Datenschutz und Datensicherheit bei Entwicklung und Einsatz mobiler Apps

HEALTHCARE SOLUTIONS

App-Entwicklung „hands-on“ für das Gesundheitswesen

conhIT 07. Mai 2014

Dr. Bernd Schütze

Worum geht es?

- Übersicht
- TMG
- TKG
- Apps: Beispiele / lessions learned
- Datenschutz-Umsetzung
- Diskussion
- Literatur

- Apps und „Internetrecht“
  - Telemediengesetz
  - Telekommunikationsgesetz
- Datenschutz bei Apps: Beispiele
- Anforderungen des Datenschutzes umsetzen

Datenschutz im Mobilen: die Sicht des Informatikers

- Übersicht
- TMG
- TKG
- Apps: Beispiele / lessions learned
- Datenschutz-Umsetzung
- Diskussion
- Literatur

OSI-Modell		Anwendende Gesetze
7	Anwendung	(Gesundheits)- Datenschutzgesetze (Bundesrecht / Landesrecht / Kirchenrecht)
6	Darstellung	Telemediengesetz
5	Sitzung	
4	Transport	Telekommunikationsgesetz
3	Vermittlung	
2	Sicherung	
1	Bitübertragung	

Schicht 7: Die Datenschutzgesetze

- Übersicht
- TMG
- TKG
- Apps: Beispiele / lessions learned
- Datenschutz-Umsetzung
- Diskussion
- Literatur

- EU
  - Europäische Grundrechte-Charta
  - Datenschutz-Richtlinie
    Wirkung über Umsetzung in deutsche Gesetze
  - Datenschutz-Verordnung
    (derzeit im Entwurf, sie würde unmittelbar gelten und deutsches Recht ersetzen)
- Bundesdatenschutzgesetz (BDSG)
  - Privatpersonen
  - Privatwirtschaft
  - Bundesbehörden
- Kirchliche Datenschutzgesetze
  - Einrichtungen der evang. und kath. Kirche
- Landesdatenschutzgesetze
  - öffentliche Verwaltung in Land und Kommunen
- Spezialgesetze
  (Vorrang vor allg. Gesetzen)
  - TeleMedienGesetz
  - TeleKommunikationsGesetz
  - Landeskrankenhausgesetze
  - Gesundheitsdatenschutz
  - Hochschulgesetz
  - SGB, AO, Polizeigesetz, Passgesetz, Personalausweisgesetz, Aufenthaltsgesetz, LandesMeldeGesetz, Landesverwaltungsgsetz, …

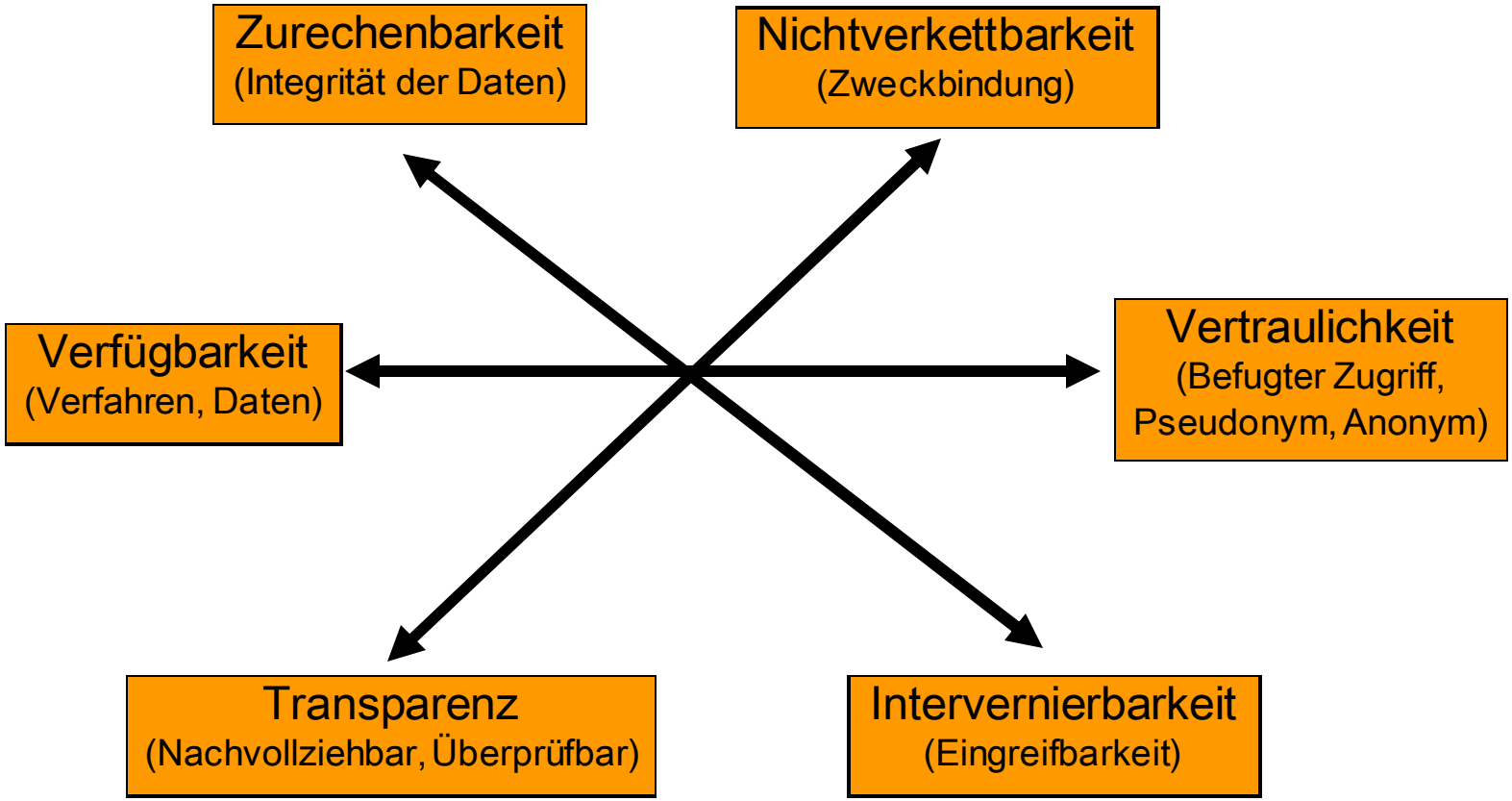
- Rechtmäßigkeit der Datenverarbeitung
  - Gesetzliche Grundlagen
  - Einwilligung
- Grundsatz der Zweckbindung
- Grundsatz der Erforderlichkeit
- Grundsatz der Datenvermeidung und Datensparsamkeit
- Grundsatz der Transparenz
- Grundsatz der klaren Verantwortlichkeiten
- Grundsatz der Kontrolle
- Grundsatz der Gewährleistung der Betroffenenrechte
  - Verbot der Profilbildung
  - Verbot der Datensammlung auf Vorrat
  - Verbot der automatisierten Einzelentscheidung
- Nutzung pseudonymisierter oder anonymisierter Daten
- Verpflichtung zum Schutz der Daten

Allgemeine datenschutzrechtliche Anforderungen

- Datenerhebung
  - Gesetzliche Grundlage
  - Einwilligung
- Zweckbindung der Daten
- Bei Verwendung externer Unterstützung
  - Auftragsdatenverarbeitung?
    (Wenn ja: An Vertrag denken!)
  - Funktionsübertragung
- Umsetzung Technisch-Organisatorische Maßnahmen (TOM)
- Cave: Gesundheitsdaten = Besondere Art von personenbezogenen Daten = besonders schützenswert

Ziele des Datenschutzes – Antagonisten zueinander?

- Übersicht
- TMG
- TKG
- Apps: Beispiele / lessions learned
- Datenschutz-Umsetzung
- Diskussion
- Literatur

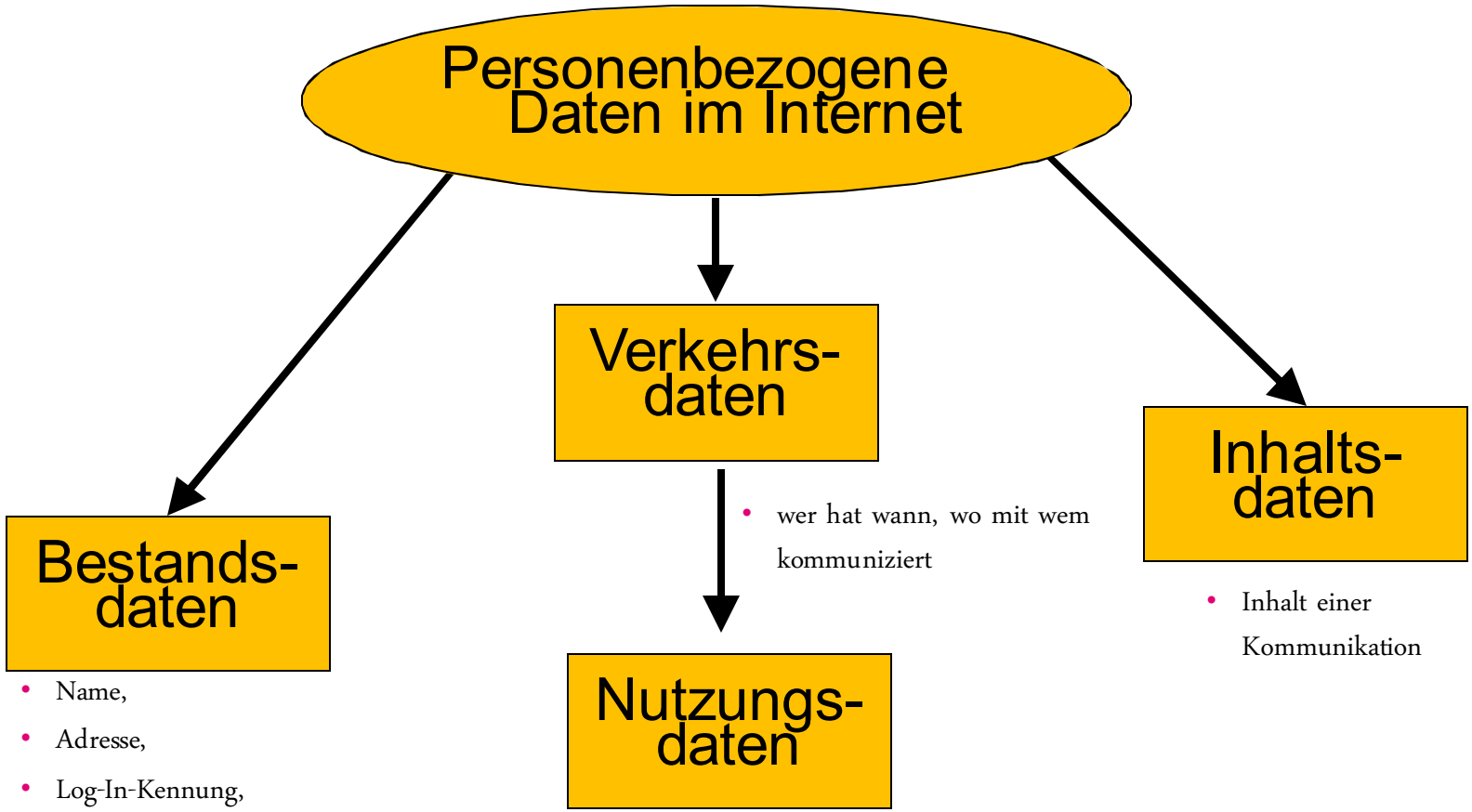


Apps und deutsches „Tele“-Recht

- TKG bspw. relevant bei Apps
  - Voice over IP (VoIP)
  - Nutzung einer eigenen Infrastruktur außerhalb des öffentlichen Internets
  - Selbstständige Veröffentlichung/Verteilung von Text-, Audio-, Bild- oder Video-Nachrichten in sozialen Netzwerken oder anderen Portalen und Diensten
  - Netzübergreifende Telefonie, E-Mail und Real Time Messaging
- TMG bspw. relevant bei Apps
  - Datendienste (Verkehr, Wetter, Umwelt, Börse)
  - Soziale Netzwerke,
  - Empfehlungs- und Ratgeberdienste,
  - Bestellungs-, Buchungs- und Maklerdienste, einschließlich Shops und Handelsplattformen,
  - Presse- und Nachrichtendienste,
  - Multiplayer-Games mit Interaktions- und Kommunikationsmöglichkeiten,
  - On-Demand- und Streaming-Dienste, soweit es sich dabei nicht um Rundfunk handelt.

Telemedienrecht – Grundlegende Begriffe

- Übersicht
- **TMG**
- TKG
- Apps: Beispiele / lessions learned
- Datenschutz-Umsetzung
- Diskussion
- Literatur



- Name,
- Adresse,
- Log-In-Kennung,
- Bankverbindungsdaten,
- ...

- wer hat wann, wo mit wem kommuniziert

- Inhalt einer Kommunikation

- Identifikation des Nutzers (IP-Adresse),
- Beginn und Ende der jeweiligen Nutzung,
- Angaben über die in Anspruch genommenen Medien,
- ...

TMG und Datenschutz

- Auskunft über Bestandsdaten für Zwecke der Strafverfolgung und Gefahrenabwehr (§14 Abs. 2)
- Grundsatz: Anonyme und pseudonyme Nutzung ist zu ermöglichen, soweit „technisch möglich und zumutbar“ (§ 13 Abs. 6 TMG)
- Cave IP-Adresse: Personenbezug kontrovers diskutiert
  - Kein Personenbezug:
    - AG München, Urteil 30.09.2008 (133 C 5677/08)
  - Personenbezug:
    - EuGH, Urteil 24.11.2011 (C70-10)
    - Amtsgericht Berlin, Urteil 27.03.2007 (5 C 314/06
  - Rat: IP-Adresse als personenbezogenes Datum betrachten

TMG und Einwilligung

- Regelungen zur Einwilligung: „Opt-In“, § 13 Abs. 2 TMG
- kann elektronisch erfolgen (§13 Abs. 2 TMG)
- Voraussetzung für gültige elektronische Einwilligung
  - der Nutzer hat seine Einwilligung bewusst und eindeutig erteilt,
  - die Einwilligung wird protokolliert,
  - der Nutzer kann den Inhalt der Einwilligung jederzeit abrufen und
  - der Nutzer kann die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen.

Cookies

- EU RL 2009/136/EG → Einsatz von Cookies grundsätzlich zustimmungsbedürftig (opt-in)
  - Ausnahmen hiervon werden in Art. 5 Abs. 3 S. 2 benannt, z.B. Sitzungscookies zur Anpassung der Benutzeroberfläche (z.B. Sprachauswahl)
  - Third-party-Cookies zu Werbezwecken erfordern immer ein opt-in
  - Aber: RL in Deutschland nicht umgesetzt
- Der Einsatz von Cookies, welche die Identifikation des Nutzers ermöglichen, erfordern
  - Das Einverständnis des Nutzers über das Setzen des Cookies
  - Die Information des Nutzers über das Setzen des Cookies

TMG: Hinweispflichten

- Unterrichtungspflichten zu Beginn des Nutzungsvorgangs (§ 13 Abs. 1 TMG)
- Unterrichtung muss beinhalten
  - Art,
  - Umfang,
  - Zwecke der Erhebung und Verwendung (Bei Erstellung Nutzungspofil immer genutzte Verfahren angeben!)
  - sowie über die Verarbeitung seiner Daten in EU-Drittstaaten
- Unterrichtung muss
  - in allgemein verständlicher Form erfolgen
  - sich an „den besonderen Risiken der Datenverarbeitung im Netz“ orientieren
- Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein

TMG: Umgang mit Logfiles

- Nicht anwendbar ist der Datenschutz auf nicht-personenbezogene Daten in Log-Files, also
  - Zugriffszeit,
  - Nutzungsdauer,
  - Auflösung
  - verwendeter Browser
  - ...
- Von Aufsichtsbehörden geduldete Speicherdauer: maximal 7 Tage (Log-Daten,die Sicherheitszwecken dienen)
- Cave: IP-Adresse innerhalb Log-Files
  - Empfehlung: vorsorglich diese Daten unverzüglich, spätestens innerhalb von 48 Stunden, löschen (§ 15 IV TMG) und dies dem Nutzer auch mitteilen

TMG: Umgang mit Logfiles

- Herausgabe an Privatleute, Unternehmen usw. ist grundsätzlich nicht erlaubt
  - Ausnahme: Auskunftsersuchen im Rahmen von Urheberrechtsverletzungen (§14 TMG)
- Herausgabe zur Strafverfolgung
  - Richterlicher Beschluss nötig
  - Einfache Anfrage seitens Ermittlungsbehörde genügt als Grundlage zur Berechtigung der Weitergabe wahrscheinlich nicht
- Weitergabe von IP-Adressen:
  - Geolocation
  - DNS-Blacklisting
  - Google Analytics
  - ...

1. Kürzung IP-Adresse oder Einverständnis Betroffener
2. Auftragsdatenverarbeitungsvertrag nötig?

Telekommunikationsgesetz (TKG)

- Übersicht
- TMG
- **TKG**
- Apps: Beispiele / lessions learned
- Datenschutz-Umsetzung
- Diskussion
- Literatur

- Fernmeldegeheimnis
- Einwilligung jeden Teilnehmers
- Nutzung von Bestands- und/oder Verkehrsdaten, z.B.
  - wer hat sich wann angemeldet
  - wer hat worauf wann zugegriffen
  - von wo hat wer wann worauf zugegriffen
    (Cave: Standortdaten nur mit expliziter Einwilligung
    → Feste IP-Adresse und Standortbestimmung?)
- §93: Unterrichtspflicht für Teilnehmer (nicht für Betroffene im Sinne der gespeicherten Daten)

„Apps“ in den Schlagzeilen

- Übersicht
- TMG
- TKG
- **Apps: Beispiele / lessions learned**
- Datenschutz-Umsetzung
- Diskussion
- Literatur

Quelle: S

Apps und Sicherheit

- Übersicht
- TMG
- TKG
- **Apps: Beispiele / lessions learned**
- Datenschutz-Umsetzung
- Diskussion
- Literatur

- 2010 App Genome Project*
  - >300.000 Apps, davon 1/3 genauer überprüft
  - Ca. 50% der Apps übermitteln ungefragt Daten an Dritte
- 2011: Studie der TU Wien, University of California, Northeastern University, Institute Eurecom**
  - 1407 iPhone-Apps (825 Apple App Store, 582 Cydia)
  - 55% übermitteln ungefragt Daten an Dritte
- 2012: Untersuchung des NDR
  - 100 Apps
  - 48% übermitteln ungefragt Daten an Dritte
- 2012: Stiftung Warentest
  - 63 Apps
  - 48% übermitteln ungefragt Daten an Dritte
- 2013 Wirtschaftswoche
  - 88 Apps greifen ungefragt auf E-Mails, Kontakte, Termine und/oder Standortdaten zu

Quelle: * App Genome Report, onile: https://www.lookout.com/resources/reports/appgenome

** PiOS, online, verfügbar unter http://www.syssec-project.eu/media/page-media/3/egele-ndss11.pdf

Apps und Sicherheit

➔ Übertragene Daten

- Geräte-Kennung
- Standort
- Adressbuch
- Kalender
- …

➔ Wozu?

- Erstellung von Nutzungs- und Bewegungsprofilen
- Kontaktdaten für Werbung
- Preisgabe vertraulicher Informationen, z.B.
  - ✓ Banking-Informationen
  - ✓ Identitäts-Diebstahl
  - ✓ Unternehmens-Zugangsdaten
  - ✓ …

Apps und Sicherheit: Beispiele

- GoodReader
  - unverschlüsselte Datenablage
  - öffnet Serverdienst
  - deaktiviert Bildschirmsperre
- SAP Cart Approval
  - Benutzername und Passwort in unverschlüsselter Log-Datei
- Citrix
  - Zugangsdaten im Klartext auf Datenträger (und Backup)
- …

Anforderungen

1. Gesundheitsdaten, die einer Person zugeordnet werden können, sind
   - Sicher aufzubewahren (Verschlüsselte Dateiablage)
   - Getrennt von anderen Daten aufzubewahren
   - Sicher zu übertragen (Verschlüsselten Übertragungsweg beachten)
   - Ggfs. Verfügbarkeit zu gewährleisten (Cave: Gesundheitsschaden bei Nicht-Verfügbarkeit?)
   - Nachweispflichtig
     - ✓ Bzgl. Zugriff auf die Daten (Logdatei)
     - ✓ Änderung der Daten (Versionskontrolle)
2. Bedenken: Eine App kann ein Medizinprodukt sein, woraus weitere Anforderungen resultieren

Hinweise: 1) Bayerische Landesamt für Datenschutzaufsicht veröffentlichte Hinweise zu datenschutzrechtlichen Anforderungen an mobile Applikationen (Webseite http://www.lda.bayern.de/MobileApplikationen/index.html, zuletzt besucht 2014-04-02)

Datenschutz – was tun?

- Übersicht
- TMG
- TKG
- Apps: Beispiele / lessions learned
- **Datenschutz-Umsetzung**
- Diskussion
- Literatur

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Verantwortlichkeiten definieren

- Übersicht
- TMG
- TKG
- Apps: Beispiele / lessions learned
- **Datenschutz-Umsetzung**
- Diskussion
- Literatur

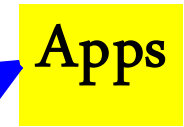
- Wer hat Einflussmöglichkeiten auf das System?
- Wer hat die Datenhoheit über die erhobenen Daten?
  - Nutzer?
  - Hersteller des Systems?
  - Betreiber des Systems?
  - “Paten“ (Verwandter/Freund/Arzt/Institution)?
  - …
- Grundlage der Tätigkeiten ist
  - gesetzlicher
  - vertraglicher
  - gewillkürter

Art?

Technische und organisatorische Maßnahmen („TOMs“)

- Übersicht
- TMG
- TKG
- Apps: Beispiele / lessions learned
- **Datenschutz-Umsetzung**
- Diskussion
- Literatur

1. **Zutrittskontrolle**
   (Bsp.: Verschlossene Türen)
2. **Zugangskontrolle**
   (Bsp.: Computer mit Passwortschutz)
3. **Zugriffskontrolle**
   (Bsp.: Zugriff auf Daten nur gemäß Berechtigungskonzept)
4. **Weitergabekontrolle**
   (Bsp.: Logmechanismen bei elektr. Datentransport)
5. **Eingabekontrolle**
   (Bsp: Eingabe personenbezogener Daten nur durch autorisiertes Personal)
6. **Auftragskontrolle**
   (Bsp.: Verarbeitung nur gemäß erteiltem Auftrag)
7. **Verfügbarkeitskontrolle**
   (Bsp.: Schutz gegen zufällige Zerstörung oder Verlust durch Backup)
8. **Gebot der Datentrennung**
   (Bsp.: zu unterschiedlichen Zwecken erhobene Daten werden getrennt verarbeitet)



Was tun?

1. Schutzbedarf ermitteln
2. Verfahren analysieren
   - Welche Daten werden erhoben, verarbeitet=
   - Welche Systeme kommen zum Einsatz?
   - Welche Prozesse werden gelebt, sind geplant?
3. Schutzziele Datenschutz umsetzen

Schutzbedarf der Daten definieren

- Übersicht
- TMG
- TKG
- Apps: Beispiele / lessions learned
- **Datenschutz-Umsetzung**
- Diskussion
- Literatur

Strukturelle Orientierung an BSI-Grundschutzdefinition

- Normal: Schadensauswirkungen sind begrenzt und überschaubar und etwaig eingetretene Schäden für Betroffene relativ leicht zu heilen.
- Hoch: die Schadensauswirkungen werden von Betroffenen als beträchtlich eingeschätzt, z.B. weil der Wegfall einer von einer Organisation zugesagten Leistung die Gestaltung des Alltags nachhaltig veränderte und der Betroffene nicht aus eigener Kraft handeln kann sondern auf Hilfe angewiesen wäre.
- sehr hoch: Die Schadensauswirkungen nehmen ein unmittelbar existentiell bedrohliches, also: katastrophales Ausmaß für Betroffene an.

nach Martin Rost (ULD), Vortrag „1. DFN-Workshop Datenschutz“, verfügbar unter http://www.dfn-cert.de/veranstaltungen/vortrage-vergangener-workshops/DFNDatenschutzworkshop2012.html

Referenzmodell für Datenschutzmaßnahmen

- 6 Schutzziele
  - Vertraulichkeit
  - Integrität
  - Transparenz
  - Verfügbarkeit
  - Nichtverkettbarkeit
  - Intervenierbarkeit
- 3 Schutzbedarfsabstufungen
  - Normal
  - Hoch
  - Sehr hoch
- 3 Verfahrenskomponenten
  - Daten
  - Systeme
  - Prozesse

➔ Erstellung eines Referenzmodells mit 6 x 3 x 3 = 54 Datenschutzmaßnahmen

Quelle: Probst T. (2012) Generische Schutzmaßnahmen für Datenschutz-Schutzziele. DuD 36(6): 439-444

Referenzmodell für Datenschutzmaßnahmen

- Übersicht
- TMG
- TKG
- Apps: Beispiele / lessions learned
- **Datenschutz-Umsetzung**
- Diskussion
- Literatur

	Daten	Systeme	Prozesse
Verfügbarkeit Findbarkeit Ermittelbarkeit Verbindlichkeit	D 1.1 Einschränkung von Lösch-/Veränderungsrechten D 1.2 Schutz vor Schadsoftware D 1.3 Backup der Daten	S 1.1: Schutz vor Schadsoftware S 1.2: Backup von Konfigurationen und Software S 1.3: Hardwareredundanz S 1.4: Ausweichräume, und -Netze	P 1.1: Vertretungspersonal P 1.2: Fähigkeit zur Aufgabenerledigung durch Dritte (Vorbereitung Outsourcing) P 1.3: Ausweichprozesse, Planung von Notfallszenarien, Amtshilfe
Vertraulichkeit Verdecktheit Anonymität Unbeobachtbarkeit	D 2.1: Einschränkung von Leserechten (für Datenverarbeiter, ggf. durch den Nutzer selbst) D 2.2: Protokollierung lesender Zugriffe D 2.3: Verschlüsselung der Daten D 2.4: Ende-zu-Ende-Verschlüsselung	S 2.1: Einschränkung von lesenden Zugriffsrechten auf IT-Systeme (z. B. Netztrennung durch Sicherheitsgateways) S 2.2: Verschlüsselung auf Systemebene (Festplatten, Datenbank)	P 2.1: Verpflichtung auf das Datengeheimnis (BDSG) P 2.2: Verschwiegenheitsvereinbarungen P 2.3: Geeignete Organisation bei der Vergabe von Zugriffsrechten („need-to-know")
Integrität Zurechenbarkeit	D 3.1: Einschränkung von Schreib- und Änderungsrechten D 3.2: Protokollierung von schreibenden/ändernden Zugriffen D 3.3: Protokollierung geänderter Daten D 3.4: Nachberichtigung D 3.5: technische Integritätskontrollen (Signaturen/Hashes)	S 3.1: Einschränkung von schreibenden Zugriffen/Konfigurationmöglichkeiten auf IT-Systeme (z. B. Netztrennung durch Sicherheitsgateways) S 3.2 Schutz vor Schadsoftware S 3.3: Regelmäßige Integritätsprüfungen/Audits	P 3.1: Detaillierte Planung von Verfahren und Verfahrensschritten P 3.2: Geordnete Zuweisung von Rechten und Rollen P 3.3: Geordnete Änderung von Verfahren und Verfahrensschritten P 3.4: Regelmäßige Überprüfung (z.B. Verfahrensqualität) und Nachsteuern
Nicht-Verkettbarkeit	D 4.1: Löschen, nach Wegfall der Erforderlichkeit; ggf. „Wipen" D 4.2 Einschränkung von Verarbeitungs- / Nutzungs- / Übermittlungsrechten für einzelne Daten D 4.3: Kennzeichnung der Zwecke auf Ebene der Daten D 4.4: Einschränkung von identifizierenden Daten; Pseudonymisierung D 4.5: Anonymisierung von Daten	S 4.1: Kennzeichnung der Zwecke auf Ebene des Systems S 4.2: Trennung von Datenbeständen S 4.3: Einschränkungen von Verarbeitungs-, Nutzungs- und Übermittlungsmöglichkeiten (Funktionalitätseinschränkung) S 4.4: Trennung auf Systemebene (Software, Hardware; Mandantenfähigkeit) S 4.5: Physikalische Trennung und unabhängige RZ-Betreiber	P 4.1: Trennung auf Verfahrensebene P 4.2: Rechte + Rollenvergabe, ggf. an eine andere rechtliche Entität (z. B. Personalvertretung) P 4.3: Gewaltenteilung (z.B. Durchführung einzelner Verfahrensschritte durch andere rechtliche Entitäten)
Transparenz	D 5.1: Dokumentation der Datenfelder einschließlich Erforderlichkeit D 5.2: Protokollierung von Datenverarbeitungen mit Schutzbedarf zunehmender Detaillierungsgrad und Speicherdauer D 5.3: Integritätsschutz der Protokolle (separater Protokollierungsserver)	S 5.1: Dokumentation der Systeme (Hardware, Software, Algorithmen) S 5.2: Protokollierung von Konfigurationsänderungen S 5.3: zunehmende Kontrolldichte bei höherem Schutzbedarfen; automatisiertes Monitoring	P 5.1: Dokumentation des Verfahren und einzelner Prozesse (einschließlich beteiligter Organisationseinheiten, Rollen und Übermittlungen an Dritte) P 5.2: Dokumentation der Änderungsprozesse
Intervenierbarkeit Kontingenz / Abstreitbarkeit	D 6.1: Schaffung notwendiger Datenfelder (z. B. für Gegendarstellungen) und Kennzeichnungen	S 6.1: Funktionalitäten in den Systemen für die Bearbeitung von Sperrungen, Widersprüchen, Beauskunftungen S 6.2: Funktionalitäten in den Systemen für die Umsetzung von weiteren Rechten Betroffener (z. B. Rufnummerunterdrückung, Pseudonyme Nutzungsmöglichkeit, etc.) S 6.3: Funktionalitäten für Betroffene einzelne Betroffenenrechte direkt wahrzunehmen (z.B. Auskunftsportal, „Datenbrief", Zusendung von Protokollen, eigene Änderungsmöglichkeiten) S 6.4: Steuerungsmöglichkeiten für einzelne Funktionen („Overrride") bei automatisierten Einzelentscheidungen S 6.5: Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem	P 6.1: Organisation der Umsetzung der Betroffenenrechte (Rechte + Rollen für Auskunft, Sperrungen) P 6.2: Single Point of Contact für Datenschutzfragen P 6.3: Organisation der Umsetzung der Betroffenenrechte (Rechte und Rollen bei der Bearbeitung von Gegendarstellungen und Einwänden; Übersteuern einzelner Prozesse, insb. automatisierter Einzelfallentscheidungen) P 6.4: Durchgriff des Nutzers auf seine Daten („Selbstverwaltung") P 6.5: (zertifiziertes) Changemanagement auf Seiten der Organisation

Quelle: Probst T. (2012) Generische Schutzmaßnahmen für Datenschutz-Schutzziele DuD 36(6): 439-444

Datenschutz: Was tun als Firma?

- Regelmäßige (interne) Audits und Tätigkeitsberichte
- Unterlagen bereithalten
  - Bestellung **DSB**
  - Betriebsvereinbarungen
  - Ergebnis interner Audits
  - Ergebnis Vorabkontrollen
  - Verfahrensverzeichnis
  - Verpflichtungserklärungen / Mitarbeiter-Schulungsnachweise
- Konzepte erstellen und aktuell halten
  - Datenschutzkonzept / Datenschutzrichtlinie
  - Berechtigungskonzept
  - Sicherheitskonzept / Notfall-Handbuch
  - Protokollierungskonzept
  - Ggf. Archivordnung

Diskussion

- Übersicht
- TMG
- TKG
- Apps: Beispiele / lessions learned
- Datenschutz-Umsetzung
- **Diskussion**
- Literatur

Kontakt: schuetze@medizin-informatik.org

Literatur (Auswahl)

- Übersicht
- TMG
- TKG
- Apps: Beispiele / lessions learned
- Datenschutz-Umsetzung
- Diskussion
- **Literatur**

Zeitschriften

- Achten OM, Pohlmann N. Sichere Apps - Vision oder Realität? DuD 2012: 161ff
- Alkassar A, Schulz S, Stüble C. Sicherheitskern(e) für Smartphones: Ansätze und Lösungen. DuD2012: 175ff
- Arning M, Moos F, Becker M. Vertragliche Absicherung von Bring Your Own Device - Was in einer Nutzungsvereinbarung zu BYOD mindestens enthalten sein sollte. CR 2012: 592ff
- Becker P, Nikolaeva J. Das Dilemma der Cloud-Anbieter zwischen US Patriot Act und BDSG - Zur Unmöglichkeit rechtskonformer Datenübermittlung für gleichzeitig in USA und Deutschland operierende Cloud-Anbieter. CR 2012: 170ff
- Bierekoven C. Bring your own Device: Schutz von Betriebs- und Geschäftsgeheimnissen - Zum Spannungsverhältnis zwischen dienstlicher Nutzung privater Mobilgeräte und Absicherung sensibler Unternehmensdaten. ITRB 2012: 106ff
- Conrad I, Antoine L. Betriebsvereinbarungen zu IT- und TK-Einrichtungen - Betriebsverfassungs- und datenschutzrechtliche Aspekte im Überblick. ITRB 2006: 90ff
- Conrad I, Schneider J. Einsatz von „privater IT“ im Unternehmen - Kein privater USB-Stick, aber „Bring your own device” (BYOD)? ZD 2011: 153ff
- Deiters G. Betriebsvereinbarung Kommunikation - Beschäftigteninteressen und Compliance bei privater Nutzung von Kommunikationsmitteln im Unternehmen. ZD 2012: 109ff
- Gola P. Datenschutz bei der Kontrolle „mobiler” Arbeitnehmer – Zulässigkeit und Transparenz. NZA 2007: 1139
- Göpfert B, Wilke E. Nutzung privater Smartphones für dienstliche Zwecke. NZA 2012: 765ff
- Grünwald A, Döpkens HR. Cloud Control - Regulierung von Cloud Computing-Angeboten. MMR 2011: 287ff
- Hassemer IM, Witzel M. Filterung und Kontrolle des Datenverkehrs - Ist die Filterung von E-Mails im Unternehmen rechtmäßig? ITRB 2006: 139ff
- Heidrich J, Wegener C. Sichere Datenwolken -Cloud Computing und Datenschutz. MMR 2010: 803ff
- Hermleben G. BYOD – die rechtlichen Fallstricke der Software-Lizenzierung für Unternehmen. MMR 2012: 205ff
- Hörl B. Bring your own Device: Nutzungsvereinbarung im Unternehmen - Mitarbeiter-PC-Programm als Steuerungsinstrument des Arbeitgebers. ITRB 2012: 258ff
- Hörl B, Buddee A. Private E-Mail-Nutzung am Arbeitsplatz - Rechte und Pflichten des Arbeitgebers und des Arbeitnehmers. ITRB 2002: 160ff
- Hornung G. Die Haftung von W-LAN Betreibern - Neue Gefahren für Anschlussinhaber – und die Idee „offener“ Netze. CR 2007: 88ff
- Hoß A. Betriebsvereinbarung über Internet-Nutzung. ArbRB 2002: 315ff
- Koch FA. Rechtsprobleme privater Nutzung betrieblicher elektronischer Kommunikationsmittel. NZA 2008: 911ff
- Koch FA. Arbeitsrechtliche Auswirkungen von „Bring your own Device“ - Die dienstliche Nutzung privater Mobilgeräte und das Arbeitsrecht. ITRB 2012: 35ff
- Kramer S. Gestaltung betrieblicher Regelungen zur IT-Nutzung. ArbRAktuell 2010: 164ff
- Kremer S, Sander S. Bring your own Device - Zusammenfassung und Fortführung der Beiträge in ITRB 11/2011 bis ITRB 11/2012. ITRB 2012: 275ff
- Kremer S. Datenschutz bei Entwicklung und Nutzung von Apps für Smart Devices. CR 2012: 438 - 446

Literatur (Auswahl)

- Übersicht
- TMG
- TKG
- Apps: Beispiele / lessions learned
- Datenschutz-Umsetzung
- Diskussion
- **Literatur**

Zeitschriften

- Marnau N, Schlehahn E. Cloud Computing und Safe Harbor. DuD2011: 311ff
- Malpricht MM. Haftung im Internet – WLAN und die möglichen Auswirkungen - Straf- und zivilrechtliche Konsequenzen der rechtswidrigen Internetnutzung. ITRB 2008: 42ff
- Nägele S. Internet und E-Mail: Abwehrrechte des Arbeitnehmers und Betriebsrats gegen unberechtigte Kontrollmaßnahmen des Arbeitgebers. ArbRB 2002: 55ff
- Niemann F, Hennrich T. Kontrollen in den Wolken? Auftragsdatenverarbeitung in Zeiten des Cloud Computings. CR 2010: 686ff
- Nordmeier CF. Cloud Computing und Internationales Privatrecht - Anwendbares Recht bei der Schädigung von in Datenwolken gespeicherten Daten. MMR 2010: 151ff
- Pohle J, Ammann T. Über den Wolken... – Chancen und Risiken des Cloud Computing. CR 2009: 276ff
- Polenz S, Thomsen S. internet- und E-Mail-Nutzung. DuD 2010: 614ff
- Pröpper M, Römermann M. Nutzung von Internet und E-Mail am Arbeitsplatz (Mustervereinbarung). MMR 2008: 514ff
- Schmidl M. E-Mail-Filterung am Arbeitsplatz. MMR 2005: 343ff
- Schoen T. Umgang mit E-Mail-Accounts ausgeschiedener Mitarbeiter. DuD 2008: 286ff
- Schröder C, Haag NC. Neue Anforderungen an Cloud Computing für die Praxis - Zusammenfassung und erste Bewertung der „Orientierungshilfe – Cloud Computing“. ZD 2011: 147ff
- Schröder C, Haag NC. Stellungnahme der Art. 29-Datenschutzgruppe zum Cloud Computing - Gibt es neue datenschutzrechtliche Anforderungen für Cloud Computing? ZD 2012: 495ff
- Söbbing T, Müller NR. Bring your own Device: Haftung des Unternehmens für urheberrechtsverletzenden Inhalt - Absicherung einer urheberrechtskonformen Hard- und Softwarenutzung für Unternehmenszwecke. ITRB 2012: 15ff
- Söbbing T, Müller NR. Bring your own Device: Strafrechtliche Rahmenbedingungen - Vorkehrungen gegen Datenmissbrauch bei Nutzung privater Geräte im Unternehmen. ITRB 2012: 263ff
- Spies A. Cloud Computing: Keine personenbezogenen Daten bei Verschlüsselung. MMR 2011: 313727
- Spindler G. Haftung für private WLANs im Delikts- und Urheberrecht. CR 2010: 592ff
- Ueckert A. Private Internet- und E-Mail-Nutzung am Arbeitsplatz - Entwurf einer Betriebsvereinbarung. ITRB 2003: 158ff
- Vietmeyer K, Byers P. Der Arbeitgeber als TK-Anbieter im Arbeitsverhältnis - Geplante BDSG-Novelle lässt Anwendbarkeit des TKG im Arbeitsverhältnis unangetastet. MMR 2010: 807
- Weichert T, Cloud Computing und Datenschutz. DuD 2010: 679ff
- Wiese G. Personale Aspekte und Überwachung der häuslichen Telearbeit. RdA 2009: 344
- Wybitul T. Neue Spielregeln bei E-Mail-Kontrollen durch den Arbeitgeber - Überblick über den aktuellen Meinungsstand und die Folgen für die Praxis. ZD 2011: 69ff
- Zimmer A. Wireless LAN und das Telekommunikationsrecht - Verpflichtungen für Betreiber nach bisherigem und künftigem Recht. CR 2003: 893ff

Literatur (Auswahl)

- Übersicht
- TMG
- TKG
- Apps: Beispiele / lessions learned
- Datenschutz-Umsetzung
- Diskussion
- **Literatur**

Internet

- Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Orientierungshilfe Cloud Computing
  http://www.datenschutz-bayern.de/technik/orient/oh_cloud.pdf
- AV-Comparatives: Mobile Security Bewertungen
  http://www.av-comparatives.org/de/vergleichstests-bewertungen/mobile-security-bewertungen
- BITKOM Leitfaden Desktop-Virtualisierung
  http://www.bitkom.org/de/publikationen/38337_66035.aspx
- BITKOM Positionspapier zu Cloud Computing
  http://www.bitkom.org/de/publikationen/38337_71486.aspx
- Bundesamt für Sicherheit in der Informationstechnik (BSI): Überblickspapier IT-Consumerisation und BYOD
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_BYOD_pdf.pdf?__blob=publicationFile
- Bundesamt für Sicherheit in der Informationstechnik (BSI): Überblickspapier Smartphones
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_Smartphone_pdf.pdf?__blob=publicationFile
- Bundesamt für Sicherheit in der Informationstechnik (BSI): Mobile Security
  https://www.bsi.bund.de/ContentBSI/Themen/Mobilsecurity/mobilsecurity.html
- Bundesamt für Sicherheit in der Informationstechnik (BSI): Cloud Computing
  https://www.bsi.bund.de/DE/Themen/CloudComputing/CloudComputing_node.html
- CyberBloc: Cloud Storages im Überblick
  http://www.cyberbloc.de/index.php?/site/v3_comments/cloud_storages_im_ueberblick/
- Esb Rechtsanwälte: Rechtliche Fallstricke bei BYOD
  http://www.kanzlei.de/publikation/Rechtliche%20Fallstricke%20bei%20Bring%20Your%20Own%20Device.pdf
- European Directory of Health Apps 2012-2013
  http://stwem.files.wordpress.com/2012/10/pv_appdirectory_final_web_300812.pdf
- Haslbeck, Franz. BYOD: pro + Contra, Alternativen, Handlungsbedarf und Handlungsempfehlungen
  http://enterprisemobilitymobi.wordpress.com/2012/08/21/byod-pro-contra-alternativen-handlungsbedarf-handlungsempfehlungen/
- Institut für IT-Recht: Bring-Your-Own-Device: Datenschutz-Empfehlungen und technische Umsetzungsmöglichkeiten
  http://www.iitr.de/bring-your-own-device-datenschutz-empfehlungen-und-technische-umsetzungsmoeglichkeiten.html
- IT-Recht Kanzlei:Cloud Computing und Datenschutz- Eine Einführung
  http://www.it-recht-kanzlei.de/cloud-computing-wolke-daten.html
- Kersten H, Klett G: Mobile Device Management. mitp Verlag. ISBN 3826692144
- Kraska S, Meuser P. BYOD – Datenschutzund technische Umsetzung
  http://www.channelpartner.de/channelcenter/mobilecomputing_smartphones/2589912/index.html
- Sidorenko A, Hoeft C, Krengel J, Spieker R. Konzeption einer BYOD Lösung auf Basis der Desktopvirtualisierung
  http://winfwiki.wi-fom.de/index.php/Konzeption_einer_BYOD_L%C3%B6sung_auf_Basis_der_Desktopvirtualisierung
- Walter T, Dorschel J: Mobile Device Management – rechtliche Fragen
  http://www.bartsch-rechtsanwaelte.de/media/docs/JD/Mobile%20Device%20Management%20-%20rechtliche%20Fragen.pdf
- Zeitschrift für Informations-Sicherheit (kes): Mobile Security
  http://www.kes.info/archiv/material/mobsec2012/mobsec2012.pdf

Literatur (Auswahl)

- Übersicht
- TMG
- TKG
- Apps: Beispiele / lessions learned
- Datenschutz-Umsetzung
- Diskussion
- **Literatur**

Bücher

- Androulidakis I. Mobile Phone Security and Forensics: A Practical Approach. Springer Verlag. ISBN 1461416493
- Barrett D, Kipper G. Virtualization and Forensics: A Digital Forensic Investigators Guide to Virtual Environments. Syngress Media. ISBN
- Baumgartner U, Ewald K. Apps und Recht.C. H. Beck Verlag. ISBN 978-3-406-63492-5
- Blaha R, Marko R, Zellhofer A, Liebel H. Rechtsfragen des Cloud Computing: Vertragsrecht - Datenschutz - Risiken und Haftung. Medien u. Recht Verlag. ISBN 3900741581
- Borges G, Schwenk J. Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce. Springer Verlag. ISBN 3642301010
- Bundschuh C, Betriebssysteme für Mobile Devices: Ein Überblick zur Historie und zum aktuellen Stand. ISBN: 3656064172
- Hoog A. Android Forensics: Investigation, Analysis and Mobile Security for Google Android. Syngress Publishing. ASIN B006V36GEE 1597495573
- Jansen W, Delaitre A. Mobile Forensic Reference Materials: A Methodology and Reification. CreateSpace Independent Publishing Platform. ISBN 1478179597
- Kersten H, Klett G. Mobile Device Management. mitp Professional. ISBN-10: 3826692144
- Leible S, Sosnitza O. Onlinerecht 2.0 Alte Fragen - neue Antworten?: Cloud Computing - Datenschutz - Urheberrecht – Haftung. Boorberg Verlag. ISBN 3415046125
- Lutz S. Vertragsrechtliche Fragen des Cloud Computing. Grin Verlag. ISBN 3640924908
- Maxwell R, Hooq A, Strzempka. Iphone and IOS Forensics: Investigation, Analysis and Mobile Security for Apple Iphone, Ipad and IOS Devices. Syngress Media. ISBN 1597496596
- Meyer JA. Vertraulichkeit in der mobilen Kommunikation: Leckagen und Schutz vertraulicher Informationen. ISBN: 3899369599
- Rohrlich M. Cloud Computing - Rechtliche Grundlagen. entwickler.press. ISBN: 3868021159
- Schmidt-Bens J. Cloud Computing Technologien und Datenschutz. OlWIR Verlag für Wirtschaft, Informatik und Recht. ISBN 3939704717
- Solmecke C, Taeger J,Feldmann T. Mobile Apps: Rechtsfragen und rechtliche Rahmenbedingungen. De Gruyter. ISBN: 3110304805
- Vossen G, Haselmann T, Hoeren T. Cloud-Computing für Unternehmen: Technische, wirtschaftliche, rechtliche und organisatorische Aspekte. dpunkt.verlag. ISBN 3898648087
- Wieczorek B. BYOD im MS Exchange Umfeld - Eine Evaluierung von Mobile Device Management Lösungen auf Basis einer Nutzwertanalyse. ISBN: 3656375143

Mobile Security und BSI: Das Grundschutz-Handbuch

- Übersicht
- TMG
- TKG
- Apps: Beispiele / lessions learned
- Datenschutz-Umsetzung
- Diskussion
- **Literatur**

M 1.33 Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz

M 1.44 Geeignete Einrichtung eines häuslichen Arbeitsplatzes

M 2.36 Geregelte Übergabe und Rücknahme eines tragbaren PC

M 2.109 Rechtevergabe für den Fernzugriff

M 2.113 Regelungen für Telearbeit

M 2.114 Informationsfluss zwischen Telearbeiter und Institution

M 2.115 Betreuungs- und Wartungskonzept für Telearbeitsplätze

M 2.116 Geregelte Nutzung der Kommunikationsmöglichkeiten bei Telearbeit

M 2.117 Erstellung eines Sicherheitskonzeptes für Telearbeit

M 2.188 Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung

M 2.189 Sperrung des Mobiltelefons bei Verlust

M 2.190 Einrichtung eines Mobiltelefon-Pools

M 2.218 Regelung der Mitnahme von Datenträgern und IT-Komponenten

M 2.241 Durchführung einer Anforderungsanalyse für den Telearbeitsplatz

M 2.303 Festlegung einer Strategie für den Einsatz von PDAs

M 2.304 Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung

M 2.305 Geeignete Auswahl von PDAs

M 2.306 Verlustmeldung

M 2.309 Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung

M 2.310 Geeignete Auswahl von Laptops

URL:https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Massnahmenkataloge/M2Organisation/m2organisation_node.html;jsessionid=56767F0568BE3133DF48B4E2DE141375.2_cid359

Mobile Security und BSI: Das Grundschutz-Handbuch

- Übersicht
- TMG
- TKG
- Apps: Beispiele / lessions learned
- Datenschutz-Umsetzung
- Diskussion
- **Literatur**

M 2.328 Einsatz von Windows XP auf mobilen Rechnern
M 2.381 Festlegung einer Strategie für die WLAN-Nutzung
M 2.382 Erstellung einer Sicherheitsrichtlinie zur WLAN-Nutzung
M 2.383 Auswahl eines geeigneten WLAN-Standards
M 2.384 Auswahl geeigneter Kryptoverfahren für WLAN
M 2.385 Geeignete Auswahl von WLAN-Komponenten
M 2.386 Sorgfältige Planung notwendiger WLAN-Migrationsschritte
M 2.387 Installation, Konfiguration und Betreuung eines WLANs durch Dritte
M 2.388 Geeignetes WLAN-Schlüsselmanagement
M 2.389 Sichere Nutzung von Hotspots
M 2.390 Außerbetriebnahme von WLAN-Komponenten
M 2.401 Umgang mit mobilen Datenträgern und Geräten
M 2.415 Durchführung einer VPN-Anforderungsanalyse
M 2.416 Planung des VPN-Einsatzes
M 2.417 Planung der technischen VPN-Realisierung
M 2.418 Erstellung einer Sicherheitsrichtlinie zur VPN-Nutzung
M 2.419 Geeignete Auswahl von VPN-Produkten M 2.420 Auswahl eines Trusted-VPN-Dienstleisters
M 2.442 Einsatz von Windows Vista auf mobilen Rechnern
M 2.461 Planung des sicheren Bluetooth-Einsatzes
M 2.462 Auswahlkriterien für die Beschaffung von Bluetooth-Geräten

URL:https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Massnahmenkataloge/M2Organisation/m2organisation_node.html;jsessionid=56767F0568BE3133DF48B4E2DE141375.2_cid359

Mobile Security und BSI: Das Grundschutz-Handbuch

- Übersicht
- TMG
- TKG
- Apps: Beispiele / lessions learned
- Datenschutz-Umsetzung
- Diskussion
- **Literatur**

M 2.463 Nutzung eines zentralen Pools an Bluetooth-Peripheriegeräten

M 3.21 Sicherheitstechnische Einweisung der Telearbeiter

M 3.60 Sensibilisierung der Mitarbeiter zum sicheren Umgang mit mobilen Datenträgern und Geräten

M 4.31 Sicherstellung der Energieversorgung im mobilen Einsatz

M 4.114 Nutzung der Sicherheitsmechanismen von Mobiltelefonen

M 4.115 Sicherstellung der Energieversorgung von Mobiltelefonen

M 4.63 Sicherheitstechnische Anforderungen an den Telearbeitsrechner

M 4.114 Nutzung der Sicherheitsmechanismen von Mobiltelefonen

M 4.115 Sicherstellung der Energieversorgung von Mobiltelefonen

M 5.51 Sicherheitstechnische Anforderungen an die Kommunikationsverbindung Telearbeitsrechner - Institution

M 5.78 Schutz vor Erstellen von Bewegungsprofilen bei der Mobiltelefon-Nutzung

M 5.79 Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung

M 5.80 Schutz vor Abhören der Raumgespräche über Mobiltelefone

M 5.81 Sichere Datenübertragung über Mobiltelefone

M 6.47 Datensicherung bei der Telearbeit

M 6.71 Datensicherung bei mobiler Nutzung des IT-Systems

M 6.72 Ausfallvorsorge bei Mobiltelefonen

URL:https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Massnahmenkataloge/M2Organisation/m2organisation_node.html;jsessionid=56767F0568BE3133DF48B4E2DE141375.2_cid359