TEMET
end-to-end IT security

EPD Bedrohungs- und Risikoanalyse

eHealth Forum Schweiz
10./11. März 2016

Thomas Kessler
Dipl. Physiker ETH
Gründer und Geschäftsführer TEMET AG

Einleitung
Mandat Temet - Ausgangslage

- Gemäss Botschaft zum EPDG ist es erforderlich, dass schweizweit einheitliche Regeln im Bereich des Datenschutzes und der Datensicherheit definiert werden.
- Für die Festlegung der Zertifizierungsvoraussetzungen ist eine Bestandsaufnahme möglicher Bedrohungen, eine Analyse der betroffenen IT-Systeme sowie des potentiellen Schadens unabdingbar.
- Als ein Input für die Festlegung der Zertifizierungskriterien in Bezug auf den Datenschutz und die Datensicherheit soll eine Bedrohungs- und Risikoanalyse für die wesentlichen Elemente der Informatikinfrastruktur von Gemeinschaften, Stammgemeinschaften und Zugangsportalen durchgeführt werden.

Ziele des Referats

- Unabhängige Expertensicht auf das Thema
- Ein Blick durch die Security-Brille
- Hinweise auf potentielle Schwachstellen
- Respekt gegenüber den Gefahren des Internet
- Verständnis für Sicherheitsvorkehrungen
- Besondere Obacht beim EPD (Awareness)

Keine Ziele sind:

- Panikmache
- Leere Versprechungen / rundum sorglos Lösung
- Technische Details

Angaben zum Referenten Thomas Kessler

- Dipl. Physiker ETH, MAS ZFH in BA
- 25 Jahre Tätigkeit in der Informationssicherheit
  - 6 Jahre Fachstelle IT-Security bei einer Grossbank
  - 3 Jahre Leiter Security Engineering bei einem Finanzdienstleister
  - 16 Jahre IT-Security Beratung bei Finanzinstituten und Verwaltung
- Geschäftsführender Partner TEMET AG
  - Firmengründung im 2010
- Persönliche Schwerpunkte
  - IT-Sicherheitsarchitektur
  - 2-Faktor Authentisierung
  - Identity and Access Management (IAM)

Wer ist TEMET AG
Eckdaten

Gründung: März 2010

Inhabergeführte Aktiengesellschaft

Sitz am Basteiplatz 5, im Herzen von Zürich

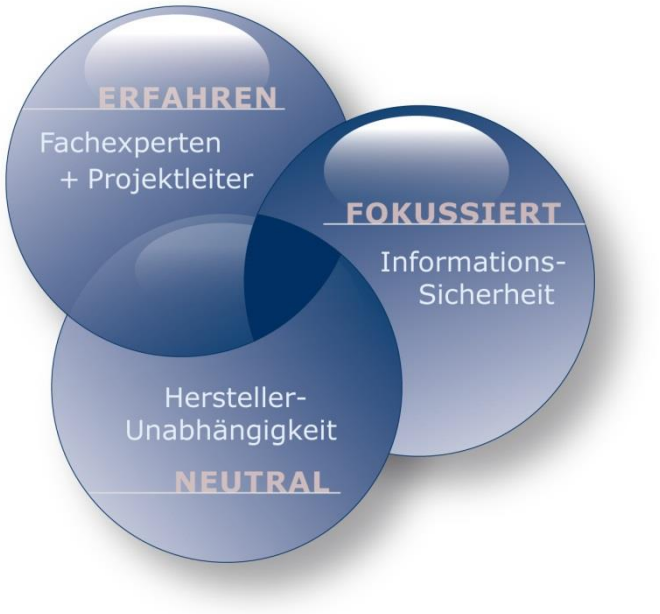
Aktuell 12 Information Security Consultants

Aktuell 56 Kunden aus Finanz, Verwaltung und Gesundheitswesen

Wir planen, konzipieren und realisieren Projekte im Bereich der Informationssicherheit

Wer ist TEMET AG
Alleinstellungsmerkmale

Die TEMET AG positioniert sich im Markt als herstellerneutrale und auf Informationssicherheit fokussierte Firma, deren Berater fachliche Expertise mit Projektmanagement-Kompetenz verbinden.



Agenda

- Einleitung
- Schutzobjekte / EPD «Big Picture»
- Bedrohungen und Schadenszenarien
- Schwachstellen und Risiken
- Massnahmen
- Restrisiken / Fazit

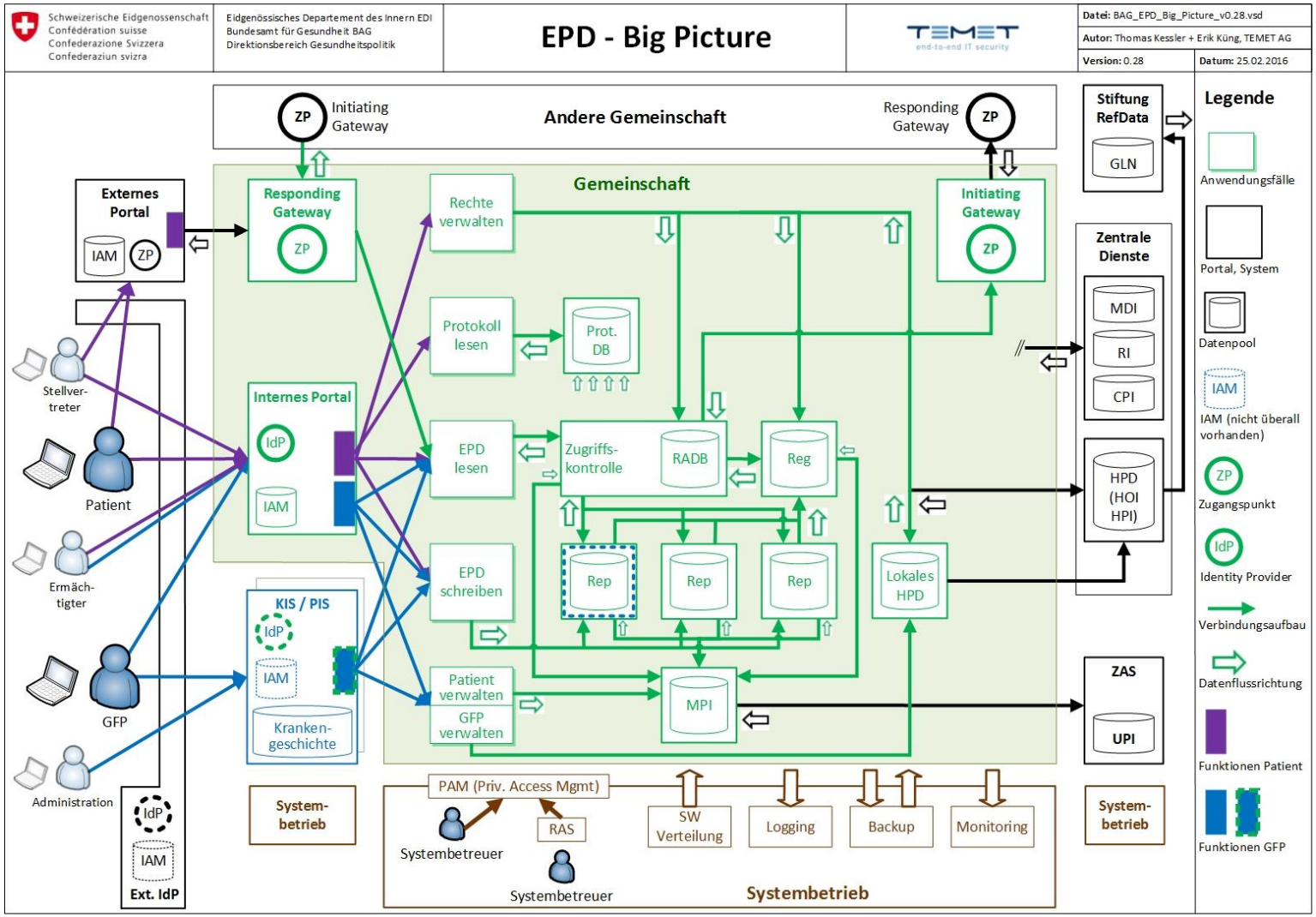
Schutzobjekte

- Daten mit ihrem Schutzbedarf
  - Applikation: DocRep, DocReg, Protokollierungsdatenbank
  - Infrastruktur: MPI, Portal IAM DB, HPD
- Benutzergruppen
  - Applikation: Patienten, GFP
  - Infrastruktur: Administrative Teilnehmer, Administration HPD
- Anwendungsfälle
  - Applikation: EPD lesen und schreiben, Zugriffsprotokoll lesen
  - Infrastruktur: Rechte verwalten, Patienten und GFP verwalten
- Systemkomponenten und Schnittstellen
  - Komponenten einer Gemeinschaft
  - Umsysteme und Schnittstellen (auch organisatorisch)

Wichtigste Informationsquellen:

- Interviews mit verschiedenen Know How Trägern
- Botschaft zum Bundesgesetz über das elektronische Patientendossier
- eHealth Suisse Standard und Architektur Empfehlungen I,II,III,IV,V
- IHE IT Infrastructure Technical Framework

Das EPD «Big Picture»



Bedrohungen
Standard Katalog gemäss ISDS*

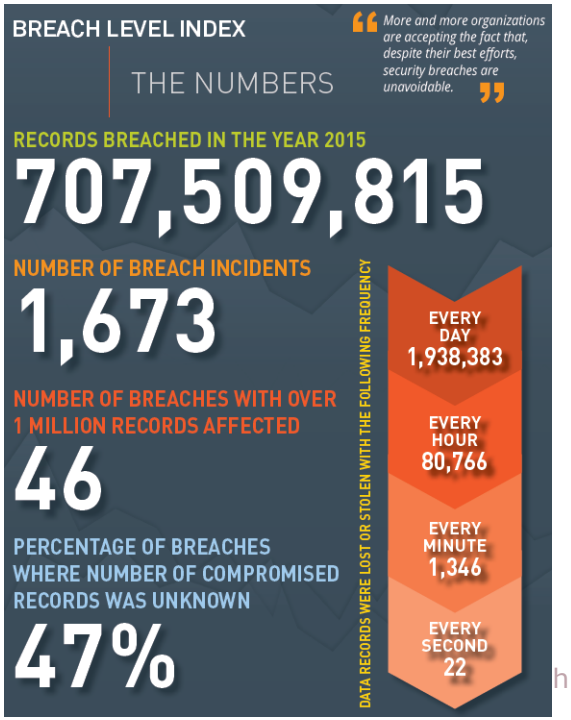
- Höhere Gewalt
- Organisatorische Mängel
- Menschliche Fehlhandlungen
- Technisches Versagen
- Vorsätzliche Handlungen

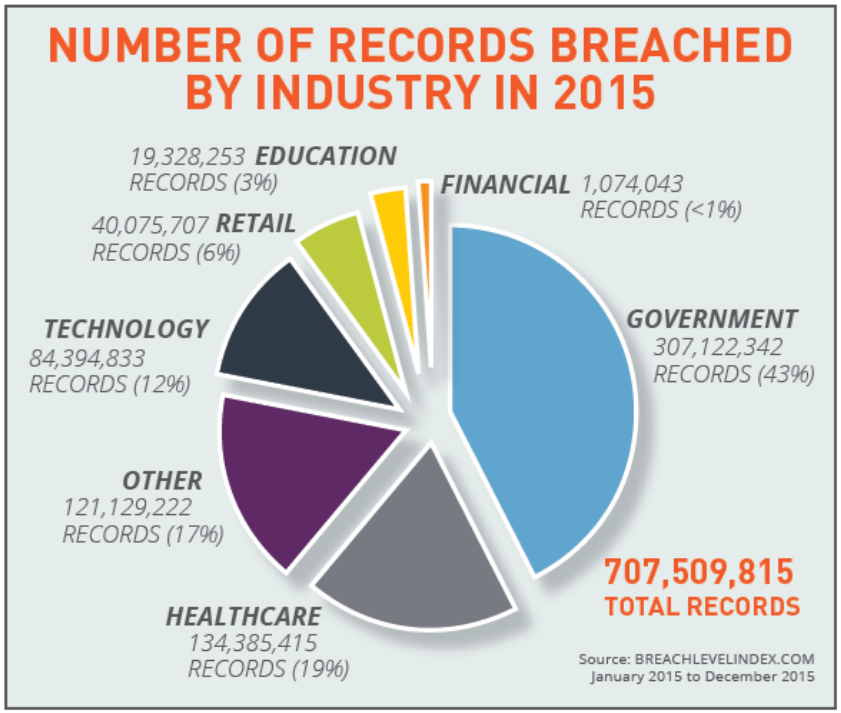
ISDS: Informationssicherheits- und Datenschutzkonzept gemäss HERMES Projektvorgehen

Bedrohungen
Gesundheitswesen ist ein Ziel

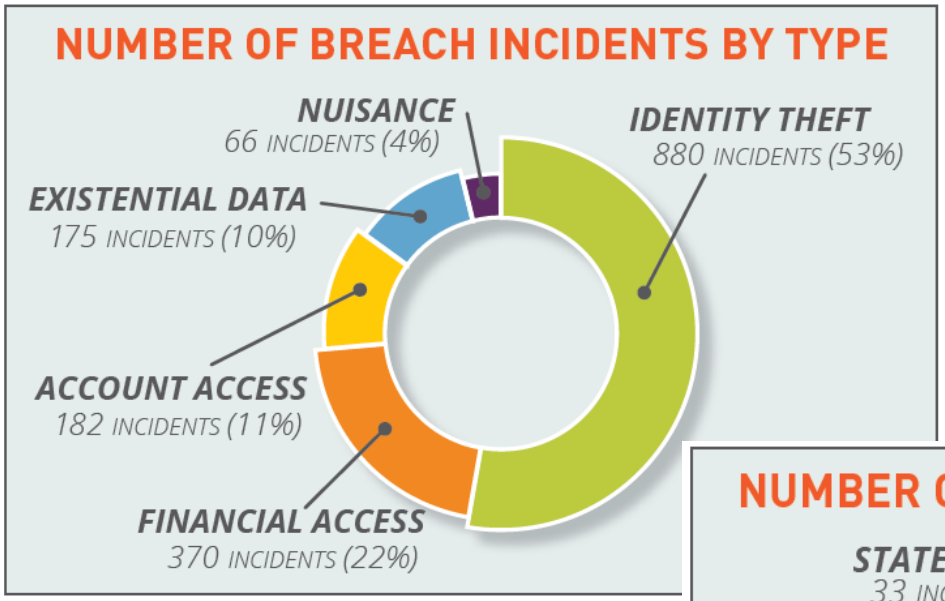
- 16.02.2016: Ransomware: Neben deutschen Krankenhäusern auch US-Klinik von Virus lahmgelegt
  «Verschlüsselt alle erreichbaren Daten...» «...mussten mehrere Operationen verschoben werden.»
  http://www.heise.de/security/meldung/Ransomware-Neben-deutschen-Krankenhaeusern-auch-US-Klinik-von-Virus-lahmgelegt-3103733.html

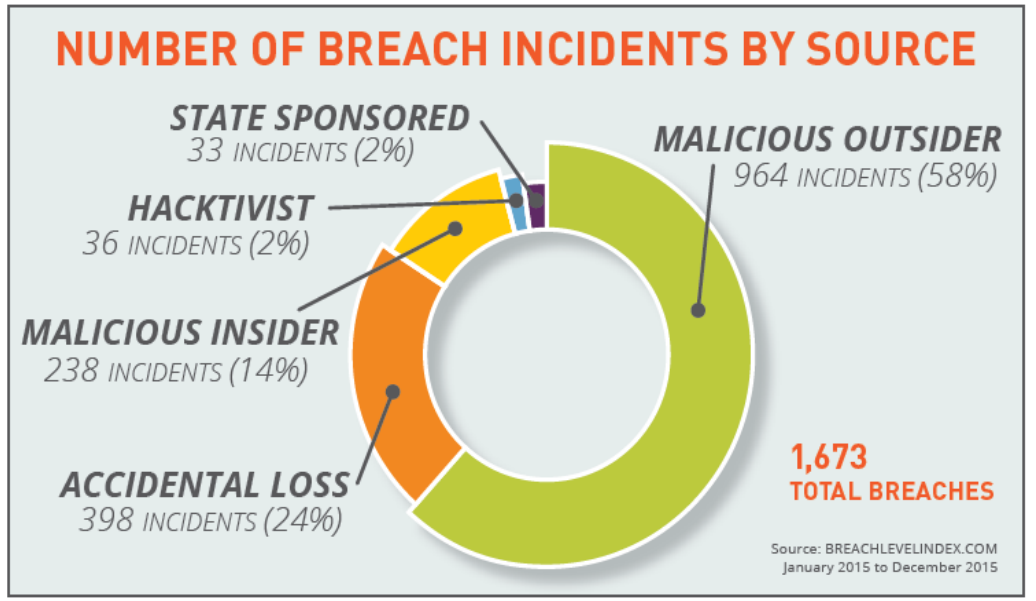
- 2015 Breach Level Index
  http://fr.sitestat.com/gemalto/gemalto/s?ent-Breach_Level_Index_Annual_Report_2015&ns_type=pdf





Bedrohungen
Typische Cyber Angriffe





Schadenszenarien
Was kann passieren?

Welcher Schaden entsteht bei Verlust von:

- Vertraulichkeit
- Integrität
- Verfügbarkeit (hier nur am Rande betrachtet)
- Nachvollziehbarkeit

Differenzierung in Abhängigkeit von:

- Art der Daten (nützlich/medizinisch/sensibel/geheim)
- Menge der Daten (einzelnes/viele/alle Dossiers)
- Art des Verlusts (zufällig oder gezielt & systematisch)

Schadenszenarien
Beispiele bzgl. Vertraulichkeit

Patientendaten werden durch Unberechtigte eingesehen bzw. kopiert und weitergegeben:

- Systematisch in grosser Menge über längere Zeit
- Durch unerkannte Dritte (z.B. Kriminelle)

⇨ Worst Case Szenario, Schadenstufe 4

- Gezielt auf Personen (z.B. PEP) oder sensible Dokumente
- Durch identifizierbare Systembenutzer (z.B. Patient, GFP)

⇨ Kritisch, Schadenstufe 3

- Zufällige einzelne Dossiers oder Dokumente (z.B. von mir)
- Durch unerkannte Dritte (z.B. Kriminelle)

⇨ Marginal, Schadenstufe 2

Schwachstellenanalyse

Wie kann das passieren?

Relevante Risiken entstehen dort, wo…

- eine allgemeine Bedrohung (z.B. Schadsoftware)…
- auf Grund einer Schwachstelle (z.B. GFP Endgerät)…
- zu einem Schadenszenario (z.B. unbemerkter Diebstahl von vielen Patientendossiers) führen kann.

Risiken
Beispiele («Top 5») 1/4

Übernahme der Kontrolle eines Endgerätes (PC, Tablet, Smartphone etc.) einer GFP durch unberechtigte Dritte

- Mit einem Trojanischen Pferd wird die Kontrolle über das Endgerät (PC, Laptop, Tablet, etc.) einer GFP übernommen, um gezielt alle Patientendossiers zu lesen, für welche diese GFP berechtigt ist (inkl. Notfallzugriff)

Übernahme der Identität einer GFP bei der Anmeldung am internen Portal (oder am KIS/PIS)

- Ein Hacker stiehlt mittels Phishing die Login Daten einer hoch berechtigten GFP und benutzt diese, um über das interne Portal auf alle Dossiers zuzugreifen, für welche diese GFP berechtigt ist.
- Er kann über den Notfallzugriff gezielt auf beliebige Dossiers (auch anderer Gemeinschaften) zugreifen

Risiken
Beispiele («Top 5») 2/4

Schwachstelle im internen Portal

- Ein Hacker dringt über eine Schwachstelle in das interne Portal ein, gelangt von dort auf weitere Systeme und kann auf einzelne oder alle Dossiers der Gemeinschaft zugreifen

Mangelhafte Sicherheitsorganisation

- Unklare Verantwortlichkeiten innerhalb der Gemeinschaft führen dazu, dass dringende Entscheide (z.B. Bewertung und Bearbeitung aktueller Schwachstellen, bis hin zur Notabschaltung) nicht zeitgerecht gefällt werden

Risiken
Beispiele («Top 5») 3/4

Betrügerischer System-Administrator

- Ein betrügerischer System-Administrator kopiert alle Patientendossiers einer von ihm betreuten Gemeinschaft und verkauft diese an den Meistbietenden
- Dies kann auch ein Dritter sein, der sich unberechtigten Zugang zur Betriebsumgebung verschafft

Mutation des Anstellungsverhältnisses einer GFP wird nicht konsequent nachgeführt («Mover» Prozess)

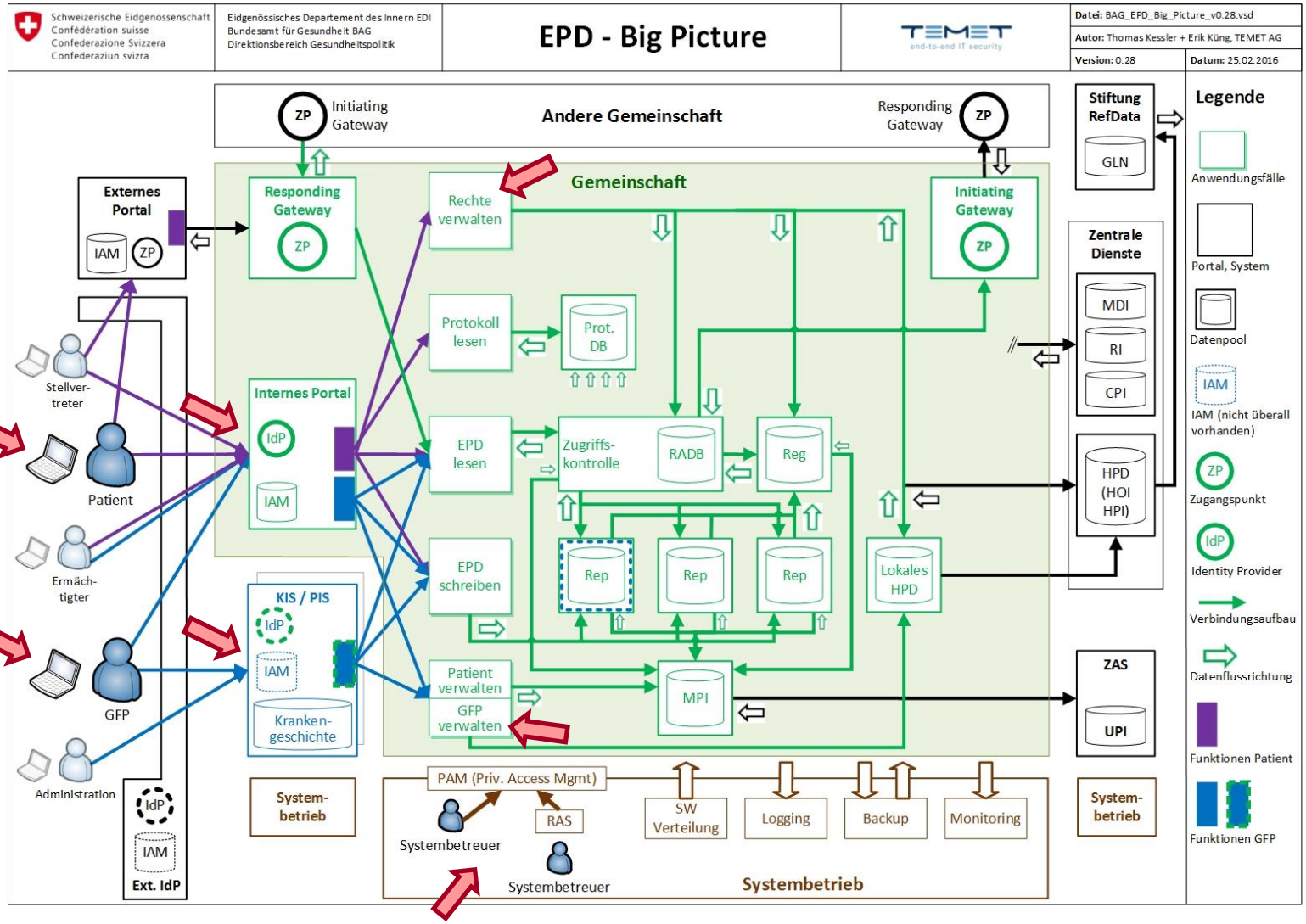
- Ein Assistenzarzt wird nach Beendigung eines Stage in der psychiatrischen Abteilung nicht aus der entsprechenden Gruppe im HPD gelöscht. Nach dem Stage behält er den Zugriff auf alle Patientendossiers, die für diese Abteilung freigegeben sind, auch wenn er in anderen Abteilungen des Spitals tätig ist

Risiken
Beispiele («Top 5») 4/4

Nachlässige Berechtigungsadministration

- Nachlässige Berechtigungsadministration seitens eines Patienten oder eines von ihm Ermächtigten führt dazu, dass sensible Daten von GFP eingesehen werden, die dazu aus Sicht des Patienten gar nicht befugt wären

Verortung im Big Picture



Massnahmenkatalog

Was kann man dagegen tun?

- Organisatorische Sicherheitsmassnahmen
- Applikatorische Sicherheitsmassnahmen
- Technische Sicherheitsmassnahmen

Massnahmen
Beispiele Organisation

Jede Gemeinschaft betreibt ein Information Security Management System (ISMS)

- Umfassend insb. die Nominierung eines Informations-sicherheits-Beauftragten (ISBO) für die Gemeinschaft

Jede Gemeinschaft betreibt ein Security Information and Event Management (SIEM)

- Dieses erkennt Anomalien im System wie Angriffe aus dem Internet oder eine unübliche Häufung von Zugriffen
- Das SIEM umfasst Prozesse für den Umgang mit Sicherheitsereignissen bis hin zur Notabschaltung

Massnahmen
Beispiele Applikation

Patienten und (noch wichtiger!) GFP werden vor dem Zugriff auf das EPD mit mind. zwei Faktoren aus den Kategorien „Wissen", „Haben" oder „Sein" authentisiert

- Diese 2-Faktor Authentisierung gilt für alle Zugriffspfade

Zusätzliche Identifikation der GFP beim Notfallzugriff

- z.B. «Transaktionsbestätigung» wie im e-Banking

Verschlüsselung aller im EPD abgelegten Daten

- Vorzugsweise auf Ebene der Applikation, damit auch unberechtigte technische Zugriffe verhindert werden

Massnahmen
Beispiele Technik

Der EPD Vertrauensraum wird durch gegenseitige Authentisierung und Verschlüsselung aller Kommunikationsverbindungen logisch vom Internet isoliert

- Technische Umsetzung gemäss IHE:ATNA Profil

Alle aus dem Internet erreichbaren Systeme (insb. das Portal) sind gegen Angriffe aus dem Internet geschützt

- Schwachstellenüberprüfung durch hierauf spezialisierte unabhängige Stellen («Penetration Testing»)

Der Systembetreiber muss die Einhaltung der für das EPD besonders relevanten Kontrollen nachweisen

- Gemäss ISO/IEC 27002:2013 resp. ISO/IEC 27799:2014

Restrisiken

Trotz aller Massnahmen wird es nicht gelingen, jede unberechtigte Einsicht in das EPD von Patienten und Patientinnen auf Dauer zu verhindern

- Dies ist (leider) ein Erfahrungswert

Als typische Ursachen dafür sind zu erwarten:

- Missbrauch unsicherer Endgeräte von Patienten und GFP
- Nachlässige Rechteverwaltung seitens Patienten und GFP
- Datendiebstahl durch Insider oder Hacker
- Erfolgreiche Angriffe aus dem Internet auf Portale

Fazit

Prävention ist wichtig aber nicht ausreichend

Für die Begrenzung der Restrisiken muss - ergänzend zur Prävention - eine zeitnahe Erkennung und Behandlung von Sicherheitsvorfällen sichergestellt sein.

- Auch die Informationssicherheit benötigt heute (leider) nicht nur Schloss und Riegel sondern auch eine Alarmanlage, Polizei und Feuerwehr

Allerdings: Niemand trägt all sein Hab und Gut ständig mit sich herum oder verzichtet auf Urlaub, nur weil Einbrüche vorkommen:

- Man schliesst einfach die Haustür und die Fenster!

Besten Dank für Ihre Aufmerksamkeit!

TEMET AG | Basteiplatz 5 | CH-8001 Zürich
044 302 24 42 | info@temet.ch | www.temet.ch