Bundesamt
für Sicherheit in der
Informationstechnik

eCare – Digitalisierung in der Pflege

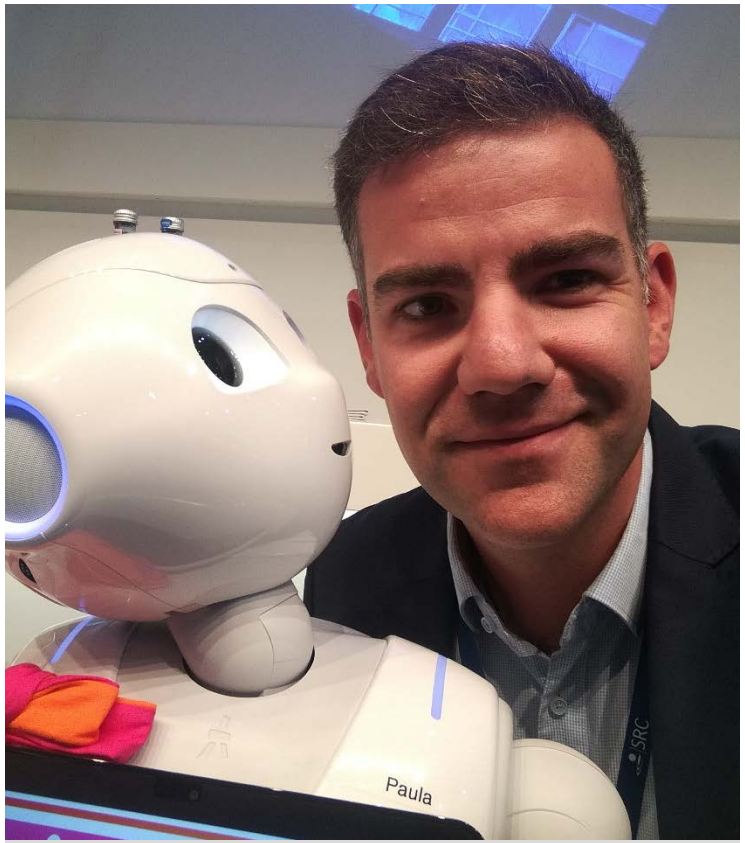
Dr. Dina C. Truxius, Bundesamt für Sicherheit in der Informationstechnik (BSI)
Dr. Deniz Ulucay, SRC Security Research & Consulting GmbH

Dr. Dina C. Truxius – BSI

- Naturwissenschaftlerin
- Seit 2018 beim BSI
  - Cyber-Sicherheit von Medizinprodukten
  - Projektarbeiten
  - Gremienarbeit
- Projektleiterin eCare

Bundesamt
für Sicherheit in der
Informationstechnik

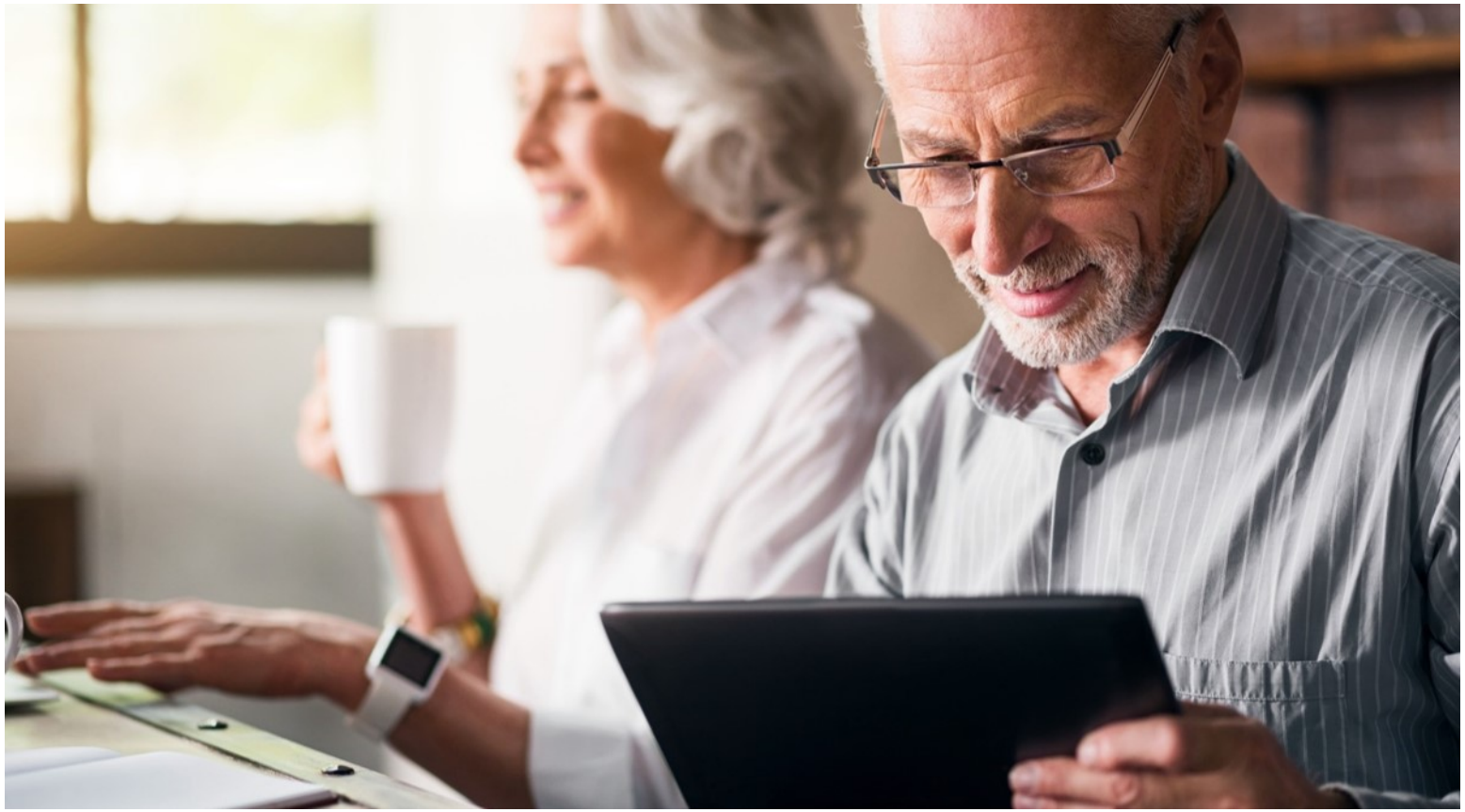
Dr. Deniz Ulucay – SRC Security Research & Consulting GmbH



- Physiker
- Seit 2015 Berater für Informationssicherheit bei SRC
  - Informationssicherheitsmanagement
  - ISO 27001 & BSI IT-Grundschutz
  - KRITIS
  - Datenschutz
- sPL eCare, Fokus IT-Sicherheitsbetrachtung

Besuch auf der Medica 2018

Wir werden alle älter…



Demografischer Wandel

Pflegepersonalstärkungsgesetz (PpSG)

Fachkräftemangel

Selbstbestimmtes und komfortables Leben

...aber nicht unsere digitale Umwelt

Wearables

Intelligentes Geschirr

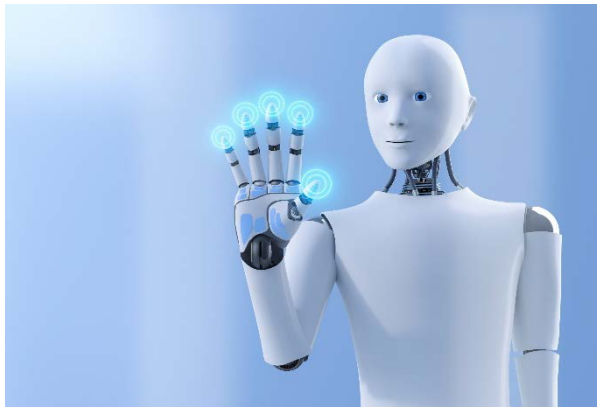
Dokumentation

Intelligente Pillendosen

Sturzerkennung

uvm.

Yes, we care! Das BSI-Projekt eCare – Digitalisierung in der Pflege?



Cyber-Sicherheitslage von vernetzten Produkten, die in der Alten-, Patienten- oder Krankenpflege Anwendung finden realistisch einzuschätzen und auf IT-Sicherheit zu untersuchen

Mensch-Maschine-Interaktion?

Aufgaben im Projekt

Marktsichtung

Auswahl

Prüfungen der IT-Sicherheit

Herstellerkommunikation

Prozesse

Abschlussbericht

Definition „Pflegegerät“

Keine einheitliche / verbindliche Definition

- Einsatz in der häuslichen oder stationären Pflege
- Hilfestellung für Alltagssituationen
- Bedienung durch Pflegepersonal oder Endanwender
- Keine „Health-Lifestyle-Produkte“

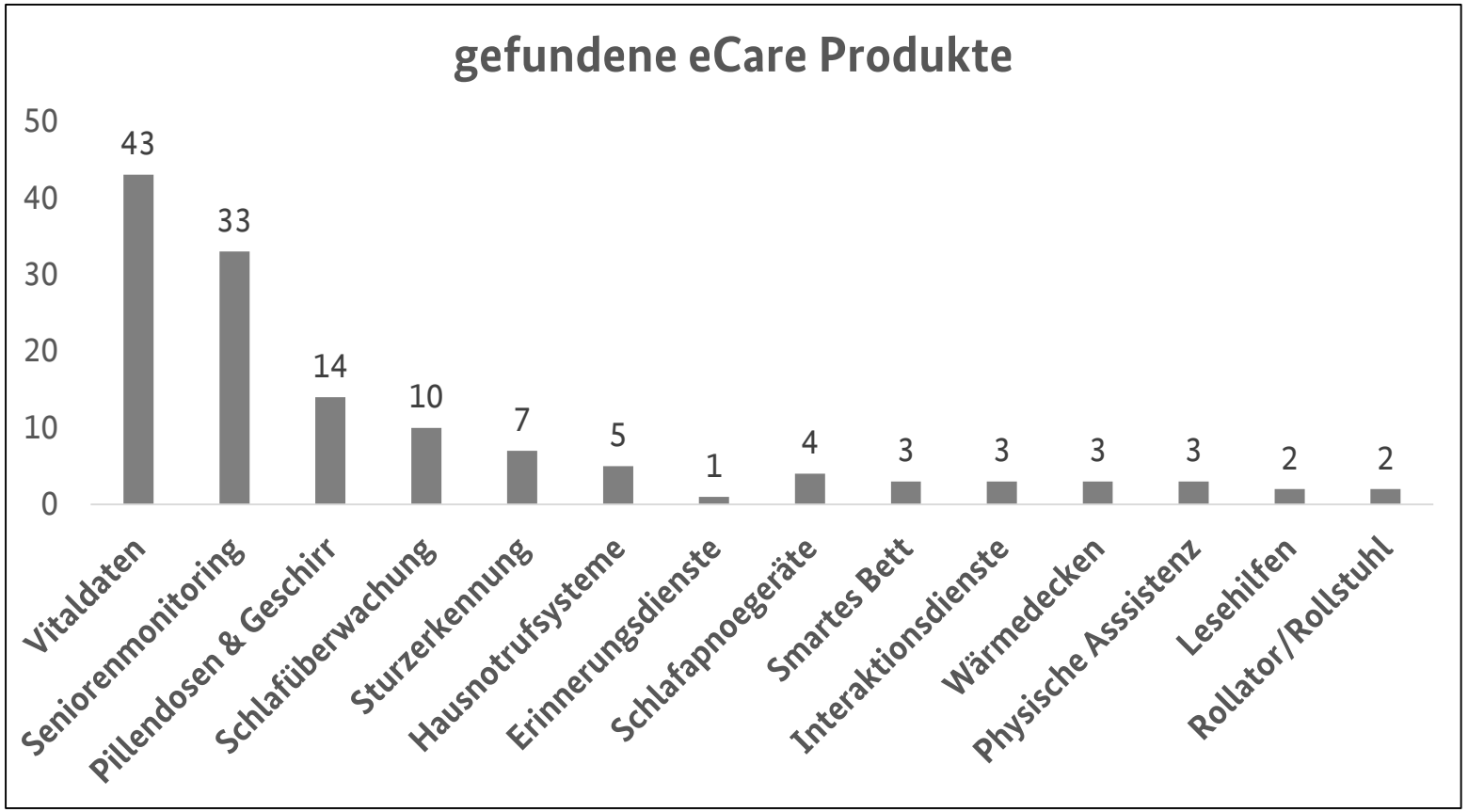
Teilweise auch „Medizinprodukte“

Google-Bilder-Suche: „Pflegegerät“
Quelle: fussballtor24.de

Besuch von Pflegeeinrichtungen, Sanitätshaus & Internetrecherche (Verfügbarkeit in Deutschland)

- Hausnotrufsysteme (aktiv) & Senioren-Monitoring (passiv)
- Sturz- und Hinderniserkennung
- Smarte Betten
- Physische Assistenz (Treppenlifte oder Badewannenlifte)
- Smarte Brillen und Lesehilfen
- Intelligentes Geschirr und Pillendosen
- Schlafüberwachung
- Erinnerungsdienste mit pflegerischem Hintergrund
- Interaktionsdienste zur Bewegung und sozialen Interaktion mit therapeutischem Hintergrund
- Rollatoren und Rollstühle
- Wärmedecken
- Schlafapnoegeräte
- Geräte zur Vitaldatenmessung (Blutzucker, Blutdruck, ...)

Auswahlkriterien



9 Produkte ausgewählt

Unterschiedliche Kategorien

Möglichst viele Schnittstellen

Verfügbarkeit

Alleinstellungsmerkmale

Herstellerkontakt

Selbsteinschätzung der Hersteller zur IT-Sicherheit - Fragebogen

Keine Informationen zu IT-Sicherheitsstandards/-labels aus Marktanalyse

Telefonischer und/oder E-Mail-Kontakt an Produkthersteller

Einladung zu anonymem Online-Fragebogen

Diverse Fragen zur Cybersicherheit

84 Hersteller aus Recherche
52 Einladungen
35 Aufrufe
12 vollständige Beantwortungen

Bundesamt für Sicherheit in der Informationstechnik

Selbsteinschätzung der Hersteller zur IT-Sicherheit - Ergebnisse

Produkte aus der Kategorie:	IT-Sicherheit von Beginn an	Rollensystem mit Privilegien	Remote Control	Transferierte Daten = Patientendaten	verschlüsselt tranferierte Daten (https)	gespeicherte Daten verschlüsselt State-of-the Art	Gerätefkt. nicht beeinträchtigt durch schwache Schnittstelle	Regulärer Update/Patch Zyklus	Authentizitätscheck bei Updates/Pactehs	Ist Login für Nutzer lesbar?
Senioren-Monitoring	Ja	Ja	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja
Senioren-Monitoring	Nein	Ja	Ja	Nein	Ja	Ja	Ja	Nein	Ja	Nein
Lesehilfen	Nein	Ja	Ja	Nein	Nicht sicher	Ja	Ja	Ja	Ja	Ja
Hausnotruf	Ja	Ja	Ja	Nein	Ja	Ja	Nicht sicher	Ja	Ja	Ja
Interaktions-dienste	Nein	Nein	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Ja
Schlafapnoe	Ja	Nein	Ja	Nein	Ja	Ja	Ja	Ja	Ja	Nein
Schlafapnoe	Ja	Ja	Ja	Yes	Ja	Ja	Ja	Ja	Nicht sicher	Ja
Smartes Bett	Ja	Nicht sicher	Nicht sicher	Nein	Ja	Ja	Nicht sicher	Nein	Ja	Nein
Smartes Bett	Ja	Ja	Yes	Nein	Nicht sicher	Nicht sicher	Ja	Ja	Ja	Nicht sicher
Vitaldaten	Ja	Nein	Nein	Nein	Ja		Ja	Ja	Nicht sicher	Nein
Vitaldaten	Ja	Ja	Nein	Ja	Ja	Nein	Yes	Ja	Nein	Nein
Vitaldaten	Ja	Nein	Nein	Ja	Ja	Nein	Nicht sicher	Nein		Nein

Positive Überraschung

Überwiegende Antwort mit „Ja“

IT-Sicherheit bei der Entwicklung berücksichtigt

Teilnahmequote gering (12 von 52/84)

Möglicherweise „Verschiebung“:
Security Awareness = Teilnahmebereitschaft

Bundesamt für Sicherheit in der Informationstechnik

Projektdiagnose: Anspruch und Wirklichkeit

6 Produkte getestet:
- Pulsoximeter
- Blutzuckermesssystem
- Pillendose
- Schlafapnoetherapiegerät
- Notrufuhr/Sturzerkennung
- Seniorentablet

Beschaffung und Kontaktaufnahme mit Herstellern oft schwierig

Fazit Marktanalyse

Connected

Cloud

Apps

Cybersicherheit

...mal sehen

Smartphone

Smart

Sicherheitslabels

Pflegeroboter

Bundesamt
für Sicherheit in der
Informationstechnik

IT-Sicherheitsbetrachtung - Methodik

Prüftiefe = „Low hanging fruits“ << vollständige Begutachtung

Dokumentation = Black-Box-Ansatz

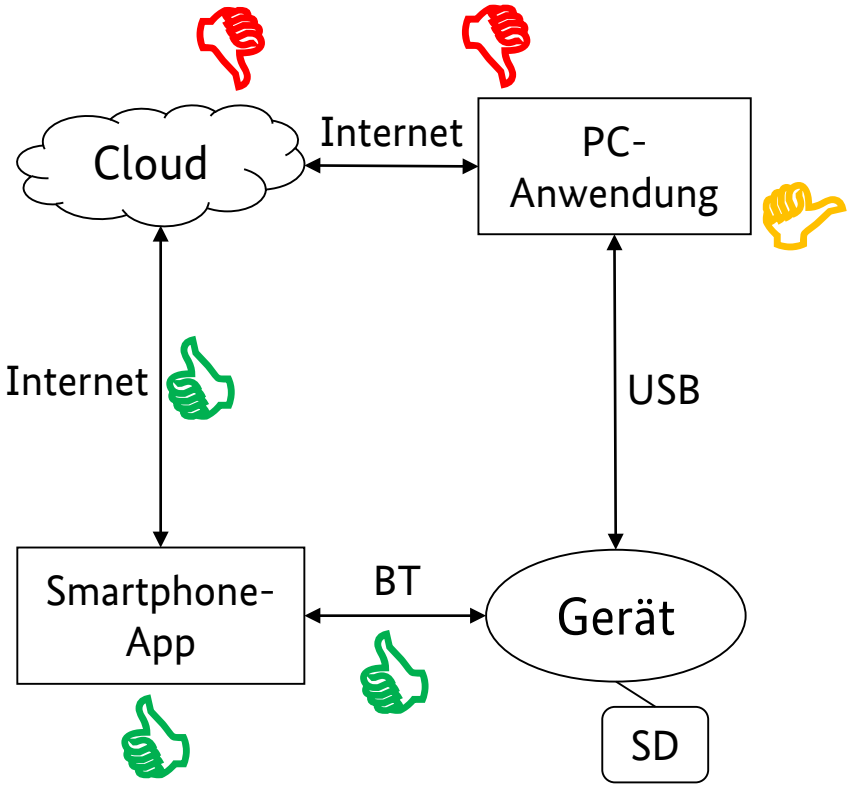
Fokus = Cyber-Security

Nicht im Fokus = Funktionale Sicherheit („Safety“)

Risikoabschätzung = „untere Schranke“

Bundesamt
für Sicherheit in der
Informationstechnik

IT-Sicherheitsbetrachtung - Schlafapnoetherapiegerät



Überwachung periodischer Atemstillstände (Schlafapnoe)

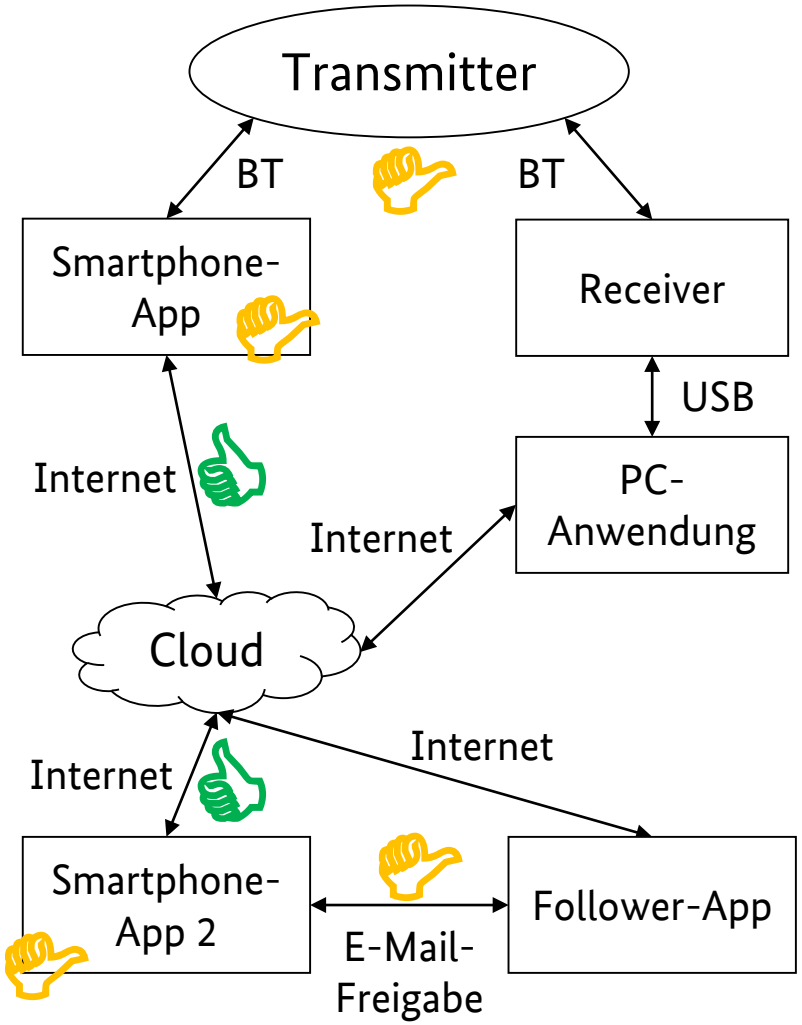
Kommunikation über Bluetooth und App-Cloud: State-of-the-Art

PC-Anwendung nur teilweise obfuskiert

- U. a. Änderung der Seriennummer → Beeinträchtigung der Funktion
- Enumeration von Accountdaten → unbemerkte Übernahme von Accounts samt Daten

Bundesamt
für Sicherheit in der
Informationstechnik

IT-Sicherheitsbetrachtung - Blutzuckermesssystem



Kontinuierliche Überwachung des Blutzuckerspiegels, auch als Follower

Bluetooth: Pairing & Verschlüsselung, einige Flags im „Just Works“-Mechanismus nicht gesetzt → Man-in-the-Middle möglich

Zertifikatspinning, tlw. erst nach Login

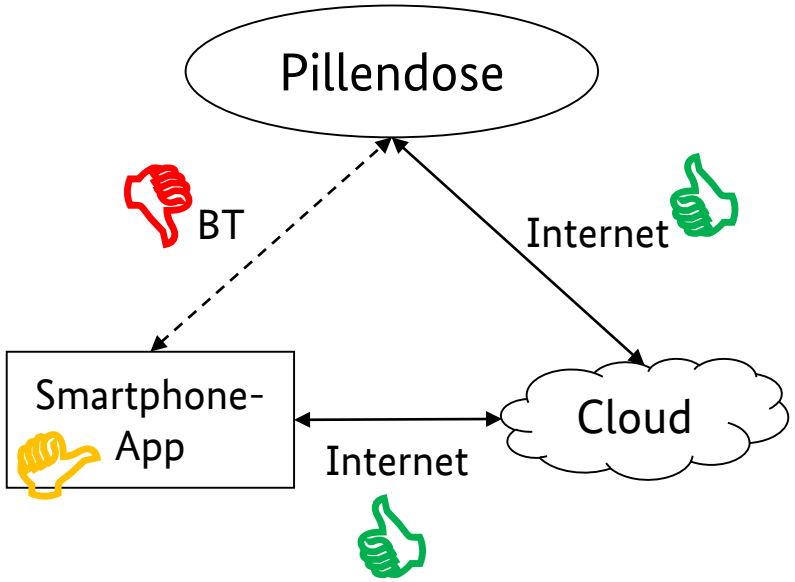
Apps fordern ausschließlich notwendige Android-Berechtigungen an, jedoch auch „WRITE_EXTERNAL_STORAGE“

Einfache Techniken für Root-Detection und Obfuskierung

Einladungslink: einmalig, unverschlüsselt, Open Redirect

Bundesamt für Sicherheit in der Informationstechnik

IT-Sicherheitsbetrachtung - Pillendose



(Bewegungs-)Sensor erkennt Entnahme von Medikamenten

Erinnerung / Alarmierung per App

Bluetooth (nur für Konfiguration):

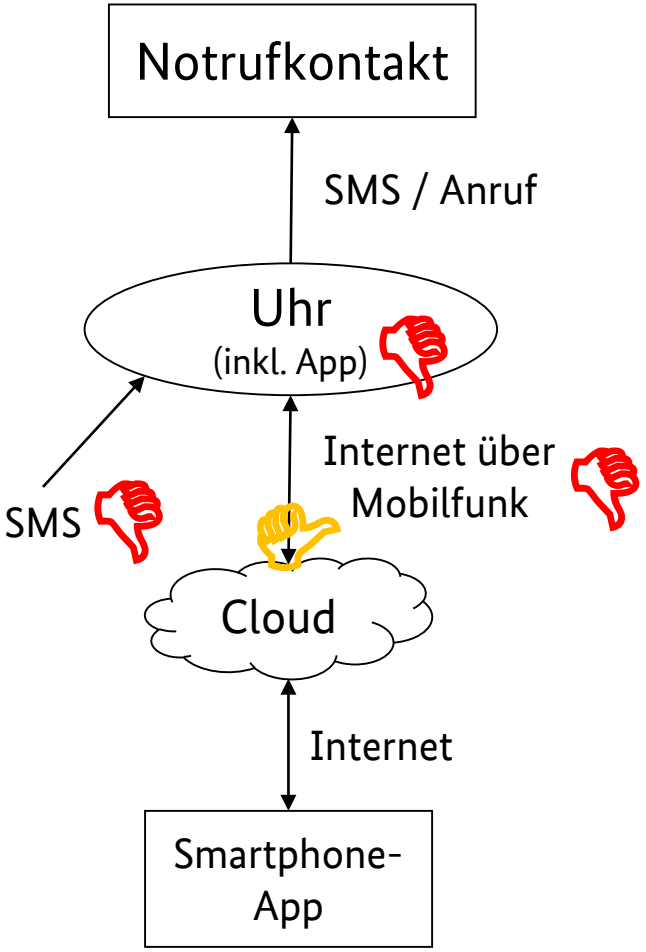
- Dauerhaft aktiv
- Kein Pairing & unverschlüsselt
- Abgriff des WLAN-Passwortes

Verschlüsselte Verbindung zur Cloud

App fordert unnötige Android-Rechte an, keine wirksame Obfuskierung, einfache Root-Detection.
Kein Zertifikatspinning, aber Zertifikatsprüfung auf bekannte CAs.

Bundesamt für Sicherheit in der Informationstechnik

IT-Sicherheitsbetrachtung – Notrufuhr mit Sturzerkennung



Smartwatch mit Notruffunktion (Anruf & SMS)

Smartphone-App für „Lebenszeichen“-Funktion

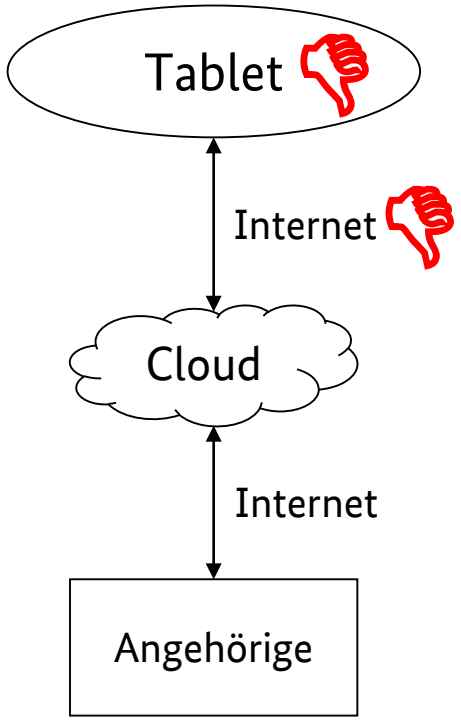
Smart-Watch
- Patchlevelstand 1.3.2018 > 1 Jahr
- Root-Rechte einfach zu erlangen

Steuerung via SMS
- Lebenszeichen, Positionsabfrage uvm.
- SMS-Sicherheitscode bietet kaum Sicherheit
- Keine Information an Träger

Unverschlüsselte Kommunikation zur Cloud, Authentifikation über weiteren schwachen Sicherheitscode

Bundesamt für Sicherheit in der Informationstechnik

IT-Sicherheitsbetrachtung - Seniorentablet



Android-Tablet mit „besonderer“ Uhr-/Kalender-App

Kalender kann von Dritten mit Informationen und Bildern gefüllt werden (Abonnement erforderlich)

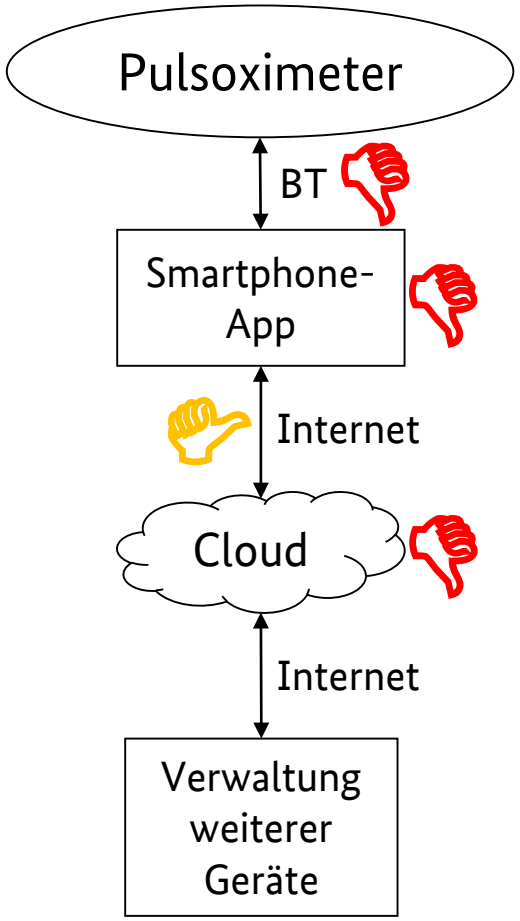
Aktivierung per Mail und Freischaltung der App durch Hersteller → nicht möglich (Beantragung erfolgt, keine Antwort)

Android
- Patchlevel 5.3.2018 > 1 Jahr
- „Ausbruch“ nach WLAN-Konfiguration möglich

Kommunikation
- Unverschlüsselt
- Passwörter als MD5-Hashes

Bundesamt für Sicherheit in der Informationstechnik

IT-Sicherheitsbetrachtung - Pulsoximeter



Fingerclip zur Puls- und Blut-Sauerstoffmessung

Anzeige der Werte über Smartphone-App
Verknüpfung weiterer Geräte des Herstellers über Cloud

Bluetooth ohne Pairing, unverschlüsselt: Manipulation möglich

Quellcode nicht obfuskiert; „WRITE_EXTERNAL_STORAGE“
https aber kein Zertifikatspinning: MitM möglich

Bei Anmeldung enthält http-Response den Aktivierungslink: Account-Anlage für beliebige E-Mail-Adressen (ohne Kontrolle dieser) möglich.
Enumeration über http-Post ist Enumeration möglich
Für einen existierenden Account kann ohne Verifikation eine Passwortrücksetzung angefordert werden.
http-Response enthält Link für (unbemerkte) Passwortänderung.

IT-Sicherheitsbetrachtung - Fazit

Sehr niedrige Prüftiefe!

Sehr hoher Schutzbedarf: Gesundheitsdaten!

Alle getesteten Geräte wiesen mittlere bis hohe Schwachstellen auf.

Keines der Geräte wurde im Vorfeld einem professionellen Penetrationstest unterzogen.

Informationssicherheitsmanagement bei Herstellern und Entwicklung auf niedrigem Niveau.

BSI-Empfehlung oder FDA-Guidelines nur unzureichend berücksichtigt.

→ Empfehlung für tiefergehende Prüfung, insbesondere Backends

Bundesamt für Sicherheit in der Informationstechnik

Was darf das BSI?

§ 7a Untersuchung der Sicherheit in der Informationstechnik

(1) Das Bundesamt kann zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14, 17 und 18 auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene **informationstechnische Produkte und Systeme untersuchen**. Es kann sich hierbei der Unterstützung Dritter bedienen, soweit berechtigte Interessen des Herstellers der betroffenen Produkte und Systeme dem nicht entgegenstehen.
(2) Die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nur zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14 und 17 genutzt werden. Das Bundesamt darf **seine Erkenntnisse weitergeben und veröffentlichen**, soweit dies zur Erfüllung dieser Aufgaben erforderlich ist. Zuvor ist dem Hersteller der betroffenen Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu geben.)

Mehr Cyber-Sicherheit in der Pflege

Alle Hersteller wurden informiert, dass die Prüfberichte vorliegen

Nach Übersenden des Prüfberichts beginnt ein 90 Tage Disclosure

Vertrauensvolle Zusammenarbeit zwischen Sicherheitsforschern, Herstellern und BSI

Vergabe einer CVE-ID (common vulnerability and exposures)

Veröffentlichung der behobenen Schwachstellen

Bundesamt
für Sicherheit in der
Informationstechnik

Wie geht es weiter?

Veröffentlichung der Cyber-Sicherheitsbetrachtung von eCare in deutscher und englischer Sprache

Nachfolgeprojekt(e)

Vertrauensvolle Zusammenarbeit zwischen Herstellern, Betreibern, Sicherheitsforschern und Behörden

Meldestelle/E-Mail für Schwachstellen

Regelmäßige Sicherheitsprüfungen seitens Hersteller

Zukünftig regulatorische Anforderungen an IoT-Produkte?

Fragen?

Anregungen?

Wünsche?

Kontakt

Dr. Dina C. Truxius
Projektleiterin eCare

dina.truxius@bsi.bund.de
Tel. +49 (0) 228 99 10 9582-6147
Fax +49 (0) 228 99 10 9582-5400

Bundesamt für Sicherheit in der Informationstechnik
Referat DI 24 - Cyber-Sicherheit im Gesundheits- und Finanzwesen
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

www.bsi.bund.de