DMEA Berlin
9.–11. April 2019
Connecting Digital Health

DEN VERNETZTEN PATIENTEN AUF DEM RADAR BEHALTEN

IT-Sicherheit nach KRITIS im hochautomatisierten Klinikumfeld

Torben Klagge, Manager IT-Security, Sopra Steria Consulting

sopra steria
CONSULTING

AGENDA

1 | Kurzvorstellung Referent & Sopra Steria Consulting

2 | KRITIS@SopraSteria

3 | KRITIS@Health

„Spezialitäten“ des Gesundheitssektors
„Spannendes“ aus unseren Projekten

4 | Ansätze & Lösungen aus unseren Projekten

5 | Resümee

1| KURZVORSTELLUNG

Referent & Sopra Steria Consulting

Manager IT-Security

> 8 Jahre IT-Security

Abschlüsse:

- M.Sc. Computer Security
- Dipl.-Ing. (FH) Elektrotechnik

Kompetenzen:

- Pentest & Forensik
- Architekturanalysen
- Zertifizierter GICSP (Global Industrial Cyber Security Professional)
- Zertifizierter GPEN (GIAC Pentester)
- Sicherheit in industriellen Netzwerken

Aktuelle Publikationen:

- Krankenhaustechnik & Management 2017/11: „Besorgniserregendes Bettgeflüster“
- Management-Kompass 2/2017: „Kritische Infrastrukturen – Mehr Security statt nur Safety“
- Management & Krankenhaus (21.09.2016): „Kliniken als Teil kritischer Infrastrukturen“
- KES 1/2016: „Sicherheit für industrielle IT: Penetrationstests in industriellen Umgebungen“

Relevante Projekte (Auszug):

- Projektleiter: Einführung eines ISMS nach ISO 27001 und IT-Sicherheitsgesetz bei einem Universitätsklinikum in München
- Projektleiter: Einführung eines ISMS nach ISO 27001 und IT-Sicherheitsgesetz bei einem Klinikum in NRW
- Projektleiter: Einführung eines ISMS nach ISO 27001 und IT-Sicherheitsgesetz bei zwei Universitätskliniken in NRW
- ICS-Spezialist, ISMS-Consultant: Pre-Check KRITIS mehrere (Uni-)Kliniken
- Projektleiter, ICS-Spezialist: Div. Security-Projekte bei der Airbus Operations GmbH
- Teilprojektleiter, ICS-Spezialist: Einführung ISMS und Beispielaudit IT-Sicherheitskatalog BNetzA bei einem Versorgungsnetzbetreiber [NDA-Projekt]
- Teilprojektleiter, ICS-Spezialist, ISMS-Consultant: Architekturanalyse, Erstellung Netzstrukturplan nach BNetzA-Vorgaben und Scope-Definition bei einem Übertragungsnetzbetreiber [NDA-Projekt]
- Projektleiter, Pentester, ICS-Spezialist: Technischer Penetrationstest auf Medizintechnik eines Krankenhausverbundes [NDA-Projekt]

KURZVORSTELLUNG SOPRA STERIA CONSULTING

2| KRITIS @ SOPRA STERIA CONSULTING

KRITIS @ SOPRA STERIA CONSULTING
DEUTSCHLANDWEIT IN MEHREREN SEKTOREN

- KRITIS@Health
  - Aktuell laufende Projekte
    - 3 Unikliniken
    - 1 Klinikum
    - 1 kommunaler Krankenhauskonzern
- KRITIS@Energy
  - Div. abgeschlossene KRITIS-Projekte mit erfolgreicher Auditierung/Zertifizierung
- KRITIS@Transport
  - Div. laufende Projekte

3| KRITIS@HEALTH

KRITIS@HEALTH
EINE SEHR KURZE EINFÜHRUNG

- Schwellwert gemäß IT-SiG für Kliniken
  - > 30.000 vollstationäre Fälle/Jahr
- Kritische Dienstleitung im Bereich der Kliniken
  - „Die stationäre Patientenversorgung“
- Zeitrahmen
  - Gesundheitssektor ist Teil des „2. Korbes“, Umsetzung daher bis Ende Juni 2019
- Vorgaben/Vorgehen im Klinikumfeld
  - ISMS nach ISO27001/27002, oder/und nach IT-Grundschutz (oder angelehnt)
  - B3S (Branchenspezifischer Sicherheitsstandard) für Kliniken, aktuell v1.0 (Anfang April 2019)
  - Aufbau auf & Beeinflussung durch:
    - ISO27799, ISO9001 (QM), RiKrIT (Risikoanalyse Krankenhaus IT), MPG, DIN EN 80001 (Risikomanagement bei vernetzter Medizintechnik), …

KRITIS@HEALTH
VORGEHEN IN UNSEREN KLINIK-PROJEKTEN

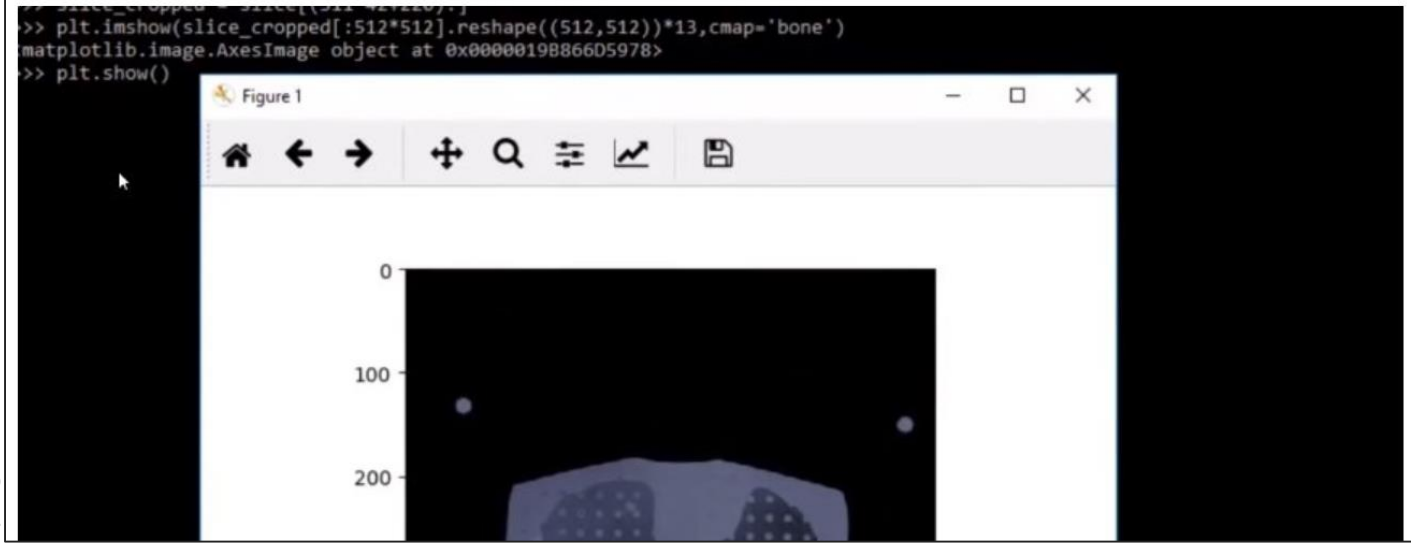
KRITIS@HEALTH
VORGEHEN IN UNSEREN KLINIK-PROJEKTEN

KRITIS@HEALTH
„SPEZIALITÄTEN“ IM KLINIKUMFELD

Simulation einer Cyberattacke im Krankenhaus

So manipulieren Forscher eine Krebsdiagnose

IT-Experten aus Israel haben eine Methode entwickelt, um Computertomografie-Scans zu fälschen. So können sie Krebs anzeigen, wo keiner ist - oder echte Krebszellen aus Bildern verschwinden lassen.



Spiegel Online, 04.04.2019

KRITIS@HEALTH
„SPEZIALITÄTEN“ IM KLINIKUMFELD

1 Medizintechnik vs. IT

2 Physische Sicherheit & physischer Zugriff auf IT im Krankenhaus

3 „Impact“: Safety vs. Security

KRITIS@HEALTH
„SPEZIALITÄTEN“ IM KLINIKUMFELD

Medizintechnik vs. IT

- Medizintechnik eher „Ingenieursdomäne“

KRITIS@HEALTH
„SPEZIALITÄTEN“ IM KLINIKUMFELD

Medizintechnik vs. IT

- Medizintechnik eher „Ingenieursdomäne“
- Zur Einordnung der Mengenverhältnisse an einem typischen Uniklinikum:
  - Ca. 5.000 bis 10.000 „klassische“ IT-Geräte (Server, Clients)
  - Ca. 40.000 bis 60.000 Medizingeräte

KRITIS@HEALTH
„SPEZIALITÄTEN“ IM KLINIKUMFELD

Medizintechnik vs. IT

- Medizintechnik eher „Ingenieursdomäne“
- Zur Einordnung der Mengenverhältnisse an einem typischen Uniklinikum:
  - Ca. 5.000 bis 10.000 „klassische“ IT-Geräte (Server, Clients)
  - Ca. 40.000 bis 60.000 Medizingeräte
- Viele Medizingeräte liegen (herstellerseitig) z.T. Jahre hinter aktuellen IT-Standards
  - Viele Medizingeräte haben „irgendwann mal einen Netzwerkanschluss dazu bekommen“
  - Z.T. Verlust der Zertifizierung nach Medizinproduktegesetz bei (Software-)-Änderung
  - Z.T. sehr minimale IT-Dokumentation der Hersteller

KRITIS@HEALTH
„SPEZIALITÄTEN“ IM KLINIKUMFELD

Medizintechnik vs. IT

- Medizintechnik eher „Ingenieursdomäne“
- Zur Einordnung der Mengenverhältnisse an einem typischen Uniklinikum:
  - Ca. 5.000 bis 10.000 „klassische“ IT-Geräte (Server, Clients)
  - Ca. 40.000 bis 60.000 Medizingeräte
- Viele Medizingeräte liegen (herstellerseitig) z.T. Jahre hinter aktuellen IT-Standards
  - Viele Medizingeräte haben „irgendwann mal einen Netzwerkanschluss dazu bekommen“
  - Z.T. Verlust der Zertifizierung nach Medizinproduktegesetz bei (Software-)-Änderung
  - Z.T. sehr minimale IT-Dokumentation der Hersteller
- **Konsequenz**:
  - *Viele Vorgaben, IT-Standardisierungen, aktuelle IT-Sicherheitsmaßnahmen etc. sind in der Medizintechnik nur rudimentär vorhanden bzw. können technisch gar nicht umgesetzt werden*

KRITIS@HEALTH
„SPEZIALITÄTEN“ IM KLINIKUMFELD

Physische Sicherheit & physischer Zugriff auf IT im Krankenhaus

- „Offene Türen überall“

KRITIS@HEALTH
„SPEZIALITÄTEN“ IM KLINIKUMFELD

Physische Sicherheit & physischer Zugriff auf IT im Krankenhaus

- „Offene Türen überall“
- Klassisches Unternehmen (und auch die meisten anderen KRITIS-Sektoren):
  - Dedizierter Besucherbereich mit Pförtner o.ä.
  - Nur in diesem Bereich kann physisch auf z.B. Netzwerkanschlüsse und Geräte zugegriffen werden

KRITIS@HEALTH
„SPEZIALITÄTEN“ IM KLINIKUMFELD

Physische Sicherheit & physischer Zugriff auf IT im Krankenhaus

- „Offene Türen überall“
- Klassisches Unternehmen (und auch die meisten anderen KRITIS-Sektoren):
  - Dedizierter Besucherbereich mit Pförtner o.ä.
  - Nur in diesem Bereich kann physisch auf z.B. Netzwerkanschlüsse und Geräte zugegriffen werden
- Klinikum:
  - Besucher und Patienten quasi überall
  - Direkter physischer Zugriff auf Geräte & Netzwerkanschlüsse, z.B. im Patientenzimmer

KRITIS@HEALTH
„SPEZIALITÄTEN“ IM KLINIKUMFELD

Physische Sicherheit & physischer Zugriff auf IT im Krankenhaus

- „Offene Türen überall“
- Klassisches Unternehmen (und auch die meisten anderen KRITIS-Sektoren):
  - Dedizierter Besucherbereich mit Pförtner o.ä.
  - Nur in diesem Bereich kann physisch auf z.B. Netzwerkanschlüsse und Geräte zugegriffen werden
- Klinikum:
  - Besucher und Patienten quasi überall
  - Direkter physischer Zugriff auf Geräte & Netzwerkanschlüsse, z.B. im Patientenzimmer
- **Konsequenz:**
  - *Die nach ISO27001 geforderte physische Sicherheit, Sicherheitsbereiche, Netzwerkzugangskontrollen etc. sind kaum wie sonst üblich realisierbar*

KRITIS@HEALTH
„SPEZIALITÄTEN“ IM KLINIKUMFELD

„Impact“: Safety vs. Security

KRITIS@HEALTH
„SPEZIALITÄTEN“ IM KLINIKUMFELD

„Impact“: Safety vs. Security

- (K)ein Zitat: *„Der Patient ist verstorben, da ich mein Passwort vergessen habe und daher das Beatmungsgerät nicht starten konnte.“*

KRITIS@HEALTH
„SPEZIALITÄTEN“ IM KLINIKUMFELD

„Impact“: Safety vs. Security

- (K)ein Zitat: *„Der Patient ist verstorben, da ich mein Passwort vergessen habe und daher das Beatmungsgerät nicht starten konnte.“*
- Der Impact bei Ausfall eines Medizingerätes geschieht meistens sofort, da das Leben eines Patienten direkt an der korrekten Funktion eines Gerätes hängt
  - Ausfallzeiten selbst im Sekundenbereich können schwerwiegende Folgen haben

KRITIS@HEALTH
„SPEZIALITÄTEN“ IM KLINIKUMFELD

„Impact“: Safety vs. Security

- (K)ein Zitat: *„Der Patient ist verstorben, da ich mein Passwort vergessen habe und daher das Beatmungsgerät nicht starten konnte.“*
- Der Impact bei Ausfall eines Medizingerätes geschieht meistens sofort, da das Leben eines Patienten direkt an der korrekten Funktion eines Gerätes hängt
  - Ausfallzeiten selbst im Sekundenbereich können schwerwiegende Folgen haben
- **Konsequenz:**
  - *Safety & Funktion hat in einem Großteil der Fälle klaren Vorrang vor IT-Security*

KRITIS@HEALTH
„SPANNENDES“ - WER ALLES TEIL DER STATIONÄREN VERSORGUNG IST

KRITIS@HEALTH
„SPANNENDES“ - WER ALLES TEIL DER STATIONÄREN VERSORGUNG IST

- Eindeutig:
  - IT (technisch, prozessual & Services)
  - Medizintechnik (technisch, vertraglich & prozessual)
  - Informationssicherheitsbeauftragter (ISB)
  - Datenschutzbeauftragter (DSB)
  - Alle Kliniken, die Teil der „stationären Patientenversorgung“ sind

KRITIS@HEALTH
„SPANNENDES“ - WER ALLES TEIL DER STATIONÄREN VERSORGUNG IST

- Eindeutig:
  - IT (technisch, prozessual & Services)
  - Medizintechnik (technisch, vertraglich & prozessual)
  - Informationssicherheitsbeauftragter (ISB)
  - Datenschutzbeauftragter (DSB)
  - Alle Kliniken, die Teil der „stationären Patientenversorgung“ sind
- Aber auch:
  - Personalabteilung
  - Einkauf
  - Zentrallabore
  - Apotheke
  - …

KRITIS@HEALTH
„SPANNENDES“ - WER ALLES TEIL DER STATIONÄREN VERSORGUNG IST

- Überraschend:

KRITIS@HEALTH
„SPANNENDES“ - WER ALLES TEIL DER STATIONÄREN VERSORGUNG IST

- Überraschend:
  - Abfallentsorgung
    - v.a. klinische Abfälle
  - Essensbestellsysteme
    - „Normales“ Essen geht über Notfallversorgung, aber „Spezialessen“ wird z.T. nirgendwo anders erfasst
  - Transportwesen
    - Bewegung der Patienten in- und außerhalb des Klinikums als elementarer Teil der Versorgung
    - Z.T. Spezialtransporte, bei denen nicht auf Dritte zurück gegriffen werden kann
  - Pathologie
    - Schnellschnitte etc.

KRITIS@HEALTH
„SPANNENDES“ AUS DER IST-AUFNAHME & GAP-ANALYSE

KRITIS@HEALTH
„SPANNENDES“ AUS DER IST-AUFNAHME & GAP-ANALYSE

- „Stations-PCs“ (im Schwesternzimmer)
  - Ein Funktionsnutzer, nie gesperrt, oft ohne Aufsicht…

KRITIS@HEALTH
„SPANNENDES“ AUS DER IST-AUFNAHME & GAP-ANALYSE

- „Stations-PCs“ (im Schwesternzimmer)
  - Ein Funktionsnutzer, nie gesperrt, oft ohne Aufsicht…
- Schlüssel- & Zutrittsverwaltung
  - „historisch gewachsen“
  - Z.T. über 150 (!) verschiedene dezentrale Schließsysteme an einem (!) Klinikum

KRITIS@HEALTH
„SPANNENDES“ AUS DER IST-AUFNAHME & GAP-ANALYSE

- „Stations-PCs“ (im Schwesternzimmer)
  - Ein Funktionsnutzer, nie gesperrt, oft ohne Aufsicht…
- Schlüssel- & Zutrittsverwaltung
  - „historisch gewachsen“
  - Z.T. über 150 (!) verschiedene dezentrale Schließsysteme an einem (!) Klinikum
- Rechte & Rollen vs. sehr mobiles Personalmanagement
  - Personal z.T. sehr mobil zwischen Abteilungen (häufige Abteilungswechsel etc.)
  - Rechte- & Rollenmanagement ist dabei oft Monate „hinterher“

KRITIS@HEALTH
„SPANNENDES“ AUS DER IST-AUFNAHME & GAP-ANALYSE

- „Stations-PCs“ (im Schwesternzimmer)
  - Ein Funktionsnutzer, nie gesperrt, oft ohne Aufsicht…
- Schlüssel- & Zutrittsverwaltung
  - „historisch gewachsen“
  - Z.T. über 150 (!) verschiedene dezentrale Schließsysteme an einem (!) Klinikum
- Rechte & Rollen vs. sehr mobiles Personalmanagement
  - Personal z.T. sehr mobil zwischen Abteilungen (häufige Abteilungswechsel etc.)
  - Rechte- & Rollenmanagement ist dabei oft Monate „hinterher“
- „Absicherung nach aktuellem Stand der Technik“
  - Passwort laut Hersteller: „nur ein Nutzer, max. 5 stelliges Passwort“
  - Auslieferung eines aktuellen Medizingerätes mit Windows XP (in 2019!)
  - Dinge wie NAC (Network Access Control / 802.1x) selten bis gar nicht unterstützt

4| GROß- & KLEINTEILIGE ANSÄTZE & LÖSUNGEN AUS UNSEREN PROJEKTEN

KRITIS@HEALTH
ANSÄTZE & LÖSUNGEN AUS UNSEREN PROJEKTEN

1 Schaffung einer Informations-Sicherheits-Organisation

2 Prozessoptimierung & Neuschaffung von (IT-)Prozessen

3 Kleinteiliges: Technische Verbesserungen

KRITIS@HEALTH
ANSÄTZE & LÖSUNGEN AUS UNSEREN PROJEKTEN

Schaffung einer Informations-Sicherheits-Organisation (IS-Organisation)

- ISMS ist **kein „Projekt“**, sondern ein ständig laufender Prozess („lebendes ISMS“)

Schaffung einer Informations-Sicherheits-Organisation (IS-Organisation)

- ISMS ist **kein „Projekt“**, sondern ein ständig laufender Prozess („lebendes ISMS“)
- Damit ein ISMS dauerhaft lauffähig ist…
  - …ist zumeist ein IS-Team nötig, da sonst die Gefahr der fehlenden Vernetzung in die Fachabteilungen besteht
  - …sollte das Thema nicht nur in der IT hängen, da es ganz klar kein reines IT-Thema ist
  - …muss das ISMS „hoch genug aufgehängt“ sein (Stabsstelle)

Schaffung einer Informations-Sicherheits-Organisation (IS-Organisation)

- ISMS ist **kein „Projekt“**, sondern ein ständig laufender Prozess („lebendes ISMS“)
- Damit ein ISMS dauerhaft lauffähig ist…
  - …ist zumeist ein IS-Team nötig, da sonst die Gefahr der fehlenden Vernetzung in die Fachabteilungen besteht
  - …sollte das Thema nicht nur in der IT hängen, da es ganz klar kein reines IT-Thema ist
  - …muss das ISMS „hoch genug aufgehängt“ sein (Stabsstelle)
- **Überlappung** mit **Datenschutz** und Notfall-/**klinischem Kontinuitäts-Management**
  - ISB ist häufig in Personalunion mit DSB
  - Das IS-Team ist auf Grund von inhaltlichen Überlappungen auch thematisch sehr gut mit Datenschutz, DSM/DSGVO sowie Notfall-Management-Inhalten vernetzbar

Prozessoptimierung & Neuschaffung von (IT-)Prozessen (Auszug)

- Z.B. Schaffung von klar definierten Ein-/Austrittsprozessen sowie deren „Verteilung“
  - Thema der Personalabteilung
  - Thema der IT (AD- und Mailkonten etc.)
  - Thema der Schlüssel- und Zutrittsverwaltung
  - Thema des Datenschutzes (Zugriff auf Patientendaten)

Prozessoptimierung & Neuschaffung von (IT-)Prozessen (Auszug)

- Z.B. Schaffung von klar definierten Ein-/Austrittsprozessen sowie deren „Verteilung“
  - Thema der Personalabteilung
  - Thema der IT (AD- und Mailkonten etc.)
  - Thema der Schlüssel- und Zutrittsverwaltung
  - Thema des Datenschutzes (Zugriff auf Patientendaten)
- Anpassung der Einkaufsprozesse an Security, damit nicht nach Beschaffung „nachgeflickt“ werden muss
  - Thema der IT
  - Thema der Medizintechnik
  - Thema der Haus- und Gebäudeleittechnik

Kleinteiliges: Technische Verbesserungen (Auszug)

- **Remote Access, v.a. Fernwartung:**
  - Anforderungen aufstellen (Session-Aufzeichnung, Freischaltung, 4-Augen-Prinzip etc.)
  - Im Rahmen unsere Projekte 5 Lösungen evaluiert

Kleinteiliges: Technische Verbesserungen (Auszug)

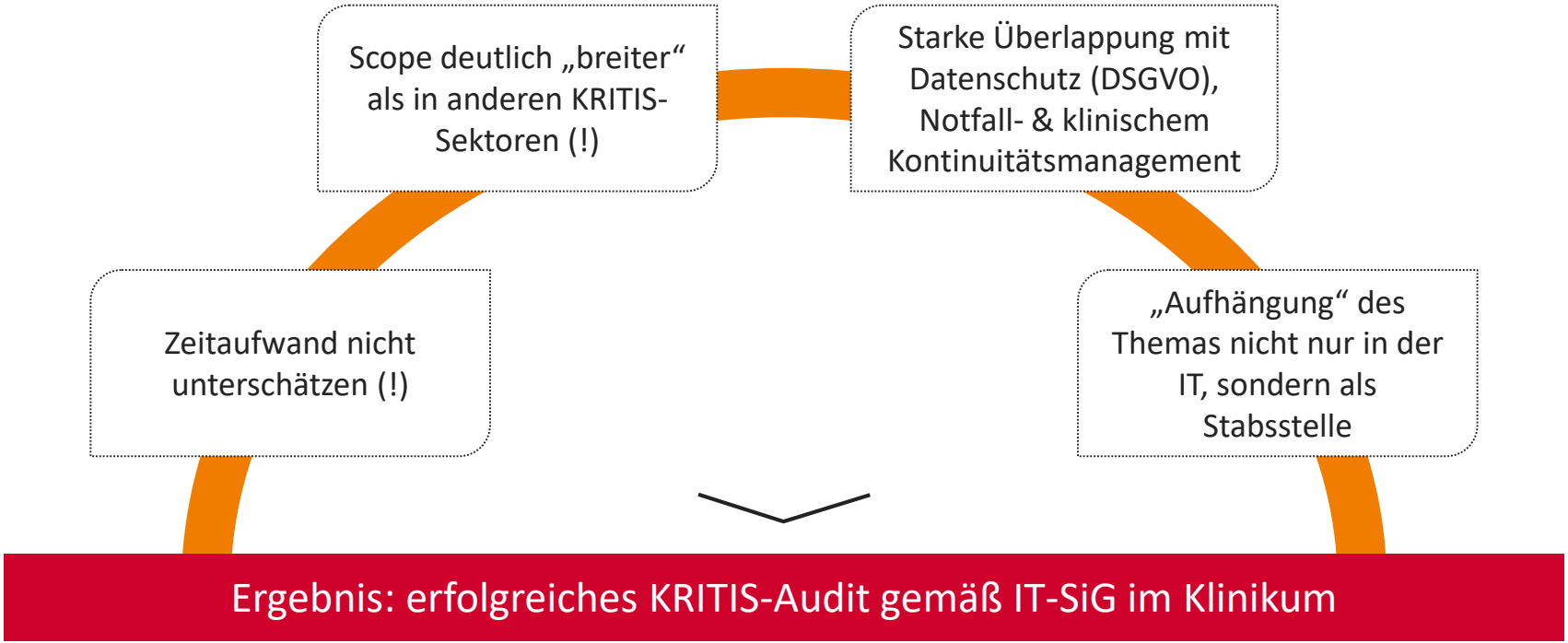
- **Remote Access, v.a. Fernwartung:**
  - Anforderungen aufstellen (Session-Aufzeichnung, Freischaltung, 4-Augen-Prinzip etc.)
  - Im Rahmen unsere Projekte 5 Lösungen evaluiert
- **Absicherung von USB bei Medizingeräten** (wer erinnert sich noch an Stuxnet?)
  - Anforderungen aufstellen (Virenscan mit „Scanstation“, BadUSB, Prozesse etc.)
  - Im Rahmen unsere Projekte 12 Lösungen evaluiert

Kleinteiliges: Technische Verbesserungen (Auszug)

- **Remote Access, v.a. Fernwartung:**
  - Anforderungen aufstellen (Session-Aufzeichnung, Freischaltung, 4-Augen-Prinzip etc.)
  - Im Rahmen unsere Projekte 5 Lösungen evaluiert
- **Absicherung von USB bei Medizingeräten** (wer erinnert sich noch an Stuxnet?)
  - Anforderungen aufstellen (Virenscan mit „Scanstation“, BadUSB, Prozesse etc.)
  - Im Rahmen unsere Projekte 12 Lösungen evaluiert
- **Monitoring in (fast reinen) OT-Netzen („Operational Technology“)**
  - **K-SOC (Klinik-SOC)**: Medizingeräte im klaren Fokus, damit man „auf dem OT-Auge nicht blind“ ist
  - K-SOC: Zusätzlich automatische Architektur- & Kommunikationsnetz-Aufnahme für „Live-Assetregister“ der IT sowie der Medizintechnik

5| RESÜMEE

RESÜMEE



FRAGEN?

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

sopra steria
CONSULTING

Torben Klagge
Manager IT-Security
Torben.Klagge@SopraSteria.com