Workshop

Datenschutzanforderungen und Lösungsansätze beim Einsatz mobiler Geräte im Gesundheitswesen

BSI Grundschutzkatalog

Alexander Stahmann und Jens Schwanke

alexander.stahmann@med.uni-goettingen.de

www.mi.med.uni-goettingen.de

Inhalt

- Ausgangssituation
- Vorgehen
- Analyse
  - Gefährdungen
  - Maßnahmen
- Zusammenführung
- Diskussion des vorgestellten Vorgehens

Ausgangssituation (1/4)

Mobile Endgeräte haben im privaten Umfeld der Mitarbeiter des Gesundheitswesens eine rasante Verbreitung gefunden

Ausgangssituation (2/4)

- Viele Hersteller von Informationssystemen für das Gesundheitswesen haben mit mehr oder weniger abgestimmten Lösungen auf die Nachfrage reagiert und Anwendungen erstellt.

Ausgangssituation (3/4)

- IT-Abteilungen im Gesundheitswesen werden massiv bedrängt mobile Endgeräte in die Prozesse zu integrieren.
- Die Voraussetzungen (bspw. WiFi) von Seiten der IT-Infrastruktur sind nicht flächendeckend verfügbar.
- Weitere Aspekte wie bspw. (Hygiene) sind oftmals ungeklärt und mit der aktuellen Hardware nur begrenzt lösbar.

Ausgangssituation (4/4)

- Viele Mitarbeiter nutzen ihre privaten Geräte im beruflichen Umfeld, auch im Gesundheitswesen.
  - Zur Recherche
  - Zur Kommunikation
  - …

Bilder: Whatsapp.com | de.wikipedia.org | openclipart.org

Vorgehen

- Zu Sicherstellung von Datenschutz und Datensicherheit wurden in die IT-Grundschutzkataloge und die zugehörigen Ableitungen der ISO Standards geschaffen.
- Beispielhaft wurde für eine mobile Pflegedokumentation mit untersucht welche Gefährdungen und Maßnahmen nach IT-Grundschutz bestehen und wie diese zusammen passen.
- Wo möglich wurde auf Ergänzungspapiere zu mobilen Endgeräten zurückgegriffen

Analyse – Gefährdungsarten

- Elementare Gefährdungen (G 0.x)
- Höhere Gewalt (G 1.x)
- Organisatorische Mängel (G 2.x)
- Menschliche Fehlhandlungen (G 3.x)
- Technisches Versagen (G 4.x)
- Vorsätzliche Handlungen (G 5.x)
- Besondere Datenschutzgefährdungen (G 6.x)

Gefährdungskategorien nach IT-Grundschutz des BSI

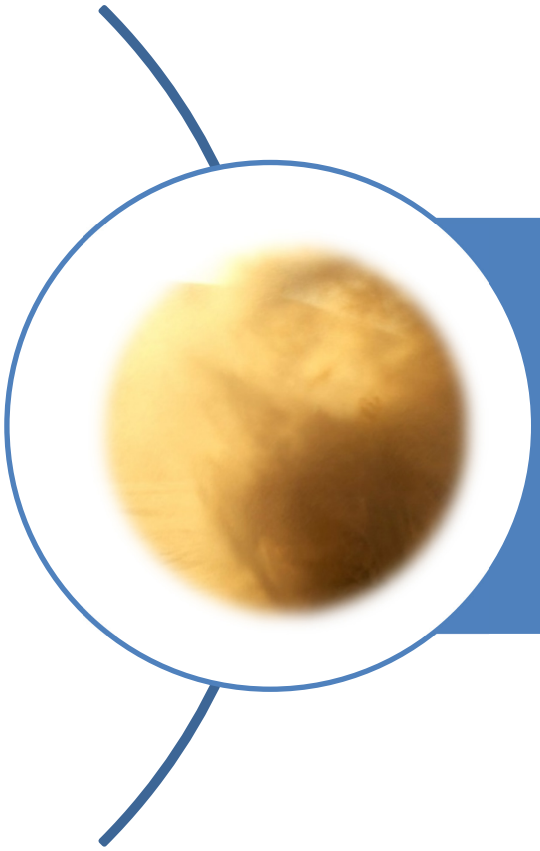
Analyse - Gefährdungen (1/7)

Elementare Gefährdungen

- Ausfall/Störung d. Stromversorgung (G 0.8)
- Ausfall/Störung d. Kommunikationsnetze (G 0.9)
- Spionage/Abhören (G 0.14/0.15)
- Verlust/Diebstahl (G 0.16/0.17)
- Zerstörung von Geräten/Systemen (G 0.24)
- Manipulation (G 0.21)
- Fehlfunktionen (G 0.26)

Gefährdungskategorien nach IT-Grundschutz des BSI

Analyse - Gefährdungen (2/7)



Höhere Gewalt

- Temperatur und Luftfeuchte / Wasser (G 1.7)
- Staub und Verschmutzung (G 1.8)
- Störung von Kommunikationsnetzen (bspw. durch Strahlung) (G 1.17)
- Ausfall eines Dienstleisters/Zulieferers (G 1.19)

Gefährdungskategorien nach IT-Grundschutz des BSI

Analyse - Gefährdungen (3/7)

Organisatorische Mängel

- Unzureichende (Leitungs-)Kapazitäten (G 2.32)
- Unkontrollierter Aufbau von Kommunikationsverbindungen (G 2.37)
- Vertraulichkeitsverlust durch Restinformationen (G 2.38)
- Verwendung unsicherer Protokolle in öffentlichen Netzen (G 2.87)
- Fehlende oder unzureichende Planung des VPN-Einsatzes (G 2.128)

Gefährdungskategorien nach IT-Grundschutz des BSI
[1] http://www.pcwelt.de/images/04/1/1/0/8/9/4/4/8f0586e035f4379a.jpg

Analyse - Gefährdungen (4/7)

Menschliche Fehlhandlungen

- Fahrlässige Zerstörung von Geräten/Daten (G 3.2)
- **Unerlaubte private Nutzung** (G 3.30)
- **Ungeeigneter Umgang mit Passwörtern** (G 3.43)
- Mangelnde Akzeptanz von Informationssicherheit (G 3.77)
- Fehler bei der Synchronisation (G 3.76)

Gefährdungskategorien nach IT-Grundschutz des BSI
[1] http://us.123rf.com/400wm/400/400/izakowski/izakowski1105/izakowski110500010/9527594-madchen-zerstoren-das-smartphone.jpg

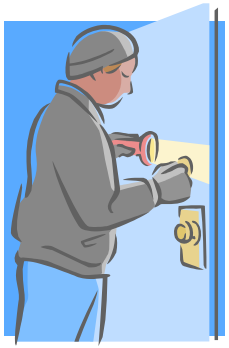
Analyse - Gefährdungen (5/7)

Technisches Versagen

- Software-Schwachstellen/-fehler (G 4.22)
- Unsichere Krypto-Algorithmen (G 4.35)
- Nicht-Verfügbarkeit des Mobilfunknetzes (G 4.41)
- Ausfall des mobilen Endgeräts (G 4.42)
- Unzureichende Sicherheitsmaßnahmen (G 4.51)
- Datenverlust durch mobilen Einsatz (G 4.52)
- Schwachstellen in den Schnittstellenimplementierungen (G 4.79)

Gefährdungskategorien nach IT-Grundschutz des BSI

Analyse - Gefährdungen (6/7)



Vorsätzliche Handlungen

- Diebstahl (G 5.4)
- Abhören von Telefon- oder Datenverbindungen (G 5.12)
- Abhören von Räumen über mobile Endgeräte (G 5.13)
- Systematisches Ausprobieren von Passwörtern (G 5.18)
- Schadprogramme (G 5.23)
- Manipulationen durch Familienangehörige oder Besucher (G 5.70)
- Auswertung von Verbindungsdaten (G 5.99)
- Unberechtigte Foto/Videoaufnahmen (G 5.126)

Gefährdungskategorien nach IT-Grundschutz des BSI

Analyse - Gefährdungen (7/7)

Besondere Datenschutzgefährdungen

- Weitergabe von personenbezogenen Daten durch Berechtigte an unberechtigte Dritte (G 6.5)
- Fehlende oder mangelhafte Vorabkontrolle (G 6.6)
- Gefährdung der Rechte von Betroffenen (G 6.7)
- Gefährdung der Kontrollziele (G 6.10)
- Fehlende oder unzureichende Absicherung der Verarbeitung personenbezogener Daten im Ausland (G 6.11)

Gefährdungskategorien nach IT-Grundschutz des BSI

Analyse – Maßnahmenarten

- Infrastruktur (M 1.x)
- Organisation (M 2.x)
- Personal (M 3.x)
- Hard- und Software (M 4.x)
- Kommunikation (M 5.x)
- Notfallvorsorge (M 6.x)
- Datenschutz (M 7.x)

Maßnahmenkategorien nach IT-Grundschutz des BSI

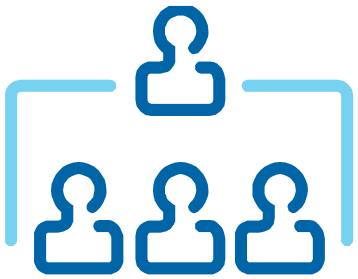
Analyse – Maßnahmen (1/7)

Infrastruktur

- Geeignete Aufbewahrung der mobilen Endgeräte (M 1.33)
- Geeignete Aufbewahrung dienstlicher Unter-lagen und Datenträger (M 1.45)

Maßnahmenkategorien nach IT-Grundschutz des BSI

Analyse – Maßnahmen (2/7)



Organisation

- Datenträgerverwaltung (M 2.3)
- Regelung für Wartungs- und Reperaturarbeiten – Sicherheitsupdates (M 2.4)
- Nutzungsverbot nicht-freigegebener Hard-/Software -> Freigabeverfahren (M 2.9)
- Regelung des Passwortgebrauchs (M 2.11)
- Beratung und Betreuung der Nutzer (M 2.12)
- Einrichtung einer eingeschränkten Benutzerumgebung (M 2.32)
- Informationsbeschaffung über Sicherheitslücken (M 2.35)
- Geregelte Übernahme und Rückgabe von mobilen Endgeräten (M 2.36)
- Reaktion auf Verletzung der Sicherheitsvorgaben (M 2.39)
- Schutz vor Schadprogrammen (M 2.154, 2.156, 2.157)
- Kryptokonzept (M 2.161)
- Geeignete Verfahren zur Löschung von Daten (M 2.176)
- Sicherheitsrichtlinien (M 2.304)

Maßnahmenkategorien nach IT-Grundschutz des BSI

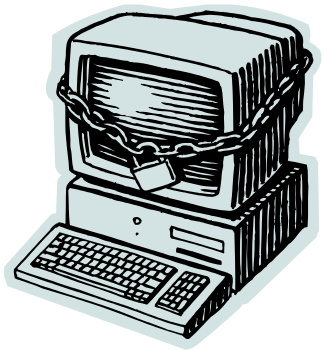
Analyse – Maßnahmen (3/7)

Personal

- Sensibilisierung der MA zum sicheren Umgang mit Informationen und Geräten (M 3.13, 3.60)
- Einführung in die Bedrohung durch Schadprogramme (M 3.69)
- Sensibilisierung für die Nutzung von Bluetooth (M 3.80)

Maßnahmenkategorien nach IT-Grundschutz des BSI

Analyse – Maßnahmen (4/7)

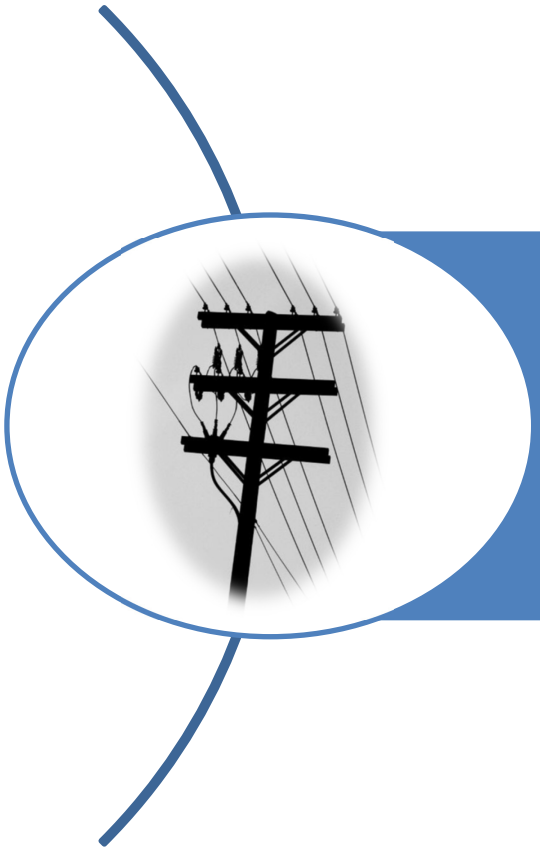


Hard- und Software

- Passwortschutz und Bildschirmsperre (M 4.1, M 4.2)
- Gesichertes Login (M 4.15)
- Schutzprogramme gegen Schadsoftware (M 4.3)
- Einsatz eines Verschlüsselungsprodukts (M 4.29)
- Abschalten von nicht benötigten Leistungsmerkmalen
- Verwendung von Verschlüsselung, Checksummen und/oder digitalen Signaturen (M 4.34)
- Einsatz von kryptographischen Verfahren auf den verschiedenen Ebenen des ISO/OSI-Referenzmodells (M 4.90)
- Geeignete Auswahl von Authentifikationsmechanismen (M 4.133)
- Zentrale Administration (Mobile Device Management) (M 4.230)

Maßnahmenkategorien nach IT-Grundschutz des BSI

Analyse – Maßnahmen (5/7)



Kommunikation

- Deaktivierung nicht benötigter Schnittstellen (M 5.1)
- Sicherung der Kommunikationsverbindungen (VPN) (M 5.51)
- Schutz vor Erstellen von Bewegungsprofilen (M 5.78)
- Schutz vor Abhören von Raumgespräche (M 5.80)
- Datenschutzaspekte bei der Internetnutzung (M 5.155)

Maßnahmenkategorien nach IT-Grundschutz des BSI

Analyse – Maßnahmen (6/7)

Notfallvorsorge

- Detektionsmaßnahmen für Sicherheitsvorfälle (M 6.67)
- Redundante Kommunikationsverbindungen (M 6.75)
- Festlegung von Ausweichverfahren (M 6.141)
  - Ausfall eigener Netze/Dienste
  - Ausfall im Netz des Internetanbieters des Unternehmens
  - Ausfall des Mobilfunknetzes

Maßnahmenkategorien nach IT-Grundschutz des BSI

Analyse – Maßnahmen (7/7)

Datenschutz

- Prüfung rechtlicher Rahmenbedingungen und Vorabkontrolle bei der Verarbeitung personenbezogener Daten (M 7.4)
- Verpflichtung/Unterrichtung der MA bei der Verarbeitung personenbezogener Daten (M 7.5)
- Datenschutzrechtliche Freigabe (M 7.9)
- Dokumentation der Zulässigkeit (M 7.13)

Maßnahmenkategorien nach IT-Grundschutz des BSI

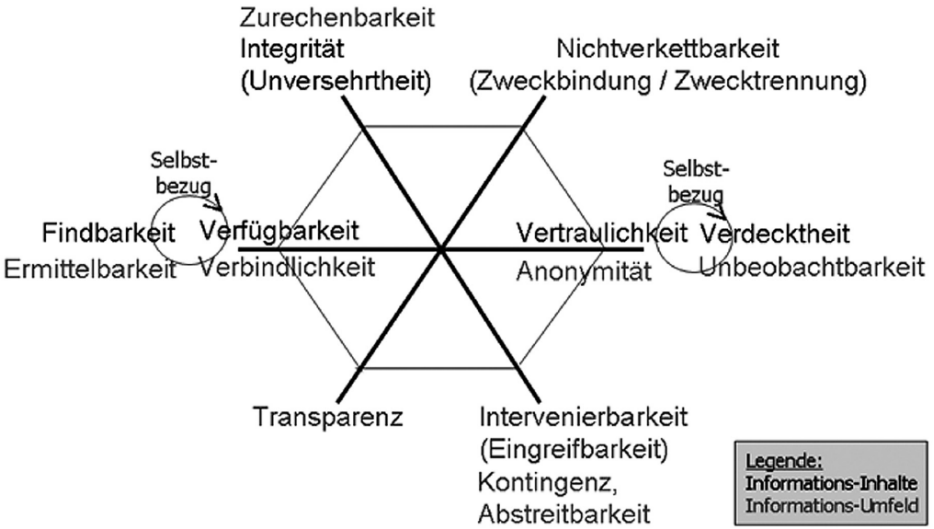
Analyse – Checkliste

| Nr. | M 1.13 | M 1.45 | Gebäudeeinsturz | M 2.3 | M 2.9 | M 2.11 | M 2.12 | M 2.32 | M 2.36 | M 2.70 | M 2.76 | M 2.78 | M 2.102 | M 2.103 | M 2.105 | M 2.107 | M 2.108 | M 2.109 | M 2.110 | M 2.111 | M 2.112 | M 2.275 | M 2.276 | M 2.278 | M 2.306 | M 2.326 | M 2.380 | M 2.415 | M 2.416 | M 2.417 | M 2.418 | M 2.450 | Zerstörung | M 3.31 | M 3.69 | M 3.70 | Hier: Brand/Schaden | M 4.1 | M 4.2 | M 4.3 | M 4.5 | M 4.16 | M 4.29 | M 4.31 | M 4.32 | M 4.90 | M 4.91 | M 4.114 | M 4.115 | M 4.132 | M 4.133 | Kommentarfeld | M 4.141 | M 4.166 | M 4.167 | M 4.28 | M 4.30 | M 4.158 | Nur Ab Kenntnis | M 5.10 | M 5.14 | M 5.15 | M 5.4 | M 5.5 | M 5.9 | M 5.13 |
|---|---|---

Diskussion (1/7)

- Datenschutzziele stehen in einem Spannungsverhältnis.
- DS-Aufsichtsbehörden legen des Fokus sehr unterschiedlich

→ frühzeitige Einbeziehung



Quelle: [1] Rost M, Bock K. Privacy By Design und die Neuen Schutzziele. DuD. 2011;2011(1):30–5.

Diskussion (2/7)

- Im Vergleich zu traditionellen Dokumentation ist es bei der elektronischen Verarbeitung einfacher, unbemerkt, große Mengen an vertraulichen Daten zu entwenden.
- Strikte Rollenkonzepte und Einschränkungen von Zugriffsberechtigungen sind nötig.
- Angriffe erfolgen in vielen Fällen nicht von extern!

Diskussion (3/7) – Gefährdungen

- Die Auswahl der Gefährdungen ist auf die zusätzlichen Gefahren durch die Verwendung von Smartphone- und Tabletapps beschränkt
- Die verwendeten Gefährdungen nach IT-Grundschutz sind nur begrenzt an die Gegebenheiten moderner mobiler Endgeräte angepasst →Überblickspapiere
- Eine eindeutige Kategorisierung und Gewichtung von Gefährdungen ist nicht möglich.
- Die Gefährdungen beim Einsatz von Smartphone- und Tabletapps gehen über die beim Einsatz von Notebooks entstehenden Gefährdungen hinaus

Diskussion (4/7) – Maßnahmen

- IT-Grundschutz trennt noch zwischen Mobiltelefonen und PDA, daher ist eine Adaption der Schutzmaßnahmen für PDAs, Mobiltelefone und Notebooks gewählt worden.
- Viele Maßnahmen sind abhängig von der Mobilplattform nicht oder nur begrenzt umsetzbar.
- Neben den technischen Maßnahmen ist die Erstellung, Anwendung und Überprüfung von Richtlinien zum Umgang mit den mobilen Endgeräten nötig.

Diskussion (5/7) – Maßnahmen

- Durch die Sensibilisierung der Mitarbeiter (Aufklärung und Einbeziehung in den Sicherheitsprozess) sind größere Effekte im Sinne der Datensicherheit zu erreichen, als durch technische Maßnahmen allein.
- Durch die Definition entsprechender Regeln im Kontext der betroffenen Prozesse kann es mittelbar zu Kosteneinsparungen kommen, wenn die Prozesse dabei analysiert und angepasst werden.

[1] Bundesamt für Sicherheit in der Informationstechnik, Herausgeber. BSI-Standard 100-1 Managementsysteme für Informationssicherheit (ISMS). 2008.

Diskussion (6/7) – Maßnahmen

- Verschlüsselung wird sowohl für die Übermittlung als auch für die Speicherung von den Mobilplattformen angeboten, die korrekte Verwendung (Prüfung) von Zertifikaten und Protokollen obliegt jedoch der App/ dem Nutzer.
- Die Sicherstellung der Integrität ist durch die Mobilplattformen nur begrenzt gegeben, sie muss für jede App selbst sichergestellt werden.

Diskussion (7/7) – Maßnahmen

- Die Verfügbarkeit steht im besonderen Spannungsverhältnis:
  - Speicherung von personenbezogenen Daten auf den Geräten
  - Abhängigkeit von Netzwerkverfügbarkeit
- Die Sicherstellung der Vertraulichkeit bei der Datenverarbeitung im Ausland ist nicht oder nur schwer realisierbar. Die Kontenbindung (Apple/Google) der Geräte stellt ein Risiko dar.

[1] http://blog.getgoods.de/wp-content/uploads/2012/09/evil-google-logo.jpg
[2] http://gamester81.com/wp-content/uploads/apple-evil.jpg
[3] Bigo D, Boulet G, Bowden C, Carrera S, Jeandesboz J, Scherrer A. Fighting cyber crime and protecting privacy in the cloud. Brüssel: European Parliament, DIRECTORATE GENERAL FOR INTERNAL POLICIES; 2012 Okt. Report No.: PE 462.509.

Kontakt

Alexander Stahmann

Universitätsmedizin Göttingen
Institut für Medizinische Informatik
Robert-Koch-Str. 40
37075 Göttingen

Web: www.mi.med.uni-goettingen.de
E-Mail: alexander.stahmann@med.uni-goettingen.de