UKD Universitätsklinikum Düsseldorf

GKD

Datenschutz und Datensicherheit – Anforderungen bei der Nutzung mobiler Endgeräte im Krankenhaus

Dr. Bernd Schütze, „IT-Trends Medizin/Health Telematics“, 25. September 2013, Essen

Was wirklich motiviert…

- MobileSpy (http://www.mobile-spy.com/)
  - Live Control Panel, SMS, Telefonliste, Webbrowser-History, GPS-Ortung, Photos, …
  - Android, Windows Mobile, iPhone, Blackberry, Symbian
  - 49,97 $ / 3 Monate
- FlexiSpy (http://www.flexispy.com/)
  - SMS, E-Mail, Instant Messenger, Adressbuch, GPS-Ortung, Telefongespräche mithören, …
  - Android, Windows Mobile, iPhone, Blackberry, Symbian
  - ~ 180 $ (oder Raubkopie übers Internet)
- FinSpy Mobile (https://www.gammagroup.com/Default.aspx)
  - Weiterleitung von Telefonaten, SMS-Mitteilungen und E-Mails, Dateien herunterladen, GPS-Ortung, Raumüberwachung über stille Telefonate
  - Android, Windows Mobile, iPhone, Blackberry, Symbian
- DaVinci (http://www.hackingteam.it/)
  - Screenshots, E-Mail, ICQ- und Skype-Kommunikation, Fernsteuerung von Mikrofon und Kamera, GPS-Ortung, Internet-Zugriffe, …
  - Android, Windows Mobile, iPhone, Blackberry, Symbian, Linux, Windows, Mac OS X
  - (Nur zur Kriminalitäts-Bekämpfung zu verwenden…)
- Weitere Anbieter
  - Elaman (http://www.elaman.de/product-portfolio.php)
  - @one IT GmbH (http://www.li-suite.com)
  - Rohde & Schwarz (http://www.rohde-schwarz.de/de/Produkte/furkueberwachungs-und-ortungstechnik/)
  - Syborg (http://www.syborg.de/)
  - …

UKD Universitätsklinikum Düsseldorf

GKD

Was wirklich motiviert…

- Mo
- Fle
- Fir
- Da
- W

…n, …

…GPS-

…d Kamera,

UKD Universitätsklinikum Düsseldorf

GKD

Was wirklich motiviert…

- Mo

DaVinci

Gute Spyware ist erschwinglich…

Und intuitiv bedienbar…

Was man von den IT-Systemen im Krankenhaus nicht unbedingt behaupten kann…

UKD Universitätsklinikum Düsseldorf

GKD

Mobile Betriebssysteme aus Unternehmenssicht

	iOS	Android	Blackberry	Windows
Sicherheit OS	+	--	+	++
Sicherheit Hardware	+	--	++	+
Management	+	--	++	++
App-Verfügbarkeit	++	++	-	+
App-Sicherheit	++	--	+	++
Infrastruktur-Anbindung	++	--	+	++

UKD Universitätsklinikum Düsseldorf

GKD

„Apps“

UKD Universitätsklinikum Düsseldorf

GKD

Apps und Sicherheit

- 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

UKD Universitätsklinikum Düsseldorf

GKD

Apps und deutsches „Tele“-Recht

- TKG gilt für 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 gilt für 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.

UKD Universitätsklinikum Düsseldorf

GKD

Apps und deutsches „Tele“-Recht

- TKG gilt für Apps
  - Voice over IP (VoIP)

Die Entwickler der Apps kennen vermutlich weder Telekommunikations- noch Telemediengesetz, wissen vielleicht nicht einmal von deren Existenz.

Wie wahrscheinlich ist es, dass die Vorgaben eingehalten wurden?

TKG: Informationspflichten, Einwilligung, Logging,…

TMG: Pseudonym, Einwilligung, Informationspflicht, Unterscheidung Nutzungs- und Bestandsdaten…

  - On-Demand- und Streaming-Dienste, sow eit es sich dabei nicht um Rundfunk handelt.

UKD Universitätsklinikum Düsseldorf

GKD

Apps und Sicherheit (Teil 2)

- 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)
- iCacti
  - unverschlüsselte Datenablage

UKD Universitätsklinikum Düsseldorf

GKD

Apps und Sicherheit: Fazit

1. Apps sind Softwareprogramme
   - Manche ebenso nützlich wie Desktop-Programme
   - Manche ebenso schädlich wie Desktop-Programme
2. Eine Sicherheitsüberprüfung, die den Namen verdient, findet in App-Stores nicht statt
3. Häufig erfolgt hier lediglich eine Prüfung mit Virenscanner(n)
4. Ach ja auch eine App kann ein Medizinprodukt sein…

Hinweise: 1) AppCheck des ZTG testet medizinische Apps (Stand August 2013 8 Apps, Webseite http://www.gesundheitsapps.info/)

2) Bayerische Landesamt für Datenschutzaufsicht veröffentlichte Hinweise zu datenschutzrechtlichen Anforderungen (Webseite http://www.lda.bayern.de/MobileApplikationen/index.html, zuletzt besucht 2013-07-06)

UKD Universitätsklinikum Düsseldorf

GKD

Speicherort der Daten

- Gesetz zum Schutz personenbezogener Daten im Gesundheitswesen (Gesundheitsdatenschutzgesetz - GDSG NRW, zuletzt geändert am 22.02.1994*)
- Gilt für Krankenhäuser (nicht Arztpraxen)
- §7 Abs. (1):
  „**Patientendaten sind grundsätzlich in der Einrichtung oder öffentlichen Stelle zu verarbeiten**“
- Mobile?

* Abgesehen von Änderungen PsychKG (1999, 2005), Anpassungen nach Änderungen SGB V (2005) Überarbeitung Krebsregistergesetz (2005)

UKD Universitätsklinikum Düsseldorf

GKD

Speicherort der Daten: die „Cloud“

Dienst	Serverstandort
1. ADrive	1. USA
2. Amazon CloudDrive	2. USA
3. Box	3. USA
4. Dropbox	4. USA
5. Google Drive	5. USA
6. iCloud	6. USA
7. SugarSync	7. USA
8. Telekom Cloud	8. Deutschland
9. Ubuntu one	9. GB
10. Windows Live / SkyDrive	10. Unbekannt (Backup in den USA)
11. Wuala	11. Schweiz, Deutschland, Frankreich

Hinweis: Cloud Computing Sicherheitsempfehlungen des BSI:
https://www.bsi.bund.de/DE/Themen/CloudComputing/Eckpunktepapier/Eckpunktepapier_node.htm
https://www.bsi.bund.de/DE/Themen/CloudComputing/Studien/Studien_node.html

UKD Universitätsklinikum Düsseldorf

GKD

Kurzer Exkurs: USA und Patriot Act

- Änderungsgesetz, das mehrere Regelungen des US Code abändert
- Sec.505 US erlaubt dem FBI und anderen Justizbehörden, selbst Anordnungen zu erlassen, ohne Zwischenschaltung eines Gerichts
- Hinsichtlich der Art der Unterlagen gibt es keine Beschränkungen
- Dem „Datenspender“ auferlegt werden über die Herausgabe der Daten Stillschweigen zu bewahren
- Amerikanische Rechtsprechung legt Patriot Act so aus, dass von amerikanischen Gesellschaften auch Daten herausverlangt werden dürfen, die sich im Ausland befinden (Sec.442(1)(a))
- Die datenschutzrechtliche Lage im betreffenden Ausland wird nicht als einer rechtlichen Herausgabemöglichkeit entgegen stehend betrachtet (Sec.442(2))
- Eine amerikanische Muttergesellschaft kann die Möglichkeit des Zugriffs auf die Unterlagen ihrer ausländischen Tochter nicht absprechen
- Eine amerikanische Tochtergesellschaft kann mittelbar gezwungen werden. Denn eine Nichtbefolgung einer FISA-Anordnung stellt einen sog. contempt of court (Missachtung des Gerichts) dar; Folge: Strafe und Bußgeld

UKD Universitätsklinikum Düsseldorf

GKD

Kurzer Exkurs: USA und Patriot Act

- Änderungsgesetz, das mehrere Regelungen des US Code abändert
- Sec.505 US erlaubt dem FBI und anderen Justizbehörden, selbst Anordnungen zu erlassen, ohne Zwischenschaltung eines Gerichts

Faktisch alle Cloud-Anbieter haben eine amerikanische Mutter oder eine amerikanische Tochter

Damit macht es für die USA keinen Unterschied, ob die Cloud in USA, Europa oder Deutschland steht

- Eine amerikanische Tochtergesellschaft kann mittelbar gezwungen werden. Denn eine Nichtbefolgung einer FISA-Anordnung stellt einen sog. contempt of court (Missachtung des Gerichts) dar; Folge: Strafe und Bußgeld

UKD Universitätsklinikum Düsseldorf

GKD

Mobiltelefone und die „Cloud“

- **Mobile Geräte**
  - Synchronisation von **Terminen, Kontakten, E-Mails, Fotos usw.**
- **iPhone, iPad, iPod**
  - Apple darf Daten zu Ihrem Konto und zu allen Geräten oder Computern, die hierunter registriert sind, erheben, nutzen, übermitteln, verarbeiten und aufbewahren
  - **Apple darf**, ohne Ihnen gegenüber zu haften, auf Ihre **Kontoinformationen** und Ihre **Inhalte zugreifen**, diese **nutzen**, aufbewahren und/oder an Strafverfolgungsbehörden, andere Behörden und/oder sonstige Dritten weitergeben darf, **wenn Apple der Meinung ist**, dass dies vernünftigerweise erforderlich oder angemessen ist, wenn dies gesetzlich vorgeschrieben ist oder wenn **Apple einen hinreichenden Grund zu der Annahme** hat, dass ein solcher Zugriff, eine solche Nutzung, Offenlegung oder Aufbewahrung **angemessenerweise notwendig ist**
  - http://www.apple.com/legal/icloud/de/terms.html bzw . http://www.apple.com/privacy/
- **Android**
  - Einstellung von Daten in Google Drive = unentgeltliches, nicht ausschließliches, weltweites und zeitlich unbegrenztes Recht die Daten zum **Zweck der Erbringung der Dienste von Google zu nutzen**
    (auch, wenn man selbst Google nicht mehr nutzt)
    → u.a. das Recht, Inhalte technisch zu vervielfältigen und Daten öffentlich zugänglich zu machen
  - https://www.google.com/intl/de/policies/terms/1

UKD Universitätsklinikum Düsseldorf

GKD

Mobiltelefone und die „Cloud“

- **Mobile Geräte**

1. Sind Sie sicher, dass in Terminen, Kontakten, Mails usw. keine personenbezogenen Daten enthalten sind?
2. Sind Sie sicher, dass keine Patientendaten (z.B. deren Namen) erwähnt werden?
3. Ist denn dann ein Vertrag über Auftragsdatenverarbeitung entsprechend §80 SGB X geschlossen worden?
4. Bei Serverstandort außerhalb EG: Auftragsdatenvereinbarung geht nicht, nur Funktionsübertragung
   → Es findet eine Übermittlung der Daten statt

zugänglich zu machen
  - https://www.google.com/intl/de/policies/terms/1

UKD Universitätsklinikum Düsseldorf

GKD

Übermittlung

- §5 Abs. (1) GDSG NRW:
  „… Als Übermittlung gilt auch die Weitergabe von Patientendaten an Personen in anderen Organisationseinheiten innerhalb der Einrichtung oder öffentlichen Stelle, sofern diese Organisationseinheiten nicht unmittelbar mit Untersuchungen, Behandlungen oder sonstigen Maßnahmen nach §2 Abs. 1 befasst sind…“

- Innere, Chirurgie, Gyn, … - Dritte im Sinne des Datenschutzes
  ➔ Sieht Ihr Rechtekonzept dies vor?
  ➔ Was heißt das für mobile (private) Geräte?

UKD Universitätsklinikum Düsseldorf

GKD

Übermittlung

Betrifft nur NRW?
In 5 Bundesländern ist der Datenaustausch zwischen Abteilungen innerhalb eines Krankenhauses geregelt:

Land	Gesetz
Bremen	BremKHDSG
Hessen	HKHG
Mecklenburg-Vorpommern	LKHG M-V
Nordrhein-Westfalen	GDSG
Saarland	SKHG

UKD Universitätsklinikum Düsseldorf

GKD

Folgen einer Übermittlung

1. Der Patient muss zustimmen
2. Änderung Behandlungsvertrag, z.B.:

   „Hiermit entbinde ich meine behandelnden Ärzte von ihrer Schweigepflicht und stimme zu, dass das Krankenhaus bei Bedarf beliebige meiner Daten an vom Krankenhaus ausgesuchte Mitarbeiter an deren private Geräte übermittelt…“

UKD Universitätsklinikum Düsseldorf

GKD

Folgen einer Übermittlung

1. Schwierig dem Patienten zu verkaufen
2. Rechtlich unwirksam: Patient muss informiert einwilligen
   → genaue Aufklärung welche Daten übermittelt werden
3. Unbrauchbare Lösung
   (Neudeutsch „Bullshit“)

UKD Universitätsklinikum Düsseldorf

GKD

BYOD

- Krankenhaus wird einerseits Mitarbeitern die Nutzung privater Geräte langfristig nicht verweigern können
- Aber: Auf dem Mitarbeiter gehörende Geräte hat der Arbeitgeber keine Weisungsbefugnis
  - ➔ Auf diesen Geräten gespeicherte Patientendaten befinden sich daher prinzipiell nicht in der Einrichtung
  - ➔ Die Patientendaten wurden übermittelt
- Erster Anhalt, wie das Unternehmen bzgl. BYOD-Einführung dasteht, durch IBM BYOD Check: http://www.challenge-check.ch/byod/

UKD Universitätsklinikum Düsseldorf

GKD

BYOD: rechtliche Anmerkungen

Was man neben Datenschutz noch so beachten sollte:

- Arbeitsrecht
- Urheberrecht
- Lizenzrecht
- Compliance / Unternehmenssicherheit
- Strafrecht
- Steuerrecht
- Haftungsrecht
- Vertragsrecht
- Geheimnisschutz
- Betriebliche Nutzung privater Accounts

UKD Universitätsklinikum Düsseldorf

GKD

BYOD: rechtliche Anmerkungen

Bring

Your

Own

Desaster…?

UKD Universitätsklinikum Düsseldorf

GKD

Was tun…?

- Cloud: nicht fragen „wo?“, sondern „Brauche ich wirklich eine Cloud?“ → Kosten-Nutzen-Analyse
- Daten des Krankenhauses werden auf externen Speicherorten oder mobilen Geräten nur verschlüsselt abgelegt
  - Bei krankenhaus-eigenen Geräten wie Laptops am besten alle Speichermedien vollständig verschlüsseln (z.B. Pre-Boot)
  - Bei Geräten des Mitarbeiters mit vom Krankenhaus kontrollierten Krypto-Containern arbeiten, die bei Bedarf vom KH gelöscht werden können
- Richtlinie für mobile Geräte erstellen
  (Richtlinie für Computer-Einsatz im Krankenhaus existiert ja sicherlich schon…;-))
- Entsprechende Management-Software einsetzen
- Betriebsvereinbarung BYOD
  (Bei BYOD zusätzlich an Individualvereinbarung mit jedem einzelnen Mitarbeiter denken)

UKD Universitätsklinikum Düsseldorf

GKD

Richtlinie mobile Geräte

- Generelle Sicherheitsmaßnahmen wie Authentifizierung usw.
- Geräteverlust und unautorisierter Zugriff auf das Gerät
  - Vorbeugende Maßnahmen wie Verschlüsselung
  - Rückwirkende Maßnahmen wie Löschmechanismen
- Datenverlust
  - Vorbeugende Maßnahmen wie Backups
  - Rückwirkende Maßnahmen wie Data Recovery
- Defekte Geräte
  - Vor Einschicken Daten löschen
- Datenübertragung und Angriff auf die Funkschnittstelle berücksichtigen
  - VPN
- Entsorgung

UKD Universitätsklinikum Düsseldorf

GKD

Mobile Device Management (MDM) Software

Anforderungen:

- Kompatibel zu allen gängigen Mobile Plattformen und Anwendungen
- Arbeitet in allen gängigen Mobilfunknetzen
- Kann direkt „over the air“ (OTA) implementiert werden unter Auswahl bestimmter Zielgeräte
- Hardware, Betriebssysteme, Konfiguration und Anwendungen können schnell und problemlos ausgeliefert werden
- Mobile Geräte können nach Bedarf von Administratoren dem System hinzugefügt oder daraus entfernt werden
- Die Integrität und Sicherheit der IT-Infrastruktur ist stets gewährleistet
- Security Policies werden konsequent durchgesetzt
- Der Anwender bekommt von der Existenz der Lösung so wenig wie möglich oder nötig mit

UKD Universitätsklinikum Düsseldorf

GKD

Mobile Device Management (MDM) Software

Anforderungen:

- Kompatibel zu allen gängigen Mobile Plattformen und Anwendungen

Die ideale
Mobile-Device-Management-Lösung
ist eine „eierlegende Wollmilchsau“
-
Diese Lösung gibt es nicht

- Der Anwender bekommt von der Existenz der Lösung so wenig wie möglich oder nötig mit

UKD Universitätsklinikum Düsseldorf

GKD

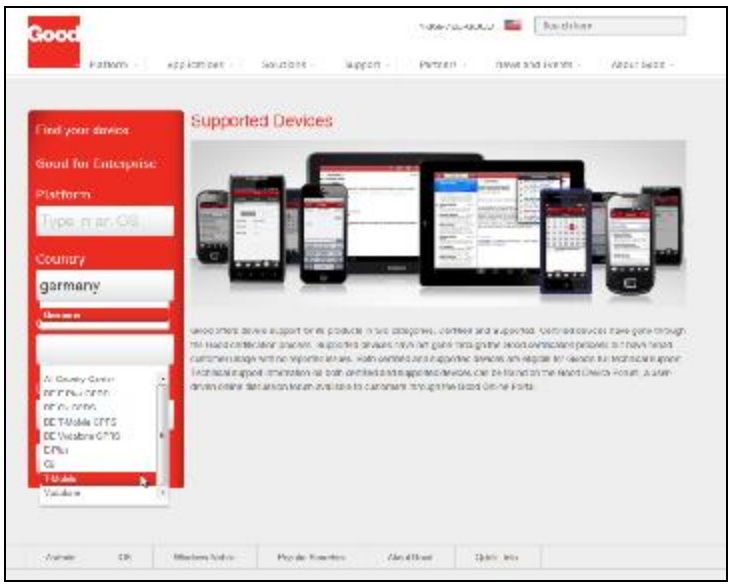
Management Software

Auswahlkriterien

- Unterstütze (mobile) OS
  - Android
  - Blackberry
  - iOS
  - Symbian
  - Windows
  - …
- Security-Features
  - App-Installation (White-List, Black-List, …)
  - Authentifizierung-/Authorisierungs-Management
  - Jailbreak-Erkennung, rooten, …
  - Passwort (Zusammensetzung, Wechsel, …)
  - Remote Control
  - Remote-Wipe
  - Verschlüsselung (PIM-Container, Container für betriebliche Daten)
  - VPN-Konfiguration (Installation, Wartung, …)
  - …
- Systemintegration
  - AD/LDAP-Integration
  - App-Management
  - …

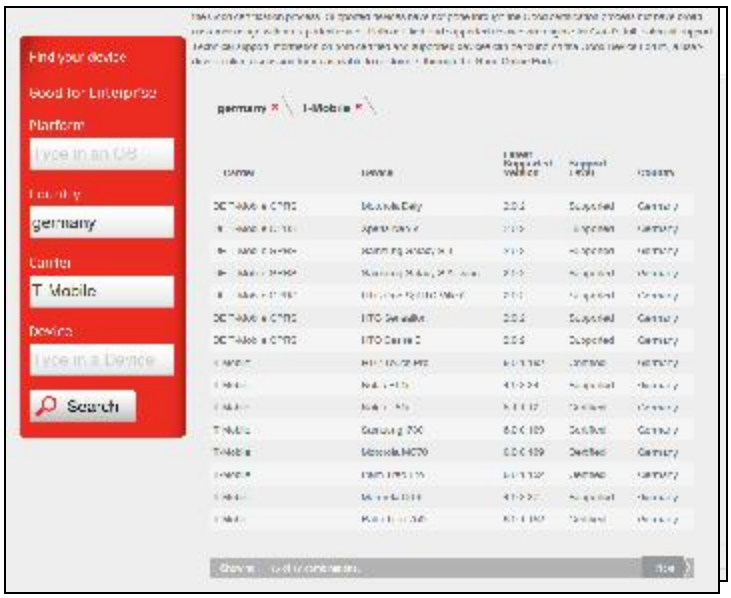
UKD Universitätsklinikum Düsseldorf

GKD



UKD Universitätsklinikum Düsseldorf

GKD



UKD Universitätsklinikum Düsseldorf

GKD

Telekom, Vodafone, O2 und E-Plus bieten zusammen etwa

- 180 mobile Endgeräte an
- Mit (theoretisch) 3 Betriebssystemen
- Faktisch aber etwa 30 unterschiedliche OS
- Wer alle unterstützen will, …

UKD Universitätsklinikum Düsseldorf

GKD

Management Software

- Eigene Anforderungen mit Anbieter abgleichen
- Anbieter (Auswahl ohne Anspruch auf Vollständigkeit):
  - 7P Group (7P MDM)
    http://www.7p-group.com/portfolio/leistungen/effizienz-durch-mobilitaet/
  - MobileIron
    http://smartling.mobileiron.com/en/germany
  - Sophos (smartMan)
    http://www.dialogs.de/de_DE/produkte/smartman.html
  - Sybase (Afaria)
    http://www.sybase.de/mobilize
  - Symantec (Endpoint Protection, Mobile Management, Access Control, SafeGuard Easy)
    http://www.symantec.com/de/de/theme.jsp?themeid=sep-family
    http://www.symantec.com/de/de/mobile-management
    http://www.symantec.com/de/de/network-access-protection
    http://www.symantec.com/business/support/index?page=content&id=TECH30951
  - T-Systems (SiMKO)
    http://www.t-systems.de/tsip/de/754852/start/branchen/oeffentlicher-sektor/aeussere-innere-sicherheit/aeussere-innere-sicherheit
  - Thinking Objects (Auralis)
    http://www.to.com/auralis.988.0.html
  - Ubitexx (ubi-Suite)
    http://www.ubitexx.com/language/de-de/products/multiplatform_management

UKD Universitätsklinikum Düsseldorf

GKD

Management Software

- Eigene Anforderungen mit Anbieter abgleichen
- Anbieter (Auswahl ohne Anspruch auf Vollständigkeit):
  - 7P Group (7P MDM)
    http://www.7p-group.com/portfolio/leistungen/effizienz-durch-mobilitaet/
  - MobileIron
    http://smartling.mobileiron.com/en/germany
  - Sophos (smartMan)

Lizenzkosten: 30 bis 100 Euro / Client

Beispiel: Klinikum mit 1000 Clients
= 30.000 bis 100.000 Euro

  - T-Systems (SiMKO)
    http://www.t-systems.de/tsip/de/754852/start/branchen/oeffentlicher-sektor/aeussere-innere-sicherheit/aeussere-innere-sicherheit
  - Thinking Objects (Auralis)
    http://www.to.com/auralis.988.0.html
  - Ubitexx (ubi-Suite)
    http://www.ubitexx.com/language/de-de/products/multiplatform_management

UKD Universitätsklinikum Düsseldorf

GKD

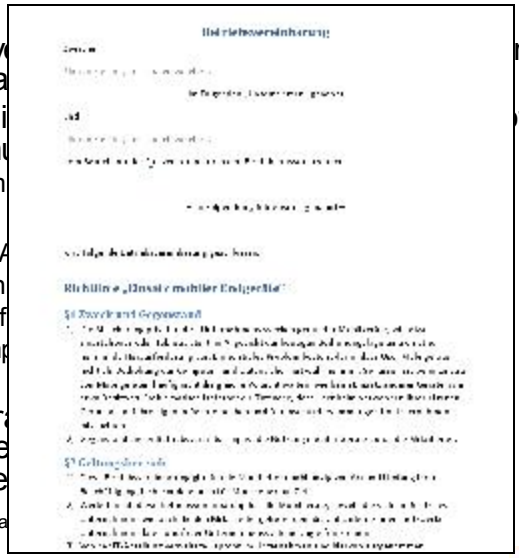
Betriebsvereinbarung

- Individualvereinbarung mit einzelnen Benutzern nicht realisierbar
- Je nach eingesetzter Managementsoftware potentielle Überwachungsmöglichkeit
  → Zustimmungspflichtig Betriebsrat/Personalrat
- Inhalt
  - Welche Apps?
  - Diebstahlsicherung / Vorgehen bei Verlust
  - Was darf wo gespeichert werden?
  - Antivirenprogramm
  - …
- Cave: Voraussetzungen beachten, damit Betriebsvereinbarung datenschutzrechtlich als vorrangige Rechtsvorschrift gilt
  (Hinweise hierzu unter http://www.datenschutz-hamburg.de/uploads/media/22._Taetigkeitsbericht_2008-2009.pdf)

UKD Universitätsklinikum Düsseldorf

GKD

Betriebsvereinbarung



Mobile Security und BSI: Das Grundschutz-Handbuch

- 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
- …

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

UKD Universitätsklinikum Düsseldorf

GKD

Mobile Security

1. IT-Sicherheitsmanagement ist
   IT-Sicherheitsmanagement ist
   IT-Sicherheitsmanagement …
   Business as usual:
   - Sicherheitsrichtlinie
   - Klassifzierungsrichtlinie
   - Richtlinie IT-Risikomanagement
   - Systemrichtlinien
   - …
2. Einzige Besonderheit: die Daten „wandern“
3. Beachtenswertes für „unser“ Krankenhaus

UKD Universitätsklinikum Düsseldorf

GKD

Fazit

- Einsatz mobiler Geräte im Krankenhaus auch Abseits der mobilen Visite sinnvoll
- Kosten sind nicht vernachlässigbar
  - Neben Anschaffungskosten bleiben
  - Lizenzkosten für Managementsoftware
  - Menschen, die
    - Software bedienen
    - Geräte einrichten
    - Anwender schulen
    - …
- (GDSG NRW könnte nach 18 Jahren langsam den Anforderungen der heutigen Krankenhaus-Welt angepasst werden)

UKD Universitätsklinikum Düsseldorf

GKD

Literatur (Auswahl)

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

UKD Universitätsklinikum Düsseldorf

GKD

Literatur (Auswahl)

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

UKD Universitätsklinikum Düsseldorf

GKD

Literatur (Auswahl)

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_cbud.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
- Hasibeck, 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 – Datenschutz und 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

UKD Universitätsklinikum Düsseldorf

GKD

Literatur (Auswahl)

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
- Schmidt-Bens J. Cloud Computing Technologien und Datenschutz. OIWIR Verlag für Wirtschaft, Informatik und Recht. ISBN 3939704717
- 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

UKD Universitätsklinikum Düsseldorf

GKD

Diskussion

schuetze@medizin-informatik.org

UKD Universitätsklinikum Düsseldorf

GKD