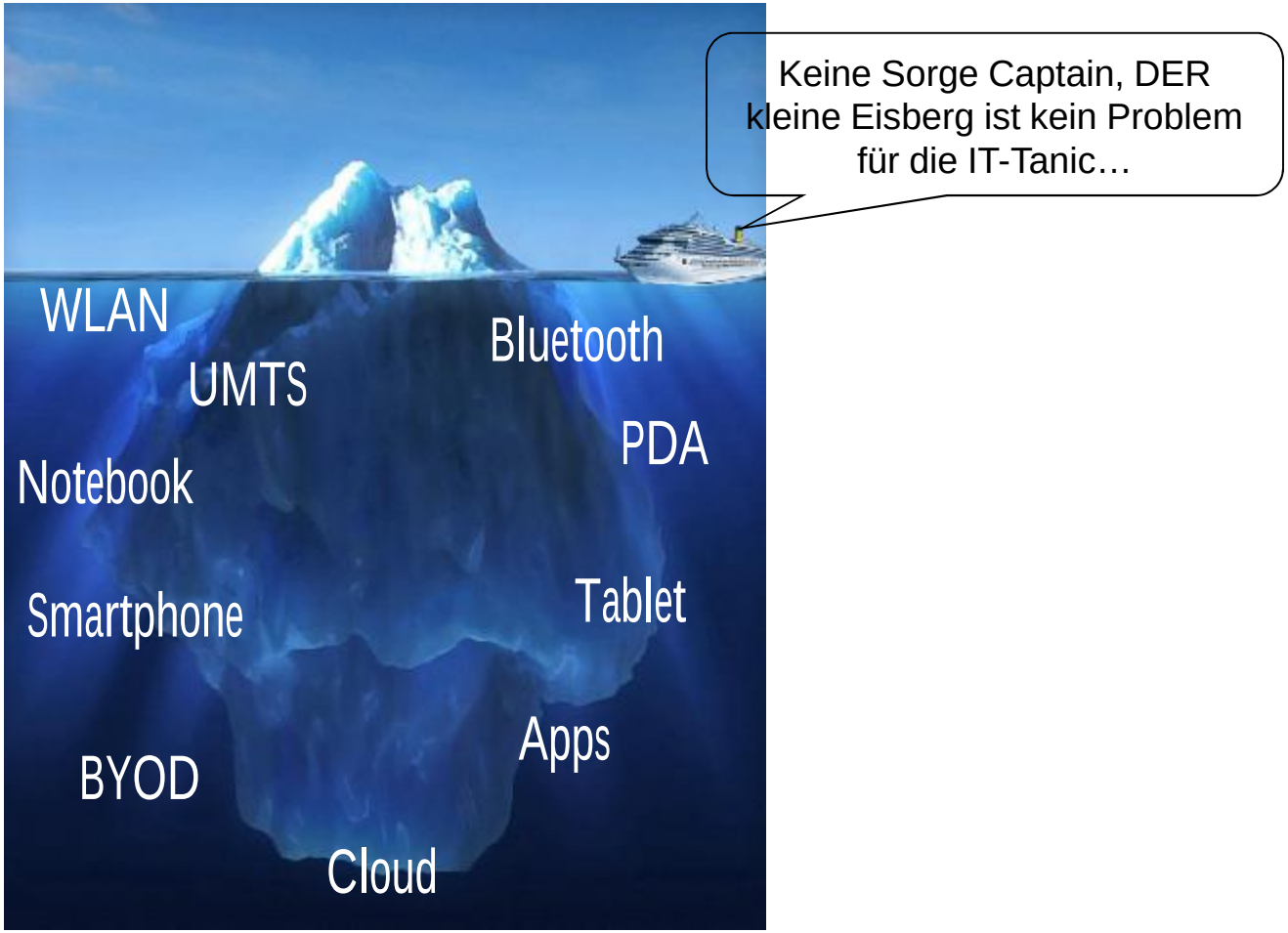
Mobile Devices im Krankenhaus –
Aspekte von Datenschutz und Datensicherheit



Datenschutz/-sicherheit: warum eigentlich…?

- 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/)
  - …

Datenschutz/-sicherheit: warum eigentlich…?

- M
- Fl
- Fi
- Da
- W

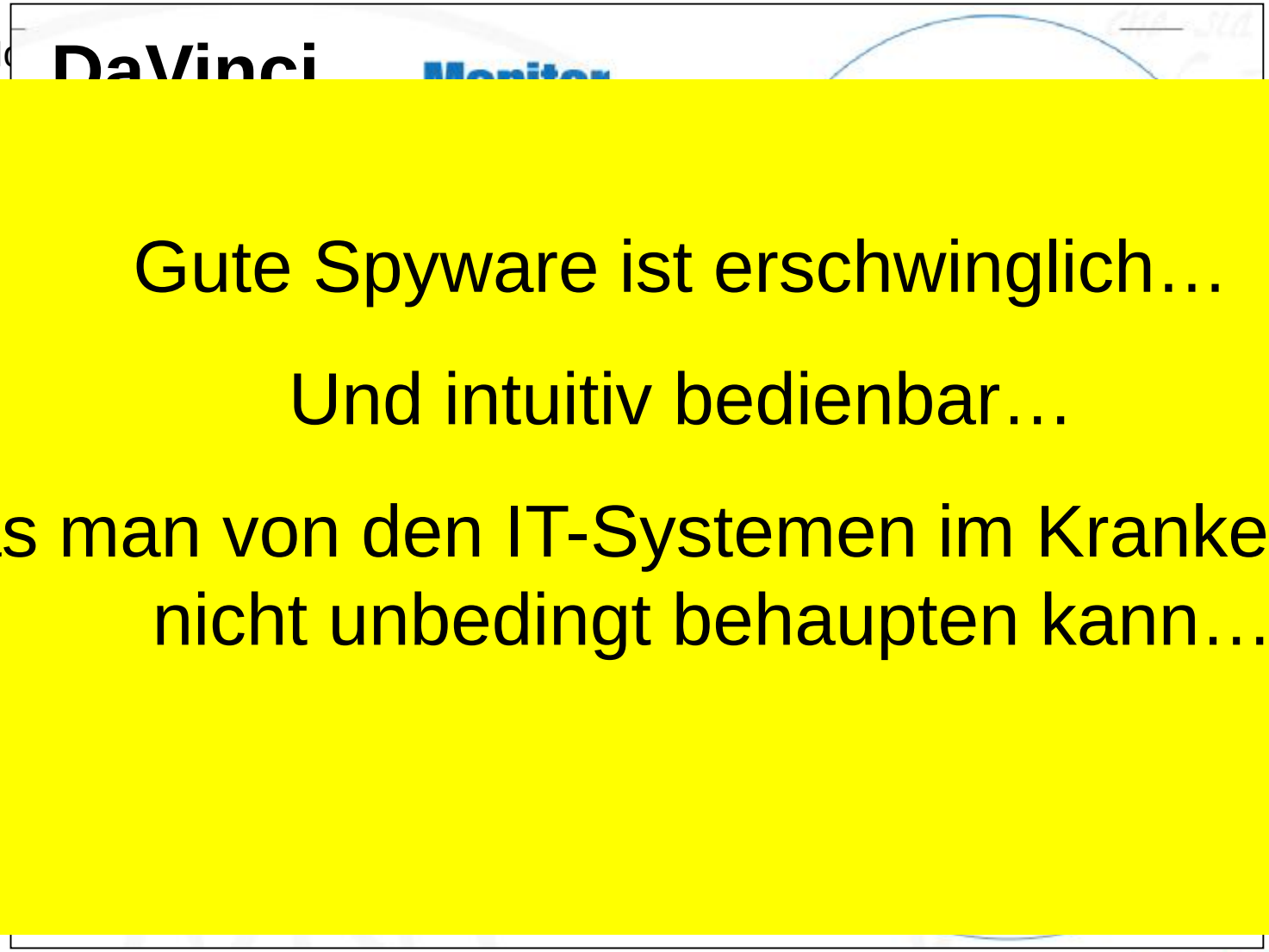
…en, …

… GPS-

…nd Kamera,

Datenschutz/-sicherheit: warum eigentlich…?

- M



Gute Spyware ist erschwinglich…

Und intuitiv bedienbar…

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

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 Gesellschaft für klinische Dienstleistungen Düsseldorf mbH

Apps und Sicherheit

- **è** Übertragene Daten
  - Geräte-Kennung
  - Standort
  - Adressbuch
  - Kalender
  - …
- **è** Wozu?
  - Erstellung von Nutzungs- und Bewegungsprofilen
  - Kontaktdaten für Werbung
  - Preisgabe vertraulicher Informationen, z.B.
    - Banking-Informationen
    - Identitäts-Diebstahl
    - Unternehmens-Zugangsdaten
    - ,,,

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…

Mobile Betriebssysteme aus Unternehmenssicht

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

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

BYOD

- Krankenhaus wird einerseits Mitarbeitern die Nutzung privater Geräte langfristig nicht verweigern können
- Aber: Auf dem Mitarbeiter gehörende Geräte hat der Arbeitgeber keine Weisungsbefugnis
  - **è** Auf diesen Geräten gespeicherte Patientendaten befinden sich daher prinzipiell nicht in der Einrichtung
  - **è** 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“)

Mobile Computing:
Was man noch so beachten könnte…

- Arbeitsrecht
  (z.B. Ruhezeit, wöchentliche Arbeitszeit)
- Urheberrecht/Lizenzrecht
  (z.B. betriebliche Software privat nutzen?)
- Compliance / Unternehmenssicherheit
  (z.B. Frage zgl. Gewährleistung Integrität mobiler IT)
- Strafrecht
  (z.B. Abfangen, Ausspähen von Daten bei privaten Endgeräten)
- Steuerrecht
  (z.B. Vergütungsanspruch für den Mitarbeiter bei Nutzung privater Geräte?)
- Haftungsrecht
  (z.B. Verlust/Beschädigung privates Endgerät)
- Vertragsrecht
  (z.B. Verantwortlichkeit für Wartung/Reparatur des Endgerätes)
- Geheimnisschutz
  (z.B. Frage bzgl. Schutz von Betriebs- u. Geschäftsgeheimnissen)
- Betriebliche Nutzung privater Accounts
  (z.B. Social Network: wem gehört der Account?)

Was tun…?

- Cloud meiden wie die P… ;-)
- 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
  (Lizenzkosten entprechender MDM-Software zwischen 30 und 100 Euro)
- Betriebsvereinbarung BYOD
  (Bei BYOD zusätzlich an Individualvereinbarung mit jedem einzelnen Mitarbeiter denken)
- Grundschutz-Handbuch des BSI zu Rate ziehen

Diskussion

schuetze@medizin-informatik.org

Diskussion

Hinweis:

8. November 2013: GI-Workshop

Sicherheitsmanagement von/für mobile Geräte

in Frankfurt bei DB Systel GmbH

60329 Frankfurt am Main, Jürgen-Ponto-Platz 1

Veranstalter: Gesellschaft für Informatik

[redacted]