Das Forum für ICT im Gesundheitswesen
Le forum pour les TIC dans le système de santé

@eHealthSummit
@read42news
www.ehealthsummit.ch

SWISS eHEALTH SUMMIT 2017 HIMSS Europe

SGMI SSIM SSMI
Schweizerische Gesellschaft für Medizinische Informatik
Société Suisse d'Informatique Médicale
Società Svizzera d'Informatica Medica
Swiss Society for Medical Informatics

SwissTech Convention Center, Lausanne
21.-22. September 2017

Sicherheitsthemen bei der EPD Anbindung

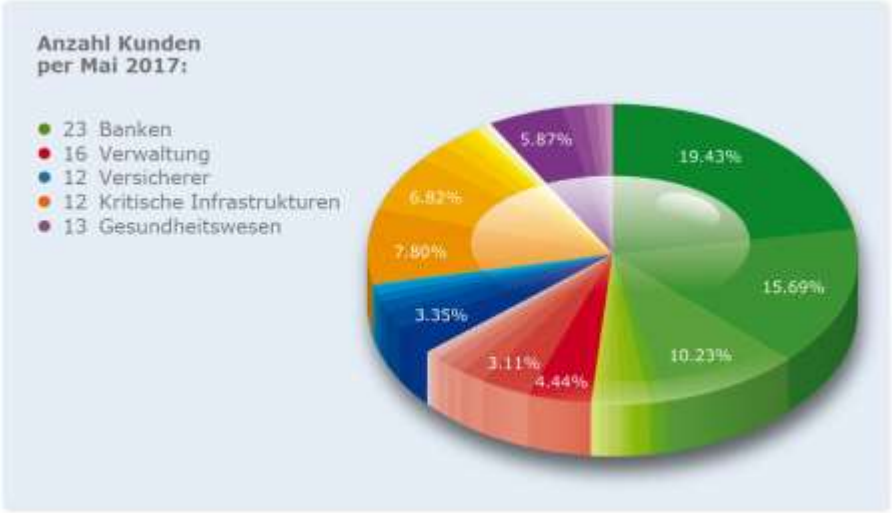
Thomas Kessler, Dipl. Physiker ETH, Geschäftsführer TEMET AG
@ Speaker twitter handle

In cooperation with

ehealthsuisse
IHE SUISSE Integrating the Healthcare Enterprise
pharmaSuisse
VGIch
HIMSS CHiME INTERNATIONAL

ANGABEN ZU THOMAS KESSLER UND ZUR TEMET AG

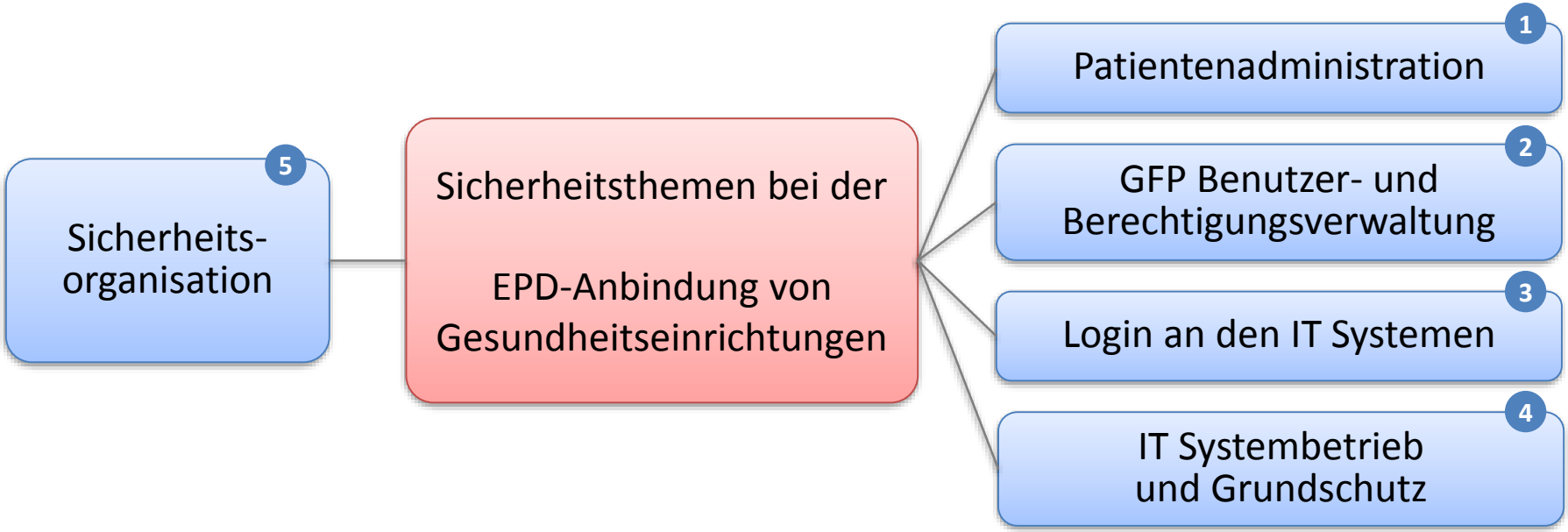
- Dipl. Physiker ETH, MAS in BA
- 26 Jahre Tätigkeit in der Informationssicherheit
  - Banken, Behörden und Gesundheitswesen
  - Schwerpunkte Sicherheitsarchitektur, Sicherheitsorganisation, IAM
- Gründer und geschäftsführender Partner TEMET AG



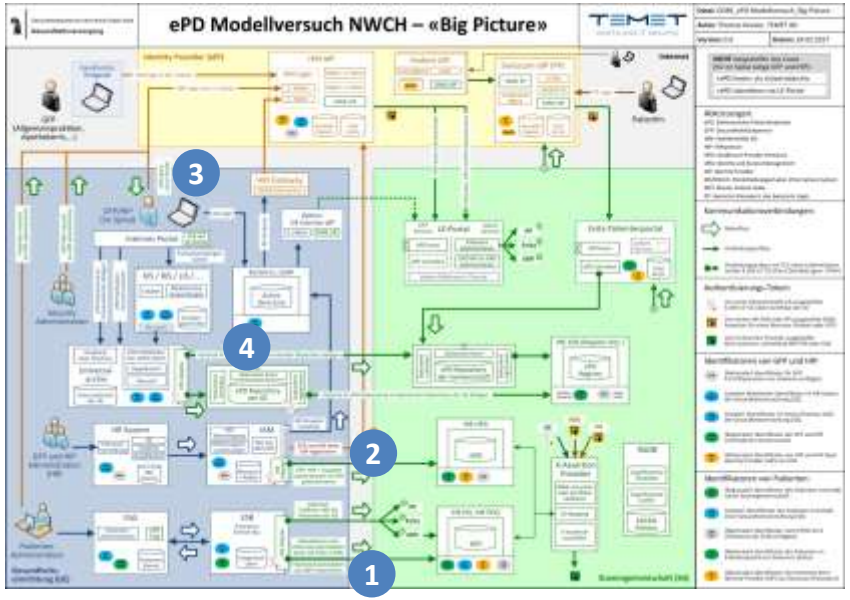
ERFAHRUNG IN BEZUG AUF INFORMATIONSSICHERHEIT IM EPD

- «Bedrohungs- und Risikoanalyse Elektronisches Patientendossier» (BAG, 2015)
- Analyse «Isolationsvarianten für EPD Repositories» (BAG, 2016)
- Teilnahme an den TOZ EPDG-Workshops zu «Datenschutz und Datensicherheit» (BAG, 2016)
- «AKV und Risiko Ownership für Informationssicherheit» (EPD Modellversuch NWCH, 2017)
- «mHealth & eHealth Sicherheits-architektur» (Spital, 2017)
- «Role-based Access Control PoC» (Spital, 2016/2017)

EPD SICHERHEIT: BETROFFENE BEREICHE BEI DEN GE (1)



EPD SICHERHEIT: BETROFFENE BEREICHE BEI DEN GE (2)



1. Patientenadministration
2. GFP Benutzer- und Berechtigungsverwaltung
3. Login an den IT Systemen
4. IT Systembetrieb und Grundschutz

1 PATIENTENADMINISTRATION

Themen

- Abgleich zwischen PAS, MPI, Patientenportal und IdP
- EPD Onboarding Prozess
  - Identifizieren
  - Einwilligung einholen
  - Registrieren (diverse Verzeichnisse)
  - ID-Mittel ausstellen
- Schulung und Support
  - Informationelle Selbstbestimmung
  - Berechtigungsverwaltung

Herausforderungen und Fragestellungen

- Prozessdefinition und Aufgabenverteilung zwischen Spitälern, EPD Plattformbetreiber und Identity Providern (IdP) — Org
- Kompromiss zwischen Effizienz, Benutzerfreundlichkeit und Sicherheit — Org
- Bidirektionale Anbindung des PAS an den MPI der Gemeinschaft — Tech

2 GFP BENUTZER- UND BERECHTIGUNGSVERWALTUNG

Themen

- Abgleich zwischen HR, HPD, GFP-Portal und IdP
- EPD Zugang von GFP verwalten
  - EPD Zugang autorisieren
  - (Identifizieren)
  - (Qualifikation prüfen)
  - Registrieren (diverse Verzeichnisse)
  - ID-Mittel ausstellen
  - GFP Gruppen zuteilen

Herausforderungen und Fragestellungen

- Prozessdefinition und Aufgabenverteilung zwischen Spitälern, EPD Plattformbetreiber und Identity Provider (IdP) — Org
- Verwaltung von GFP Gruppen, insb. laufende Aktualisierung der Gruppenzuteilungen — Org
- (Bidirektionale) Anbindung des HR an das HPD (via Spital IAM) — Tech

3 LOGIN AN DEN IT SYSTEMEN

Themen

- Einbindung des EPD Login in die Spital-interne (SSO) Lösung
- «Starke» Authentifizierung mit zwei Faktoren beim EPD Login
  - Prüfen der Endgeräte-Sicherheit
  - Prüfen 1. Faktor (Passwort)
  - Prüfen 2. Faktor (z.B. Einmalpasswort)
  - Weiterleitung an GFP Portal

Herausforderungen und Fragestellungen

- Nutzung internes Passwort als erster Faktor des EPD Login — Policy
- Nutzung EPD ID-Mittel für interne starke Authentifizierung — Tech
- Kontext-abhängige EPD Zugriffskontrolle: «Must» oder «No Go»? — Policy

Fragestellung zur Kontext-abhängigen EPD Zugriffskontrolle: Kann eine am Spital angestellte GFP diejenigen EPD-Zugriffsrechte, die sie über eine Gruppenzugehörigkeit erhalten hat (z.B. Tätigkeit in einer spezifischen Klinik), nur am entsprechenden Spital-Arbeitsplatz ausüben oder auch in der eigenen (evt. weniger gut gesicherten) Praxis sowie während eines Einsatzes in einer anderen Klinik?

4 IT SYSTEMBETRIEB UND GRUNDSCHUTZ

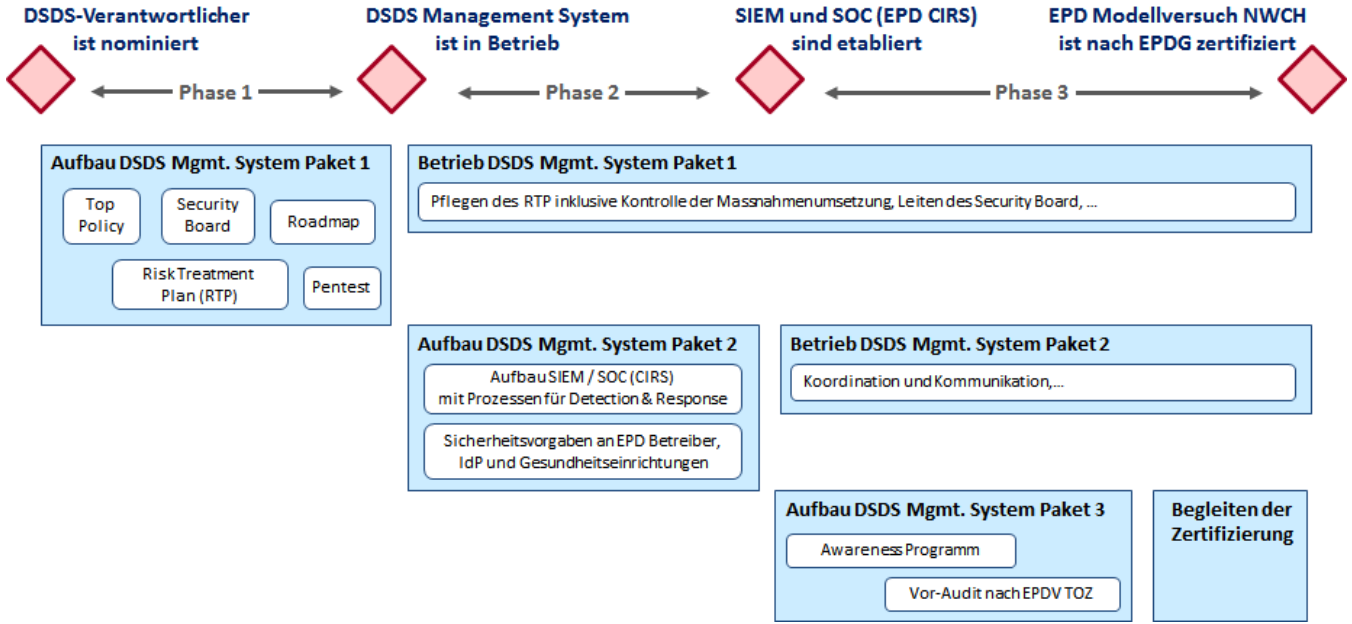
Themen

- EPDG, EPDV und TOZ Vorgaben gelten für alle Systeme innerhalb des EPD Vertrauensraums
- Massnahmenbereiche:
  - Identify (Planung und Steuerung)
  - Protect (Prävention)
  - Detect (Detektion)
  - Respond (Behandlung)
  - Recover (Verbesserung)

Herausforderungen und Fragestellungen

- Sicherheit der internen Endgeräte mit EPD Zugang — Tech
- Sicherheit der allfälligen lokalen EPD Repositories (insb. Verschlüsselung) — Tech
- Sicherheit der Schnittstellen (IHE Adapter) — Tech

5 SICHERHEITSORGANISATION: VORGEHENSVORSCHLAG



DSDS MS:
Management System für Datenschutz und Datensicherheit

SIEM:
Security Information and Event Mgmt.

SOC:
Security Operations Center

CIRS:
Critical Incident Reporting System

SCHLUSSWORT: RISIKEN UND CHANCEN

Risiken

- Die Lernkurve für den sicheren Betrieb von Internetanwendungen wird eventuell unterschätzt.
- Auf (leider unvermeidbare) Sicherheitsvorfälle wird möglicherweise überreagiert.
- Perfektionistische Regulierung könnte praktikable Lösungen und Prozesse verhindern.

Chancen

- Das Gesundheitswesen erlebt einen mit dem Online Banking vergleichbaren Innovationsschub.
- Der Digitalisierungsschub wird von einem Sicherheitsgewinn für die gesamte Branche begleitet.
- Die Umsetzung des EPDG bringt neue innovative Lösungen hervor
  - z.B.: IdP-Verbund mit Schweizer Banken

ANHANG: TEMET CYBERSECURITY BIG PICTURE