilbildung
  - Verbot der Sammlung auf Vorrat
  - Verbot der automatisierten Einzelentscheidung
- Nutzung anonymisierter oder pseudonymisierter Daten

Zum Verhältnis von Datenschutz und Datensicherheit

Die IT-Sicherheit unterstellt:

Jede Person kann ein Angreifer sein!

Die Person muss nachweisen, dass sie kein Angreifer auf die Geschäftsprozesse ist und dass sie ggfs. mit einem Zugriff auf ihre Person rechnen muss.

Der Datenschutz unterstellt:

***Jede* Organisation IST ein Angreifer!**

Ein Organisation muss prüffähig nachweisen, dass sie kein Angreifer ist, sich an die Gesetze hält und ihre Verfahren und Prozesse vertrauenswürdig, d.h. ordnungsgemäß beherrscht.

mHealth - Die Vision

mHealth
Definition

Unter *Mobile Health* („mHealth“) versteht man *„medizinische Verfahren und Praktiken der öffentlichen Gesundheitsfürsorge, die durch Mobilgeräte wie Mobiltelefone, Patienten-überwachungsgeräte, persönliche digitale Assistenten (PDA) und andere drahtlos angebundene Geräte unterstützt werden.“*

(EU-Kommission 2014: Grünbuch mHealth, S. 3)

mHealth
Die Vision (1)

„Was bedeutet dies für das Gesundheitswesen?

1. „Neue Kommunikation zwischen Patienten und Ärzten wird den Praxisbesuch teilweise verdrängen und durch einem 24x7 email-, Text-, Wort- und Photoaustausch ersetzen. Dies erfordert **eine neue Datenschutzformulierung und ein neues Management der Informationsflüsse**, das verhindert, dass ein Arzt in der Flut der Kommunikation ertrinkt.“

2. „Mit mehreren tausend neuen medizinischen Applikationen sehen wir den Anfang der Umsetzung der medizinischen Wissenschaft von Büchern und vom Gedächtnis zu **Software Applikationen, die in den Handys und im Internet zur Verfügung stehen** und im auch im „Sprechzimmer“ zunehmend angewendet werden.“

(aus: C. Peter Waegemann: „Der Weg von eHealth zu mHealth“, S. 21f)

mHealth
Die Vision (2)

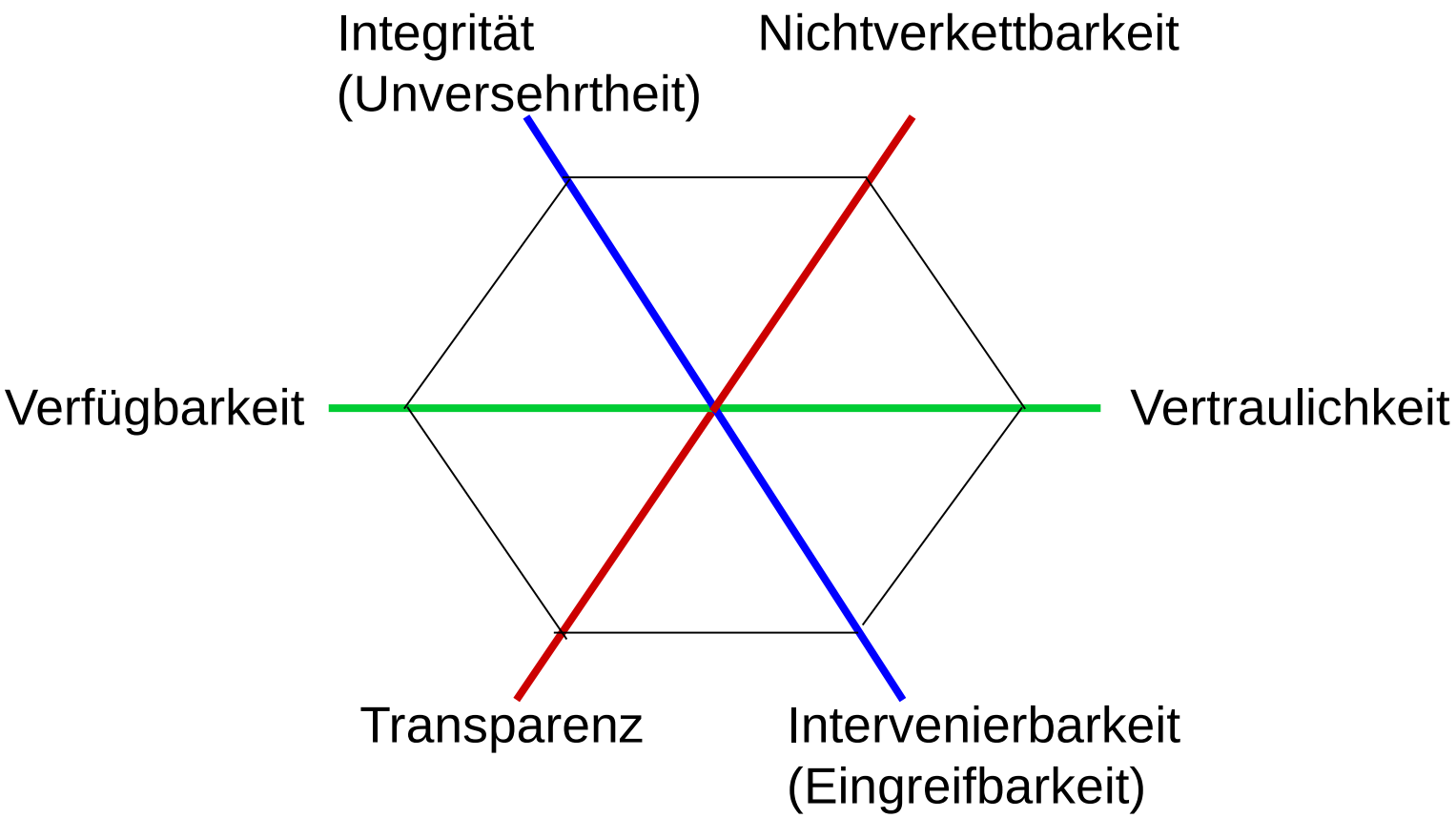
1. „**Globale Richtlinien** für Disease Management und medizinische Entscheidungen werden sich langsam durchsetzen und in **automatischen Decisonsupport** Applikationen eingebaut werden.“

2. „Das Konzept der neuen Kommunikation, die tagein, tagaus stattfinden kann, wird in Amerika **„Oberservations of Daily Living“** (ODL) genannt. Diese Beobachtungen des täglichen Lebens können per Telefon (durch Sprache), per Text oder Bild vermittelt werden.“

(aus: C. Peter Waegemann: „Der Weg von eHealth zu mHealth“, S. 21f)

Das Standard-Datenschutzmodell (SDM)

Die elementaren Schutzziele und deren Systematik



Schutzziele § 5 LDSG-SH

(1) Die Ausführung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz im Sinne von § 3 Abs. 3 ist durch technische und organisatorische Maßnahmen sicherzustellen, die nach dem Stand der Technik und der Schutzbedürftigkeit der Daten erforderlich und angemessen sind. Sie müssen gewährleisten, dass

- Verfahren und Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß angewendet werden können (**Verfügbarkeit**),
- Daten unversehrt, vollständig, zurechenbar und aktuell bleiben (**Integrität**),
- nur befugt auf Verfahren und Daten zugegriffen werden kann (**Vertraulichkeit**),
- die Verarbeitung von personenbezogenen Daten mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden kann (**Transparenz**),
- personenbezogene Daten nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden können (**Nicht-Verkettbarkeit**) und
- Verfahren so gestaltet werden, dass sie den Betroffenen die Ausübung der ihnen zustehenden Rechte nach den §§ 26 bis 30 wirksam ermöglichen (**Intervenierbarkeit**).

Schutzmaßnahmen

Sicherstellung von *Verfügbarkeit*
- Daten/Prozesse: **Redundanz**, Schutz, Reparaturstrategien

Sicherstellung von *Integrität*
- Daten / Systeme: **Hash-Wert-Vergleiche**
- Prozesse: Festlegen von Min./Max.-Referenzen, Steuerung der Regulation

Sicherstellung von *Vertraulichkeit*
- Daten: **Verschlüsselung**
- Systeme / Prozesse: Rollentrennungen, Abschottung, Containern

Sicherstellen von *Nichtverkettbarkeit* durch Zweckbestimmung/-bindung
- Daten: Pseudonymität, **Anonymität** (anonyme Credential)
- Prozesse: Identitymanagement, Anonymitätsinfrastruktur, Audit

Sicherstellen von *Transparenz* durch Prüffähigkeit
- Daten / Systeme / Prozesse: **Protokollierung, Dokumentation** von Verfahren

Sicherstellen von *Intervenierbarkeit* durch Ankerpunkte
- Daten: Zugriff auf Betroffenen-Daten durch den Betroffenen
- Prozesse: SPOC für Änderungen, Korrekturen, Löschen, **Aus-Schalter**, Changemanagement,

Verfahrens-komponenten

Zur Beurteilung der Datenschutz-gerechtigkeit eines Verfahrens sind drei Komponenten zu betrachten:

- Daten (und Datenformaten)
- IT-Systeme (und Schnittstellen)
- Prozesse (und Rollen)

Schutzbedarfe für Betroffene

normal: Schadensauswirkungen sind begrenzt und überschaubar und etwaig eingetretene Schäden für *Betroffene* relativ leicht durch eigene Aktivitäten zu heilen.

hoch: Schadensauswirkungen werden für *Betroffene* als beträchtlich eingeschätzt, z.B. weil durch Wegfall einer Leistung die Gestaltung des Alltags nachhaltig verändert wird und der Betroffene nicht aus eigener Kraft handeln kann und auf externe Hilfe angewiesen ist.

sehr hoch: Die Schadensauswirkungen nehmen ein unmittelbar existentiell bedrohliches, katastrophales Ausmaß für *Betroffene* an.

(orientiert an: https://www.bsi.bund.de/cae/servlet/contentblob/471452/publicationFile/30748/standard_1002_pdf.pdf, S. 49.)

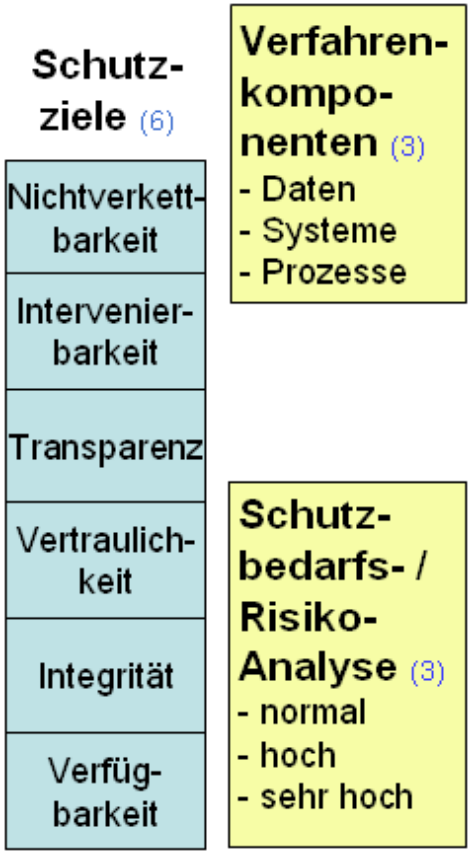
Komponenten des Standard-Datenschutzmodells

6 Schutzziele, hinterlegt mit Maßnahmen-Katalog!

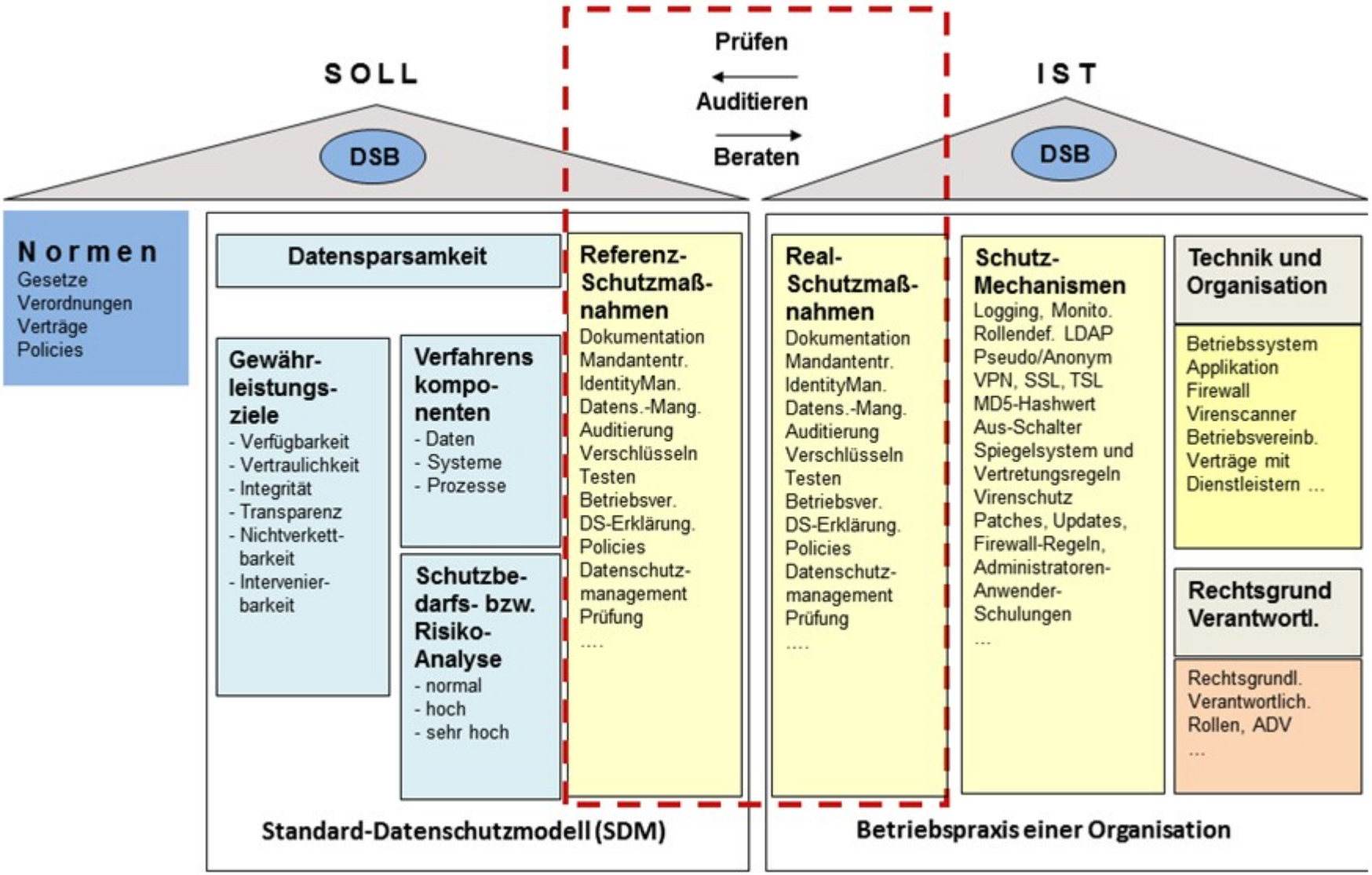
3 Verfahrenskomponenten!

3 Schutzbedarfsabstufungen, aus der Betroffenenperspektive!

Erlaubt die Formulierung eines Referenzmodells für 6x3x3 (54) spezifische Datenschutz-maßnahmen, gegen das sich jedes personenbezogene Verfahren standardisiert prüfen lässt!



Prüfprozess mit SDM



Aktueller Status des SDM

Beschluss der 88. Datenschutzkonferenz Oktober (2014):

- Der Entwurf des Handbuchs zum Standard-Datenschutzmodell (Version 0.8) wurde zustimmend zur Kenntnis genommen.
- Auftrag: Ein **Katalog mit Referenzschutzmaßnahmen ist bis Oktober 2015** zu entwickeln.
- Übersetzung des Handbuchs ins Englische und Vorlage bei der Art. 29-Gruppe.
- Status: Bleibt internes Arbeitspapier der DSK.

Mobile Devices

Devices

- Handies und Smart Phones
- Wearables
- Dedizierte Devices
- Tablets
- Laptops

Vorteile Mobile Devices

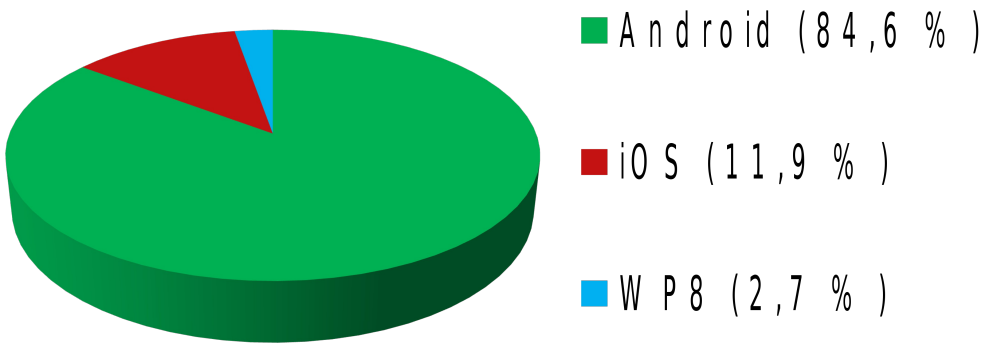
Einsatz von mobile Computing ist heute eine Selbstverständlichkeit, weil

- billig,
- jederzeit verfügbar, auch auf dem Land
- leistungsfähig, sogar Ferndiagnosen durch Daten-, Audio-, Videoübertragung möglich
- bedienungsfreundlich
- kurz: funktional und praktisch

Statistik mobile OS

Definition: Mobile Endgeräte sind Geräte mit **mobilen Betriebssystemen.**

- Android (Google, USA)
- iOS (Apple, USA)
- Windows Phone 8 (Microsoft, USA)



Aufstellung: Dr. Malte Engeler, U

Mobile OS und personenbezogene Daten

Personenbezogene Daten in mobilen Geräten

- IMEI (Gerätenummer)
- UDID (Gerätenummer eines iOS-Gerätes)
- IMSI (SIM-Kartennummer)
- MAC-Adresse (Hardware-Adresse eines Netzwerkadapters)
- MSISDN (=Mobilfunknummer)
- Name des Telefons
- Standortdaten (Verknüpfung mit anderen Daten)
- Audiodaten (Stimmabgleich, Gyroscope)
- Biometrie (Fingerabdruck, Iris, Gesichtsgeometrie)
- Informationen über die App-Nutzung (Werbe- und Interessenprofile)
- Kontakte, Kalender, SMS-Historien, Browserverläufe

Die Betriebssystem-Ebene

- **Schutzziel:** Verfügbarkeit
  (Gesicherter Zugriff auf Daten innerhalb festgelegter Zeit)

- **Android**
  - Linux/Java-Grundgerüst
  - Gingerbread instabil ***mit 1,7 % Crash Rate***
  - Ab 4.0 nur 0,7 % CR
  - Problem: Fragmentierung
  - Gingerbread noch immer 14 % nach JB/KK mit 75 %

- **iOS**
  - Objective C/Swift
  - iOS 7 mit 2,1 % CR
  - iOS 7.1 am stabilsten ***mit 1,6 % CR***
  - iOS 7 bei fast 90 %
  - Offline-Backup über iTunes
  - iOS 8?

- **WP8**
  - C/C++
  - ***Stabilität unklar***
  - WP8.1 Rollout läuft
  - Seit 8.1 jedenfalls auch Backup über WLAN

Die Betriebssystem-Ebene

- **Schutzziel:** Vertraulichkeit
  (Gesicherter Nichtzugriff auf Informationen)

- **Android**
  - Ab 3.0 (Honeycomb) Verschlüsselung
  - Fakultativ
  - Performance
  - Entsperr-PIN = Master Key
  - Akku oft entnehmbar

- **iOS**
  - Seit iOS 4: Verschlüsselung (Ziel: schnelles Löschen)
  - Seit iOS 7: „Data Protection“ sichert einzelne sensible Daten in Abstufungen (PIN)

- **WP8**
  - Verschlüsselung nur über Active-Sync-Gruppen-Richtlinien
  - PIN schützt nur vor Benutzung
  - Kein CalDAV, VPN erst mit WP8.1

Die Betriebssystem-Ebene

- **Schutzziel:** Integrität
  (Information ist gesichert echt)

- **Android**
  - 47 % - 92 % Malware
  - Fragmentierung schadet (z.B. Curesec Phonebug, fixed in 4.4.4.)
  - Dritt-Appstores
  - SMS-Trojaner möglich

- **iOS**
  - Basisfunktionen nicht änderbar
  - Umstrittene Kontrolle auf Malware und Copyware
  - Cydia kaum verbreitet
  - Fast keine Malware, 0 Samples 2011

- **WP8**
  - Ähnlich enges Konzept wie iOS
  - Erst jüngst Kontrolle auf Copyware
  - Wenige Daten im Übrigen

Die Betriebssystem-Ebene

- **Schutzziel:** Nichtverkettbarkeit
  (Zweckbindung und -trennung der Daten)

- **Android**
  - MAC, IMEI frei zugänglich
  - Google-Integration
  - Standortdaten an Google (Wahl)
  - WLAN-Scan im Standby
- **iOS**
  - Nutzung der MAC, UDID durch Apps untersagt seit iOS 7
  - iAD parallel
  - Zufalls-MAC ab iOS 8
- **WP8**
  - Standortdaten über MAC-Adresse

Hersteller können immer verketten

Die Betriebssystem-Ebene

- **Schutzziel :** Intervenierbarkeit
  (Jederzeit Auskunft, Sperrung, Löschung, Kontrolle über/von Daten)

- **Android**
  - Google Dashboard gibt Minimalauskunft, aber interne Protokolle unberührt
  - Niederlassung in Europa?
  - Kontrolle mit Root möglich, aber Risiko
  - System- und interner Speicher: Reset

- **iOS**
  - Datenschutz-Kontaktformular
  - Irisches Recht, also Datenschutzrichtlinie
  - Jailbreak nötig für Kontrolle über Gerät
  - iOS „löscht“ durch Vergessen des Verschlüsselungs-Keys

- **WP8**
  - Kontaktformular verfügbar
  - Ansonsten kein Dateimanager mit Systemzugriff
  - Jailbreak kaum verbreitet

Die Betriebssystem-Ebene

- **Schutzziele: Wesentliche Charakteristika**

- **Android**
  - Intervenierbarkeit dank Root jedenfalls technisch möglich
  - Verfügbarkeit leidet etwas an Fragmentierung
  - Verkettbarkeit durch starke Google-Integration
- **iOS**
  - Transparenz akut in Frage gestellt
  - Intervenierbarkeit problematisch wegen Apple-Kontrolle
  - Gute Verfügbarkeit dank lokalem Offline-Backup
- **WP8**
  - Kaum Transparenz und Intervenierbarkeit
  - Verbesserungsfähige Vertraulichkeit durch CalDAC u.ä.

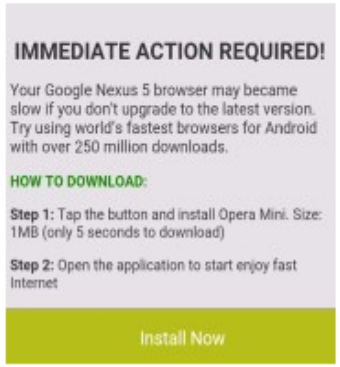
Die Anwendungsebene

- **Biometrie**
  - Fingerabdrücke, Iris, Gesichtserkennung
  - Speicherort? Hashwert? Zugang?
  - API? Absicherung?
- **Mobiles Bezahlen**
  - Seit Android 4.4 KitKat „HCE“
  - Ohne Secure Element (SIM, NFC) kritisch
- **Akku wechselbar?**
  - Ultimativer Off-Switch -> Kontrolle über Hardware, wenn nicht, keine Kontrolle über Ortbarkeit

Fazit Anwendungsebene

- Apps sind notorisch unzuverlässig, unsicher. Funktionieren als Datenspione für Hersteller und staatliche Überwachungsapparate
- Vollkommen intransparent, welchen Schutz „Sicherheitsapps“ bieten (Passwortcontainer)
- Speichern und Backups: nur lokal? Aber was heisst das? Und wo wird sonst noch gespeichert? Cloud?

NETZWELT



SPIEGEL ONLINE

Politik | Wirtschaft | Panorama | Sport | K

4. Februar 2015 Themen: "Islamischer S

Getarnte Apps

Versteckte Malware bedroht Millionen Android-Anwender

Drei Android-Apps, die millionenfach heruntergeladen wurden, sind eine Gefahr für Smartphone-Nutzer. Gut getarnt manipulieren sie Warnmeldungen, versuchen weitere Schadsoftware aufs Handy zu bekommen. mehr... [Forum]

Abo | Shop | E-Paper | Apps | Audio | Archiv | Spiele | Jobs | Partnersuche | Immobilien | Autom

ZEIT ONLINE | DATENSCHUTZ

START POLITIK WIRTSCHAFT GESELLSCHAFT KULTUR WISSEN DIGITAL STUDIUM KARRIERE

Start › Digital › Datenschutz › Cryptowars: De Maizière will Verschlüsselung knacken

CRYPTOWARS

De Maizière will Verschlüsselung knacken

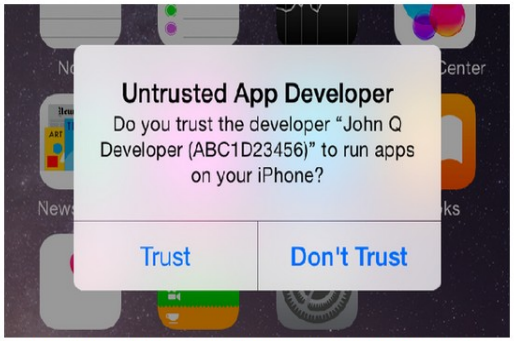
Der Kampf um Verschlüsselung wird härter: Sicherheitsbehörden in ganz Europa fordern einen Zugang zu verschlüsselten Daten. Deutschland will dabei offenbar mitspielen. VON KAI BIERMANN

21. Januar 2015 14:50 Uhr 151 Kommentare

05.02.2015 10:32 Mac&i « Vorige | Nächste »

Spionage-App soll Daten aus unmodifizierten iPhones auslesen

vorlesen / MP3-Download



Die Vertrauensfrage von Apps mit Firmen-Zertifikat lässt sich durch eine Schwachstelle umgehen – bis hin zu iOS 8.1.2 (Bild: Apple)

Ein Antivirenhersteller warnt vor iOS-Malware, die für gezielte Angriffe eingesetzt wird – sie soll das Mikrofon des iPhones aktivieren und verschiedene Nutzerdaten entwenden. Eine der Apps lasse sich auch auf Geräten ohne Jailbreak installieren.

26.01.15 10:30

Staatlicher Zugriff auf Verschlüsselung ist kein zielführender Ansatz

Die aktuelle Diskussion bezüglich staatlicher Einflussnahme auf Verschlüsselung mag angesichts der aktuellen Bedrohungslage von der grundsätzlichen Motivation her zwar nachvollziehbar erscheinen, gleichwohl bedarf das Thema «Verschlüsselung» der sorgfältigen Güter- und Interessenabwägung.

Der Ansatz, bei Nutzung von Verschlüsselung dem Staat Schlüsselzugang gewähren, beachtet unzureichend die politische, rechtliche und technische Dimension. Derartige Erwägungen sind nicht zielführend. Die Politik sollte Konsultationsangebote der Fachleute nutzen.

bitmi Bundesverband IT-Mittelstand e.V.

Thesen zu Mobile

- Die Standard-Betriebssysteme für mobile Geräte e**rfüllen keine Vorgaben der IT-Sicherheit und des Datenschutzes**.
- Der Betrieb mobiler Endgeräte ist für Betroffene und nutzende Organisationen **unbeherrschbar**, der Einsatz ist professionell nicht verantwortbar, keine Wahrung der beruflichen Schweigepflicht, des Patienten-geheimnisses bzw. Sozialgeheimnisses, **Einwilligung bietet Betroffenen keinen Schutz**
- Europa kann derzeit **keine mobile Endgeräte marktfähig** gestalten. Es ist nicht damit zu rechnen, dass grundrechtskonforme Geräte für den Consumermarkt zur Verfügung stehen werden. Spezialgeräte dann sehr teuer („Kanzlerin-Handy“)

Was ist zu tun im Kontext von mHealth?

- Es sollten Usecases für einen *geringen Schutzbedarf* formuliert werden, die den Einsatz von Standard-Mobiledevices rechtfertigen könnten. (Bsp: Niemand verlässt sich aufs Gerät, aber es kann mit guter Chance an der richtigen Stelle Alarm ausgelöst werden.)
- Für mobile-Usecases mit *normalem Schutzbedarf*: Laptops mit Standard-Betriebssystemen und Standard-Schutzmaßnahmen (Bsp: Standard-Securitypaket, bekannte VPN-Clients, bekannte Speicher-Container, Protokollierung, vor allem: gesicherte Prozesse der Kommunikation) gemanaged nutzen.
- Für mobile-Usecases mit *hohem Schutzbedarf:* Nur vollkontrollierbare technische Eigenentwicklung denkbar, die sicherheits- und datenschutztechnisch überprüft bzw. auditiert sind.

Was ist zu tun im Kontext von mHealth?

- Abschichten von Perfektionsvorstellungen gegenüber den Möglichkeite der Überwachungstechnik am Menschen (es geht nicht immer um *Leben oder Tod*).

- Wenn es um Leben oder Tod oder um das Verhindern bedrohlicher Folgen geht, dann muss die Überwachungstechnik **zuverlässig, robust und sicher** sein. Mit AUS-Schalter für den Betroffenen!

Auftraggeber: VDI/VDE Innovation + Technik GmbH, Steinplatz 1, 10623 Berlin

Verfasser: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD) – Holstenstr. 98, 24103 Kiel

Stand: Dezember 2010

Format: DIN A4, 187 Seiten

www.datenschutzzentrum.de

ULD

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Vielen Dank für Ihre Aufmerksamkeit!

ULD

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein
Martin Rost
Telefon: 0431 988 – 1200
uld32@datenschutzzentrum.de
https://www.datenschutzzentrum.de/