"T.I.S.P. Community Meeting 2022"

Berlin, 09.-10.11.2022

Angriffserkennung

Mike Zimmermann, Universitätsklinikum Dresden

Zur Person: Mike Zimmermann

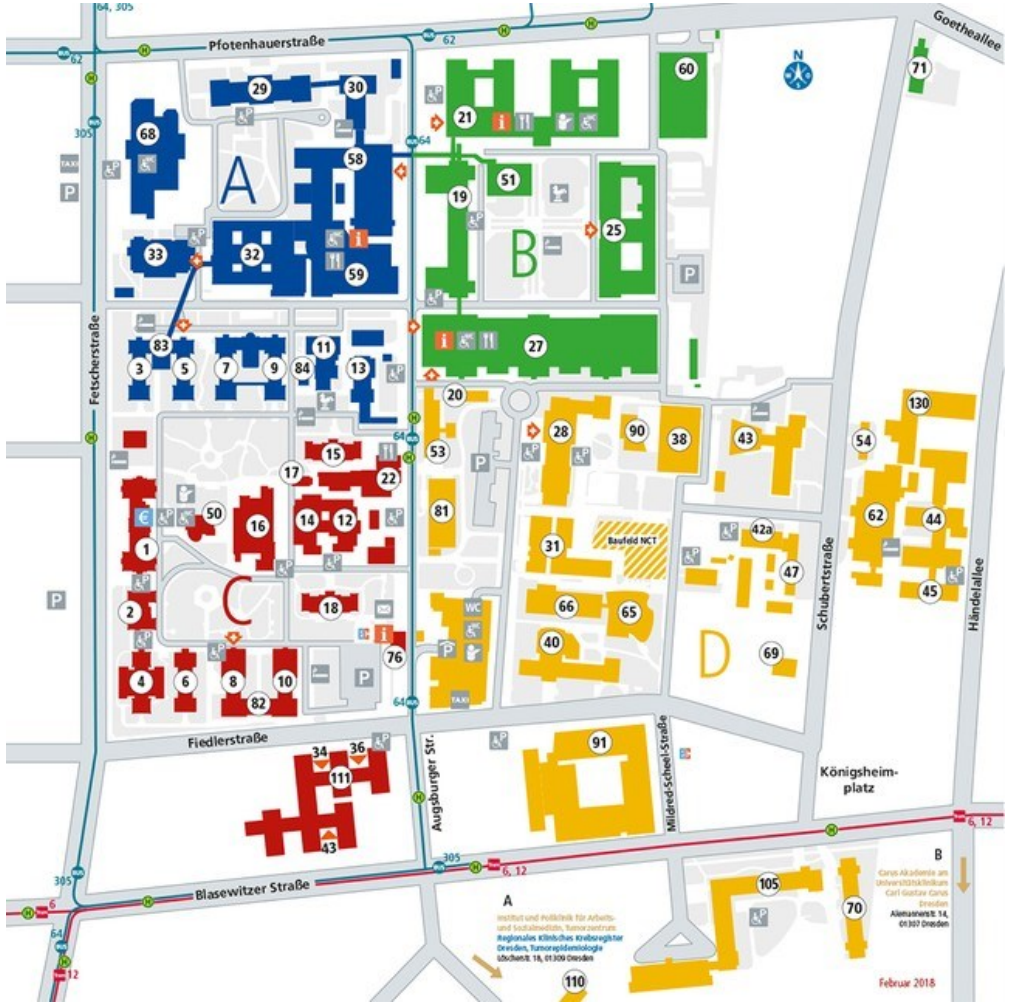
- am UK Dresden seit Januar 2012 im IT-Bereich
- IT-Sicherheitsbeauftragter UK Dresden und Medizinische Fakultät der TU Dresden seit März 2016

- Berufserfahrung:
  - 8 Jahre - IT Infrastruktur - Pharmabranche
  - 8 Jahre - IT Testdatenanalysecenter - Luftfahrtbranche

- Mitarbeit in externen Gremien
  - UP KRITIS Branchenarbeitskreis „Medizinische Versorgung“
  - UP KRITIS Arbeitskreis „TAK OpInAt“ (Operativer Informationsaustausch)
  - Verband der Universitätsklinika (AG Informationssicherheit)
  - Krankenhausgesellschaft (AG §75c SBG V)
  - KRITIScher Stammtisch (https://kritischer-stammtisch.de/)

Das Uniklinikum Carl Gustav Carus Dresden

- 1.410 Betten
- 26 Kliniken, 4 Institute und
  17 interdisziplinäre Zentren
- 6.546 Mitarbeiter
  - 2.166 Pflegedienst
  - 965 Ärztlicher Dienst
- 469 Auszubildende
- 3.008 Studierende
- 58.672 stationäre Fälle pro Jahr
  -> Kritische Infrastruktur
- 300.000 Patienten pro Jahr



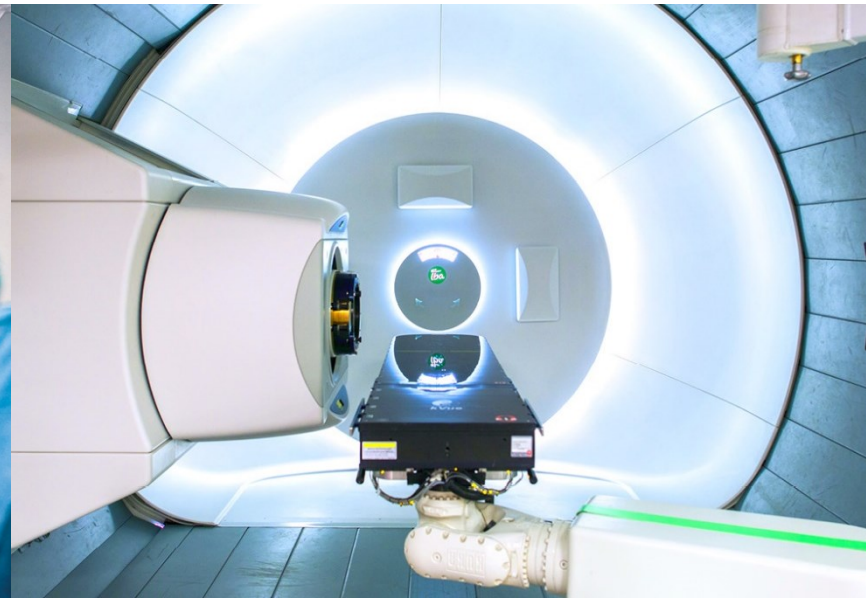
IT-Infrastruktur

- 11.000 stationäre und mobile Clients
- 12.000 Benutzerkonten
- 550 physische Server & 900 virtualisierte Server
- 1.700 Drucker
- 15.000 vernetzte Medizintechniksysteme
- 120.000 Netzwerkports, davon 50.000 aktiv
- TK Anlage (12 redundante TK Module) 5.300 digitale Anschlüsse, 2.1000 analoge, 3.800 DECT)

Anforderungen an die Informationssicherheit

- rechtliche Rahmenbedingen
- Gefährdungs- und Bedrohungslage





Die Ausgangslage

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Unsere Kernaufgabe ist die Behandlung unserer Patienten*innen unter Einhaltung der Grundwerte Patientensicherheit und Behandlungseffektivität

Aber:

„Alle wesentlichen strategischen und operativen Funktionen und Aufgaben, insbesondere auch die Kernkompetenz im Bereich der medizinischen und pflegerischen Patientenversorgung, werden durch Informationstechnik (IT) maßgeblich unterstützt!“

<<Auszug aus der InfoSec Leitlinie der Krankenhausleitung (Standardführungsprozess für alle Mitarbeiter)>>

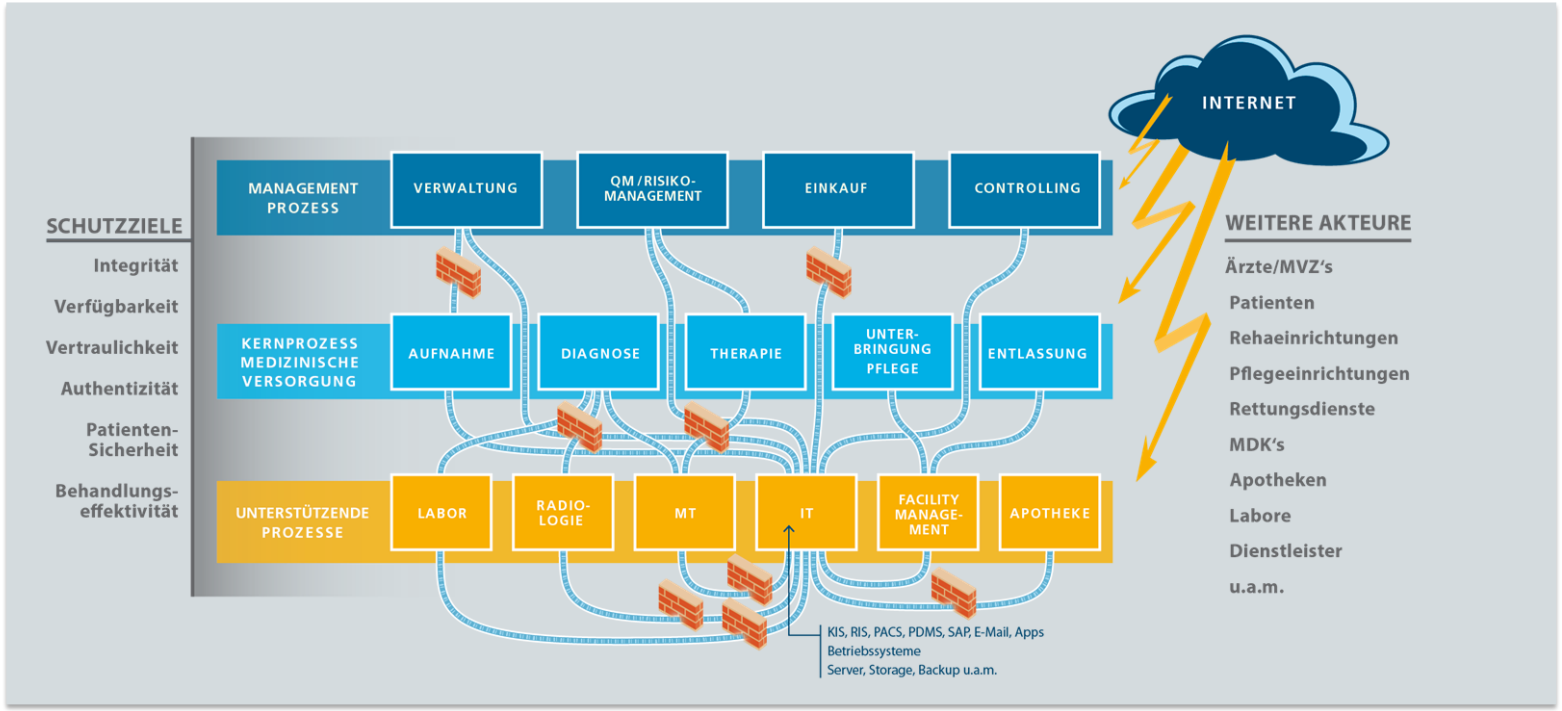
Der Stellenwert der IT, MT und GLT wird oft den Ansprüchen nicht gerecht!

Komplexität eines Krankenhauses

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

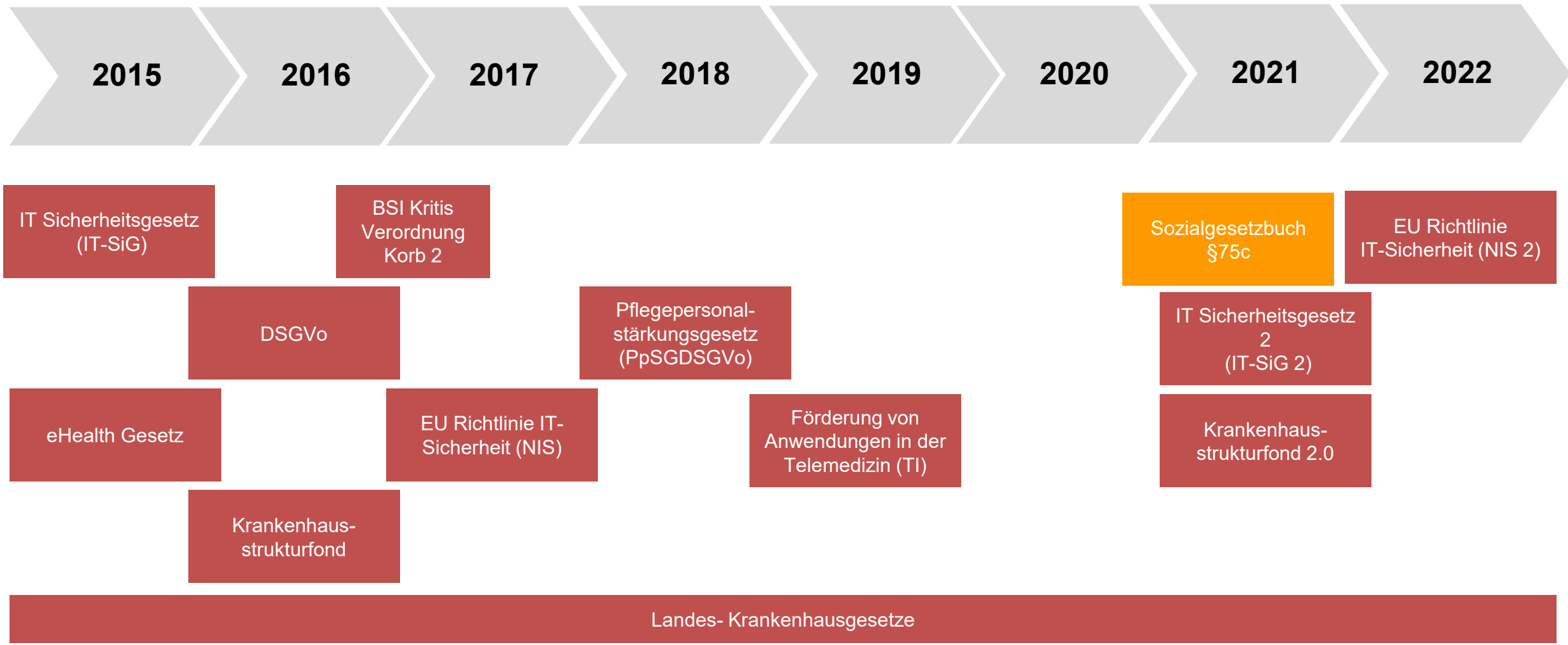
Krankenhäuser haben eine höhere Komplexität (MT, IT, Facility-Management, Labor, Apotheke) als andere Bereiche in der Wirtschaft, das ist die besondere Herausforderung

Sicherheit ist kein Produkt – Sicherheit ist ein Prozess



Rechtliche Rahmenbedingungen

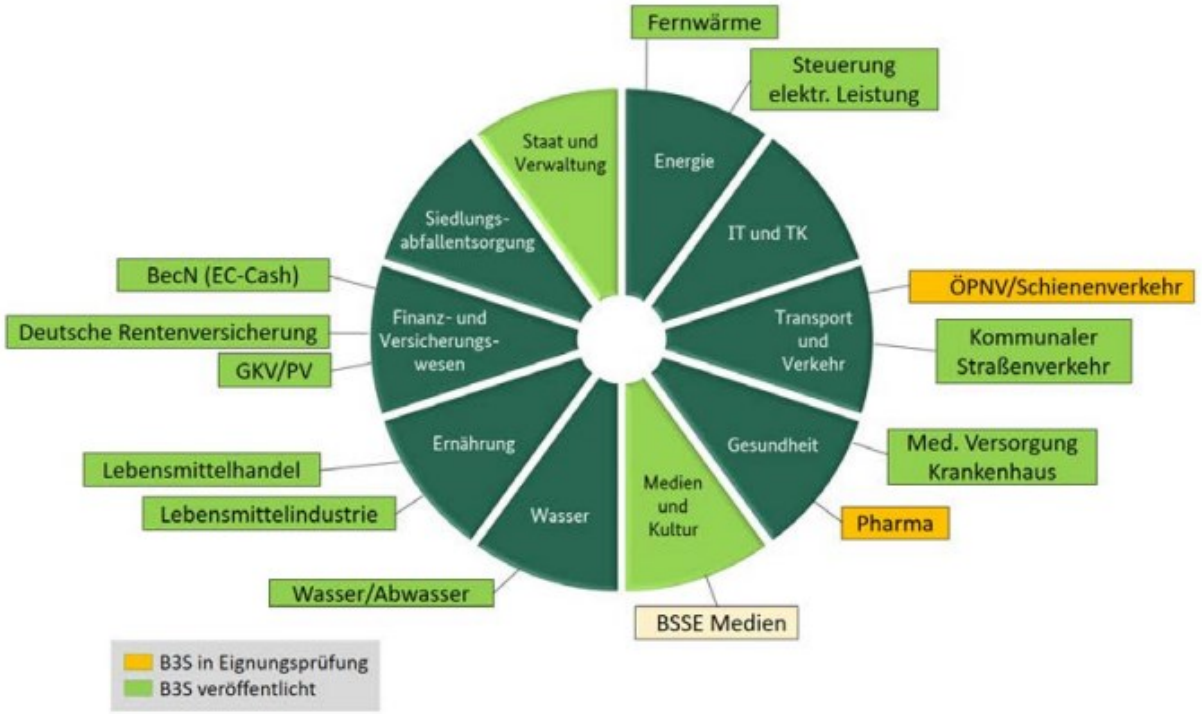
TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.



Sicherheitsstandards

- **Jeder kritischen Infrastruktur ist freigestellt, welchen Sicherheitsstandard sie einsetzt!**
  - BSI IT-Grundschutz, ISO 27001, eigene Standards, Branchenspezifischer Sicherheitsstandard (B3S) usw

- **Der B3S des UP KRITIS BAK „Medizinische Versorgung“ ist das Standardwerk für KH**
  - basiert auf ISO 27001 und berücksichtigt die branchenspezifischen Gegebenheiten
  - gemeinsam entwickelt mit der DKG und aktuell in Überarbeitung
  - Eignungsprüfung durch das BSI und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)



B3S Risikomanagement

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

„Zur Aufrechterhaltung der Funktionsfähigkeit der kritischen Dienstleistung ist ein angemessenes und wirksames Risikomanagement zur Informationssicherheit zu betreiben“

- **Management- / Organisatorische Anforderungen**

- **Etablierung einer Standard Risikomanagement Prozessmethodik:**
  - Informationswerte (Risikoobjekte) und Verantwortliche (Risiko-Eigentümer) ermitteln
  - Kritikalität der Informationswerte festlegen
  - Risikokriterien festlegen
  - Bedrohungen und Schwachstellen identifizieren
  - Risiken bewerten (Eintrittswahrscheinlichkeit & Schadenspotenzial)
  - Risiken behandeln (akzeptieren, vermeiden, reduzieren usw.)
  - Risiken kommunizieren und überwachen

- **Inklusive Risikomanagement für Medizingeräte, Kommunikationstechnik und Versorgungstechnik in IT-Netzwerken**

- **B3S definiert 37 MUSS und SOLL Anforderungen**

B3S Maßnahmen ISMS

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

„Kernforderung ist die Implementierung eines Informationssicherheitsmanagementsystems (ISMS). Hier werden die Regeln, Verfahren, Maßnahmen und Tools definiert, mit denen sich die Informationssicherheit steuern, kontrollieren, sicherstellen und optimieren lässt.“

- **Informationssicherheitsmanagementsystems (ISMS)**
  - Organisationsanforderungen (KH-Leitung, Beauftragter für Informationssicherheit)
  - Meldepflichten nach §8b BSI-Gesetz
  - Kontinuitätsmanagement (Notfallmanagement)
  - Asset Management (Unternehmenswerte)
  - Robuste / Resiliente Architektur (Ausfallschutz)
  - Physische Sicherheit (Gebäudeschutz)
  - Personelle und organisatorische Sicherheit (Schulung & Awareness)
  - Vorfallerkennung und Behandlung (Incident Management)
  - Überprüfungen im laufenden Betrieb (Audit / Revision)
  - Externe Informationsversorgung und Unterstützung
  - Lieferanten, Dienstleister und Dritte


DEUTSCHE KRANKENHAUS GESELLSCHAFT DKG

Bundesverband der Krankenhausträger in der Bundesrepublik Deutschland

Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus

Gesamtdokument

22.10.2019

Gemäß Feststellungsbescheid vom 22.10.2019 zur Gewährleistung der Anforderungen nach § 8a Absatz 1 BSIG geeignet.

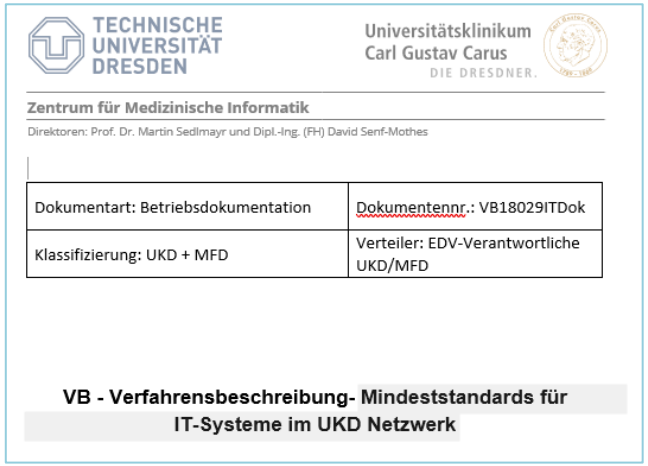
TLP-Klassifikation: WHITE
Kategorie: öffentlich
Version: 1.1

B3S Technische Maßnahmen

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- **Technische Informationssicherheit Teil 1**
  - Netz- und Systemmanagement (Netztrennung / Segmentierung)
  - Absicherung Fernzugriffe
  - Härtung und sichere Basiskonfiguration
  - Schutz vor Schadsoftware
  - Intrusion Detection / Prevention (Erkennung von Anomalien)
  - Identitäts- und Rechtemanagement (Rollen- und Berechtigungskonzept)
  - Sichere Authentisierung
  - Kryptographie
  - Mobile Sicherheit, Mobiler Zugang und Telearbeit

- **Technische Informationssicherheit Teil 2**
  - Vernetzung von Medizingeräten (DIN-EN 80001)
  - Datensicherung, Datenwiederherstellung und Archivierung
  - Ordnungsgemäße IT-Administration (Qualifikation, Vertretungsregel usw.)
  - Patch- und Änderungsmanagement (Wartung)
  - Umgang mit Datenträgern
  - Sicheres Löschen und Entsorgung von Datenträgern
  - Softwaretests und Freigaben (Einsatz Entwicklungs-/ Testumgebungen)
  - Beschaffungsprozesse
  - Protokollierung
  - Datenschutz


TECHNISCHE UNIVERSITÄT DRESDEN
Universitätsklinikum Carl Gustav Carus
DIE DRESDNER.

Zentrum für Medizinische Informatik

Direktoren: Prof. Dr. Martin Sedlmayr und Dipl.-Ing. (FH) David Senf-Mothes

Dokumentart: Betriebsdokumentation	Dokumentennr.: VB18029ITDok
Klassifizierung: UKD + MFD	Verteiler: EDV-Verantwortliche UKD/MFD

VB - Verfahrensbeschreibung- Mindeststandards für IT-Systeme im UKD Netzwerk

- **B3S definiert 168 MUSS und SOLL Anforderungen**

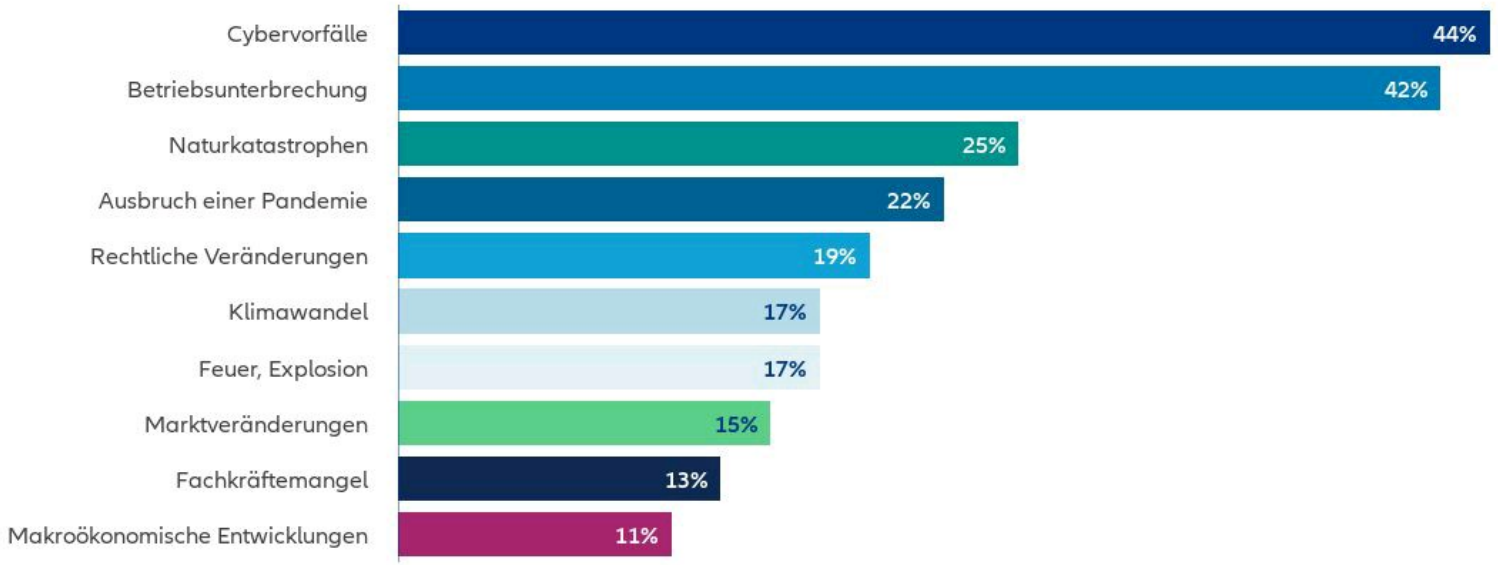
Geschäftsrisiken

Allianz

Top 10 Geschäftsrisiken weltweit in 2022

Allianz Risk Barometer 2022

Basierend auf den Antworten von 2.650 Risikomanagement-Experten aus 89 Ländern und Gebieten (% der Antworten). Die Zahlen ergeben nicht 100%, da jeweils bis zu drei Risiken ausgewählt werden konnten.



AGCS News & Insights

Source: Allianz Global Corporate & Specialty

Die Bedrohungslage

- E-Mails mit Schadsoftware im Anhang oder als Link
  - Trickbot, Formbook, Ryuk, Maze, Clop, Dridex, Loki, Agent Tesla, Conti, Emotet…
- Ausnutzen von Schwachstellen in Hard- und Software
  - Adobe, Microsoft, Apple, SAP, Oracle, Apache, Java…
- Phishing - Identitätsdiebstahl & -missbrauch
- Vorfälle bei Partner & Lieferanten

- Zusätzlich seit Corona, u.a.:
  - Videokonferenzen -> Störung und Datendiebstahl
  - Desinformation (Fake News, Deepfake) -> Chaos
  - Gefälschte Webseiten -> Betrug

Von: NCT-HR <dingman@ridgeviewtel.us>
Gesendet: Montag, 29. April 2019 08:43
An: [redacted]@uniklinikum-dresden.de>
Betreff: Neuer Gehaltsbrief

Universitäts KrebsCentrum (UCC)

Hallo,

Wie vom HR & Finance Team genehmigt, wird Ihr Monatsgehalt mit Wirkung vom Mai 2019 um 12,26% erhöht.

Laden Sie sich den beiliegenden Brief unten für genehmigte Abzüge herunter

Bitte unterschreiben Sie und senden Sie einen Brief an HR

Dokumente hier herunterladen

Kreditorenabteilung
Personalwesen und Leistungen an Arbeitnehmer
Universitätsklinikum Dresden

Vorfälle aus den letzten Monaten (Gesundheitswesen)

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

**Cyberkriminelle, die Patientendaten stehlen... Erpresser, die Daten verschlüsseln…
Hacker, die Medizintechnik manipulieren… Cyberangriffe auf Krankenhäuser nehmen zu!**

ST.-ADOLF-STIFT

Hackerangriff? Krankenhaus Reinbek widerspricht

Aktualisiert: 15.06.2022, 17:30

Eine Technik-Panne hat das St. Adolf-Stift in die Schlagzeilen katapultiert. Foto: Susanne Tamm

Es mussten mehrere Operationen verschoben werden. Die Klinik erklärt, dass der Fehler schnell behoben werden konnte. Es sei ein Defekt auf dem Server des Krankenhaus-informationssystem aufgetreten. Daraufhin hätte das System automatisch auf den zweiten Server umschalten müssen und dies habe aber nicht funktioniert.

28.06.2022 12:41 | BUNDESLÄNDER > TIROL

AUSMASS NOCH UNKLAR

Hacker-Angriff auf Med-Uni: Daten nun im Darknet

(Bild: stock.adobe.com, krone.at-Grafik)

Nach dem Hacker-Angriff auf die Medizinische Universität Innsbruck Mitte Juni sind offenbar Daten von Servern der Universität im Darknet veröffentlicht worden. Analysen und Ermittlungen zu Ausmaß und Art der Daten seien im Gange.

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

IT-Sicherheitslage

TLP:GREEN

Ausgabe: August 2022
Berichtszeitraum: Juli 2022

4.1 Ausfall der Strom- und Notstromversorgung

Sachverhalt

In der zweiten Julihälfte 2022 war ein KRITIS-Betreiber aus dem Sektor Gesundheit von einem Stromausfall betroffen. Die Notstromversorgung funktionierte ebenso nicht. Es kam zu einem Ausfall der IT-Infrastruktur. In der Folge war die kritische Dienstleistung zeitweise beeinträchtigt.

Maßnahmen

Der Betreiber griff auf Notfallkonzepte zurück. Nachdem die Stromversorgung zeitnah entstört worden war, konnten die Systeme wieder hochgefahren werden.

Vorfälle aus den letzten Monaten (Gesundheitswesen)

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Cyberkriminelle, die Patientendaten stehlen... Erpresser, die Daten verschlüsseln… Hacker, die Medizintechnik manipulieren… Cyberangriffe auf Krankenhäuser nehmen zu!

Die EDV wird neu aufgebaut

Klinikum in Bad Säckingen nach Hackerangriff auf dem Weg zurück in den Alltag

Von Axel Kremp
Mo, 31. Oktober 2022 um 19:00 Uhr
Bad Säckingen

Nach dem Hackerangriff vor einigen Tagen läuft der Betrieb im Rehaklinikum in Bad Säckingen – wenn auch noch eingeschränkt – wieder EDV-gestützt.

Cyberangriffe 2022 – Gesundheitswesen Europa:

28.10.22 KH Bad Säckingen (DE)
17.10.22 Gesundheitsportal Carenzorgt (Holland)
09.10.22 KH Les Bluets (Frankreich)
07.10.22 KH-Kette Barcelona (Spanien)
28.09.22 Kathol. Sozialdienstleister SKM (De)
15.09.22 KH Cahors Departement Lot (Frankreich)
12.09.22 Caritasverband München & Freising (De)
20.08.22 KH Corbeil-Essonnes (Frankreich)
19.08.22 Gesundheitsbehörde Turin (Italien)
05.08.22 Zahnarztpraxen (130 Praxen) (Holland/Belgien)
04.08.22 NHS 111 (UK)
25.07.22 AMEOS Klinikum St.Elisabeth Neuburg (De)
28.06.22 Uniklinik Innsbruck (Österreich)
27.05.22 KH Macon Saone-et-Loire (Frankreich)
25.05.22 Uniklinikum Lüttich (Belgien)
18.05.22 Gesundheitssystem Grönland
14.05.22 KH-Kette Region Wallone (Belgien)
05.05.22 Gesundheitsbehörde Italien
01.05.22 KH-Kette in Mailand (Italien)
01.05.22 KH Vila Verde (Portugal)
26.04.22 KH Garcia de Orta (Portugal)
21.04.22 AZ Herentals (Belgien)
19.04.22 KH-Kette GHT (Frankreich)
15.04.22 KH ASP Messina (Italien)
05.04.22 KH Granada (Spanien)
29.03.22 KH Korsika (Frankreich)
21.03.22 KH Dublin (Irland)
20.02.22 Med.Luftrettung Polen
10.02.22 KH Pajeczno (Polen)
10.02.22 Laborkette Lissabon (Portugal)
13.01.22 Medizin Campus Bodensee (De)
07.01.22 KH Tours (Frankreich)

Essonne. Centre hospitalier visé par une cyberattaque: une rançon de 10 millions de dollars demandée

L'hôpital de Corbeil-Essonnes a été attaqué par un rançongiciel, dans la nuit de samedi 20 à dimanche 21 août 2022. Un plan blanc a été déclaré pour éviter que les patients n'en pâtissent.

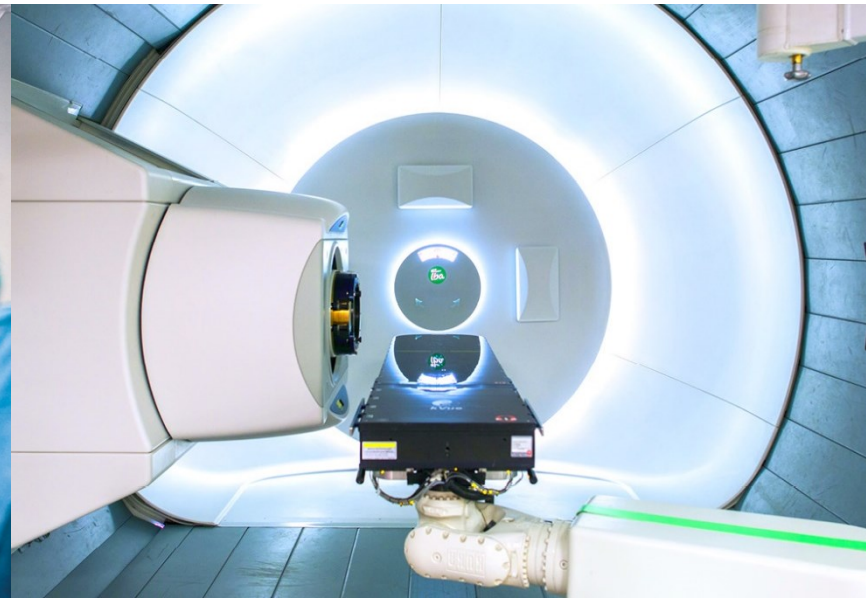
Cyberangriff auf ein Krankenhaus in Frankreich

Das Centre Hospitalier Sud Francilien (CHSF) in Corbeil-Essonnes, südöstlich von Paris, wurde seit der Nacht von Samstag, dem 20. August 2022, auf Sonntag, den 21. August 2022, gegen 1 Uhr Opfer eines Cyberangriffs, der seine Abteilungen und die Notfallversorgung stark beeinträchtigte, möglicherweise wochenlang, wie die Leitung des Krankenhauses mitteilte. Lösegeld in Höhe von 10 Millionen US-Dollar gefordert!

Die Umsetzung am UK Dresden

- gelebter Informationssicherheitsmanagementprozess





Informationssicherheitsmanagementsystem

- Standardisierte Dokumentenlenkung / -klassifizierung
- Verknüpfung IT-Assets + Krankenhausprozesse für das ganzheitliche Identifizieren von Risiken
- IT-Revision und Integration in das zentrale Audit- & Begehungsmanagement
- User Awareness – InfoSec Mitarbeiter Kompetenzmanagement

Organisationshandbuch	
UKD-STD	UKD Standardführungsprozess Informationssicherheit (Leitlinie)
Geltungsbereich	
ISMS Scope	Anwendungsbereich des ISMS (Scope Dokument)
Konzepte / Strategien	
Konzept	Informationssicherheit an der HSMD
Konzept	Cloud
Konzept	User Awareness
Konzept	Kryptographie
Konzept	elektronische Signatur
Sicherheitsrichtlinien	
SR	IT-Nutzung (2.01)
SR	Internetnutzung und Email (2.02)
SR	Schutz vor Schadsoftware (2.03)
SR	Mobile Geräte (2.04)
SR	Datensicherung (2.05)
SR	Archivierung (2.06)
SR	Einsatz von Verzeichnisdiensten (2.07)
SR	Behandlung eines Informationssicherheitsvorfalls (IS-Vorfall) (2.09)
SR	Externe Kommunikation und Fernzugriff (2.10)
SR	Wechseldatenträger (2.11)
SR	Outsourcing von IT-Leistungen (2.12)
SR	Einführung eines neuen IT-Verfahrens (IT-System, IT-Hardware, IT-Software) (2.13)
SR	Server (2.14)
SR	TK-Anlage (2.15)
SR	Sicherheitskonzept für das ERP-Softwaresystem SAP R/3 am UKD (2.16)
SR	Software (2.17)
SR	IT-Beschaffung (2.18)
SR	Notfallvorsorge (2.19)
SR	Netzwerkinfrastruktur (2.20)
SR	IT-Revision (2.21)
SR	Kryptographie (2.22)
SR	Mindeststandards für IT-Systeme im UKD Netzwerk
SR	Einsatz von Sammelkonten
SR	Ausführung von Makros in Office-Dateien
SR	Fernwartung innerhalb des UKD - Netzwerkes
SR	Trennung Admin-/Userdomainkonto
SR	Berechtigungskonzept für administrative Gruppen in der AD Domain "MED"

IT-Risikomanagement

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Hacking
  - Phishing
  - Identitätsmissbrauch
  - Ransomware
  - Datendiebstahl
  - Störung Collaboration
  - Desinformation
  - Fälschung/Betrug
- Techn. Versagen
  - IT Ausfall
  - Elektro Ausfall
- Allg. Gefahren
  - Hochwasser
  - Feuer

Bedrohungsmatrix UK Dresden Stand 01.09.2022

Bedrohung / Gefährdung			Risiko Vormonat	Tendenz	Risiko Trend	Eintrittswahrscheinlichkeit	Schadenspotential	Verwundbarkeit (nach Maßnahmen)	Bemerkung
	B3S OH A	B3S ID			ohne Maßnahmen 1 = gering 2 = mittel 3 = hoch 4 = kritisch	1 = gering 2 = mittel 3 = hoch 4 = kritisch	1 = gering 2 = mittel 3 = hoch 4 = kritisch	1 = gering 2 = mittel 3 = hoch 4 = kritisch	
					EW*SP	auszufüllen	auszufüllen	auszufüllen	
Kategorie "Allgemeine Gefährdungen"									
Naturgefahren (Höhere Gewalt und Elementarschadensereignisse)	A1.3	BED1	3		6	2	3	2	Gefahren speziell für Systeme, Anlagen, Standorte, die zur Erbringung des Geschäfts notwendig sind (z.B. RZ-Standorte, Stromtrassen, Kläranlagen usw.)
Abhängigkeiten von Dienstleistern und Herstellern (Ausfall externer Dienstleister)	A1.6	BED2	9		3	1	3	3	Dedizierte Lieferanten sowie Partner, Cloud-Dienstleister usw. Abhängigkeiten von Dienstleistern und Herstellern (Ausfall externer Dienstleister, unberechtigter Zugriff, versteckte Funktionen in Hard- und Software)
Ausfall von Basisinfrastrukturen mit direktem Bezug zur IT	A1.14	BED3	6		8	2	4	3	Sekundäreffekte, z.B. Wasser (als Kühlung für Server), Strom und GLT
Manipulation, Diebstahl, Verlust, Zerstörung von IT oder IT-relevanten Anlagen	A1.8	BED4	3		6	2	3	3	
Beschädigung oder Zerstörung verfahrenstechnischer Komponenten, Ausrüstungen und Syste	A1.13	BED5	neu		0				
Terroristische Akte	A1.2	BED6	neu		4	1	4	3	physisch mit Wirkung auf die IT oder direkt IT-bezogen
Kategorie "IT-spezifische Gefährdungen"									
Hacking und Manipulation	A1.1	BED7	6		9	3	3	3	externe Angreifer
Schadprogramme	A1.9	BED8			0				Erfolgreiches Einnisten von Malware (beliebige Quelle)
.- Allgemein			9		6	3	2	3	
.- Emotet			9		6	2	3	2	Trojaner (PW-Diebstahl, Datenabfluss, Verbreitung, Verschlüsselung)
.- Gozi/Ursnif			9		6	2	3	3	Trojaner (PW-Diebstahl, Datenabfluss, Verbreitung, Verschlüsselung)
.- Ransomware			9		9	3	3	2	Trojaner (Verschlüsselung)
Gezielte Störung / Verhinderung von Diensten (DDoS, gezielte Systemabstürze)	A1.11	BED10	6		6	3	2	3	externe (Überlast-)Angriffe gegen IT-Systeme / Applikationen
Social Engineering (Voice-Phishing)	A1.10	BED11	3		6	3	2	2	Angriffe gegen Personen, um Informationen über Dritte und Org-Einheiten zu erhalten
.- CxO Fraud			6		3	3	1	1	E-Mails von bekannten Absender mit Überweisungsaufforderung
Identitätsmissbrauch (Phishing, Skimming, Zertifikatsfälschung)	A1.4	BED12	6		6	3	2	2	technische Angriffe mit dem Ziel Identitäten Dritter anzunehmen
Advanced Persistent Threat (APT)	A1.12	BED13	4		4	2	2	2	gezielte, zeitl. ausgedehnte Angriffe gegen dedizierte Unternehmen (meist Wirtschaftsspionage, Wettbewerber)
Spam		BED14	3		6	3	2	2	allgemeines Spam-E-Mail-Aufkommen
Mobile Security / Home Office			8		8	4	2	3	
Kategorie "Schwachstellen"									
Organisatorische Mängel	A2.1	SW1			0				
.- Unbefugter Zugriff	A1.7	BED9	4		2	2	1	1	Prozesse)
.- Infrastrukturelle Mängel (baulich, Versorgung mit Strom etc.)	A2.5	SW5			0				
.- Verwendung ungeeigneter Netze/ Kommunikationsverbindungen	A2.6	SW6			0				sonstige Schwächen in der Kommunikationsarchitektur
Schwachstellen / fehlende Sicherheits-Patches	A2.2	SW2			0				System- und Anwendungssicherheit incl. Patch-Mngt-Prozess
.- Allgemein			6		9	3	3	3	
.- VPN			2		2	1	2	1	
.- Konferenzsysteme			6		4	2	2	2	
Technisches Versagen von IT-Systemen, Anwendungen oder Netzen	A2.3	SW3	6		12	3	4	3	
Menschliche Fehlhandlungen, menschliches Versagen	A2.4	SW4	6		6	2	3		
Missbrauch (Innentäter)	A1.5		2		2	1	2	1	bewusste Handlungen von (unzufriedenen) Mitarbeitern
Fehlendes Personal (z.B. Krankheit, Fluktuation)			12		9	3	3	3	Betriebs- und Sicherheitsprozesse können nicht aufrecht erhalten werden, auf Ereignisse / Vorfälle kann nicht angemessen reagiert werden
Verkopplung von Diensten	A2.7	SW7			0				Beeinträchtigung eines Dienstes durch Störung anderer Dienste
Kategorie "Branchenspezifische Gefährdungen"									

IT-Vorfallsmanagement

- Etablierung eines ganzheitlichen Vorfallsmanagement-Prozesses
  - Verantwortlichkeiten
  - Definition IT-Vorfall, u.a.:
    - Nichteinhaltung Richtlinien
    - Außergewöhnliches Systemverhalten
    - Missbrauch von IT-Systemen
    - Verlust von IT-Systemen
    - Verbreitung von Schadcode / Viren
    - Identitätsdiebstahl von Zugangsdaten
    - sicherheitskritische Schwachstellen
  - Meldewege intern
  - Meldeverpflichtungen extern:
    - IT-Sicherheitsgesetz
    - DGVO
    - Medizinprodukte-Sicherheitsplanverordnung
    - Sächsisches IT-Sicherheitsgesetz

TECHNISCHE UNIVERSITÄT DRESDEN

Universitätsklinikum Carl Gustav Carus DIE DRESDNER.

Zentrum für Medizinische Informatik

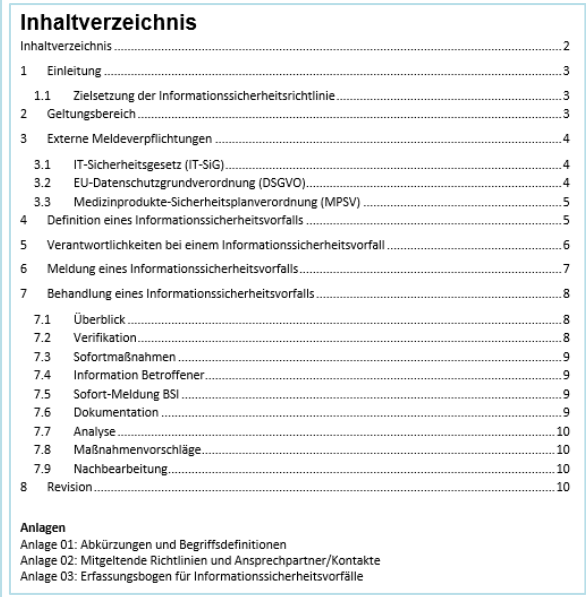
Direktoren: Prof. Dr. Martin Sedlmayr und Dipl.-Ing. (FH) David Senf-Mothes

Version: 1.1 Datum: 28.07.2021	Anwendung: IT-Sicherheit

Informationssicherheitsrichtlinie
Behandlung eines Informationssicherheitsvorfalls
(IS-Vorfall)

Verfasser	Mike Zimmermann

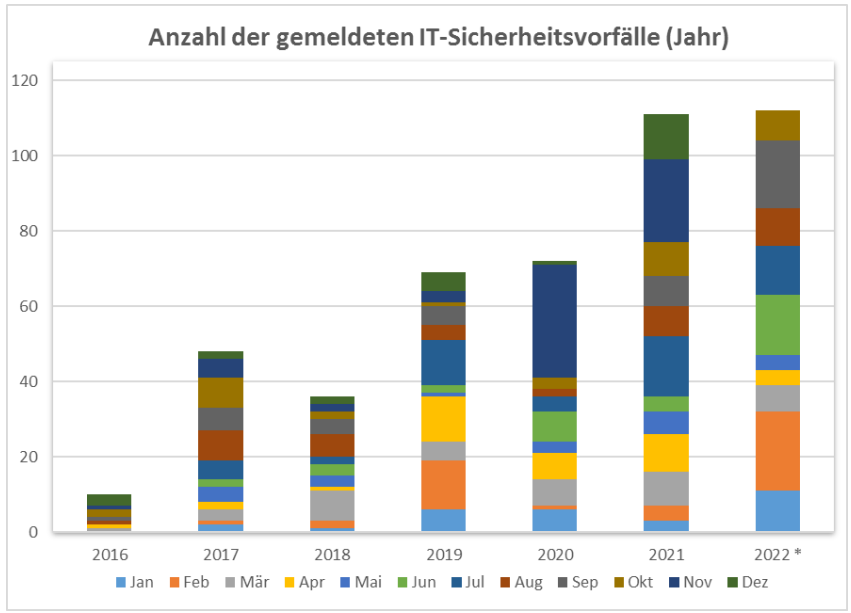
Version	Bearbeiter	Änderung	Datum
1.0	Mike Zimmermann		18.10.2019
1.1	Mike Zimmermann	Allg.Aktualisierung	28.07.2021

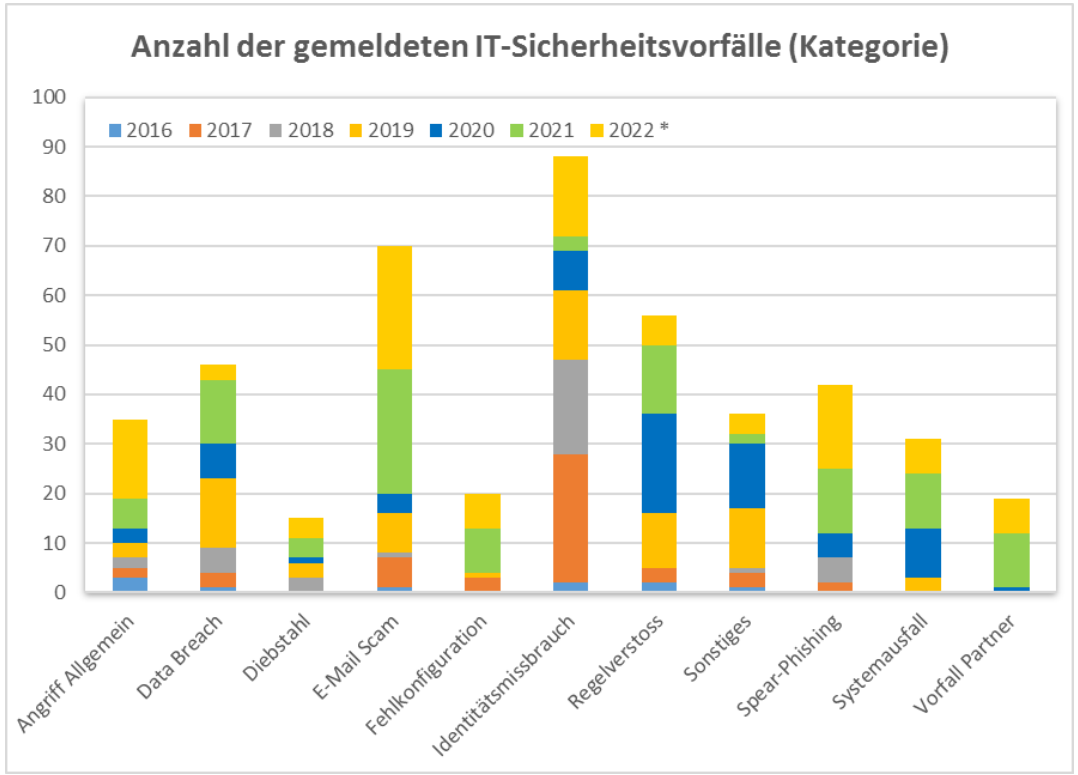


Inhaltverzeichnis

Anlagen

IT-Vorfälle – Statistik UK Dresden





LAGEBILD HOCHSCHULMEDIZIN DRESDEN (HSMD)

Aktuelle Bedrohungslage

Allgemeine Übersicht

	2022	Tendenz	2021
Bearbeitung von Schwachstellen	285	↑	59
Bewertung neuer IT-Verfahren	88	↑	53
Risikomeldungen	0	↓	2
CarusNet Meldungen	10	↗	9
Bearbeitung von IT-Vorfällen, darunter:	112	↗	111
.- Angriff Allgemein	16	↑	6
.- Data Breaches	3	↓	13
.- Diebstahl	4	→	4
.- E-Mail Scam	25	↗	25
.- Fehlkonfiguration	7	→	9
.- Identitätsmissbrauch	16	↑	3
.- Regelverstöße	6	↓	14
.- Spear Phishing	17	↗	13
.- Systemausfall	7	↘	11
.- Vorfälle bei Partner o. Lieferanten	7	↘	11

(*) = bis 26.10.2022

Schwachstellenmanagement

Ziel: Aufbau eines systematischen und kontinuierlichen Schwachstellenmanagement-Prozesses!

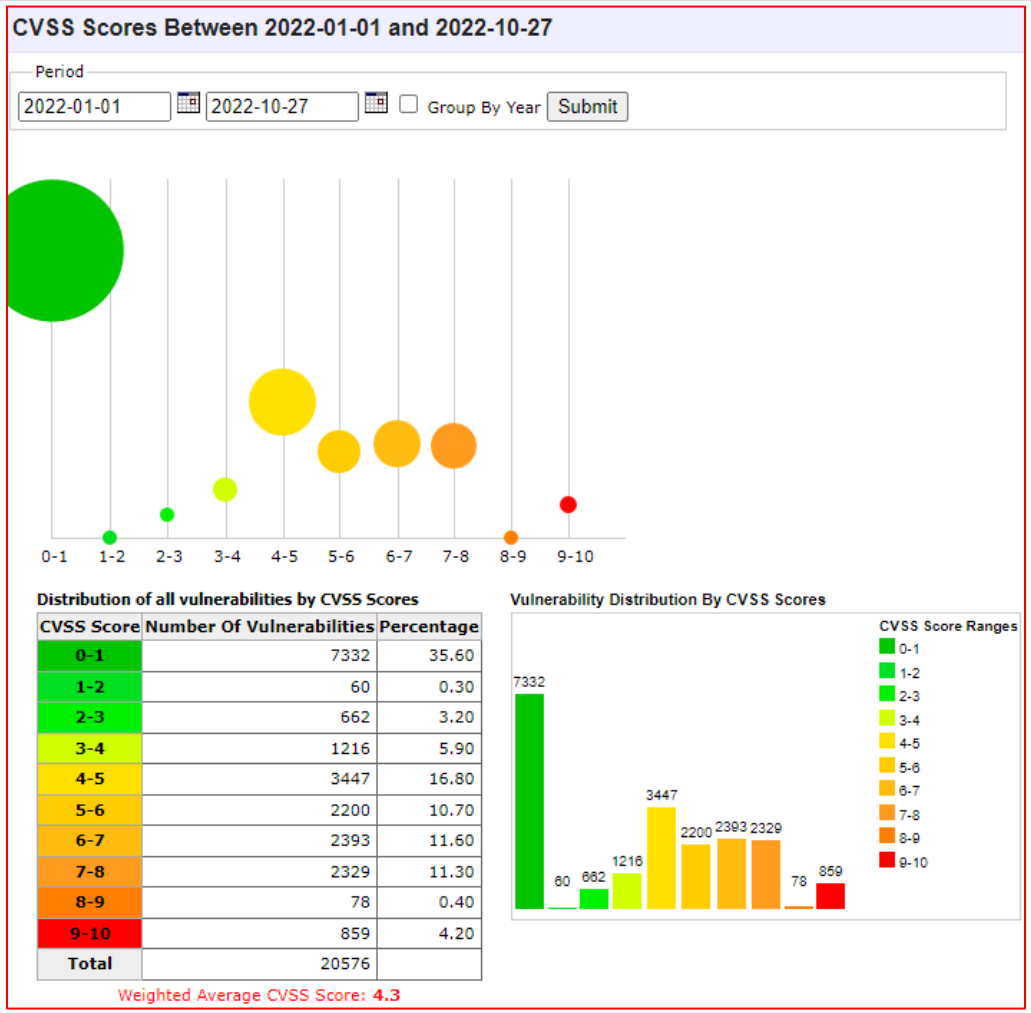
WARUM?

Beispiele:

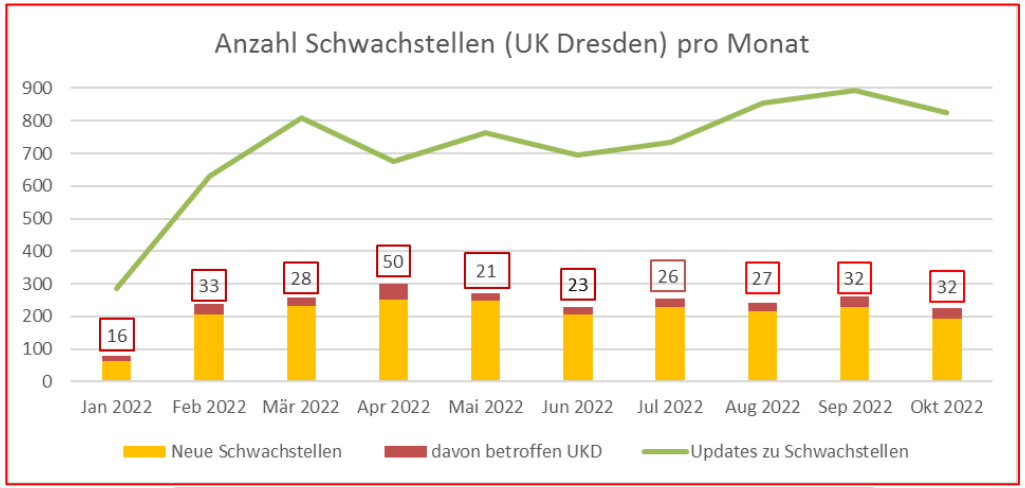
- Citrix - 2020
- MS Exchange (#hafnium, #ProxyLogon) – 2021
- Medizintechnik (Olympus, Phillips, Infusionspumpen) – 2021
- GLT (Rohrpostanlagen Swisslog, Siemens) - 2021
- Log4J (#log4Shell) - 2021/22
- Bios (#InsideH2O) – 2022
- Fernwartung MT Axeda Agent (#Access:7) – 2022
- USV (APC – Schneider Electric) - 2022
- HP Drucker - 2022

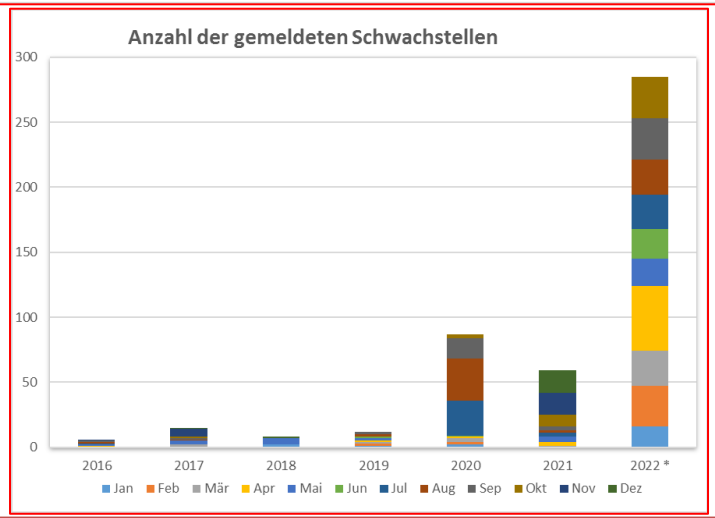
Quelle: F-Secure

Schwachstellen – Wieviel?



Quelle: https://www.cvedetails.com/ 27.10.2022

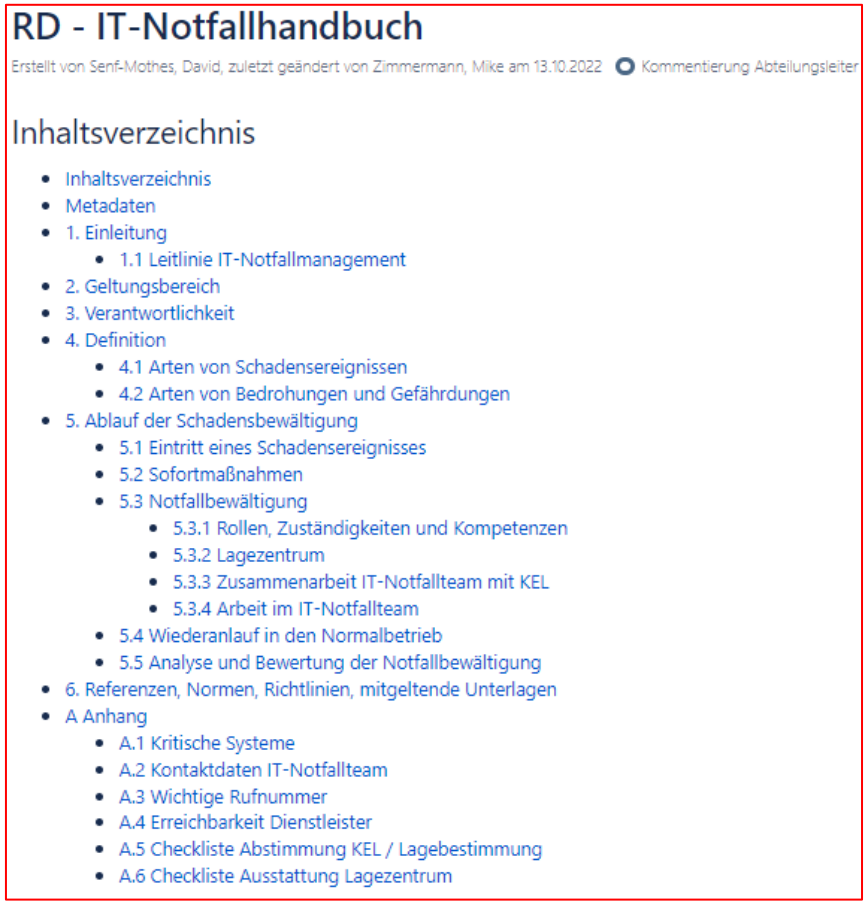




Übersicht der am UK Dresden bearbeiteten Schwachstellen (Stand 26.10.2022)

Notfallmanagement

- Kliniken und Geschäftsbereiche benötigen ein Ausfall- / Notfall-konzept
- Erarbeitung eines IT-Notfallhandbuch
- Auswirkung auf die IT:
  - Definition der kritischen Prozesse und Dienstleitungen
  - Aktualisierung der Verantwortlichkeiten und Entscheidungsregularien
  - Überprüfung der Notfallprozesse in den Kliniken & Geschäftsbereichen
  - Anpassung der Notfallorganisationsstruktur
    - Lagezentrum
    - Schnittstellen
    - Dokumentation
    - Meldeverpflichtungen
  - Kommunikationskonzept
- Durchführung IT-Notfallübungen



RD - IT-Notfallhandbuch

Erstellt von Senf-Mothes, David, zuletzt geändert von Zimmermann, Mike am 13.10.2022 Kommentierung Abteilungsleiter

Inhaltsverzeichnis

TOM – Vielzahl an Maßnahmen

- Netzwerksicherheit: Absicherung von Netzübergängen / Firewall / Segmentierung / NAC
- Härtung und sichere Basiskonfiguration der Systeme
  - SOP Mindeststandards für IT-Systeme im UKD NT
  - Geprüfte Standard Images und Softwarepaketierung
  - Schwachstellen- und Patchmanagement
  - Need-to-know Prinzip
- Absicherung Fernzugriffe
  - Sicherheitsrichtlinie Externe Kommunikation und Fernzugriff
  - VPN Zugang mit definierten Beantragungsprozess für Mitarbeiter*innen oder für Firmen
  - Zweifaktorauthentifizierung und Protokollierung
- Schutz vor Schadsoftware
  - Endpoint-Protection
  - E-Mail-Security
  - URL & Content Filterung (EndPoint und Proxy)
  - Makrosicherheit (nur signierte Makros erlaubt)
  - Application Whitelisting
  - Logging und Monitoring (SIEM)
  - SOP Emotet Check
  - SOP Schutz vor Ransomware (inkl. Checkliste)
- Intrusion Detection / Prevention
  - Cisco Stealthwatch

TOM – Vielzahl an Maßnahmen

- Identitäts- und Rechtemanagement
  - Rollen und Berechtigungskonzepte für die führenden IT-Systeme
  - Need-to-Know und Least Privileges
  - Dokumentation und Freigabeworkflow im zentralen Ticketsystem oder direkt im IT-System
  - Regelmäßige Prüfung im Rahmen der IT-Revision
  - SOP Mitarbeiteraustritt aus dem Unternehmen
  - Richtlinie Trennung Admin/Userdomainkonto
- Patch- und Änderungsmanagement; Softwaretest und -freigaben
  - SOP Changemanagement (Freigabeprozess und Dokumentation)
  - Zentrales Updatemanagement (WSUS, Baramundi)
  - Test vorab bei ausgewählten Systemen oder in Testumgebung
- Datensicherung und Datenwiederherstellung
  - Zentrales Backupkonzept
- Kryptographische Absicherung
  - Datenträgerverschlüsselung mobilen Systeme
  - E-Mail Verschlüsselung
  - Netzwerkverbindungen (SSL/TLS, HTTPS)
  - DFN-PKI (Nutzer und Serverzertifikate)
- Mobile Sicherheit
  - Datenträgerverschlüsselung
  - Kein BYOD
  - Mobil-Device-Management
    - Management der mobilen Systeme
    - Trennung private und dienstliche Nutzung
    - Fernlöschung/-sperrung
- Sichere Authentifizierung
  - Passwortkomplexität und regelm. Änderung
  - Bei externen Zugriff Zweifaktorauthentifizierung
  - Monitoring und Sperrung bei Auffälligkeiten

TOM – Vielzahl an Maßnahmen

- Beschaffungsprozesse
  - Vorgaben Technischer und organisatorischer Maßnahmen
  - Richtlinie Einführung eines neuen IT-Verfahrens
- Sicheres Löschen und Entsorgungsprozess
  - Entsorgungsordnung – Abfallwegweiser für datenschutzkonformes Löschen von Daten und Systemen
- Externe Informationsversorgung und Unterstützung
  - CERT.BUND (Lageberichte, Schwachstellen und Auffälligkeiten)
  - SAX.CERT (Lageberichte, Schwachstellen und Auffälligkeiten)
  - DFN.CERT (Schwachstellen und Auffälligkeiten)
  - BSI, UP Kritis, Allianz für Cybersicherheit
  - LKA Sachsen ZAC, BSI Mobile Incident Response Team
  - Austausch in diversen externen Arbeitsgruppen (z.B. VUD AG InfoSec)
- Aufbau eines zentralen Identity Management Systems (IDM)
  - Integration aller relevanten IT-Systeme (u.a. SAP HR, MS AD, KIS Orbis)
  - Automatisierte Bereitstellung der Identitäten (On-/Off-Boarding) und Berechtigungen (IAM)
- Aufbau und Etablierung eines Security Operation Centers (SOC)
  - Förderung im Rahmen des Krankenhauszukunftsgesetz (KHZG)
  - Operatives IT-Sicherheitsmanagement

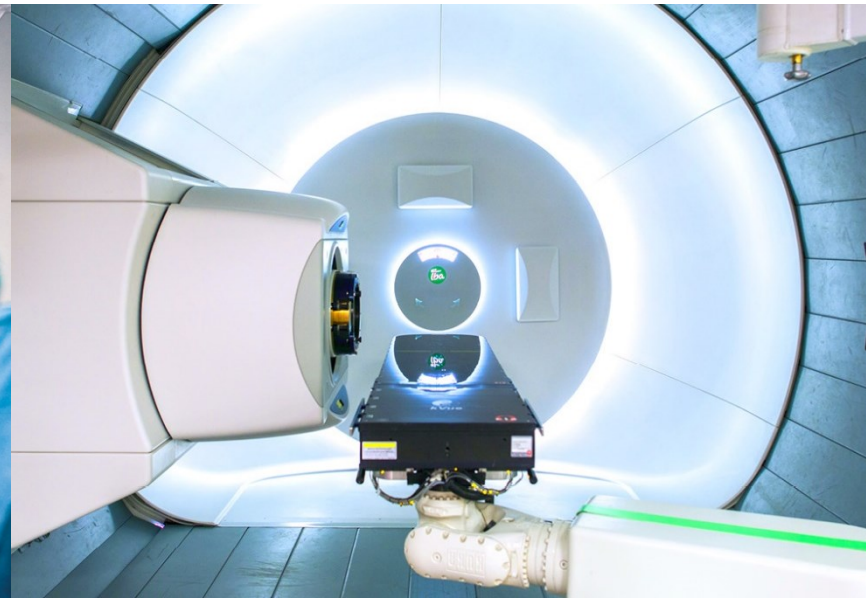
Fazit

- Angriffe werden weiter zunehmen!
- Komplexität wird weiter steigen, ganzheitliche Betrachtung!
- Ressourcen sind knapp, deshalb die Zusammenarbeit zwischen den Kliniken fördern!
- Gesetzliche Anforderung werden verschärft!
- Wichtigste Aufgaben:
  - Dokumentation (Assetmanagement)
  - User Awareness / Medienkompetenz
  - Schwachstellen- und Patchmanagement
  - Notfallmanagement

Angriffserkennung

- rechtliche Rahmenbedingungen
- praktische Umsetzung





Rechtliche Rahmenbedingungen

- BSIG §8a (1a)
  - (1a) Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Absatz 1 Satz 2 und 3 gilt entsprechend.
  - Dabei soll der Stand der Technik eingehalten werden.
  - Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.
- Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung (OH SzA)

  -> https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.html

OH SzA im Detail

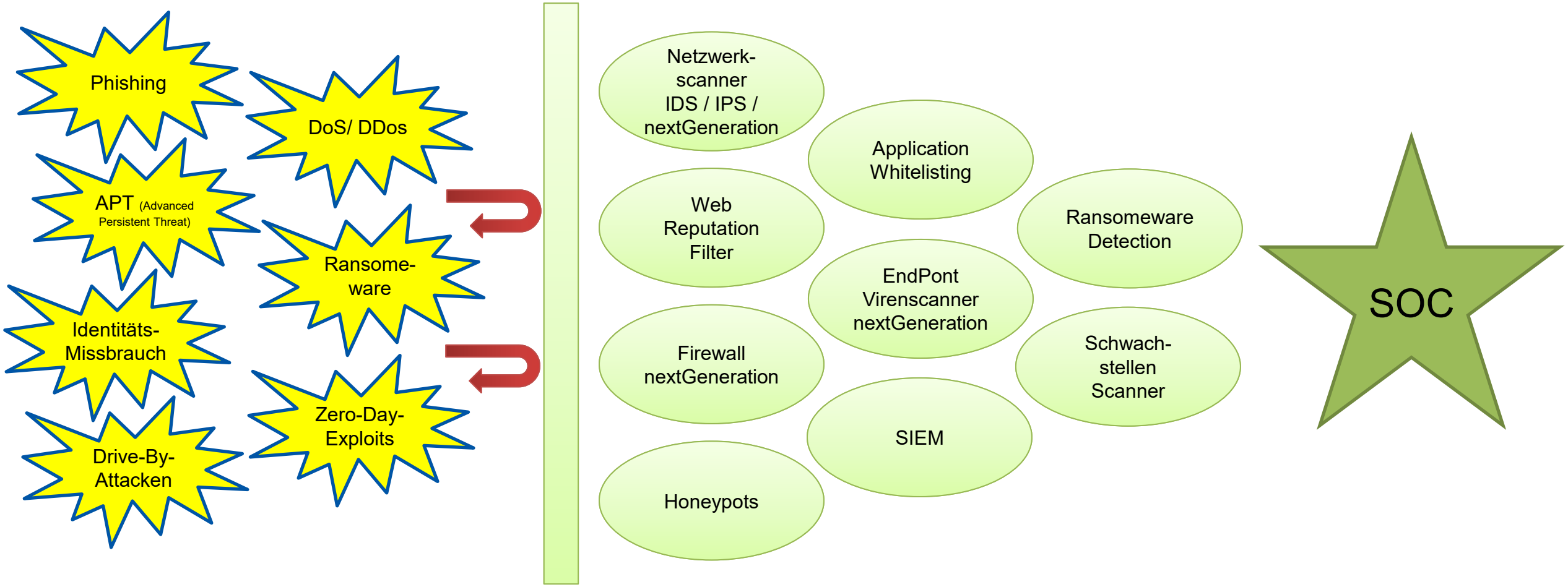
- Definiert den „Stand der Technik“?
- Beschreibt 88 Anforderungen (63x MUSS, 19x SOLL, 6 KANN)
- Struktur:
  - Grundsätzliche Anforderungen
  - Protokollierung (Planung + Umsetzung)
  - Detektion (Planung + Umsetzung)
  - Reaktion
- Nachweiserbringung für kritische Infrastrukturen ab dem 01.05.2023!
- Umsetzungsgradmodell (6 Stufen)
  - 2023 sollte mindestens Stufe 3 erfüllt sein – Alle MUSS Anforderungen werden erfüllt!
  - Grundsätzlich wird Stufe 4 erwartet – Alle MUSS und SOLL Anforderungen werden erfüllt!

Orientierungshilfe zum Einsatz von Maßnahmen zur Angriffserkennung

Nr	Prio	Anforderungen und Maßnahmen	Status	Umsetzungsgra
Grundsätzliche Anforderungen				
1	MUSS	Die notwendigen technischen, organisatorischen und personellen Rahmenbedingungen MÜSSEN geschaffen werden.		
2	MUSS	Informationen zu aktuellen Angriffsmustern für technische Vulnerabilitäten MÜSSEN fortlaufend für die im Anwendungsbereich eingesetzten Systeme eingeholt werden.		
3	MUSS	Alle zur effektiven Angriffserkennung erforderliche Hard- und Software MUSS durchgängig auf einem aktuellen Stand gehalten werden.		
4	MUSS	Die Signaturen von Detektionssystemen MÜSSEN immer aktuell sein.		
5	MUSS	Alle relevanten Systeme MÜSSEN so konfiguriert sein, dass Versuche, bekannte Schwachstellen auszunutzen, erkannt werden können, sofern keine schwerwiegenden Gründe dagegensprechen.		
Protokollierung (Planung)				
6	SOLL	In der Planungsphase SOLLTE, basierend auf den Ergebnissen der Risikoanalyse und in Anbetracht der kritischen Prozesse des Betreibers, eine schrittweise Vorgehensweise für die Umsetzung der Protokollierung geplant werden.		
7	MUSS	Die Schritte MÜSSEN dabei so gewählt werden, dass eine angemessene Sichtbarkeit innerhalb angemessener Zeit erzielt wird.		
8	MUSS	Der Betreiber MUSS alle zur wirksamen Angriffserkennung auf System- bzw. Netzebene notwendigen Protokoll- und Protokollierungsdaten erheben, speichern und für die Auswertung bereitstellen, um sicherheitsrelevante Ereignisse (SRE) erkennen und bewerten zu können.		
9	KANN	Hierzu KÖNNEN zusätzliche Systeme eingesetzt werden, sodass zur wirksamen Angriffserkennung nicht jedes einzelne Gerät Protokollierungsdaten aufzeichnen muss und damit die Verfügbarkeit der Produktivsysteme und damit der kritischen Dienstleistung gewährleistet werden kann.		
10	MUSS	Die zur Speicherung notwendigen Systeme und deren IT-Sicherheitsvorkehrungen MÜSSEN schon in der Planung bedacht werden.		
11	MUSS	Da die Protokollierung teilweise auch datenschutzrechtlich relevante Datensätze beinhalten kann, MUSS der legale Umgang mit diesen bei der Planung einbezogen werden. Ggf. ist dazu eine Anonymisierung bzw. Pseudonymisierung der Protokoll- und Protokollierungsdaten erforderlich.		
12	MUSS	Im Rahmen der Planung MÜSSEN alle Systeme identifiziert werden, die zur Aufrechterhaltung der kritischen Dienstleistung maßgeblich sind, damit deren Protokoll- und Protokollierungsdaten später erfasst werden können.		
13	SOLL	Sind die bestehenden Systeme nicht in der Lage, auskömmliche Protokoll- und Protokollierungsdaten bereitzustellen, SOLLTE die Protokollierungsinfrastruktur so angepasst und/oder durch zusätzliche Maßnahmen, Software oder Systeme ergänzt werden, dass Detektion und Reaktion im entsprechend der Risikoanalyse notwendigen Rahmen möglich sind.		
14	KANN	Das anfallende Protokoll- und Protokollierungsdatenaufkommen KANN anhand eines repräsentativen Systems pro Systemgruppe bestimmt werden.		
15	MUSS	Die Ergebnisse der Planungsphase MÜSSEN in einer geeigneten Form		

Praktische Umsetzung

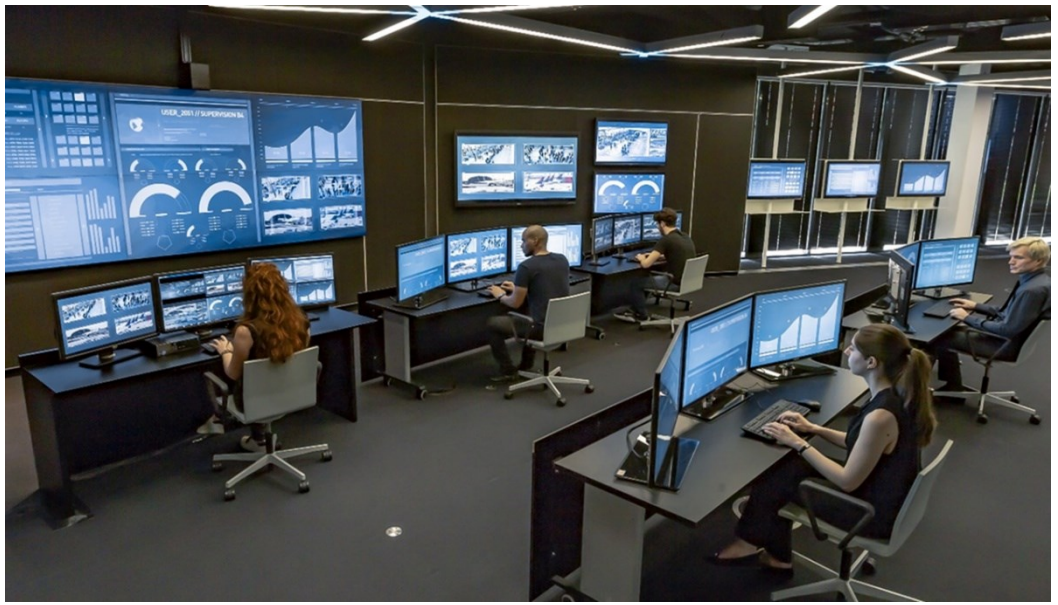
- Reicht ein signaturbasierter EndPoint Virenscanner, eine Firewall und ein Mailfiltering?



SOC - Security Operation Center

Persönliche Meinung:

- Marketingbegriff, Buzzword, Mythos mit übersteigerten Erwartungen!
- Kein Produkt! <kaufen -> einschalten -> glücklich sein>



Bildquelle: Thales Group

- Ist eine Strategie / Prinzip
- Für eine zeitnahe Auswertung und Reaktion werden im SOC alle sicherheitsrelevanten Informationen der Krankenhaus-Infrastruktur aggregiert und korreliert!

Security Operations Center - Aufgaben

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Das SOC befasst sich mit proaktiver Bedrohungsanalyse, Planung der Risikominimierung und Schadensbegrenzung, Sicherheitsarchitektur sowie Erkennung und Reaktion auf Vorfälle!

- Security Controls Management – Weiterentwicklung IT-Sicherheitsarchitektur
- Security Threat Intelligence – Ermittlung möglicher Bedrohungen
- Security Monitoring – Bewertung von Ereignissen
- Security Incident Response - Vorfallsbewältigung
- Security Training und Awareness – Sensibilisierung Sicherheitsbewusstsein diverser Benutzergruppen
- Security Reporting – Messbarkeit und Transparenz
- Vulnerability Management – Schwachstellen ermitteln und bewerten
- Compliance Management – Sicherstellung interner und externer Standards und Vorschriften

...

- ...

Vielen Dank für Ihre Aufmerksamkeit

Kontakt:
Mike Zimmermann
Telefon: 0351 458 15434
Mobil: 0162 255 0892
E-Mail: Mike.Zimmermann@ukdd.de
Internet: https://www.uniklinikum-dresden.de

Adresse:
Universitätsklinikum Carl Gustav Carus
an der TU Dresden AöR
Informationssicherheit
Haus 2, 2. Etage, Zimmer 303
Fetscherstraße 74, 01307 Dresden

„Es ist nicht mehr die Frage, ob man angegriffen wird, es ist nur noch die Frage, wann!“
Zitat Matthias Schmidt ZAC/ LKA Bayern am 14.03.2018

Antwort darauf könnte sein: „Das Glück bevorzugt den, der vorbereitet ist“
Louis Pasteur (1822-1895)