Erfahrungsberichte zum Thema Informationssicherheit in Kliniken

Health-IT Talk

12. Juli 2021

Vorstellung

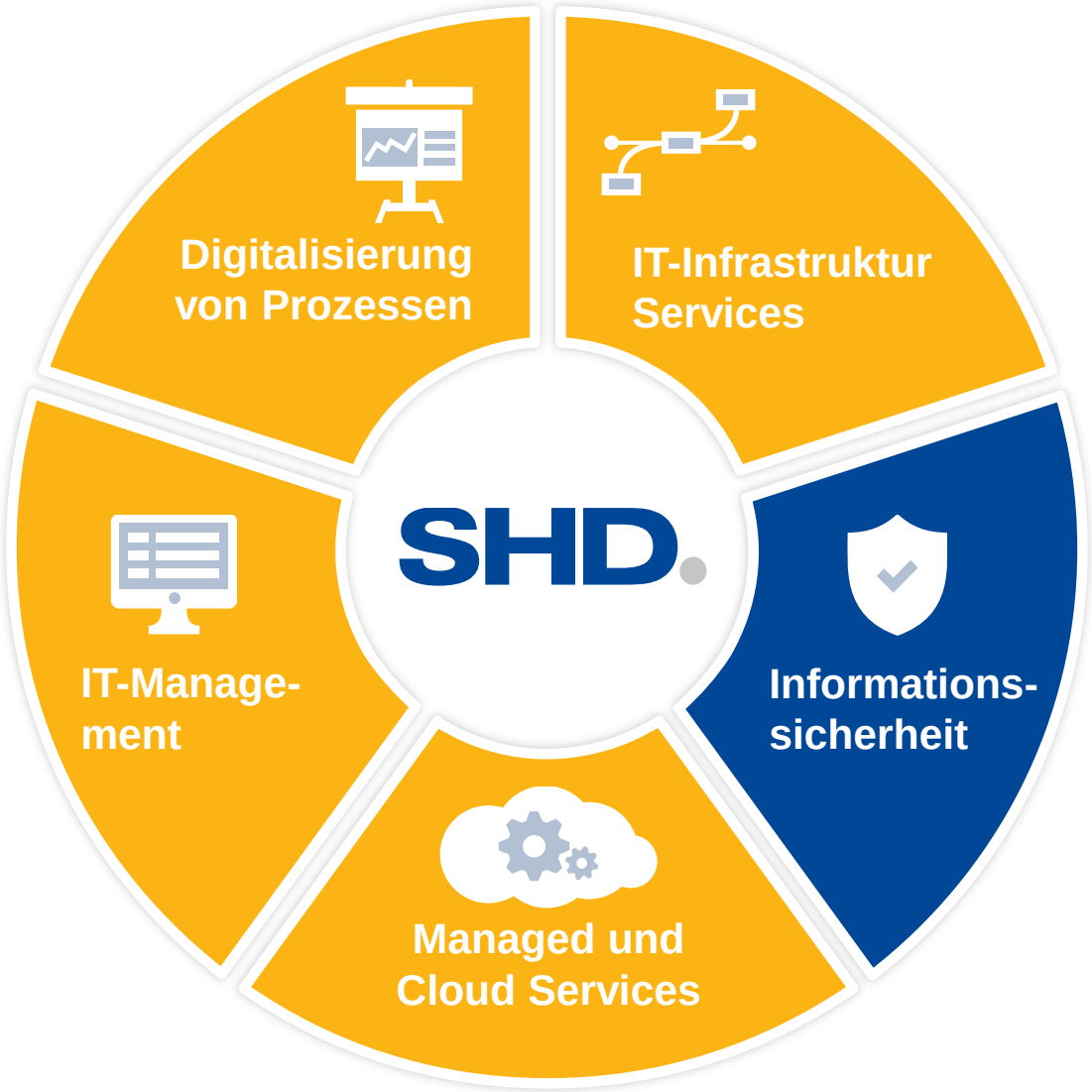
Universitätsklinikum
Carl Gustav Carus

- 1.410 Betten
- 26 Kliniken, 4 Institute und 17 interdisziplinäre Zentren
- 6.300 Mitarbeiter
  - 2.000 Pflegedienst
  - 1.000 Ärztlicher Dienst
- 2.900 Studenten
- 58.500 stationäre Fälle pro Jahr
- 310.000 Patienten pro Jahr (60.000 stationär & 250.000 ambulant)

Vorstellung

SHD.

- Seit 1990 erfolgreich am Markt
- 40 Mio. € Umsatz im Jahr 2020
- 165 Mitarbeiter an 6 Standorten (Dresden, Berlin, Leipzig, Hamburg, Nürnberg, Spremberg)
- SHD ist zertifiziert nach ISO 9001 und ISO 27001



Gesetzliche Rahmenbedingungen - BSI-KritisV für kDL

BSI verabschiedet am 25.7.2015

BSI-Kritis-Verordnungen (BSI-KritisV) treten in Kraft

Anforderungen BSI-KritisV

Nachgewiesenes, funktionierendes ISMS bis 06/2018 für Korb1 und 06/2019 Korb2 !

IT Sicherheitsgesetz (IT-SiG)

„Korb1“ verabschiedet 03. Mai 2016

„Korb2“ verabschiedet 30.Juni 2017

Pflegepersonalstärkungs-gesetz (PpSG) Krankenhausstrukturfond 2.0

eine Kontaktstelle für BSI zu benennen (innerhalb 6 Monate)

IT-Sicherheit gemäß "Stand der Technik" umsetzen (in 2 Jahren !)

Nachweispflicht gegenüber dem BSI aller zwei Jahre

Patienten-Schutz-Gesetz (PDSG) April 2020

Mit dem geänderten § 75c SGB V werden alle Krankenhäuser, nicht nur die gemäß KRITISVerordnung als „Kritische Infrastruktur“ eingestuften, ab 1. Januar 2022 verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von IT-Störungen zu treffen und spätestens alle zwei Jahre an den Stand der Technik anzupassen.

Achtung:

Bei Nichteinhaltung können evtl. Sanktionen aus der DSGVO greifen, da häufig Schutzziele wie Vertraulichkeit usw. verletzt werden.

Krankenhauszukunftgesetz (KHZG) 19.09.2020 v. Bundestag beschlossen

- §4b Evaluierung des Reifegrades der Krankenhäuser hinsichtlich der Digitalisierung
  - zwei Stichtage: Juni 2021/Juni 2023
- §22 2. Nachweise darüber, dass mindestens 15 Prozent der für das Vorhaben beantragten Fördermittel für Maßnahmen zur Verbesserung der Informationssicherheit eingesetzt werden, und Nachweise, um welche Maßnahmen zur Verbesserung der Informationssicherheit es sich handelt

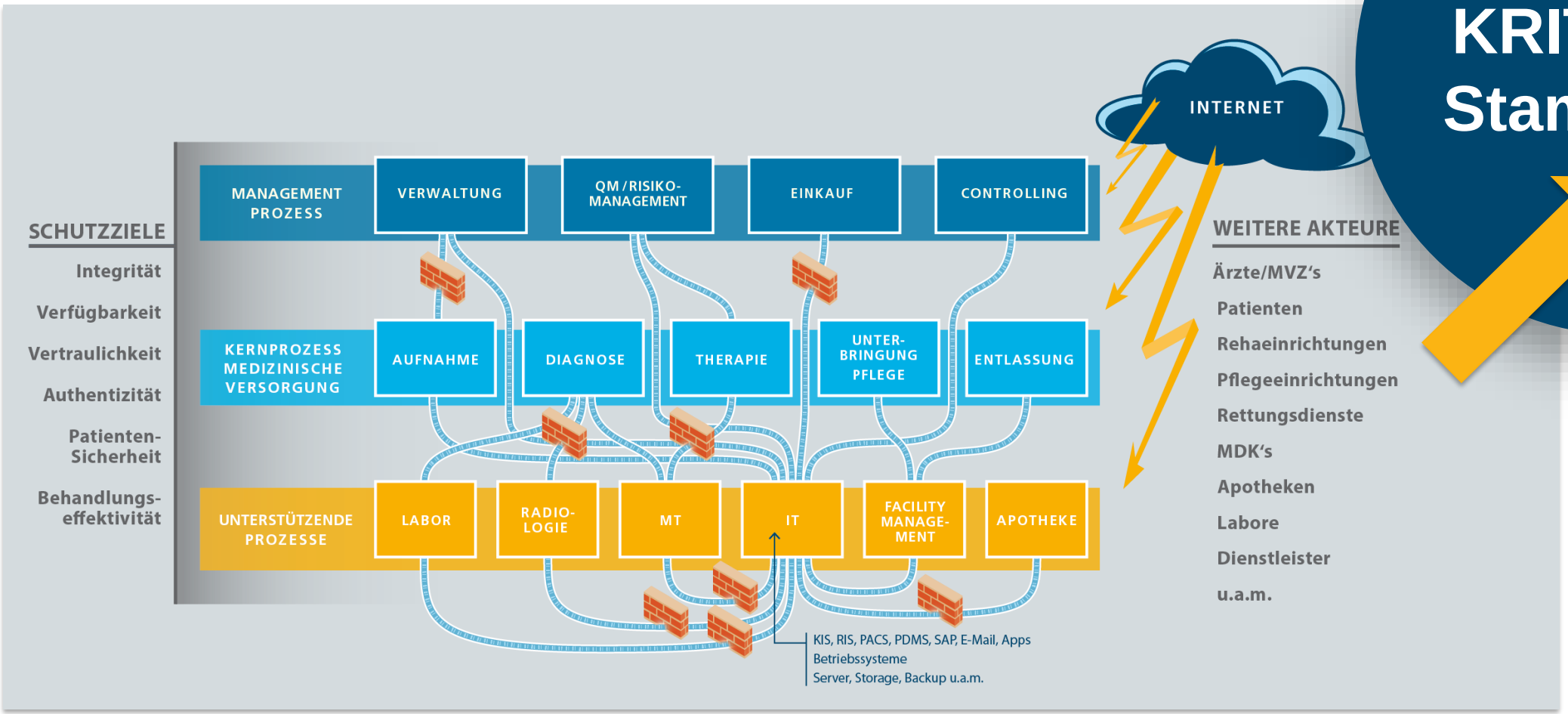
Krankenhaus-Zukunftsfonds (§14a KHZG)

4,3 Mrd. € (3 Mrd. € Bund + Länder/KH Träger)
Verteilung nach dem Verteilung nach Königsteiner Schlüssel Stand 2018

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

Sicherheit ist keine Produkt – Sicherheit ist ein Prozess

KRITIScher Stammtisch



- wurde 2017 durch die Uniklinik Dresden und SHD System-Haus-Dresden GmbH gegründet
- ein Arbeitskreis, bestehend aus:
- Informationssicherheitsbeauftragte (ISB)
- IT Leiter
- Auditoren
- Vertreter aus BSI
- Vertreter aus LKA
- Vertreter aus DKG/KGS
- Vertreter aus Ministerien
- Teilnehmer aus 6 Bundesländer
- am 12.05.2021 fand der 12. KRITIScher Stammtisch statt

Universitätsklinikum
Carl Gustav Carus

Information zum IT-SIG 2.0 Sektor Gesundheit – Auswirkungen

- **Schwellenwert (30.000 stat. Fallzahlen) bleibt**
  - Aber Schärfung bei Klinikverbünden oder –ketten!
- **Stärkung der Rolle und der Befugnisse des BSI**
  - Erweiterung der Kontroll- und Prüfbefugnisse & Aktive Schwachstellensuche und –beseitigung
- **Systeme zur Angriffserkennung werden verpflichtend**
  - Stand der Technik muss definiert werden
- **Überarbeitung Bußgeldkatalog**
  - von max. 100.000 Euro auf nun max. 2.000.000 Euro
- **Kernkomponenten bekommen Standards**
  - Gesetzgeber kann Mindeststandards für kritische Komponenten definieren
  - Herstellerkontrolle durch Einführung einer Vertrauenswürdigkeitserklärung (schließt die gesamte Zuliefererkette ein)
- **Untersagung Einsatz kritischer Komponenten**
  - BMI kann den Einsatz (1 Monat) untersagen, sofern öffentliches Interesse oder sicherheitspolitische Belange relevant sind
- **Einheitliches IT-Sicherheitskennzeichen**
  - Einheitliches und transparentes IT-Gütesiegel

-> Details sind in den jeweiligen Rechtsverordnungen noch zu definieren!

Der Ausgangspunkt

Die Kernkompetenz von Krankenhäuser ist die Patientenversorgung!

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!“

Der Stellenwert der IT wird oft den Ansprüchen nicht gerecht!

Hinzukommen unzählige Herausforderungen, u.a.:

- Digitalisierung und zunehmende Vernetzung der Systeme bis hin zu Big-Data-Center!
- vernetzte Medizin- & Haustechnik
- zunehmende Vermischung von Consumer- & Businessprodukten
- Telemedizin
- enge Verbindung zu Forschung und Lehre
- Cloud / IT-Systeme as a Service / IOT / Home Health Care / Künstliche Intelligenz

Bedrohungstrends und Ziele der Angreifer

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

Phishing / Identitätsmissbrauch

- Ausnutzung von digitalen Identitäten für kriminelle Aktivitäten

Ransomware / Verschlüsselung von Daten

- Erpressung – Lösegeldforderung um die Verfügbarkeit wieder herzustellen
- Erpressung – Lösegeldforderung um sensible Daten nicht zu verlieren

Datendiebstahl

- Verarbeitung von sensiblen Daten für kriminelle Aktivitäten

DDoS

- Beeinflussung der Verfügbarkeit von IT-Diensten
- Schwachstellen in Soft- und Hardware

Zusätzlich seit Corona:

- Videokonferenzen ⟶ Störung und Datendiebstahl
- Desinformation (Fake News, Deepfake) ⟶ Chaos
- Gefälschte Webseiten ⟶ Betrug

Wert der Daten: (Datenbasis: Dark Web Price Index 2020, Firma Privacy Affairs)

- ein Electronic Health Record (EHR) erzielt ca. 250-1.000 USD
- geklonte VISA mit PIN: 25 USD
- gestohlene PayPal-Kontodaten: 100 USD
- LinkedIn Follower (1000x): 10 USD

Vorfälle aus den letzten Monaten im Gesundheitswesen

Laufende Ermittlungen zum IT-Ausfall an Uniklinik Düsseldorf

Freitag, 11. September 2020

Syda Productions, stoc

"Akt von Cyberkriminalität" in Frankreich – Patientendaten aus Laboren im Netz

Im Internet tauchen massenhaft Gesundheitsinformationen aus Frankreich auf. Das Leck ist wohl auf eine Firma für Labor-Software zurückzuführen.

Lesezeit: 1 Min. In Pocket speichern 42

15. Februar 2021, 7:04 Uhr Cybercrime

Hackerangriff auf Urologische Klinik München Planegg

Die Urologische Klinik München-Planegg - das Foto ist schon etwas älter, weshalb noch eine Baustelle zu sehen ist. (Foto: Florian Peljak)

Das Krankenhaus wurde im Januar von Kriminellen erpresst - Lösegeldzahlungen gab es wohl nicht. Aber die Hacker bekamen durch ihre Attacke offenbar Einblicke in sensible Patienten-Unterlagen.

r/Shutterstock.com)

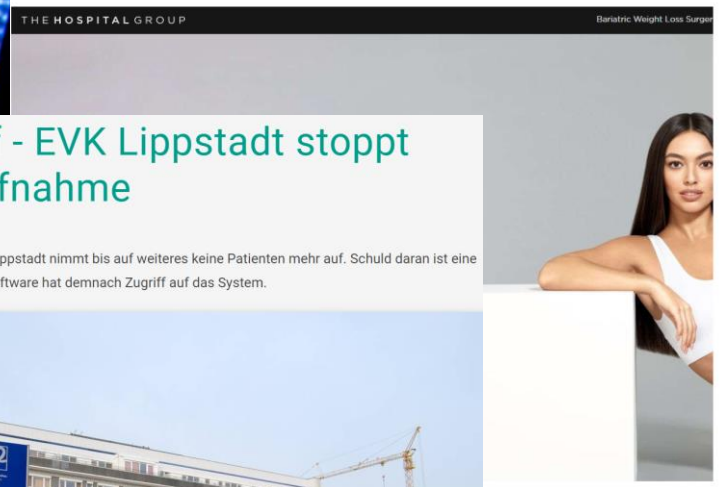
"Diese Menschen haben keinerlei Mitgefühl"

pf gegen Emotet. Das Botnet

essen eine finnische
endaten. Als diese n
Patienten selbst.

Hacker erpressen Schönheitsklinik

Dr. Jakob Jung 29.12.2020



Cyberangriff - EVK Lippstadt stoppt Patientenaufnahme

Veröffentlicht: Dienstag, 30.03.2021 15:22

Das evangelische Krankenhaus in Lippstadt nimmt bis auf weiteres keine Patienten mehr auf. Schuld daran ist eine Cyberattacke. Eine externe Schadsoftware hat demnach Zugriff auf das System.

Die Umsetzung

„Anforderungen an organisatorische, technische und personelle Maßnahmen“

Informationssicherheit ist kein Projekt, sondern ein fortlaufender Prozess!

Stellenwert der Informationstechnik neu definieren

- Abhängigkeit von der IT anhand praktischer Beispiele (OP ohne IT?)
- Förderung des Sicherheitsbewusstsein

Treiber der Standardisierung - Silodenken auflösen!

- die zunehmende Komplexität der IT kann nur mit Standardisierung und Transparenz beherrscht werden

Informationssicherheitsmanagement

- Etablierung eines IT-Sicherheitsbeauftragten und IT-Sicherheitskoordinatoren
- nur GEMEINSAM kann das Ziel erreicht werden (KH-Leitung + IT + IT-Sicherheit)
- enge Zusammenarbeit mit IT, DS, QM, RM, MT, GLT, Beschaffung, Personal

Die Umsetzung

Aufbau und Etablierung eines Informationssicherheitsmanagementsystems (ISMS)

- Einführung eines Standardführungsprozess Informationssicherheit (Leitlinie)
- Standardisierte Dokumentenlenkung / -klassifizierung
- Verknüpfung IT-Assets + Krankenhausprozesse für das ganzheitliche Identifizieren von Risiken
- Aufbau IT-Vorfallsmanagement (IT-SiG, DSGVO, Medizinprodukte-Sicherheitsplanverordnung)
- Aufbau IT-Risikomanagement und Integration in das vorhandene Krankenhaus RM
- Aufbau Business Continuity Management / Notfallmanagement
- Aufbau IT-Revision (inkl. Integration in das zentrale Audit- und Begehungsmanagement)

Einführung und Etablierung technischer Maßnahmen, u.a.:

- IT-Infrastruktur (z.B. Netzwerksegmentierung)
- Kommunikationssicherheit (Daten- und Kommunikationsverschlüsselung – E-Mail, Zertifikate)
- Prävention (Tools zur frühzeitigen Erkennung von Anomalien - IPS, SIEM, Web Reputation)
- Compliance (Penetrationstest, Schwachstellenüberwachung)

Vielen Dank für Ihre Aufmerksamkeit !

Konrad Christoph
Tel. +49 (0)151 120 569 16
E-Mail: konrad.christoph_extern@shd-online.de

Mike Zimmermann
IT-Sicherheitsbeauftragte des UK Dresden und
der Medizinischen Fakultät der TU Dresden
Tel. +49 (0)351 458 15434
E-Mail: Mike.Zimmermann@uniklinikum-dresden.de

„Es ist nicht die 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)