Cyber-Sicherheitslücken in Ihrer Gebäudetechnik aufdecken und handeln

Soheil Djafari, Head of Vertical Market Smart Hospitals
Timo Dauenhauer, Portfoliomanager Cybersecurity Services for Buildings

SIEMENS

Faktencheck IT & Cybersicherheit in Deutschland

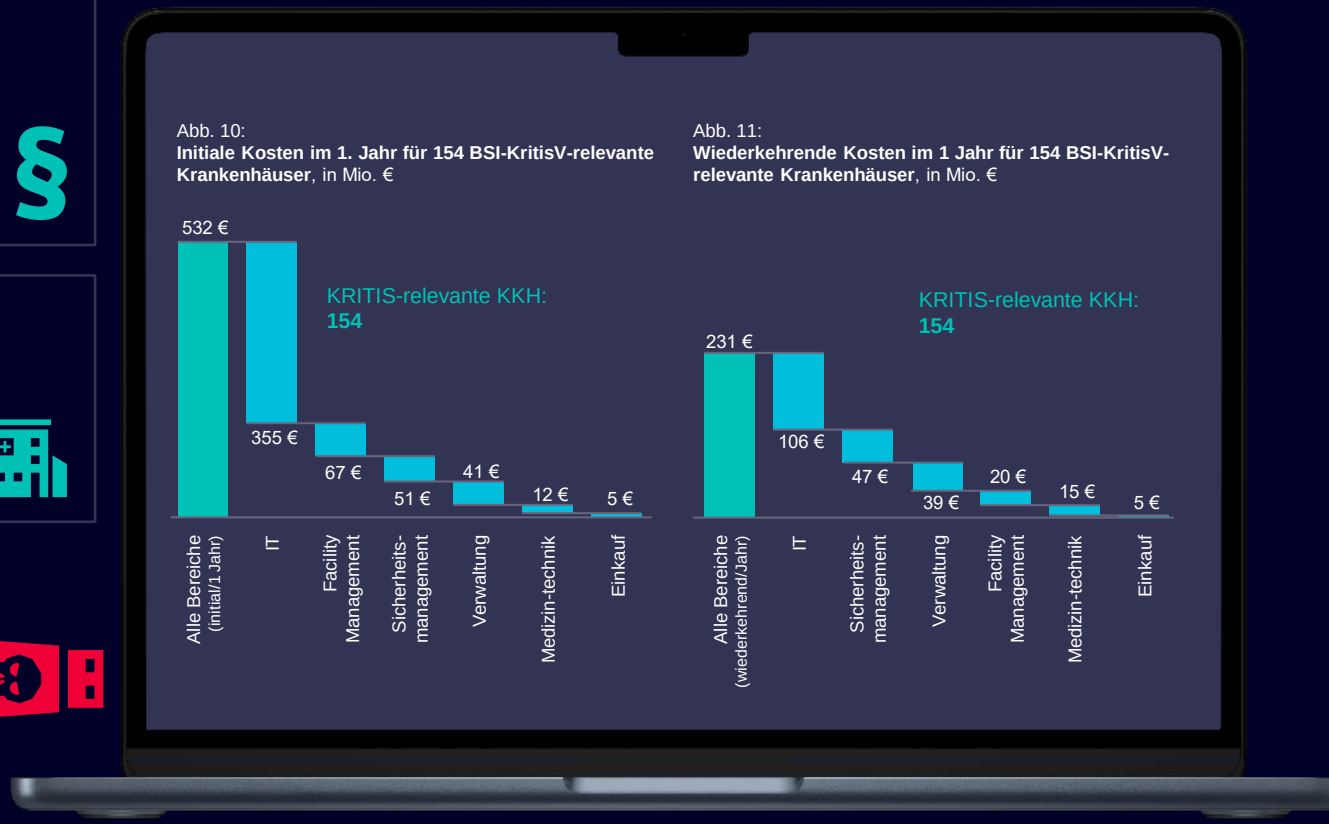
IT-Sicherheitsgesetz
(§ 8 BSI-Gesetz KRITS)
Fälle >29,000[1]
von 2017
> 150 Krankenhäuser

IT-Sicherheit im Krankenhaus
(§ 75c SGB V)
ab 2022
>1.800 Krankenhäuser

Kosten
532 € Mio. (initial)
231 € Mio. (wiederkehrend)

Gesamtkosten für alle Krankenhäuser
Milliarden Euro

Krankenhausangriffe (erfolgreich)
2019: <20
2020: >40



Quelle: 1 Die Größenordnung der Fallzahlen ist auf >30.000 Fälle angepasst worden (Definition KRITIS Betreiber)

Deutsche Krankenhausgesellschaft e.V., Erhebung der Kosten zur Umsetzung des ITSG in BSI-KritisV-relevanten Krankenhäusern, 2019
Abb. 10: Initiale Mehrkosten durch die Umsetzung im B3S definierten Maßnahmen für die BSI-KRITSV-relevanten Krankenhäuser
Abb. 11: Wiederkehrende Mehrkosten durch die Umsetzung im B3S definierten Maßnahmen für die BSI-KRITSV-relevanten Krankenhäuser

SIEMENS

Die gesetzlichen Bestimmungen zur IT-Sicherheit in Krankenhäusern wurden verschärft

Ab dem 1. Januar 2022 sind Krankenhäuser verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung des Krankenhauses oder der Sicherheit der verarbeiteten Patienteninformationen steht. Die informationstechnischen Systeme sind spätestens alle zwei Jahre an den aktuellen Stand der Technik anzupassen.

Die Krankenhäuser können die Verpflichtungen nach Absatz 1 insbesondere erfüllen, indem sie einen branchenspezifischen Sicherheitsstandard für die informationstechnische Sicherheit der Gesundheitsversorgung im Krankenhaus in der jeweils gültigen Fassung anwenden, dessen Eignung vom Bundesamt für Sicherheit in der Informationstechnik nach § 8a Absatz 2 des BSI-Gesetzes festgestellt wurde.

Die Verpflichtung nach Absatz 1 gilt für alle Krankenhäuser, soweit sie nicht ohnehin als Betreiber Kritischer Infrastrukturen gemäß § 8a des BSI-Gesetzes angemessene technische Vorkehrungen zu treffen haben.

SGB V
Gesetzliche Krankenversicherung

Sozialgesetzbuch (SGB) Fünftes Buch (V)

§75c IT-Sicherheit in Krankenhäusern

Quelle: https://www.gesetze-im-internet.de/sgb_5/__75c.html

SIEMENS

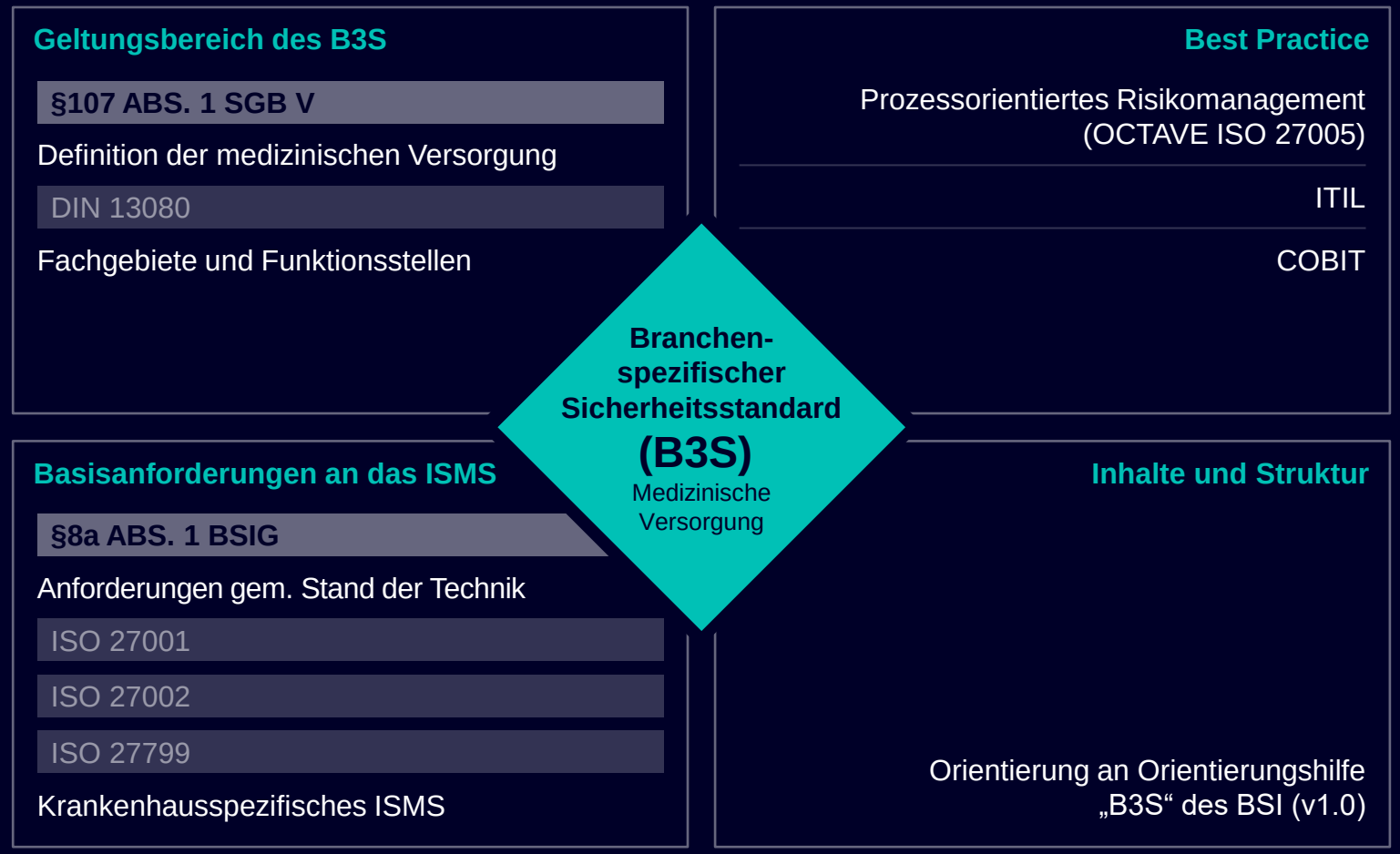
Der branchenspezifische Sicherheitsstandard (B3S) dient Krankenhäusern als roter Faden auf dem Weg zur Digitalisierung und mehr IT-Sicherheit

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Bundesamt für Sicherheit in der Informationstechnik

Ziel ist es …

… die **medizinische Versorgung** von Patienten im Krankenhaus und die **Förderung** ihrer **Gesundheit zu gewährleisten.**



Quelle: Abbildung rechts: Rahmenbedingungen und Quellen zur Erstellung des B3S

SIEMENS

B3S-Standard für Krankenhäuser
Überblick

Der Standard beschreibt Prozesse und Maßnahmen.

Der Standard BS3 …

… beschreibt **168 Maßnahmen**, die nötig sind, um eine resiliente Informationstechnik zu gewährleisten und die medizinische Versorgung und Gesundheit der Patienten sicherzustellen.

Der B3S-Katalog …

… empfiehlt insgesamt 168 Maßnahmen, die in **Muss-, Soll- und Kann**-Anforderungen untergliedert sind.
Das Regelwerk dient als Leitfaden für die Praxis und auch als **Grundlage für Kontrollen**.
95 MUSS Kriterien

Es werden …

… 40 verschiedene **Bedrohungsszenarien**, Schwachstellen und mögliche Gefahren betrachtet.
(Beispiel: Elementarschaden, Stromausfall, Cyber-Attacken, menschliche Fehler).
Der B3S Katalog beinhaltet auch 37 reine Management-Anforderungen.

SIEMENS

B3S definiert folgende Systeme als

Versorgungstechnik

- Energieversorgung, Elektroversorgung (Netzversorgung (Einspeisung), Ersatzversorgung)
- Lichttechnische Systeme
- Gebäudeleittechnik und Gebäudeautomatisierungstechnik
- Wärme/Heizung (z.B. Patienten- und Untersuchungsräume)
- Klimatisierung und Kühlung (z.B. OPs und technische Anlagen)
- Digitale Zugangs- und Schließsysteme
- Videoüberwachung

SIEMENS

B3S definiert folgende Systeme als

Informationstechnik

- Arbeitsplatzsysteme & Peripherie-Geräte
  z.B. Arbeitsplätze, Notebooks, Tablets, Smartphones, Drucker, Scanner
- Serversysteme (Virtualisierung, Anwendungen, Datenbanken, Basisdienste,
  z.B. Verzeichnisdienste, DNS, DHCP)
- Storagesysteme (SAN, NAS)
- IP-Netzwerke (WAN, LAN, WLAN, VLAN)
- Netzbereitstellung z.B. Telekommunikation, Medizintechnik und Versorgungstechnik
- Softwaresysteme (Lebenszyklus von Betriebs- und Anwendungssystemen)
  - Krankenhausinformationssystem (KIS), Laborinformationssystem (LIS), Radiologieinformationssystem (RIS)
  - Picture Archive and Communication System (PACS)
  - Dokumenten-Management-System (DMS/ECM)
  - Alle weiteren spezialisierten Anwendungen im klinischen Umfeld
- Sicherheitskomponenten
  (Firewall, DMZ, VPN, Malware-Schutz, Spamabwehr, Überwachungssysteme)
- Backup und Wiederherstellung
- Fernwartungsbetrieb, Rechenzentrumsbetrieb und USV-Betrieb

SIEMENS

B3S definiert folgende Systeme als

Medizintechnik

- Patientendatenmanagementsysteme (PDMS)
- Informationsverarbeitung der für diagnostische bzw. therapeutische Zwecke benötigten und zur Verfügung gestellten Daten von medizintechnischen Systemen (z. B. bildgebende Verfahren) inklusive der entsprechenden Schnittstellen zwischen den beteiligten Systemen
- Telemedizinische Systeme/Telemetriesysteme zur Überwachung wichtiger Parameter bei Erhöhung von Freiheitsgraden in der Patientenversorgung
- Patientengebundene Alarmierungssysteme (häufig gekoppelt mit IT-Komponenten, im Einzelfall auch Teil der Kommunikationstechnik)
- Steuerung der Instandhaltung medizintechnischer Anlagen für Diagnostik und Therapie (herstellerbasierte Leistungserbringung)
- Instandhaltung und Austausch von Einzelgeräten (z. B. „Kleingeräte“, wie Infusionspumpen o.ä.)

SIEMENS

Bundesministerium für Gesundheit

Krankenhaus-zukunftsgesetz
(KHZG)

Krankenhauszukunftsgesetz für die Digitalisierung von Krankenhäusern

Mit einem Investitionsprogramm verschafft Bundesgesundheitsminister Jens Spahn den Krankenhäusern ein digitales Update.

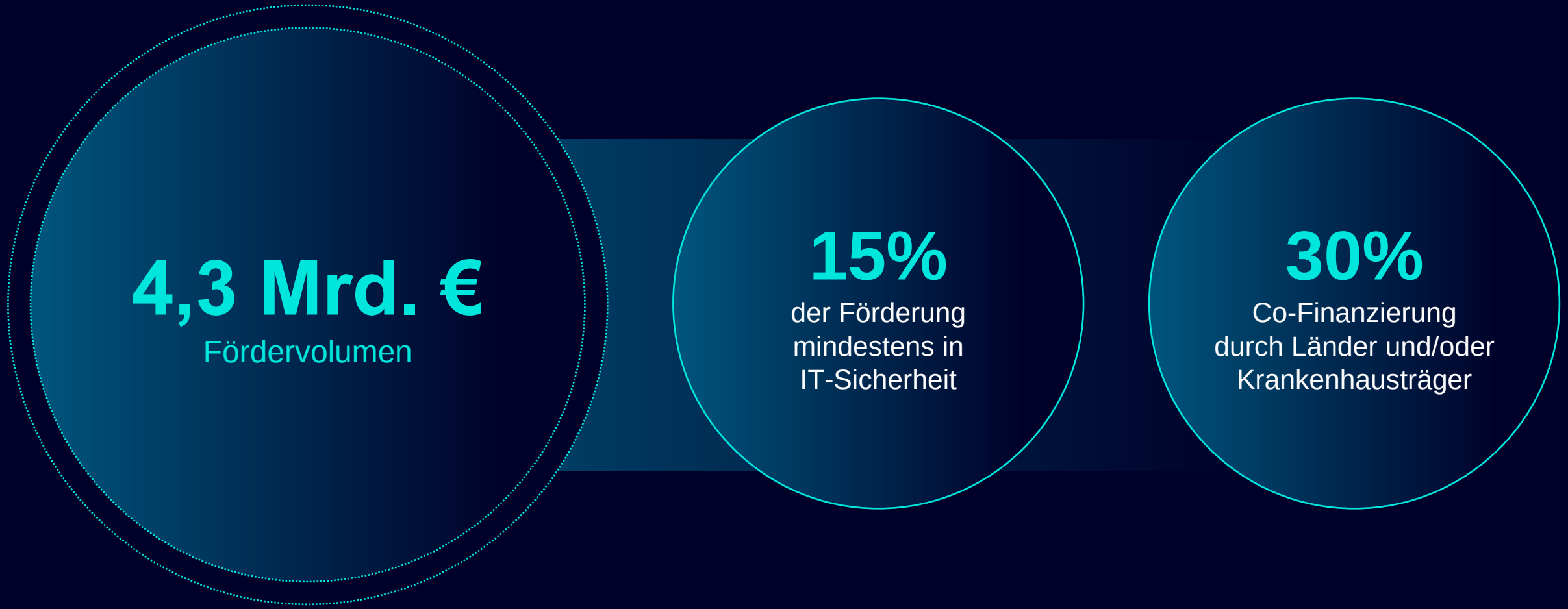
Der Bund hat ab dem 1. Januar 2021 3 Mrd. € bereitgestellt, damit Krankenhäuser in moderne Notfallkapazitäten, die Digitalisierung und ihre IT-Sicherheit investieren können.

Die Länder sollen weitere Investitionsmittel von 1,3 Mrd. € aufbringen.

Mit dem Gesetz wird das durch die Koalition am 3. Juni 2020 beschlossenen „Zukunftsprogramm Krankenhäuser“ umgesetzt. Am 29. Oktober 2020 ist das KHZG in Kraft getreten.

SIEMENS

Krankenhauszukunftsgesetz (KHZG)
Eckdaten und Fördertatbestände



Quellen: Bundesministerium für Gesundheit – Krankenhauszukunftsgesetz Bundesamt für Soziale Sicherung – Krankenhauszukunftsfonds

SIEMENS

Unsere Vorgehensweise für eine ganzheitliche Betrachtung im Krankenhaus (B3S), welche alle geforderten Aspekte aus dem B3S umfassen

01

CYBERSICHERHEIT GAP ASSESSMENT

Versorgungstechnik

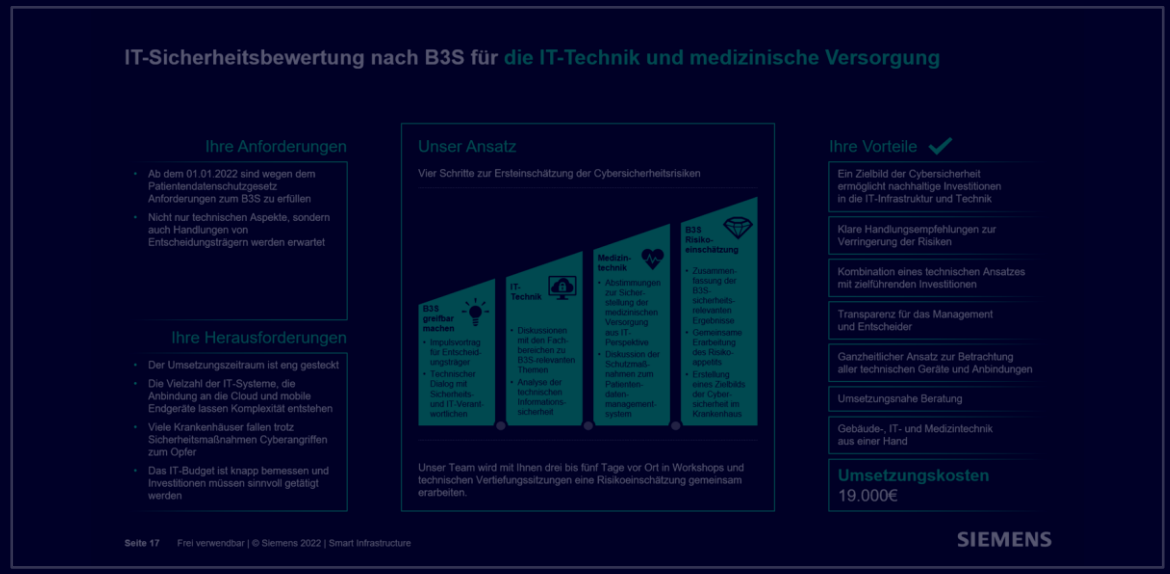
Wir decken Ihre Cybersicherheitslücken auf - zum Schutz Ihrer kritischen Versorgungstechnik

02

IT-SICHERHEITSBEWERTUNG

IT-Technik und medizinische Versorgung

Wir schaffen eine Managementperspektive & erstellen eine Risikoeinschätzung sowie ein Zielbild Ihrer Cybersicherheit



SIEMENS

Auch OT-Umgebungen sind mögliche Angriffsflächen

Über die Gebäudetechnik ist es möglich, in IT-Systeme einzudringen und Schaden anzurichten

Wir kennen beide Welten

SIEMENS

Es ist Zeit, zu handeln

Die Frage lautet nicht **ob**, sondern **wann**.

Was kann ich tun, um mein Unternehmen vor Cyberangriffen zu schützen?

SCHRITT 1

Sicherheitslücken identifizieren und Maßnahmen zur Risiko-Minimierung definieren

SIEMENS

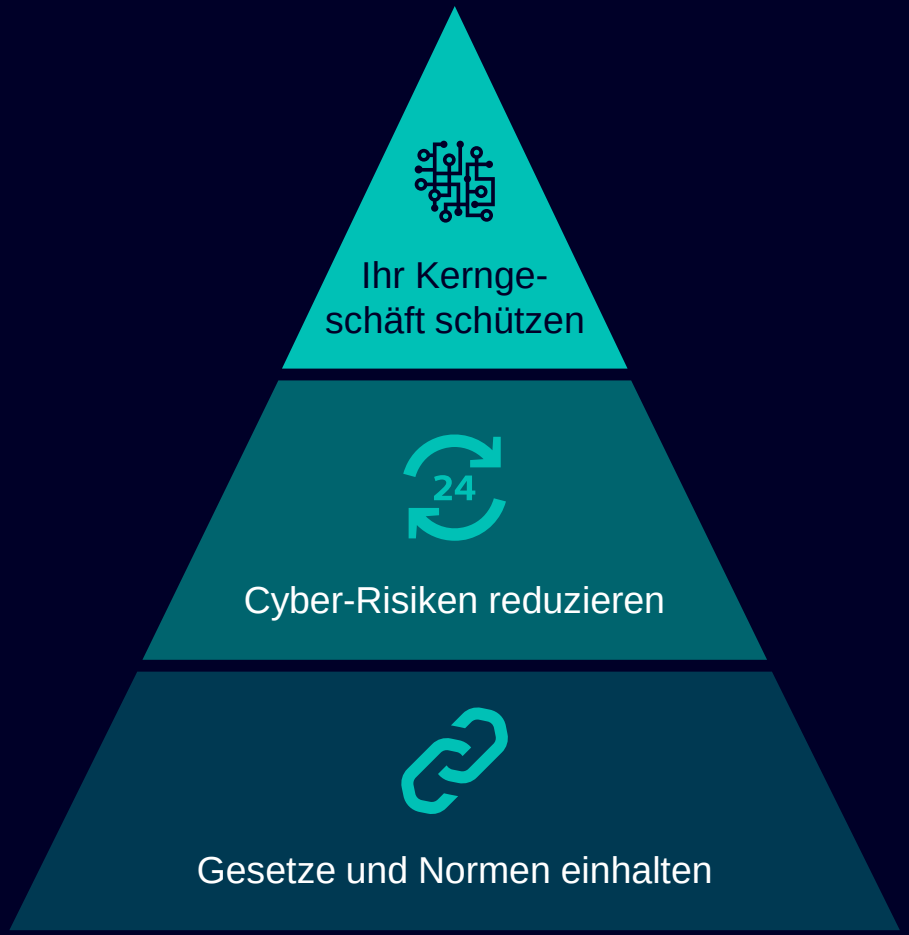
Sicherheitslücken aufdecken
mit dem Gap Assessment

Beim Gap Assessment geht es um die Vermeidung von Lücken – aber nicht um die zwischen Zug und Bahnsteig, sondern um Sicherheitslücken in der Gebäudetechnik.

Sicherheitshinweis in der Londoner U-Bahn lautet: „Mind the gap“

SIEMENS

Mehrwerte durch Gap Assessment



Vorteil

Sie erhalten eine schnelle, systematische und umfassende Beurteilung Ihres Cybersicherheits-Status inklusive konkreter Handlungsempfehlungen

SIEMENS

Ablauf eines Gap Assessments:
Transparenz schaffen über den Sicherheitszustand der Gebäudetechnik

1 Discovery

Cybersecurity: Definition von Zielen und Umfang

Voranalyse durch Cybersecurity-Experten

Vorbereitung des Assessments

2 Gap Assessment

Gemeinsame Begehung vor Ort

Interviewgestütztes Analyseverfahren

Erste Auswertung und Feedback

3 Handlungs-empfehlung

Abgabe des Abschlussberichts und der Abschlusspräsentation

Abstimmung der nächsten Schritte

Terminplanung

SIEMENS

Praxisbeispiele

Erfahrungsberichte

SIEMENS

Beispiel:

Unsicheres Feldgerät mit Cloud-Verbindung

Ein Casino wird durch ein mit dem Internet verbundenes Aquarium-Thermometer gehackt

Lösung:
Netzwerk-Separierung; regelmäßige Software-Updates; sicherer Entwicklungsprozess

Quelle: thehackernews.com, Forbes, Washingtonpost, …

SIEMENS

Beispiel:

Ungeschützte Gebäudetechnik

Der Kunde hatte keine Trennung zwischen der Office-IT und den Netzwerkanschlüssen, die im öffentlichen Bereich zugänglich waren.

Lösung:
Netzwerk-Infrastrukturen schützen; neue Gebäude-automationsprotokolle nutzen (z.B. BACnet/SC)

SIEMENS

Beispiel:

Physische Sicherheit / Zutrittskontrolle

In Vorbereitung auf eine ISO-Zertifizierung fielen bei einem Kunden diverse Sicherheitslücken auf.

Lösung:
Ordentliches Schließkonzept und Prozess-Definition

SIEMENS

Beispiel:

Nicht gepflegte Systeme

Eine bekannte Ransomware verursacht nachts eine Störung im Produktionsablauf

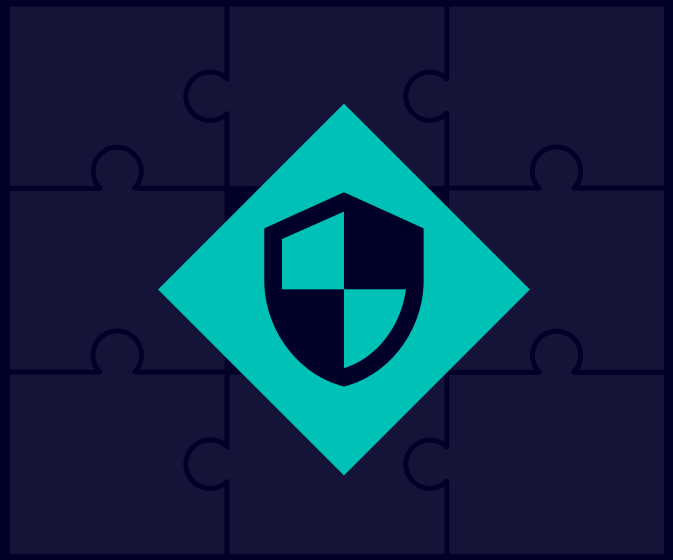
Lösung:
Software-Updates einspielen; System-Sicherung durchführen

SIEMENS

Zusammenfassung
Was können Sie tun?

Sie als Betreiber …

- haben die Verantwortung für einen sicheren Betrieb
- sollten regelmäßige Wartungen Ihrer Systeme durchführen, **zum Beispiel**: Software-Updates / Patches einspielen, Back-up-Recovery, Schwachstellen-Scan und weitere Maßnahmen



Wir bei Siemens …

- kümmern uns als Hersteller um eine sichere Produktentwicklung und liefern Systeme und Features mit sicheren Produkteigenschaften
- unterstützen Sie dabei, gesetzliche Anforderungen und Normen zum Gebäudebetrieb zu erfüllen
- denken über die Technik hinaus und berücksichtigen auch Ihre Prozesse und Organisation

SIEMENS

Vielen Dank

für Ihre Aufmerksamkeit!

Haben Sie noch Fragen?

SIEMENS

Disclaimer

Änderungen und Irrtümer vorbehalten. Die Informationen in diesem Dokument enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, welche im konkreten Anwendungsfall nicht immer in der beschriebenen Form zutreffen bzw. welche sich durch Weiterentwicklung der Produkte ändern können.
Die gewünschten Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart werden.

Alle Produktbezeichnungen können Marken oder sonstige Rechte der Siemens AG, ihrer verbundenen Unternehmen oder dritter Gesellschaften sein, deren Benutzung durch Dritte für ihre eigenen Zwecke die Rechte der jeweiligen Inhaber verletzen kann.

Soheil Djafari
Head of Vertical Market
Smart Hospital
Siemens AG

Lyoner Straße 27
60528 Frankfurt am Main

soheil-alexander.djafari@siemens.com

Timo Dauenhauer
Portfoliomanager Cyber-security Services
Siemens AG

Dynamostrasse 4
68165 Mannheim

timo.dauenhauer@siemens.com

SIEMENS