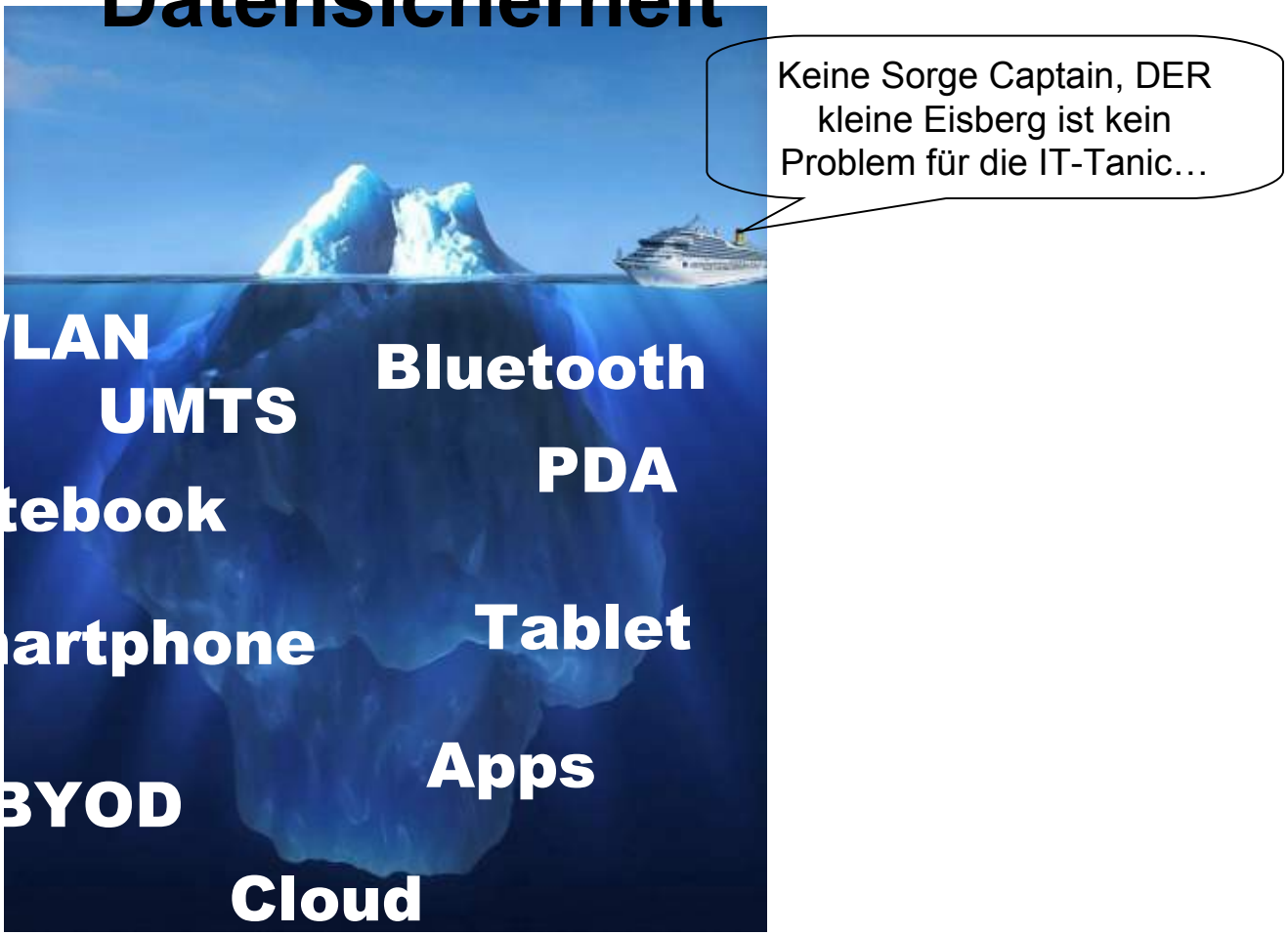
UKD Universitätsklinikum Düsseldorf

GKD Gesellschaft für klinische Dienstleistungen Düsseldorf mbH

Mobile Devices im Krankenhaus – Aspekte von Datenschutz und Datensicherheit



Zu meiner Person

- Ausbildung
  - Studium Informatik
    (FH-Dortmund)
  - Studium Humanmedizin
    (Uni Düsseldorf / Uni Witten/Herdecke)
  - Studium Jura
    (Fern-Uni Hagen)
  - Zusatzausbildung Datenschutzbeauftragter
    (Ulmer Akademie für Datenschutz und IT-Sicherheit)
  - Zusatzausbildung Datenschutz-Auditor
    (TüV Rheinland)
  - Zusatzausbildung Medizin-Produkte-Integrator
    (VDE Prüf- und Zertifizierungsinstitut)
- Berufserfahrung
  - 12 Jahre klinische Erfahrung
  - 20 Jahre IT im Krankenhäusern
  - 18 Jahre Datenschutz im Gesundheitswesen
- Mitarbeit in Verbänden
  - GMDS
  - Berufsverband Medizinischer Informatiker e.V. (BVMI)
  - Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (BvD)
  - Gesellschaft für Datenschutz und Datensicherung e.V. (GDD)
  - HL7 Deutschland e.V.
  - Fachverband Biomedizinische Technik e.V. (fbmt)

Motivation…

- 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/funkueberwachungs-und-ortungstechnik/)
  - Syborg (http://www.syborg.de/)
  - …

Motivation…

- M
  - –
  - –
- Fle
  - –
  - –
  - –
  - –
- Fir
  - –
  - –
- Da
  - –
  - –
  - –
- W
  - –
  - –
  - –
  - –
  - –
  - –

DaVinci

…en, …

…, GPS-

…nd Kamera,

Motivation…

- M

Gute Spyware ist erschwinglich…

Und intuitiv bedienbar…

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

Mobile Security

1. IT-Sicherheitsmanagement ist
   IT-Sicherheitsmanagement ist
   IT-Sicherheitsmanagement …
   Business as usual:
   - Sicherheitsrichtlinie
   - Klassifzierungsrichtlinie
   - Richtlinie IT-Risikomanagement
   - Systemrichtlinien
   - …

1. Einzige Besonderheit: die Daten „wandern“
2. Beachtenswertes für „unser“ Krankenhaus

Mobile Betriebssysteme aus Unternehmenssicht

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

„Apps“

Technology Review

Forum Archiv Heft bestellen

Energie Infotech Leben Materie Pro

Technology Review > Infotech > Undichte Apps

Undichte Apps

11.08.10 – **Robert Lemos**

Schlagwörter: iPhone, Datenschutz, Android, Sicherheitslücke, Apple, Lookout, App Genome Project, Google

Zahlreiche Smartphone-Anwendungen sammeln sensible Daten und leiten diese weiter – manchmal sogar ohne das Wissen ihrer Programmierer.

Eine Untersuchung von Programmen für die Plattformen iPhone und Android hat ergeben, dass erstaunlich viele Apps ohne Wissen ihrer Nutzer Daten sammeln und diese potenziell ins Internet übertragen können.

Quelle: Stiftung Warentest, 6/2012

„Apps“

NDR.de Das Beste am Norden

HOME | REGIONAL | SPORT | RATGEBER | UNTERHALTUNG | KULTUR | GESCHICHTE | FERNSEHEN

KOCHEN | REISE | GARTEN | GESUNDHEIT | NETZWELT | VERBRAUCHER

- Datenschutz & Sicherheit
- Digitales für Einsteiger
- Internet-Stadt Hamburg
- Frühling der Piraten
- CeBIT

NETZWELT IN RADIO UND TV

NDR Fernsehen

Sendedatum: 22.05.2012 23:20 Uhr

Medien-Apps: Programme spähen Nutzer aus

Mal eben schauen wie das Wetter wird, wo der Weg lang führt oder was in der Welt passiert - für fast alles gibt es heutzutage sogenannte Apps. Kleine kompakte Programme für Smartphone oder Tablet PCs. Weltweit wurden bereits Milliarden heruntergeladen. Doch was so harmlos wirkt, ist es oft nicht - im Gegenteil. ZAPP hat etwa 100 iPhone- und iPad-Apps von unabhängigen Experten untersuchen lassen und dabei feststellen müssen: Viele Apps, darunter auch solche von öffentlich-rechtlichen Radios, Privatsendern und Verlagen, geben unbemerkt Daten ihrer Nutzer an Dritte weiter.

Nutzer Daten sammeln und diese potenziell ins Internet übertragen können.

Quelle: Stiftung Warentest, 6/2012

„Apps“

NDR.de Das Beste am Norden

HOME REGIONAL SPORT RATGEBER UNTERHALTUNG KULTUR GESCHICHTE FERNSEHEN

Macwelt iPhoneWelt iPadWelt

News Tests Tipps iPhoneWelt iPadWelt Forum Premium Specials

macwelt.de > iPhoneWelt > News

iPhoneWelt Das unabhängige Webportal der Zeitschrift

Von Thomas Hartmann - 02.02.2011, 15:52

Empfehlen 0 Twittern 0 +1 0

Datenschutz

TU Wien bestätigt: iPhone-Apps spionieren Nutzer aus

Ein Forscher an der TU Wien hat laut IT-Magazin Futurezone herausgefunden, dass 55 Prozent von insgesamt 1407 untersuchten iPhone-Apps die jeweilige Gerätenummer an App-Entwickler oder Werbefirmen übermitteln. Dies entspricht Ergebnissen anderer Studien.

„Apps“

test

Ausgespäht

Datenschutz bei Apps Viele Apps übertragen persönliche Informationen der Smartphone-Besitzer an Datensammler – manche sogar unverschlüsselt. Für den Service, den diese Apps bieten, zahlen Nutzer mit ihrer Privatsphäre.

So sind wir vorgegangen

Im Test: 63 exemplarisch ausgesuchte Zusatzprogramme „Apps“ für die Smartphone-Betriebssysteme Android, iOS oder Windows Phone. Acht dieser Apps wurden im Test Navigationssysteme auch auf ihre Navigationsfunktion geprüft (siehe Tabelle Seite 46/47). Geprüft auf Samsung Galaxy Nexus (Android 4.0.2), Apple iPhone 4S (iOS 5.0.1) oder Nokia Lumia 800 (Windows Phone 7.5).

Erhebungszeitraum: Februar bis April 2012.

METHODIK

Ziel war es, herauszufinden, in welchem Umfang Apps Daten über Nutzer und Nutzerverhalten (wie Start und Bedienen der Apps, Standort, gespeicherte Kontakte) und über das Smartphone (wie die Gerätekennung) an welche Serveradressen senden. Wir verbanden die Smartphones in den Standardeinstellungen über einen als WLan-Zugangspunkt eingerichteten Rechner mit dem Internet. Mit diesem Rechner konnte der Datenverkehr protokolliert, gegebenenfalls entschlüsselt (SSL) und analysiert werden. Datenschutzerklärungen wurden nicht untersucht.

DARSTELLUNG

Apps, die persönliche Daten wie Telefonnummern oder Namen nicht anonymisieren, oder Apps, die Passwörter unverschlüsselt übertragen, stufen wir als sehr kritisch ein. Apps, die für den Betrieb nicht notwendige Daten wie Benutzungsstatistik übertragen, stufen wir als kritisch ein. Unkritisch sind Apps, die keine oder höchstens die für ihre Funktion erforderlichen Daten übertragen.

Interview

„Sie beobachten uns“

Nur 26 der 63 geprüften Apps sind verschwiegen, 9 geben sogar sehr persönliche Daten ihrer Nutzer weiter. Dr. Alexander Dix, Berliner Beauftragter für Datenschutz, rät zum Umdenken.

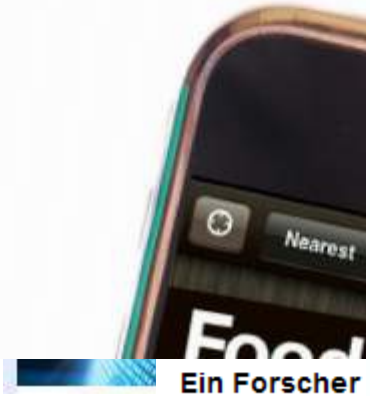
Ein Forscher an der TU Wien hat laut … Prozent von insgesamt 1407 untersuc… App-Entwickler oder Werbefirmen übermitteln. Dies entspricht Ergebnissen anderer Studien.

„Apps“

test

Ausges

Datenschutz bei Apps Viele A
Informationen der Smartphon
manche sogar unverschlüsselt
Apps bieten, zahlen Nutzer mit



Ein Forscher
Prozent von i
App-Entwickl
Studien.

Wirtschafts Woche

3

Vererben und erben Regeln fürs Testament

Falsche Freunde

88 Smartphone-Apps im Sicherheits-Check:
die fiesen Tricks der populärsten Helferlein

ngen

senden. Wir verbanden die Smartphones in den Standardeinstellungen über einen als WLan-Zugangspunkt eingerichteten Rechner mit dem Internet. Mit diesem Rechner konnte der Datenverkehr protokolliert, gegebenenfalls entschlüsselt (SSL) und analysiert werden. Datenschutzerklärungen wurden nicht untersucht.

DARSTELLUNG

Apps, die persönliche Daten wie Telefonnummern oder Namen nicht anonymisieren, oder Apps, die Passwörter unverschlüsselt übertragen, stufen wir als sehr kritisch ein. Apps, die für den Betrieb nicht notwendige Daten wie Benutzungsstatistik übertragen, stufen wir als kritisch ein. Unkritisch sind Apps, die keine oder höchstens die für ihre Funktion erforderlichen Daten übertragen.

schwie-
aten ihrer
er Beauf-
nken.

ssen anderer

UKD Universitätsklinikum Düsseldorf

GKD Gesellschaft für klinische Dienstleistungen Düsseldorf mbH

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

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 Werbung: Beispiele

- Sixt Autovermietung
  - Übertragen geräteeindeutiger Identifikationsmerkmale an verschiedene Werbenetzwerke
- N24
  - Übertragung eindeutiger Gerätedaten an verschiedene Banner-Netzwerke
  - Datenübertragung an Google Analytics
- Handelsblatt
  - Übertragung eindeutiger Gerätedaten an verschiedene Banner-Netzwerke
- …

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)
- iCacti
  - unverschlüsselte Datenablage

Apps und deutsches 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.

Apps und deutsches Recht

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…

Ach ja: und medizinische Apps können ein Medizinprodukt darstellen -> Betreiberverordnung, Risikomanagement…

Apps: Fazit aus Sicht Datenschutz/Datensicherheit

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

Hinweise: 1) AppCheck des ZTG testet medizinische Apps
(Stand Juli 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)

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

Kurzer Exkurs: USA und Patriot Act

- Änderungsgesetz, das mehrere Regelungen des US Code abändert
- Sec. 215 US Patriot Act ändert „Foreign Intelligence Surveillance Act“ (FISA)
- FISA erlaubt Sicherheitsbehörden beim sog. FSI Court eine Anordnung zu beantragen, die eine Person dazu verpflichtet, die bei ihr befindlichen Geschäftsunterlagen herauszugeben
- Patriot Act ermöglicht nun Unterlagen von jeder beliebigen Stelle und bereits unter der Voraussetzung, dass sie mit einer Untersuchung von Terrorismus und Spionage in Verbindung stehen, zu erhalten
- Hinsichtlich der Art der Unterlagen gibt es keine Beschränkungen
- Sec.505 US erlaubt dem FBI und anderen Justizbehörden, selbst Anordnungen zu erlassen, ohne Zwischenschaltung eines Gerichts
- In Zusammenhang mit FISA kann dem „Datenspender“ auferlegt werden über die Herausgabe der Daten Stillschweigen zu bewahren

Patriot Act und Europa

- 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))
- Steht das Recht des außeramerikanischen Staates der Herausgabe entgegen („blocking statute"), so findet vor dem Erlass einer Herausgabeanordnung eine Abwägung statt (Sec.442(1)(c))
- In Fällen, in welchen eine Anordnung nach US Patriot Act im Raum steht (Terrorismus, Spionage), dürften die Interessen der USA verstärkt gewichtet und eine Herausgabe als unumgänglich angesehen werden
- 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

Speicherort der Daten: 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

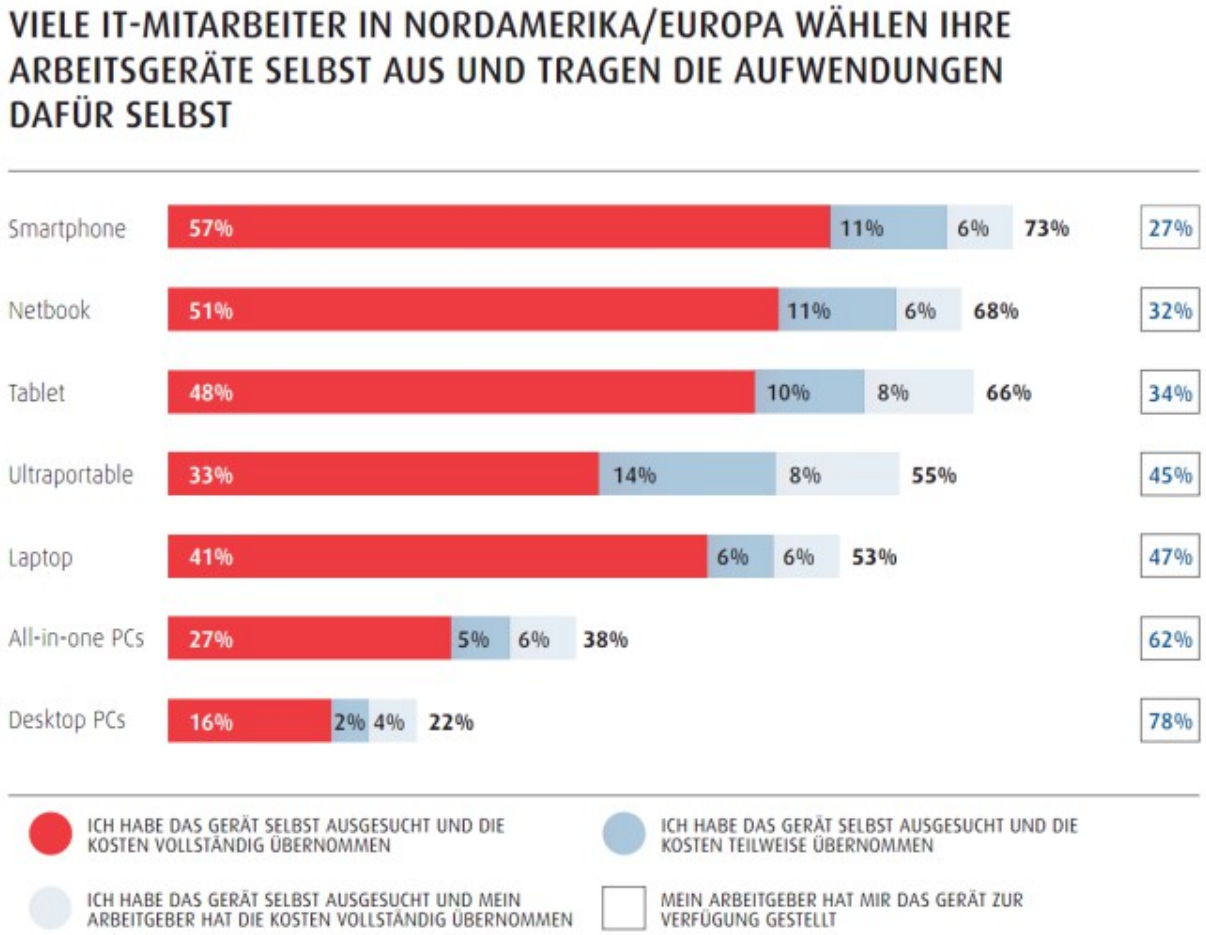
Speicherort der Daten: die „Cloud“

- **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 EWR:
   Auftragsdatenvereinbarung geht nicht, nur Funktionsübertragung
   → Es findet eine Übermittlung der Daten statt

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

BYOD



Befragte: IT-Mitarbeiter in Nordamerika und Europa
Quelle: Forrsights Workforce Employee Survey, 4. Quartal 2011

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/

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…“

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“)

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

Beispiele aufzeigen

BYOD: rechtliche Anmerkungen

Bring

Your

Own

Desaster…?

Beispiele aufzeigen

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)

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

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

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

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
  - …

the Good certification process. Supported devices have not gone through the Good certification process but have broad customer usage with no reported issues. Both certified and supported devices are eligible for Good's full technical support. Technical support information on both certified and supported devices can be found on the Good Device Forum, a user-driven online discussion forum available to customers through the Good Online Portal.

Find your device

Good for Enterprise

Platform

Type in an OS

Country

germany

Carrier

T-Mobile

Device

Type in a Device

Search

germany × \ T-Mobile × \

Carrier	Device	Latest Supported Version	Support Level	Country
DE T-Mobile GPRS	Motorola Defy	2.0.2	Supported	Germany
DE T-Mobile GPRS	Xperia Neo V	2.0.2	Supported	Germany
DE T-Mobile GPRS	Samsung Galaxy S II	2.0.2	Supported	Germany
DE T-Mobile GPRS	Samsung Galaxy S Advance	2.0.2	Supported	Germany
DE T-Mobile GPRS	HTC One S; HTC Ville C	2.0.2	Supported	Germany
DE T-Mobile GPRS	HTC Sensation	2.0.2	Supported	Germany
DE T-Mobile GPRS	HTC Desire S	2.0.2	Supported	Germany
T-Mobile	HTC Touch Pro	6.0.1.152	Certified	Germany
T-Mobile	Nokia E61i	4.9.3.34	Supported	Germany
T-Mobile	Nokia E61i	5.1.1.12	Certified	Germany
T-Mobile	Samsung i780	6.0.0.109	Certified	Germany
T-Mobile	Motorola MC70	6.0.0.109	Certified	Germany
T-Mobile	Palm Treo Pro	6.0.1.152	Certified	Germany
T-Mobile	Motorola Q 9h	4.9.3.37	Supported	Germany
T-Mobile	Palm Treo 750	6.0.1.152	Certified	Germany

Showing 1 - 15 of 17 combinations. Next

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

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

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

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)

Betriebsvereinbarung

- Individualv … n nicht realisierba
- Je nach ei … tentielle Überwachu
  → Zustimm
- Inhalt
  - Welche A
  - Diebstah
  - Was darf
  - Antiviren
  - …
- Cave: Vora … Betriebsve … vorrangige … (Hinweise hierzu … hamburg.de/uploa

Betriebsvereinbarung

Zwischen

Klicken Sie hier, um Text einzugeben.

– im Folgenden „Unternehmen" genannt –

und

Klicken Sie hier, um Text einzugeben.

dem Betriebsrat der Fa., vertreten durch den Betriebsratsvorsitzenden

– im Folgenden „Betriebsrat" genannt –

wird folgende Betriebsvereinbarung geschlossen:

Richtlinie „Einsatz mobiler Endgeräte"

§1 Zweck und Gegenstand

(1) Die Absicherung privat und zu Unternehmenszwecken genutzter Mobilgeräte, wie etwa Smartphones oder Tablets, stellt im Angesicht der heutigen Bedrohungslage eine ernst zu nehmende Herausforderung dar. Ein zentrales Problem besteht darin, dass User Mobilgeräte nicht als Bedrohung der Computer- und Datensicherheit wahrnehmen. So lassen sie beim Einsatz von Mobilgeräten häufig nicht die gleiche Vorsicht walten, wie beim Einsatz anderer Geräte, wie etwa Desktops. Problematisch ist ferner die Tatsache, dass User beim Verwenden ihrer eigenen Geräte oft auf ihre eigenen Rechte pochen und Datenschutzbestimmungen im Unternehmen missachten.

(2) Gegenstand dieser Betriebsvereinbarung ist die Nutzung mobiler Geräte durch die Mitarbeiter.

§2 Geltungsbereich

(1) Diese Betriebsvereinbarung gilt für alle Mitarbeiter unabhängig von Art und Umfang ihrer Beschäftigung, insbesondere auch für Mitarbeiter auf Zeit.

(2) Weiterhin gilt diese Betriebsvereinbarung für alle Mobilgeräte, sowohl die sich im Besitz des Unternehmens wie auch die den Mitarbeiter gehörenden, die auf Unternehmensnetzwerke, Unternehmensdaten und/oder Unternehmenssysteme zugreifen können.

(3) Von der IT-Abteilung verwaltete Laptops im Unternehmen sind hiervon ausgenommen.

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
    - …

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
- Herrnleben 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)

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)

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 – 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

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

Diskussion

schuetze@medizin-informatik.org

BYOD: rechtliche Anmerkungen

- Arbeitsrecht:
  - Ergänzungen zum Arbeitsvertrag müssen mindestens den Anforderungen an AGB entsprechen (→ §§ 305ff. BGB beachten)
  - Werktägliche Arbeitszeit ist begrenzt (§3 ArbZG), Ruhezeit von mindestens 11 Stunden vorgeschrieben (§5 ArbZG)
  - Kontrollmöglichkeit des Arbeitgebers bei privater Hardware entfällt
    ("Computer-Grundrecht", BVerfG 27.02.2008)
  - TKG/TMG: Diensteanbieter -> begrenzter Zugriff auf Protokolldaten usw.
  - Kein Zugriff auf dienstl. E-Mails
  - …
- Urheberrecht/Lizenzrecht:
  - Installation von Software des Unternehmens auf privater Hardware vs. Urheberrecht
    (Evtl. Hinweis des Herstellers „Nutzung nur auf Rechnern, die im Eigentum des Lizenznehmers stehen"?)
  - §99 UrhG: „Ist in einem Unternehmen von einem Arbeitnehmer oder Beauftragten ein nach diesem Gesetz geschütztes Recht widerrechtlich verletzt worden, hat der Verletzte die Ansprüche aus § 97 Abs. 1 und § 98 auch gegen den Inhaber des Unternehmens"

BYOD: rechtliche Anmerkungen

- Compliance / Unternehmenssicherheit:
  - Compliance := Auftraggeber hat insbesondere sicherzustellen, dass die
    - Integrität,
    - Vertraulichkeit,
    - Verfügbarkeit und
    - Zurechenbarkeit

    von Daten des Unternehmens bei unternehmenskritischen Prozessen und Anwendungen jederzeit sichergestellt ist.
  - Arbeitgeber ist bei BYOD Auftragnehmer…
- Strafrecht:
  - Neben TKG, TMG und Datenschutz ist §202 a-c StGB zu betrachten
  - §202a StGB: Ausspähen von Daten
    - Keine Straftat, wenn private Daten beim Einsatz von BYOD nicht gesondert gesichert sind
  - §202b StGB: Abfangen von Daten
    - Keine Straftat, wenn Übermittlung über Unternehmenskommunikationsnetz erfolgt
  - §202c StGB: Vorbereiten des Ausspähens und Abfangens von Daten
    - Keine Straftat, wenn der Täter nicht eine eigene oder fremde Straftat nach §202 a oder §202b StGB unterstützen will

BYOD: rechtliche Anmerkungen

- Steuerrecht
  - Vergütungsanspruch des Mitarbeiters für die betriebliche Nutzung?
  - Geldwerter Vorteil
- Haftungsrecht
  - Verlust/Beschädigung Smartphone während Arbeit (§670 BGB analog)
  - Datenveränderung (§303a StGB), z.B. private Daten und Virenschutz des Krankenhauses
- Vertragsrecht
  - Vertragspartner für Wartung/Reparatur des Gerätes
  - Verantwortlich für Updates?
- Geheimnisschutz
  - Schutz von Betriebs- und Geschäftsgeheimnisse (§§ 17, 18 UWG)
  - Verletzung von Privatgeheimnissen (§203 StGB)
- Betriebliche Nutzung privater Accounts
  - Social Network: wem gehört der Account?

Zurück