Cybersicherheit: Aktuelle Bedrohungslage und davon abgeleitetes strategisches Handeln »

IT. Sicher. Machen.

EnBW Full Kritis Service
Klaus Frank, Sönke Pingel
6. November 2019

Aktuelle Herausforderungen

Zunehmende Vernetzung führt oft dazu, dass jede Schwachstelle im System über das Internet gezielt angegriffen werden kann

Umsetzung des **IT-Sicherheitsgesetzes** nach BSI Kritis-Verordnung sowie branchenspezifischen Sicherheitsstandards (B3S)

Einhaltung der **Datenschutz-Grundverordnung** (EU-DSGVO)

Fehlende Expertise sowie Mangel an **Zeit und Ressourcen**

Erhöhte Gefahr von **schwerwiegenden Cyber-Angriffen** (z. B. Emotet)

Gefahr von **funktionsbeeinträchtigenden Eingriffen/Störungen** bei kritischen Infrastrukturen

Risk Barometer der Allianz Versicherung

Platz 1
37 %
Betriebsunter-brechungen*

Platz 1
37 %
Cybervorfälle

Platz 3
28 %
Naturkatastrophen

Platz 6
19 %
Feuer und Explosionen

Platz 5
23 %
Marktentwicklungen

Platz 4
27 %
Veränderungen in Gesetzgebung und Verordnung

Bem.: * Cybervorfälle sind zudem die am meisten gefürchteten Auslöser von Betriebsunterbrechungen.
Quelle: Allianz AGCS Risiko Barometer 2019

Erfolgreiche Angriffe der letzten 6 Monate

Trojaner „RobbinHood“ in Baltimore

Gesamtschaden: ca. 18 Mio. US-Dollar

Ransomware-Angriff auf Schulen in Louisiana

US-Bundesstaat ruft Notstand aus, genauer Schaden unbekannt

Angriff auf Capital One

Massiver DDOS-Angriff auf Wikipedia

diverse Webseiten von Wikipedia nicht erreichbar

Apr | Mai | Jun | Jul | Aug | Sep

Spionage-Angriff „Winnti“ auf Konzerne

Lösegeldzahlung von 600.000 US-Dollar

Malware-Befall „Sodinokibi“ auf DRK Einrichtungen

Mehre Tage nur noch Arbeiten ohne IT möglich

Patientendaten ungeschützt im Netz

In Deutschland 13.000 Patientendatensätze, weltweit Millionen

Quellen: Heise, Presseportal, Tagesschau

Beispiel: Angriff im Finanzwesen

Capital One

Was?	Hackerin stiehlt Daten von ca. 100 Millionen Bankkunden
Wie?	Angriff erfolgte über Schwachstelle in der falsch konfigurierten Firewall
Wann?	Juli 2019
Schaden:	Bank erwartet aufgrund des Angriffs Mehrkosten von rund 100 Millionen USD

Cybersicherheit ist eine existenzielle unternehmerische Herausforderung

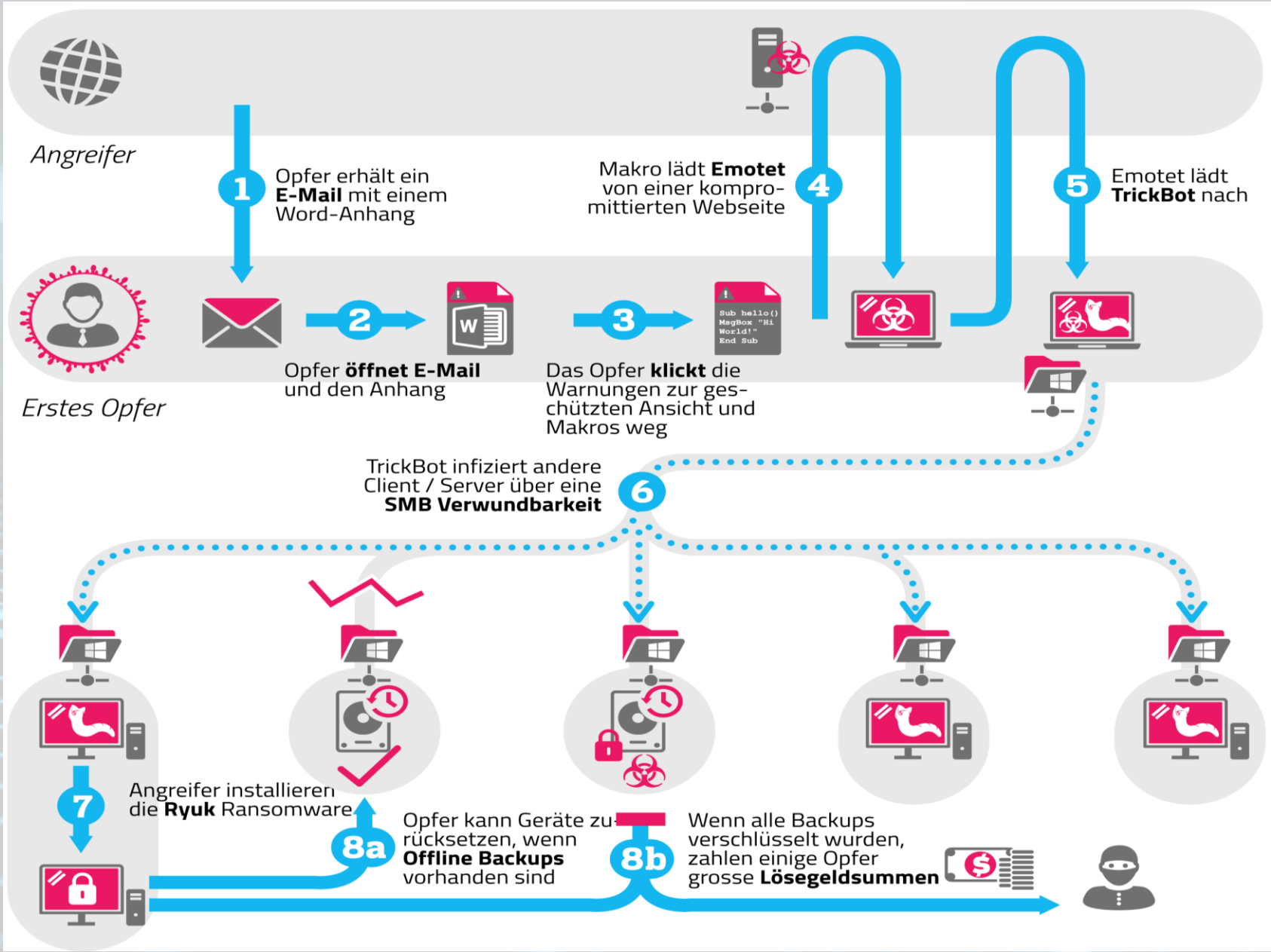
Änderung der **Qualität der Bedrohungen**

*„Es ist nicht die Frage **ob, sondern wann** man erfolgreich angegriffen wird und dies überhaupt/ rechtzeitig wahrnimmt.“*

- **Spezifisch**: immer häufiger **branchenspezifische** oder firmenspezifische Angriffswellen
- **Opfer**: mehr **Fokus auf IT-Dienstleister** (Kundenzugang per Fernwartung)
- **Schaden**: mehr **Härte** bei Erpressung -> bis zur **Auslöschung der Firma** (teils inkl. Back-ups)
- **Tatwaffen**: sehr **dynamische Weiterentwicklung** der erfolgreichen Trojaner wie Emotet und GandCrab

Russland: 67 Prozent

Beispiel Emotet



Quelle: Schweizer Melde- und Analysestelle Informationssicherung MELANI (Link)

Cybersicherheit ist eine existenzielle unternehmerische Herausforderung

EnBW

Echte Krisenszenarien möglich

Strom-
versorgung

Kommunikation

Transport
und Verkehr

- **Mittelfristiger verketteter Ausfall** von kritischen Infrastrukturen bei regionaler/ nationaler Krisensituation
- Auch bei **staatlicher großflächiger Cybersabotage** sollten kritische Infrastrukturen weiter funktionieren

Cybersicherheit ist eine existenzielle unternehmerische Herausforderung

EnBW

Gefahren durch **Störfallszenarien / Tätermodelle**

- **natürliche** Gefährdungen (Unwetter, Sonnenstürme etc.)
- **zivilisatorische** Gefährdungen (Brand, Flugzeugabsturz etc.)
- vorsätzliche **Straftaten** von **Einzel-/Innentätern**
- Geschäftsmodelle für **organisierte Cyberkriminalität**
- staatl. **Wirtschaftsspionage** oder staatl. **Hacking** (z. B. zur Geldbeschaffung)
- staatl. **angeordnete Zerstörung** von Infrastrukturen (z. B. Cyberangriff der USA auf den Iran im Juni 2019)

Rechtslage

Erwartungen zum **IT-Sicherheitsgesetz 2.0**

- Ziel: **schnellere** Prävention
- mehr **Befugnisse für Durchgriff** für das BSI (inkl. **Sensorik** vor Ort)
- gleiches **Strafmaß wie Datenschutz**
- erweiterter Geltungsbereich (Sektor **Entsorgung**, Kritis-**„Kernkomponenten“**)
- bedarfsweiser Durchgriff auf Kritis-**Lieferanten** und **andere Infrastrukturen**
- mehr **Rechte/Pflichten** für Kritis-Betreiber (z. B. Krisenkommunikationssystem)
- Präventionsmaßnahmen zur **Großkrisenbeherrschung**

Strategische Handlungsfelder zur Verbesserung der Cyber-Resilienz

- Vertiefung der **Zusammenarbeit von Diensten** (BSI, LKA, LfV) **und Industrie** auf Landes-/Bundesebene
- **Begrenzung der digitalen Abhängigkeit der Europäer** durch kooperative Geschäftsmodelle in Deutschland und Europa
- Konzeption, Bau und Absicherung von **schnellen, sicheren und stabilen IT-Infrastrukturen**
- Weiterentwicklung der Konzepte zur **Beherrschung von Großkrisen**

Cyberschutzprogramm »

Am Beispiel der Kritis-Branche
„Gesundversorgung im Krankenhaus“

IT. Sicher. Machen.

Klaus Frank
Full Kritis Service
Oktober 2019

Konzept der Risikolandkarte BW

Messen der richtigen KPIs zum Nachweis der Cybersicherheitsqualität pro IT Infrastruktur (Anlage)

Wissen über das wahre Lagebild, die Bedrohungen und die aktuellen Angriffswellen

Maßnahmen gegen aktuelle Lage durch technische und organisatorische Mittel

Branchenspezifische Risikolandkarte = Erster Schritt zu einem zentralen Lagebild kritischer Infrastrukturen in BW

Krankenhaus
IT-Infrastruktur

M2

Innenmessung
IT und OT

M3

Messung
Prozessreifegrad
(Interview)

Digitaler
Fußabdruck im
Internet

M1

Cybersecurity
Leitstand BW
Technik / Analysten

LKA

Innenministerium

Brancheverbände/BSI

EnBW Full Kritis Service

Kontakt:

Klaus Frank (Leiter FKS)
k.frank@kk.enbw.com
Mobil: +49 160 94608500

Jürgen Franke (Leiter FKS Vertrieb)
j.franke@enbw.com
Mobil: +49 173 3420062

www.enbw.com/kritis

0800 0 KRITIS
kritis@enbw.com

B3S fordert ganzheitlichen Rahmen für Informationssicherheit in Krankenhäusern, insbesondere für Patientensicherheit und Behandlungseffektivität

EnBW

Kernprozesse

Kernsysteme

Krankenhausinformationssystem (KIS)

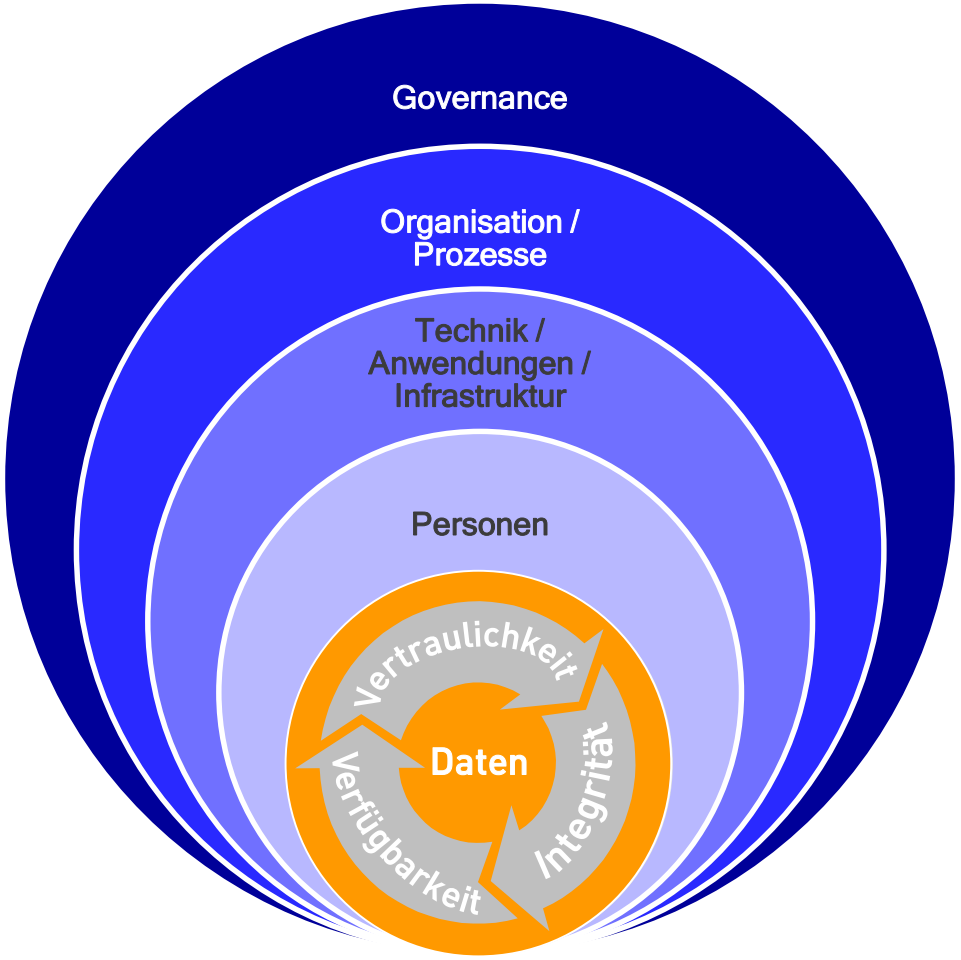
LIS	RIS	PACS	DMS	OP-Planung
Labor-Informationssystem	Radiologie-Informationssystem	Bilddatenarchivierungs- und -kommunikationssystem	Dokumenten-managementsystem	

Infrastruktur

alle vernetzten Systeme und Komponenten
(Medizintechnik, Versorgungstechnik, Transportlogistik, ITK-Infrastruktur, Sicherheitstechnik)

Quellen: DKG e.V. (B3S Gesundheitsversorgung im Krankenhaus, Entwurfsstand 0.84); EnBW FKS mit Feedback von BSI und DKG

Basierend auf den Kernprozessen wird ein Risikomanagement für Informationssicherheit aufgebaut, via ISO 27001 bzw. BSI IT-Grundschutz



Definition Risikomanagementprozess:

- **kontinuierliche Führungsaufgabe**, im Rahmen derer die Risiken einer Organisation identifiziert, analysiert, bewertet, behandelt und dokumentiert werden

Wesentliche Aspekte:

- **Committment der Geschäftsführung zur Investition in die Krisenresilienz** und zur Wahrnehmung der Risikoverantwortung
- **Wissen über eigenes Kerngeschäft** und einhergehende Risiken:
  - Gefährdung von Leben / Gesellschaft,
  - wirtschaftliche Treiber / Gefahren,
  - Rechtslage / persönliche Haftung
- Geeignete, **begrenzte** Auswahl eines zielführenden Umfangs / Geltungsbereichs (**Scope**)
- Effiziente und **angemessene** organisatorische und technische Maßnahmen (**TOM**)
- Schaffung eines **Risikobewusstseins** bei den Mitarbeitern
- **Regelmäßige Prüfung** / Optimierung

Vorgehensmodell zur Umsetzung eines Risikomanagements zur Informationssicherheit nach ISO 27001, IT-Grundschutz, B3S etc.

EnBW

Initialisierung (Geschäftsführung) → **Analyse und Planung** → **Umsetzung und Betrieb** → **Zertifizierung und Verbesserung**





1: Scope

- **Kontextanalyse** der Organisation (Geschäfts-prozesse, Bereiche)
- Festlegung **Geltungsbereich** des ISMS (Scope)
- Erstellung **Informationssicherheits-Leitlinie** inkl. **Schutzziele**
- Festlegung von Organisation und Methoden des **ISMS**
- Erstellung **Dokumentations-Rahmenwerk**

2: Assets

- **Strukturanalyse** der Komponenten/Verfahren (IST- und PLAN-Assets)
- Identifizierung **Wirkkette**
- Erstellung **Assetregister**

3: Risiko-Analyse

- **Schutzbedarfsfeststellung** je Komponente entsprechend ihrer Schutzziele, Prozesse und Kritikalität
- **Konsolidierung** in sinnvoll definierte Asset-Gruppen
- **Modellierung** im Risiko-management-Tool
- Beantwortung der **Kontrollfragen** der Regelwerke
- Festlegung der technischen und organisatorischen Maßnahmen **(TOM)**

4: Umsetzung

- **Umsetzungsdetailplanung** (Priorisierung, Ressourcen)
- Erstellung der **Erklärung zur Anwendbarkeit (SOA)** als zentrales Instrument für Management/Auditor
- **Projektmanagement** der TOM Umsetzung
- praktische **Vorbereitung des potentiellen Ernstfalls** (BCM, Notfallmaßnahmen, Kommunikationswege, Entscheidungsfähigkeit)
- finale Bewertung, **Abnahme und Dokumentation**

5: ISMS Betrieb

- **Compliance-Regelbetrieb** mit Monitoring/Reporting/ Dokumentation (neue Komponenten, neue Anforderungen, neuer Stand der Technik)
- zielführende Beteiligung und **Sensibilisierung der Mitarbeiter**
- regelmäßige **Übung** eines potentiellen Ernstfalls
- stetige **ISMS Optimierung** (Plan-Do-Check-Act)
- Durchführung von **Audits** (intern, bei Lieferanten)

Weiteres branchenspezifisches Vorgehen von EnBW FKS mit CRISAM®

Eigene gute Erfahrungen mit CRISAM®…

- EnBW nutzt CRISAM® seit Jahren erfolgreich für **Risikomanagement und Compliance** (besonders effizient für sich überschneidende Anforderungen verschiedener Regelwerke)
- **neue Anforderungsmodule** können gemeinsam mit Calpana entwickelt werden (s. Erfahrungsbeispiel)

Geplanter Einsatz bei Kunden…

- CRISAM® hilft zur **Kundenbindung** und zur **Qualitätssicherung**
- methodische Unterstützung und langfristige **Bündelung** in einem Tool
- **vollständige, komponentenscharfe Dokumentation** in CRISAM® ab Stunde Null

EnBW FKS und Calpana entwickeln gemeinsam branchenspezifische B3S Module für CRISAM®…

- eine **native ISO 27001** Nutzung ist für Kritische Infrastrukturen in der Regel **nicht hinreichend**
- CRISAM® hat derzeit **noch keine B3S-Module** pro Branche abgebildet
- **EnBW FKS Erfahrung mit CRISAM® und Kritis-Branchen-Fachkenntnisse** sind für Calpana werthaltig
- Ergänzungsmodule mit Spezialthemen pro Branche, teilweise IT-Grundschutz- und §8a* BSIG/B3S-Ergänzungen

*§8a: „Sicherheit in der Informationstechnik Kritischer Infrastrukturen“ im „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)“

Erfahrungsbeispiel: **Projekt „UmSI“** (Umsetzung SEWD-Richtlinie IT)

Bundesministerium
für Umwelt, Naturschutz
und Reaktorsicherheit

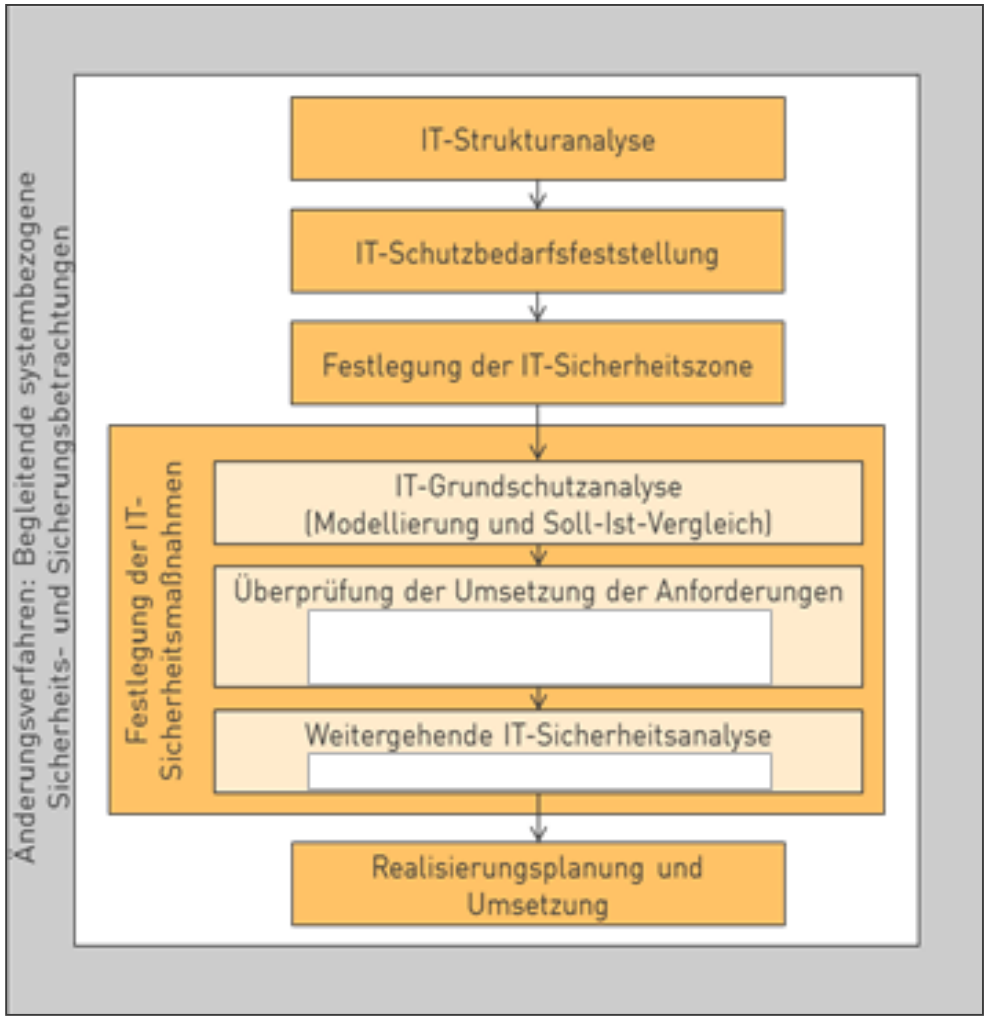
Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter

(SEWD-Richtlinie IT)

Hintergrund / organisatorische Eckpunkte

- Richtlinie des **BMU**, veröffentlicht: 13.08.2013
  (nach BMI Kritis-Strategie 2009 und Stuxnet 2010)
- bindend für alle nach §§ 6 oder 7 AtG genehmigten **kerntechnischen Anlagen**
- Zweck: **Schutz von IT-Systemen gegen Störmaßnahmen oder sonstige Einwirkungen Dritter**
- Geltungsbereich:
  alle schutzbedürftigen IT-Systeme der Anlage
  (z. B. Diagnosesysteme, Betriebsführungssystem, leittechnische Steuerungen, Büro-IT/PCs, …)

IT-Sicherheitsanalysen auf Basis IT-Grundschutz, ergänzt um SEWD-RL IT, Entscheidung für zentralen Ansatz, Produktentscheidung für CRISAM®



Ergebnis einer Produktevaluation und Testphase

- Produkt CRISAM®, **gelistetes IT-Grundschutz Tool beim BSI**
- **formale Voraussetzungen** von AtZüV und VS-NfD sind eingehalten

Zentraler Ansatz (fachbereichs- und standortübergreifend):

- Erstellung der IT-Sicherheitsanalysen **zentral durch IT-Sicherheitsteam**
- Zusammenarbeit zwischen Modellierer, Koordinator und federführendem Sachbearbeiter im Fachbereich
- Prüfung/Freigabe durch IT-Systemverantw. und IT-SB/Anlagensicherung
- **CRISAM® Betrieb**: verschlüsselt, rollenbasiert, in entkoppelter Umgebung

Ermittlung übergreifender IT-Sicherheitsmaßnahmen

- Bausteine aus Schicht 1 der IT-Grundschutzkataloge (vor Modernisierung)
- übergreifend geltende Anforderungen aus der SEWD-Richtlinie IT
- **Zusammenfassung in einen eigenen Baustein** nach BSI-Schema „SEWD-Anforderungen Informationsverbund EnKK“

Ermittlung spezifischer IT-Sicherheitsmaßnahmen (1 Analyse je Verbund)

- **je ein eigener„SEWD-RL IT-Baustein“ pro Schutzbedarfsklasse** nach BSI-Schema (4x: sehr hoch, hoch, erhöht, normal)

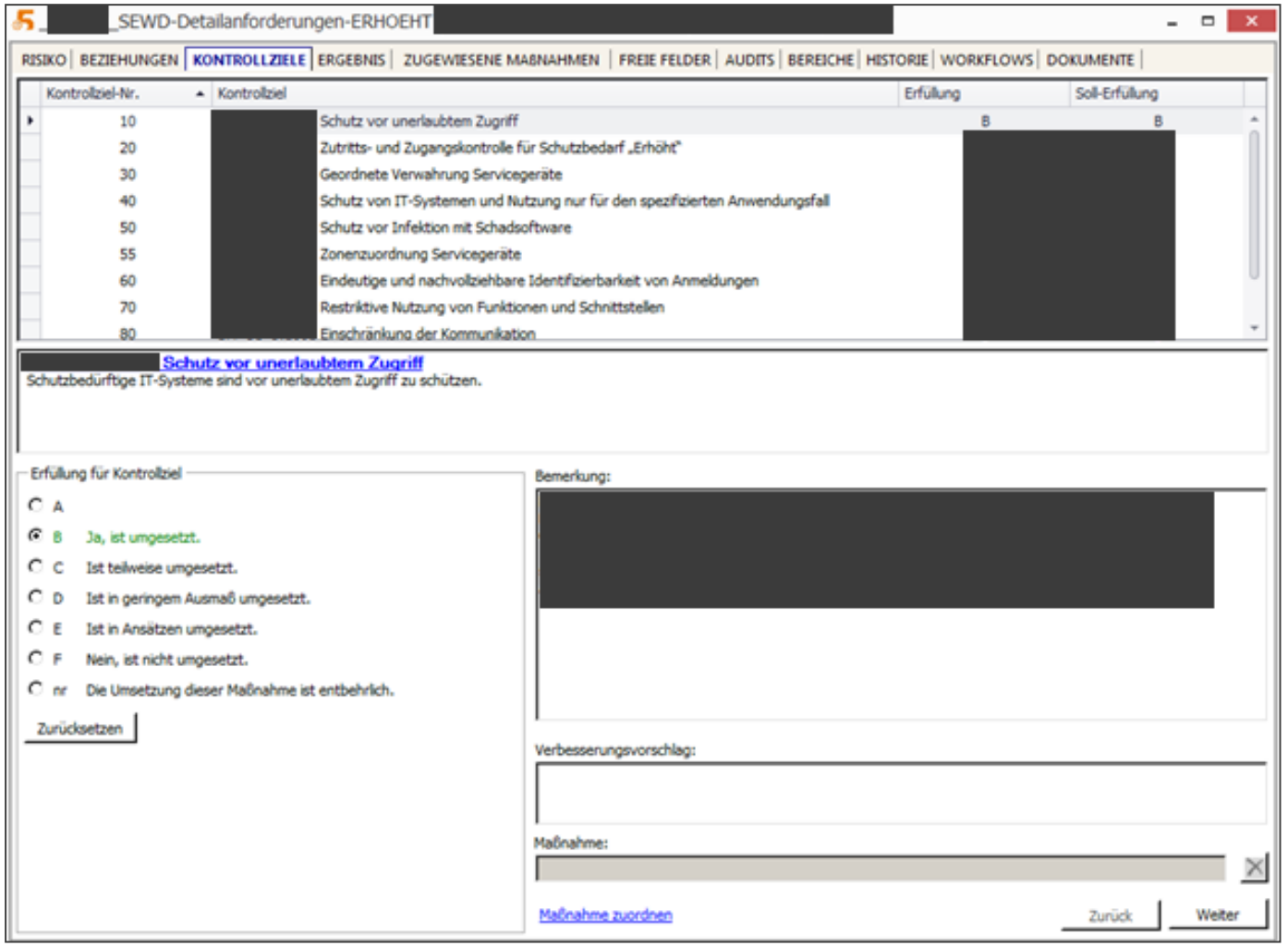
Kennzahlen, Ergebnisse, beispielhafte Auszüge

Größenordnungen der Kennzahlen:

- ca. **10 Modellierer** im Einsatz
- Strukturanalyse:
  ca. **5.000 Objekte in CRISAM** erfasst
- Konsolidierung inkl. Schutzbedarfsklasse:
  ca. **200** konsolidierte **IT-Systemverbünde**
- Bewertung von Kontrollzielen je IT-Verbund:
  ca. **30.000 Kontrollziele** modelliert

Projektergebnisse

- zentrale Projektsteuerung sehr wertvoll
- standortübergreifender, **homogener Qualitätslevel**
- zentraler, toolgesteuerter Ansatz ermöglicht Nutzung von **Synergie- und Skaleneffekten**
- **vollständige, komponentenweise Dokumentation** mit weitgehend automatisierter Auswertung



Handlungsempfehlung Kritis-Krankenhäuser/-verbünde

Wahrnehmung der Situation

Faktor Mensch:

- **Investitionsprioritäten** in Kritis-Krankenhäusern:
  1. digitale Personalakte und Patientenapps
  2. Datenschutz (weitgehend in Arbeit)
  3. **Umsetzung IT-SiG** (ca. **50% keine Aktivitäten**, da B3S bisher nicht final verabschiedet, Rest Minimalansatz mit 50-100 T€, Fördertöpfe nach Pflegepersonalstärkungsgesetz (11/2018) für Investitionskosten in IT-Sicherheit (ohne Betriebskosten, nur Kritis) sind beim Land noch in Vorbereitung

Faktor Technik:

- **IT-Infrastruktur** (Rechenzentren, Netze, Server, etc.) ist **in der Regel veraltet**, oft sogar aus der Wartung (außer Neubauten)
- hinsichtlich **IT-Sicherheit weit entfernt vom Stand der Technik** (u.v.a. keine Trennung zwischen klassischer IT, Medizintechnik und Haustechnik; sehr heterogene Systemlandschaft)

Faktor Organisation:

- **ca. 50% haben keinen ISB und auch keine Planstelle dafür**
- Aufbauorganisatorisch sind IT, Medizin- u. Haustechnik getrennt
- **Verhältnis IT-Personal zu IT-Nutzern weit unter Industriemaß**
- Priorität haben stets Patientenprozesse vor Sicherheitsprozessen

Vorschläge zu Verbesserungen

Faktor Mensch:

- geeignete **Branchenpflichtveranstaltung für Geschäftsführungen**
- regelmäßige, aktuelle **Pflichtschulungen** für alle wesentlichen Rollen von der Geschäftsführung bis zum Mitarbeiter
- verbindliche **Cyberübungen**/-simulationen (mind. 2 Mal pro Jahr)

Faktor Technik:

- gefördertes oder **zentral aufgebautes/koordiniertes gehärtetes Branchennetz Gesundheit** (zunächst in Baden-Württemberg) mit zentraler Schnittstellt zur TI via Krankenhauskonnektor
- **Minimumstandards für Informationssicherheitskonzepte** (inkl. Zonenkonzepte) mit Umsetzungsfrist bis max. 2022

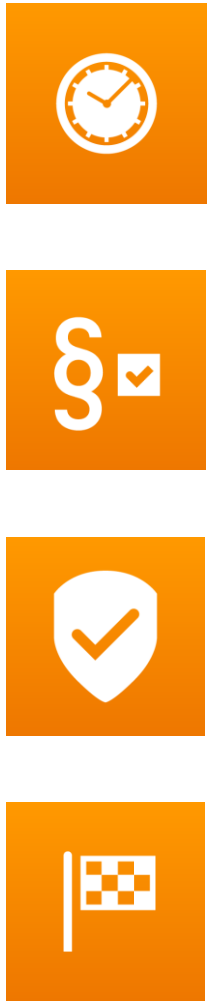
Faktor Organisation:

- Bereitstellung eines **Pools** fachlich geeigneter, erfahrener **ISBs**, der die Krankenhäuser berät und die Umsetzung begleitet
- **Standardisierung der B3S Einführung** durch zentrale Vorgabe zur Nutzung des **B3S-Compliance-Modells** von FKS
- zur Verfügung Stellung **ausreichender, dedizierter, einfacher Fördertöpfe für Investitions- und Betriebskosten** zur Umsetzung

FKS Standardmodell für B3S Einführung in Krankenhäusern

Beschreibung

- **alle Regelwerksanforderungen für Krankenhäuser** hinsichtlich Informations-sicherheit, Datenschutz und medizinischen Belangen **in einem Risikomanagementsystem gebündelt** (basierend auf langjähriger EnBW FKS Erfahrung mit CRISAM® von Calpana und Kritis-Branchen-Kenntnissen)
- **Perspektivenwechsel**: vollständige Simulation - was brauche ich daraus nicht



Vorteile

- **zeitnahe B3S-Umsetzung möglich**, sogar per Anordnung (für Kritis und unter Kritis)
- hohes Maß an **Standardisierung** über viele Krankenhäuser (unternehmens- und standortübergreifender homogener Qualitätslevel)
- **methodische Unterstützung** und **langfristige Bündelung** in einem Tool
- **Zeitgewinn** bei der Umsetzung
- der zentrale, toolgesteuerte Ansatz ermöglicht Nutzung von **Synergie- und Skaleneffekten**
- **vollständige, komponentenweise Dokumentation** mit weitgehend automatisierter Auswertung

Abbildung der B3S Anforderungen

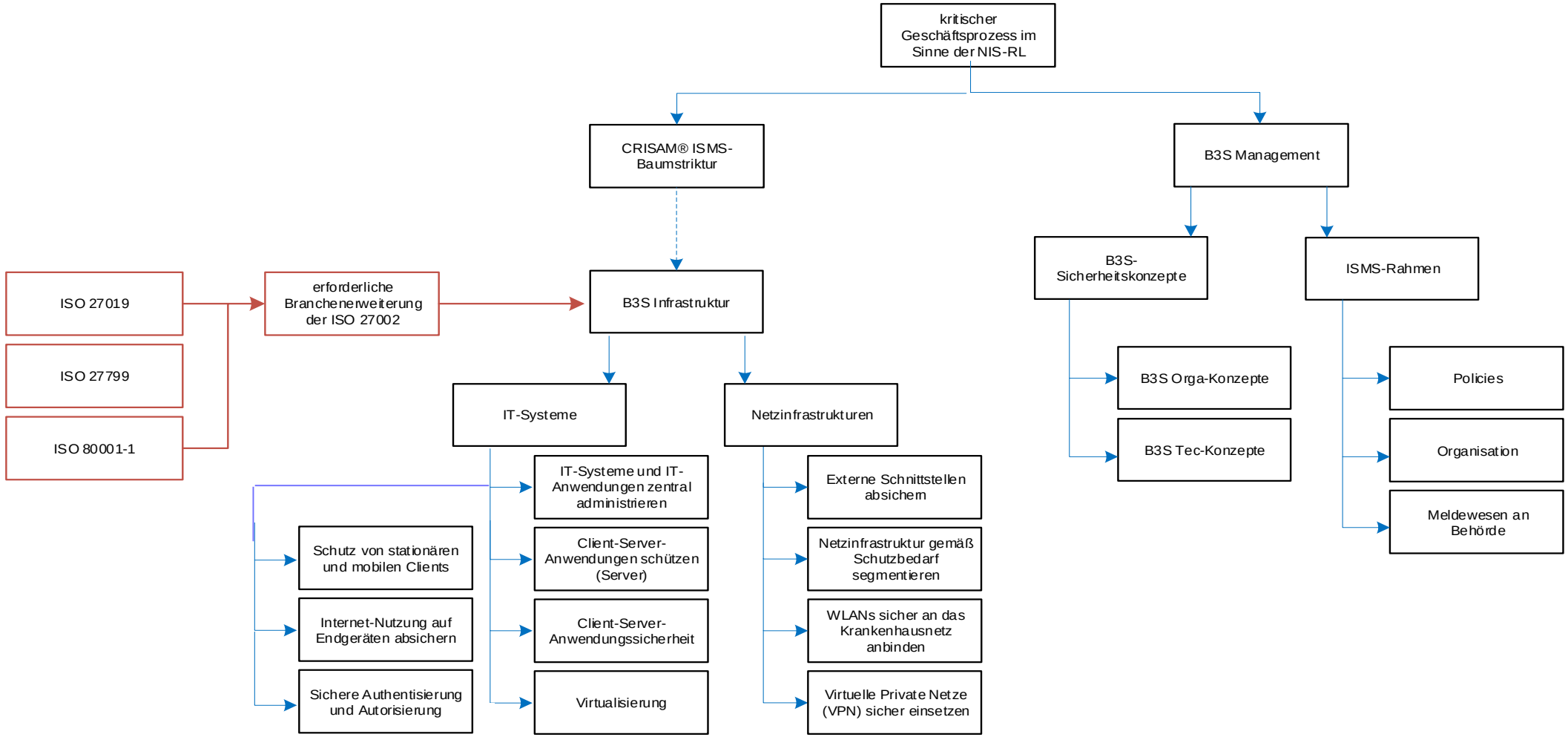
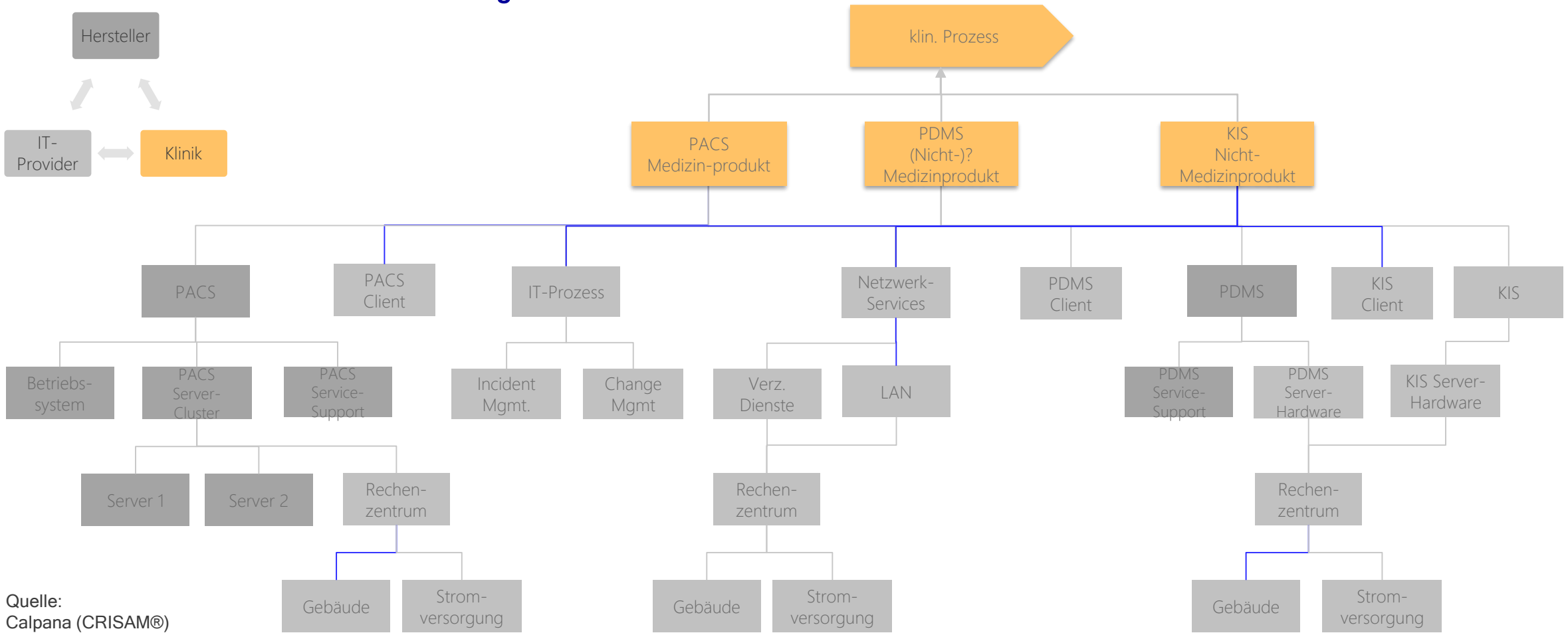


Abbildung der klinischen IT-Infrastruktur

Risiken werden in ihrer Ursache Wirkungskette vererbt!



Quelle:
Calpana (CRISAM®)

Grundfunktionalitäten des verwendeten IT-Tools

Methode

1. Risikobaum Methode (analog DIN 25424)
2. ISO 31000 Risikomanagement
3. BSI 200-x Sicherheitsmanagement
4. BIA Business Impact Analyse
5. Risikoaggregation
6. Mapping zu Standards
7. CBA Kosten-Nutzen Analyse
8. SAM Szenario Analyse Methode
9. Rating

Content

1. Information Security
2. Datenschutz
3. Payment (PCI)
4. Medical
5. SCADA
6. Kritis

Software

1. Explorer
2. Server
3. Workflow
4. WEB-Access
5. Rechte Management
6. Reporting
7. Content Management
8. Reporting

Compliance

1. ISO 9001
2. ISO 20000
3. ISO 2700x
4. ISO 27019
5. ISO 80001-1
6. BSI 100-x / 200-x
7. EU-DSGVO
8. COSO
9. COBIT
10. SOX
11. EN 50600
12. BDEW
13. VDA / TISAX
14. etc.

Quelle:
Calpana (CRISAM®)

Unser Versprechen

Ihre IT.

Sie behalten zu jedem Zeitpunkt den Überblick über den aktuellen Stand Ihrer IT-Sicherheit, auch bei komplexen Vorhaben.

Sicher.

Maßgeschneiderte, aufeinander abgestimmte Produkte unterstützen Sie bei der Umsetzung Ihrer IT-Security-Compliance-Ziele.

Machen.

Unser Ansatz ist ganzheitlich und hat das Zusammenwirken von Mensch, Technik und Organisation im Blick.

EnBW betreibt kritische Infrastrukturen

\+

Wirtschaftlicher Einsatz von Security-Experten

〉

Kosteneffiziente Lösung für Ihr Unternehmen

Unser Produktportfolio

Quick Wins

- Quick-Check
- Pen-Testing
- CyberRating
- Top Risiken
- GAP Analyse
- EU-DSGVO Check

Ihre Compliance

- EU-DSGVO
- ISO 27001
- B3S
- Cyber Security
- Audit Vor-/Nachbereitung oder Durchführung
- Awareness Maßnahmen

Sicherer Betrieb

- ext. DSB / ext. ISB
- IT Housing mit sicheren WAN-Verbindungen
- Security Operations Center
- Commodity BüKo
- Leittechnik
- Sensorik, Aktorik und Objektschutz-IT

Zur Empfehlung

Vortrag von Arne Schönbohm zum Thema „Zahlungsverkehrssymposium – Cyber-Resilienz im Finanzsektor“

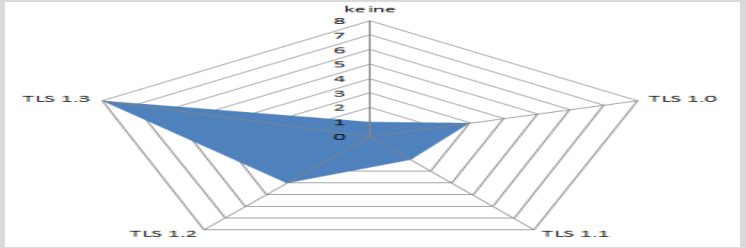
Abrufbar unter:

https://www.youtube.com/watch?v=Yp5rXxxSskM&feature=youtu.be

Außenmessungen

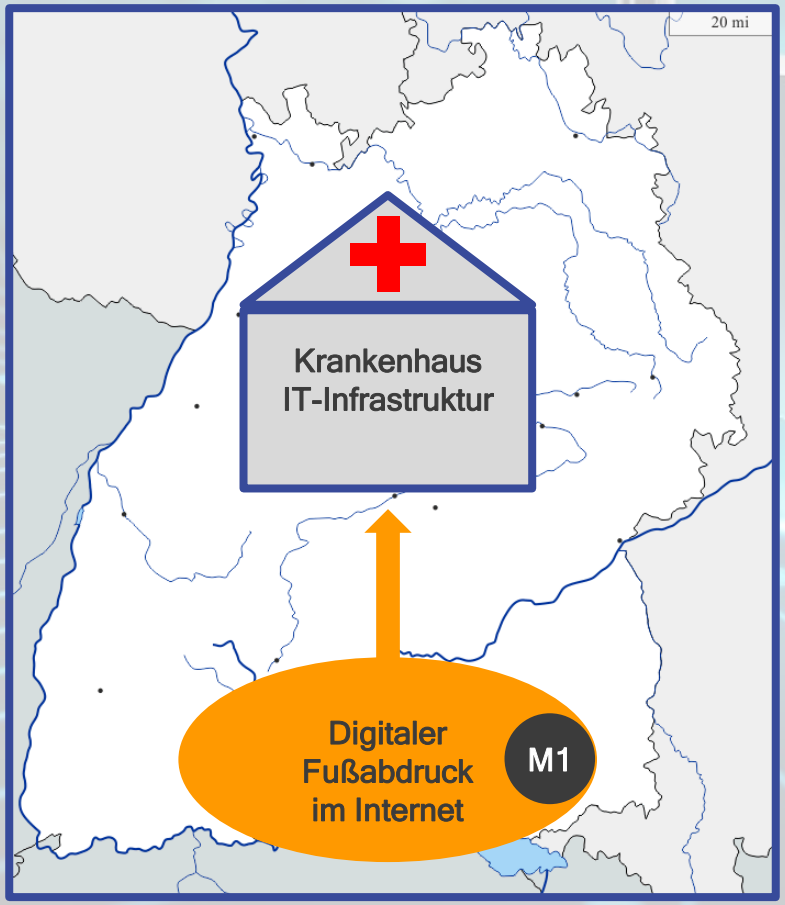
KPI A1) E-Mail-Transportwegverschlüsselung

Transportwegverschlüsselung mittels TLS (inkl. Version)



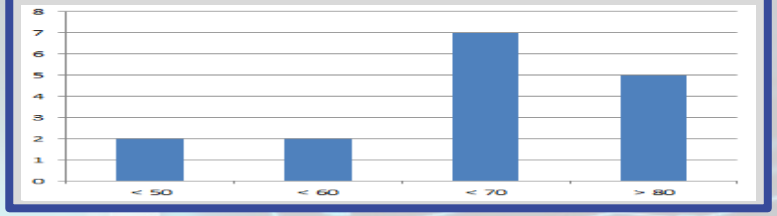
KPI A2) Erfüllung BSI TR 02120-2 (Nutzung TLS)

Einsatz empfohlener Algorithmen zur TLS-Verschlüsselung



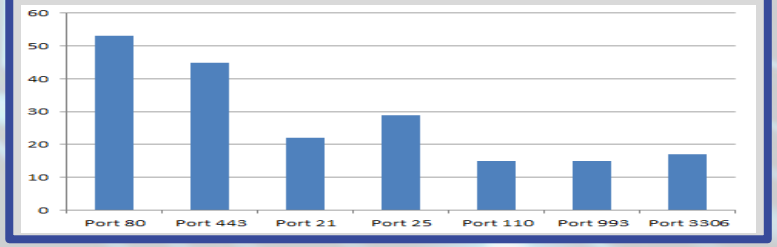
KPI A3) Reputation des Unternehmens im Cyberraum (Vertrauenswürdigkeit)

Bewertungszahl der Domains bei Reputationssystem (wie z. B. Google)



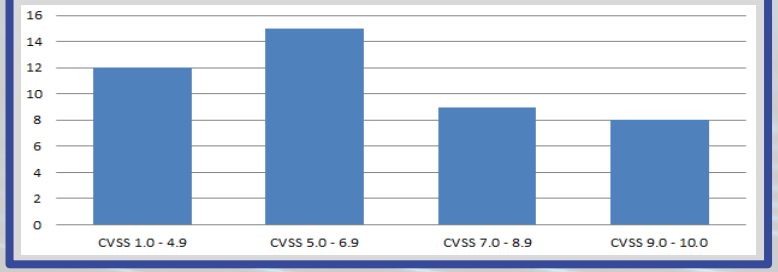
KPI A4) Angriffsfläche im Internet

Anzahl erreichbarer IT-Systeme / IT-Dienste aus dem Internet

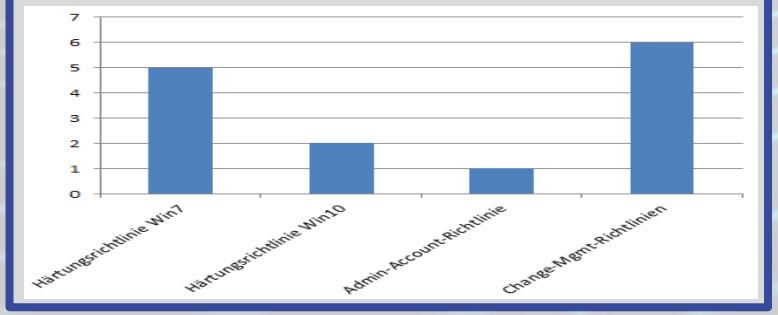


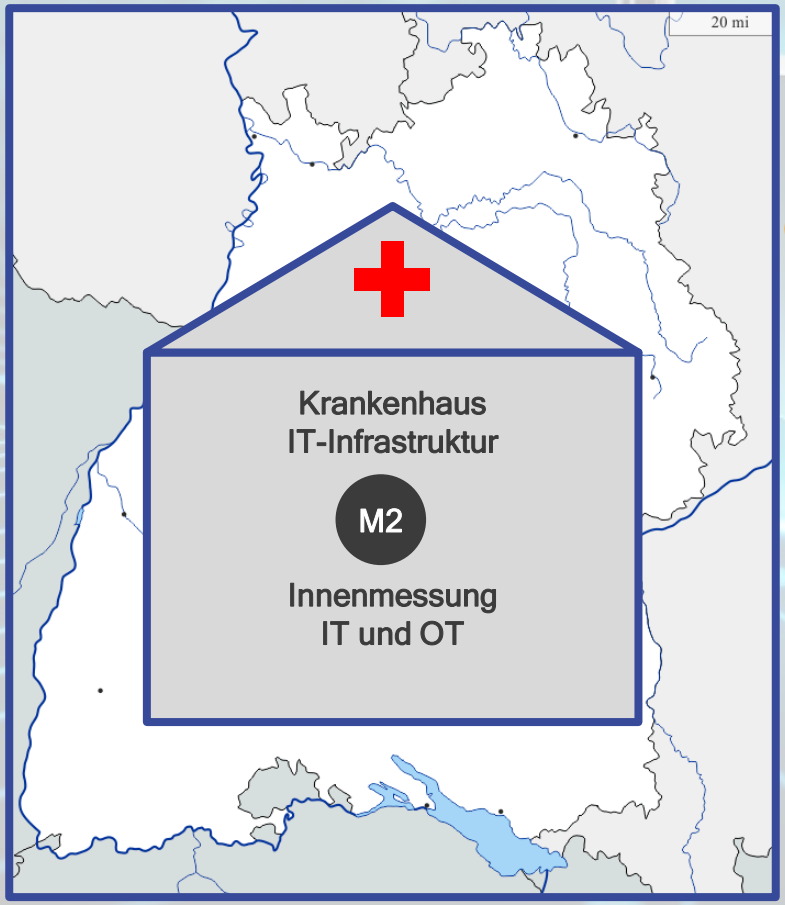
Innenmessung

KPI B1) Anzahl vorhandener Schwachstellen
basierend auf CVE-Datenbank

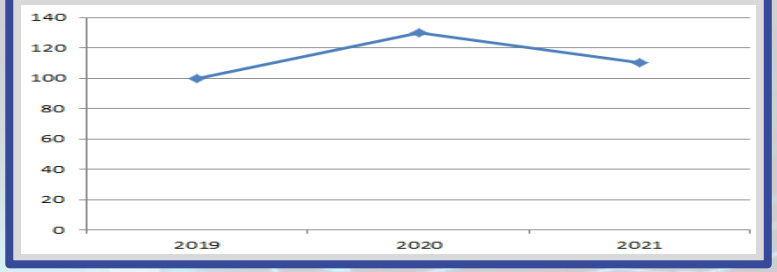


KPI B2) Anzahl Richtlinienverletzungen

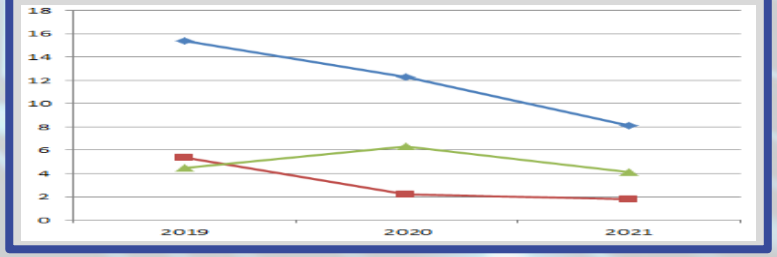




KPI B3) Anzahl identifizierter Netzwerkanomalien



KPI B4) interne Bearbeitungsdauer für Risiken
durchschnittliche Bearbeitungsdauer von Schwachstellen, Anomalien, Richtlinienverletzungen in Tagen



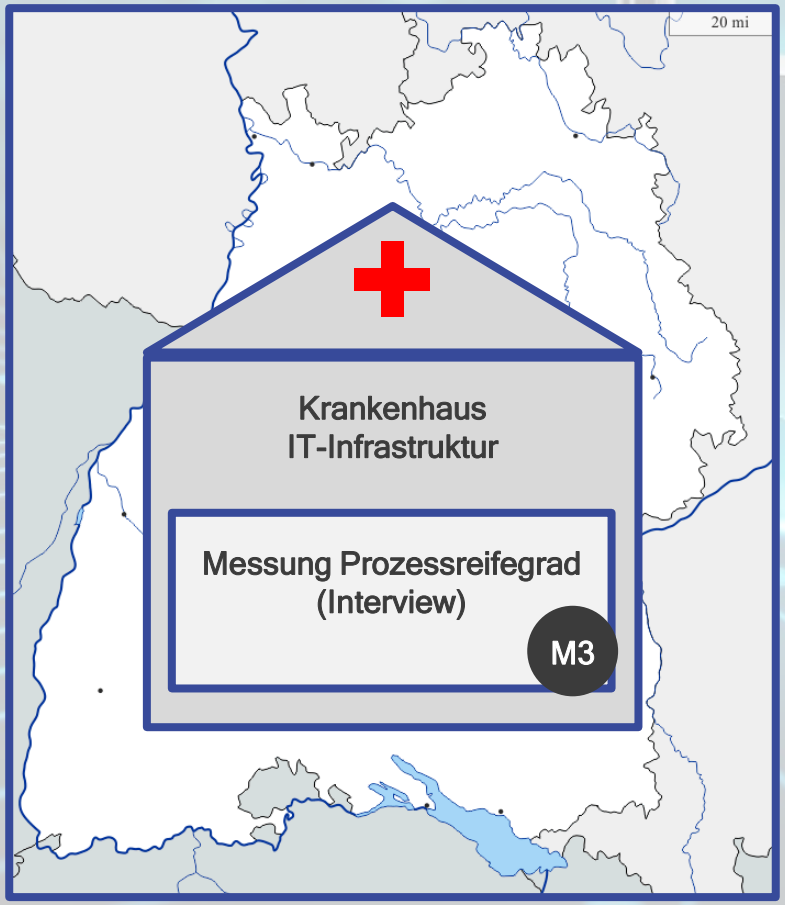
Messung Prozessqualität mittels Quick Check Workshop

EnBW

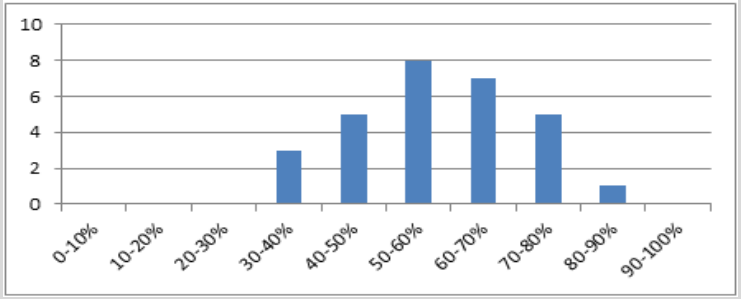
KPI B1) Anzahl vorhandener Schwachstellen

Quick Check Methodik:

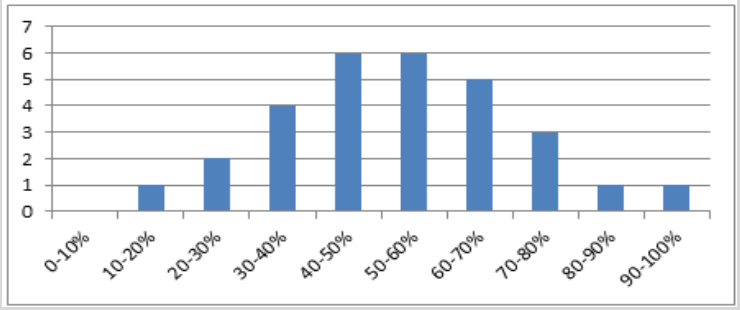
- **Workshop mit GF, CIO, ISB, DSB**
- Beantwortung **ausgewählter Fragen** mit **textlich vordefinierten Antworten** (Erfüllungsgrade je 25 %)
- Praxis **Ergebnis**: **gute Gesamteinschätzung + alle Beteiligten profitieren** durch Abstimmung
- **zeitliche Entwicklung** darstellbar



KPI C2) Technik



KPI C1) Organisation



KPI C3) Datenschutz