Offenlegung f inanzieller Interessen Ch. Brodowski für den o. g. Vortrag

P- Produkt: Finanzielles Interesse bei der Ausrüstung, dem beschriebenen Verfahren und/oder dem beschriebenen Produkt (z. B. Forschungsunterstützungen, Referentenhonorare, Reisekostenunterstützungen, Stipendien etc.)

I – Investor:Finanzielles Interesse an Firmen, die eine beschriebene Ausrüstung, ein Verfahren oder Produkte liefern (z. B. Aktienbesitz, Anteilseigner etc.)

B – Berater: Kommerzielle Vergütung oder Unterstützung des Autors in den letzten drei Jahren in Form von Beratungsverträgen (Mitgliedschaft in Gremien, Beiräten, Aufsichtsräten etc.)

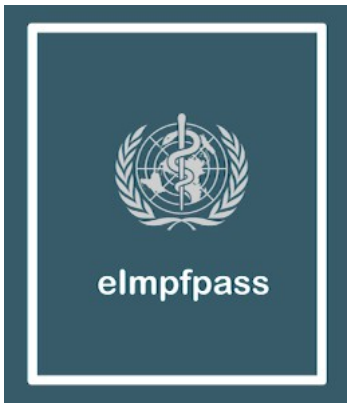
X K – Keine: Keine Interessenskonf lkte; keine kommerzielle Unterstützung der vorgelegten Arbeit in irgendeiner Form

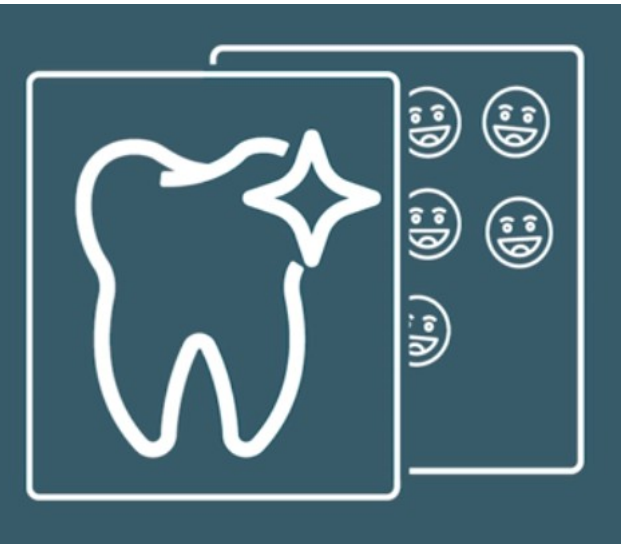
IT-Sicherheit aktuell – ist digital wirklich immer besser?

https://www.pinterest.de/pin/662944007640272506/

Was kommt auf uns zu?

https://i.ytimg.com/vi/VbUgeHVcwQY/hqdefault.jpg





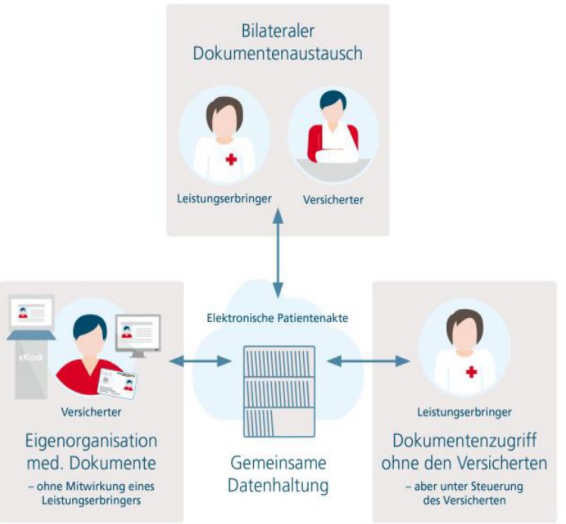
https://www.kbv.de/html/mio.php

Was bedeutet das für den niedergelassenen Anästhesisten?

Vorteile:
- Evtl. Mehr Informationen verfügbar (U-Heft, ePA, NFD, eMP)
- Dokumente ggf. schon vorab elektronisch einsehbar, wenn der Patient über sein Mobiltelefon die Freigabe dafür erteilt

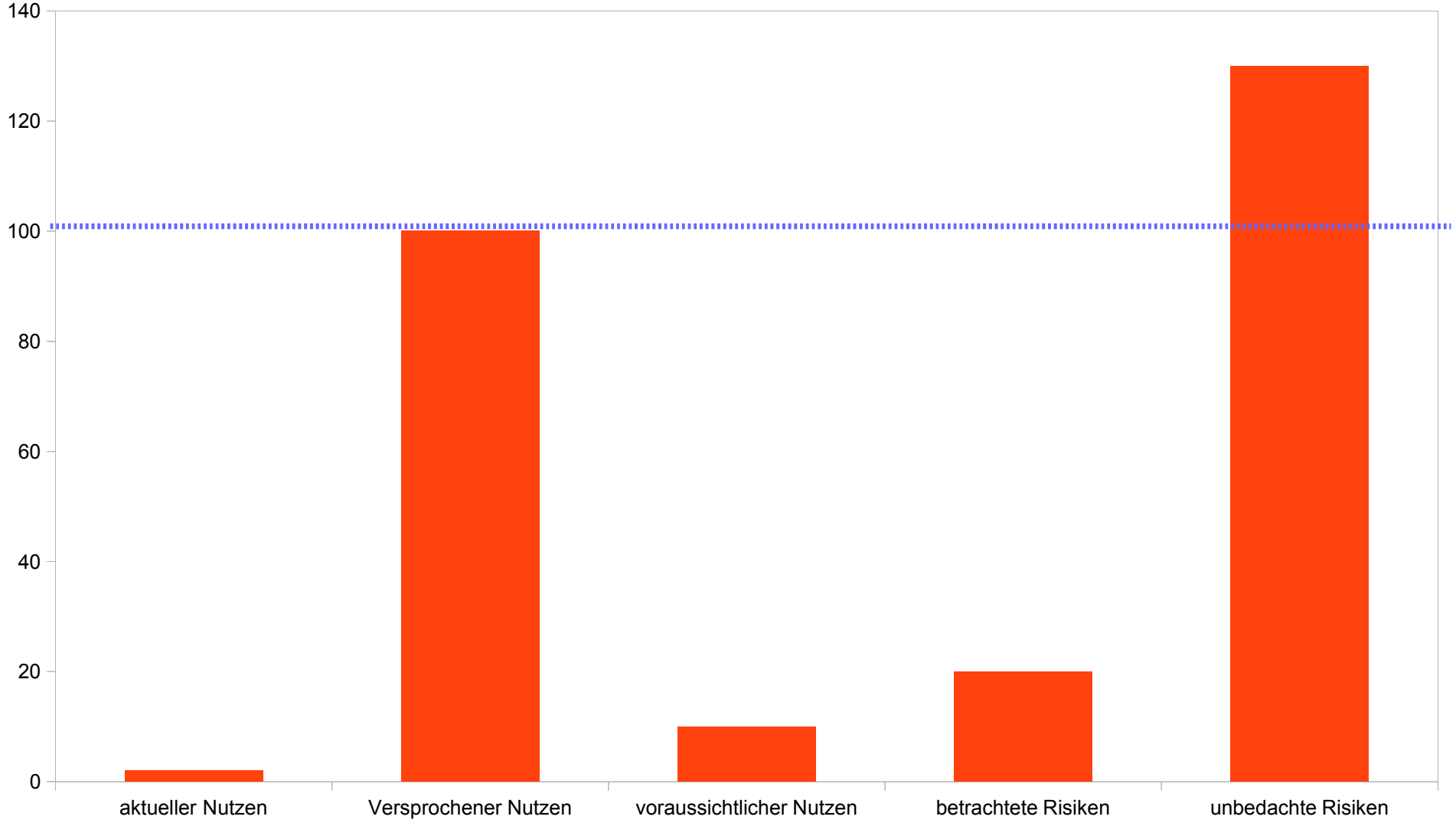
Nachteile:
- Große Informationsmenge evtl. unübersichtlicher
- Dokumente müssen ggf. alle gesichtet werden
- Es darf nicht von einer Vollständigkeit ausgegangen werden (Patientenhoheit)
- Dokumentation der für den Arzt zu dem Zeitpunkt einsehbaren Dokumente und Informationen

Probleme
- Einbindung in PVS noch nicht mal geplant
- Röntgenbilder nicht im DICOM-Format, nicht befundbar
- Laborwerte nicht sortierbar
- Keine Textsuche



https://www.kbv.de

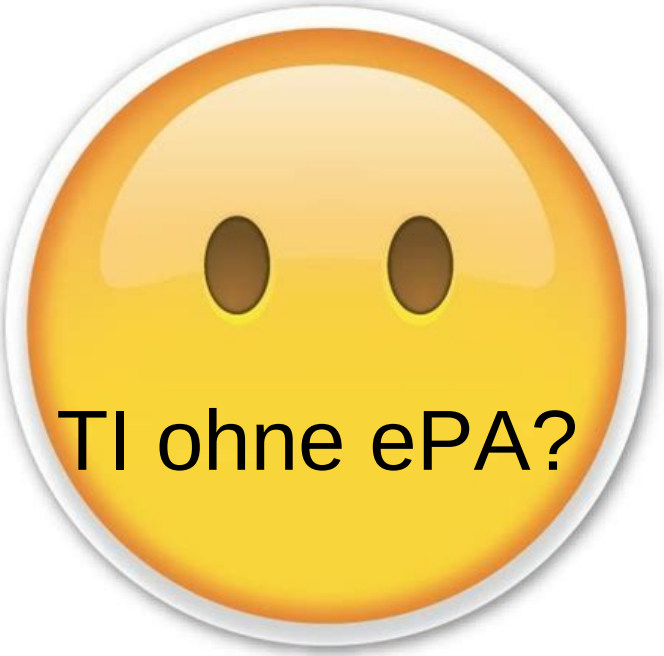
Aktueller Stand Telematik-Infrastruktur - Nützlichkeit



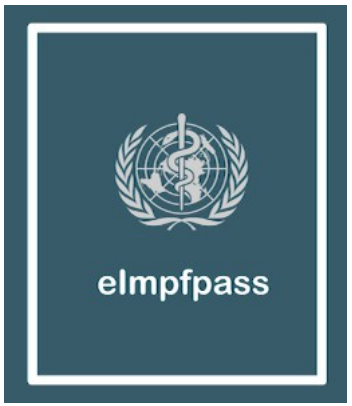
(eigene Schätzungen)

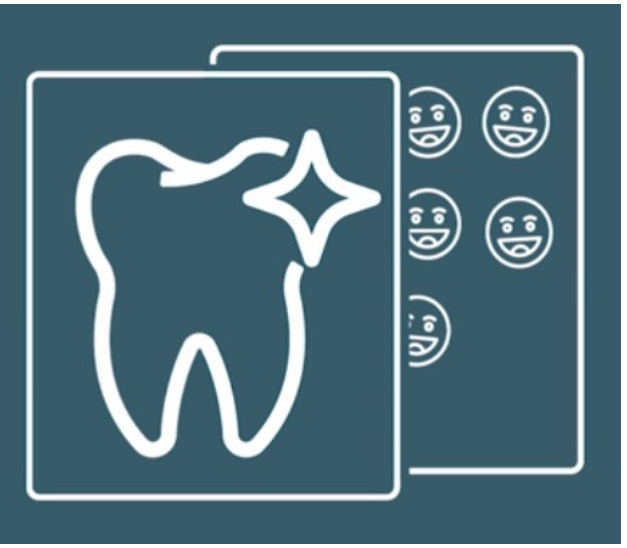
Feingranulares Rechtemanagement

http://www.umweltbundesamt.de/en/topics/waste-resources/product-stewardship-waste-management/plastics

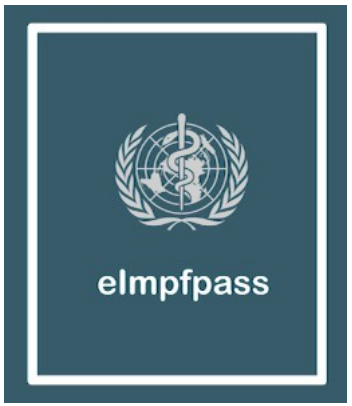


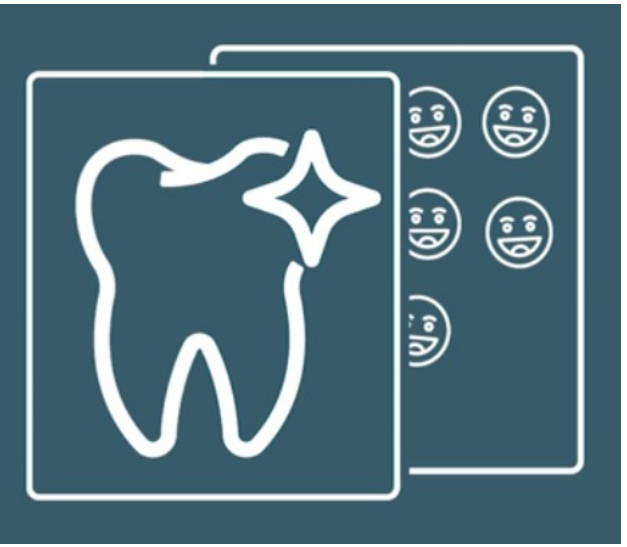
https://www.pinterest.de/pin/389983648963255778/





https://www.kbv.de/html/mio.php





https://www.kbv.de/html/mio.php

aok-bv.de

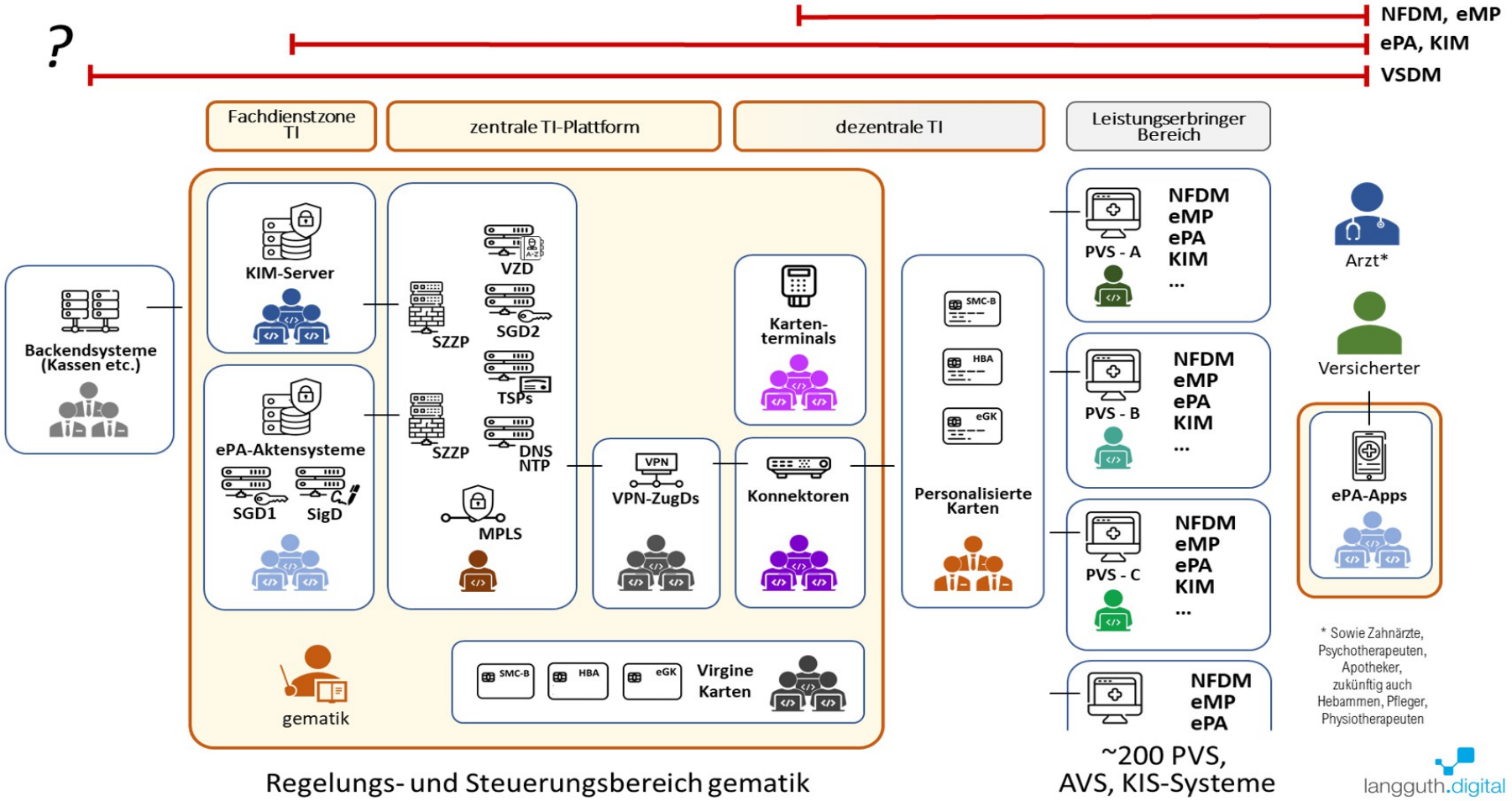
Kommunikation im Medizinwesen (KIM)

kv.dox der KBV erster und derzeit einziger angebotener (kostenpf lchtiger) Dienst

Was kommt danach?

https://www.youtube.com/watch?v=4fdCw_xSlMI

(Fehlende) Verantwortlichkeiten in der Telematik



https://de.linkedin.com/pulse/fehlende-verantwortlichkeiten-zur-ti-plattform-und-den-mark-langguth

(Fehlende) Verantwortlichkeiten in der Telematik

§307 PDSG: **"Die datenschutzrechtliche Verantwortlichkeit für die Datenverarbeitung in der Telematikinfrastruktur wird lückenlos gesetzlich geregelt ... "**

Referentenentwurf des BMG abgerufen 31.01.2020 „Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur“

… So „lückenlos“ dass es zu viele Überlappungen gibt...

…. statt individuell zurechenbare Verantwortung.

Foto: hersfelder-zeitung.de

https://de.linkedin.com/pulse/fehlende-verantwortlichkeiten-zur-ti-plattform-und-den-mark-langguth

(Fehlende) Verantwortlichkeiten in der Telematik

Im PDSG wird nun das BfArM als Anlaufstelle für Anregungen der Nutzer eingeführt,
das BfArM diesbezüglich bislang überhaupt nicht eingebunden.

Entwicklungszyklus 3-6 Jahre, evtl. etwas schneller. keine Prüfung und Verantwortlichkeiten, ob die Anpassungen dann die Probleme der Nutzer überhaupt lösen.

https://de.linkedin.com/pulse/fehlende-verantwortlichkeiten-zur-ti-plattform-und-den-mark-langguth

(Fehlende) Verantwortlichkeiten in der Telematik

Im PDSG wird nun das BfArM als Anlaufstelle für Anregungen der Nutzer eingeführt,
das BfArM diesbezüglich bislang überhaupt nicht eingebunden.

Entwicklungszyklus 3-6 Jahre, evtl. etwas schneller. keine Prüfung und Verantwortlichkeiten, ob die Anpassungen dann die Probleme der Nutzer überhaupt lösen.

https://de.linkedin.com/pulse/fehlende-verantwortlichkeiten-zur-ti-plattform-und-den-mark-langguth

IT-Sicherheit aktuell – ist digital wirklich immer besser?

Neue Verfahren müssen erst einmal insgesamt besser sein als die, die sie ersetzen (sollen).

Papier ist nicht unbedingt schlechter als eine digitale Lösung
insbesondere im Bereich Datensicherheit (Corona-Daten in Restaurants)
Und wenn es um Resilienz eines Systems geht.

Natürlich sollten wir Recycling-Papier verwenden ;)

Statements:

- Bei einer OP schneiden sie ja auch nicht erst rein und schauen dann was sie machen wollen.
- Bei Medikamenten wird auch erst untersucht, ob sie sicher sind und wirksamer als das existierende Verfahren.
- Integrität (und Authentizität) sind mindestens so wichtige Schutzziele wie die Verfügbarkeit.
- Wie bei Corona-App muss gesetzlich festgelegt werden, dass Patienten bei Nichtnutzung kein Nachteil entstehen darf
- Papier nicht unbedingt schlechter, neue Verfahren müssen erst einmal insgesamt besser sein als die, die sie ersetzen (sollen). Natürlich sollten wir Recycling-Papier verwenden ;)
  - Gute Behandlung kann man nicht erzwingen, genauso wenig gute Digitalisierung
  - TI-Vorfall Zertif kate: So als ob Geschäftsführer den Generalschlüssel für 1/3 der Räume am Uni-KLinikum Essen in der U-Bahn verlieren würde und 1/3 der Räume 6 Wochen lang zugesperrt blieben. Was würden sie mit dem Mitarbeiter machen?

TI ist nicht sehr resilient, wie wir gesehen haben

Digitalisierung kommt, geht gar nicht mehr anders Patienten können sie noch stoppen, indem sie die Dienste nicht nutzen. Ärzte sind leider so blöd, sich das aufdrücken zu lassen. Ärzte können dazu beitragen, indem sie die Patienten rückhaltlos aufklären

.

§307 PDSG: Datenschutzrechtliche Verantwortlichkeit – individuell zurechenbare Verantwortung statt „lückenloser Regelung“ = organisierter Verantwortungslosigkeit Love Parade Urteil

Statements:

Common Criteria kennen 7 Pru fniveaus (EAL = Evaluation Assurance Level)

EAL 7+ existiert ein einziges o ffentlich bekanntes Produkt

Pru fniveau EAL 4+ („methodisch entwickelt, getestet und durchgesehen“) digitale Fahrtenschreiber oder das Smart-Meter-Gateway

Die dezentralen TI-Komponenten – sowohl die derzeit verbauten Konnektoren und eKT, wie auch die na chste Generation – sind auf Pru ftiefe EAL 3+ zertif iziert. (also nur „methodisch getestet und u berpru ft“).

Ich halte fu r TI-Komponenten jedes Sorgfaltsniveau unterhalb EAL 6 (mit den richtigen „+“- Komponenten!) fu r vo llig indiskutabel.

Sicherheit

- Sicherheit bei TI, ePA und anderen Komponenten nicht mal anfänglich untersucht
- Sicherheit nicht von Anfang an eingef bssen, vor allem nicht Systemübergreifend
- Keine Notfallpläne, die das Vorgehen bei einem Angriff oder einem Datenleck beschreiben, Keine Pläne zur Schadensbegrenzung
- Datenschutzfolgeabschätzung wäre ein Anfang

Wer ein langfristig erfolgreiches System kreieren und betreiben möchte, kommt um Datenschutz und Datensicherheit nicht herum. Es geht dabei ganz basal um Vertrauen und niemand kauft oder benutzt ein IT-System dem er nicht vertrauen kann.

Die Risiken werden fast nie von denen ausgebadet, die sie eingeführt haben. Politiker sind abgewählt, Firmeninhaber und Leitungsebene sind schon lange in der Karibik, wenn so was raus kommt und justiziabel wird

Statements:

kein de-facto-Zwang zur Nutzung, weder für Ärzte noch für Patienten

Zwangslage der Kranken nicht ausnutzen um Daten abzupressen

wir sind nicht total dagegen, wollen aber dass es richtig gemacht wird

Übergreifende Sicherheitsbetrachtung, nicht nur Test der Einzelkomponenten

Nicht-Technikfolgen-Abschätzung – was wäre wenn man es nicht macht

lässt sich nicht durch Markt regeln weil Sicherheit ein Wettbewerbsnachteil ist

Gibt Produkte, die sind so gut, dass ich Geld dafür bezahlte. Gibt auch welche, die sind kostenlos und so gut, dass ich freiwillig dafür Spende.

O

Ansätze der Corona-Warn-app aufgreifen und für ein von Anfang an auf Sicherheit und Datensparsamkeit konzipiertes, vollständig transparentes System plädieren. Ein guter erster Schritt dazu war die Publikation der Spezif kationen der TI

Der CCC hat Ende 2019 beispielsweise aufgezeigt, dass ein wesentlicher Punkt, nämlich die Zuordnung einer Person zu einer digitalen Identität schwierig ist. Dazu zählt z.B. Die Zuordnung Patient – ePA/eGK und den damit verwalteten Daten, aber auch Arzt Arztausweis und den damit verbundenen Zugriffsmöglichkeiten. Das Problem wurde vom Gesetzgeber erkannt aber im PDSG letztlich nicht gelöst.

Die ePA und insbesondere die technischen Möglichkeiten, diese von Endgeräten aus zu bearbeiten, bieten natürlich eine deutlich vergrößerte Angriffsoberf äche und die Möglichkeit, solche Angriffe zu automatisieren und schlechtenstenfalls millionenfach durchzuführen

Fragen an das Publikum:

Konnektor- update schon gemacht?
Erfahrungen damit? Gehen die mobilen Lesegeräte noch?

Was wäre wenn plötzlich alle Arztdaten weg wären, sind sie drauf vorbereitet?

Was wenn jemand drohen würde, die Daten auf Ihrem Rechner zu veröffentlichen?

Wer würde für wie viel € einen USB-Stick in einen Klinikrechner stecken?