Informationssicherheit in der stationären medizinischen Versorgung

TÜVRheinland®
Genau. Richtig.

Agenda

Kapitel	Thema	Dauer	Referent	Seite
1	Informationssicherheit im Krankenhaus			
2	Rechtsgrundlagen			
3	Was ist B3S			
4	Die Anforderungsfelder des B3S			
5	TÜV Rheinland Klinikservices			
6	Die Leistungen der TÜV Rheinland i-sec GmbH			

TÜVRheinland®
Genau. Richtig.

Informationssicherheit in der stationären medizinischen Versorgung

Wo stehen wir heute - Der Status Quo

- Krankenhäuser stehen vermehrt vor großen Herausforderungen im Hinblick auf die Absicherung ihrer IT-Systeme, -Prozesse und -Komponenten.

- Eine Vielzahl von Krankenhäusern fallen auch schon heute unter die Anforderungen des BSI-Gesetz (BSIG) sowie der Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV)

- Aufgrund zunehmender Digitalisierung in der medizinischen Versorgung sowie der Erfahrungen aus der SARS-CoV-2 Pandemie rücken nun auch die Krankenhäuser unterhalb der Schwellenwerte der KritisV in den Fokus der Regulierung

- Während der Pandemie wurde ein erhöhtes Aufkommen von Cyberattacken registriert

TÜVRheinland®
Genau. Richtig.

Informationssicherheit in der stationären medizinischen Versorgung

Status Quo - BSI Studie zur Informationssicherheit in der stationären medizinischen Versorgung

- ein systematisches IT-Risikomanagement in vielen Häusern noch nicht auf dem notwendigen Niveau
- Schutzkonzepte und Compliance-Regelungen werden oftmals nur unvollständig entwickelt und eine darauf aufbauende Schulung findet häufig nicht im erforderlichen Umfang statt
- Systematische Zugangskontrollen für Besucherinnen und Besucher sind im Krankenhaus weiterhin eine Ausnahme
- bei der Umsetzung technischer Schutzmaßnahmen, die eine aktive Mitwirkung der Beschäftigten erfordern, kommt es … zu Akzeptanzproblemen

TÜVRheinland®
Genau. Richtig.

Informationssicherheit in der stationären medizinischen Versorgung

BSI Studie zur Informationssicherheit in der stationären medizinischen Versorgung[1]

- Eine (virtuelle) Netztrennung und Netzsegmentierung in Medizintechnik-Netz, Verwaltungsnetz, Applikationsnetz und Patienten-/Gästenetz ist oftmals noch nicht vollständig vollzogen.
- Krankenhäuser führen häufig keine Tests-und Freigabeprozesse für neue Softwaresysteme oder Gerätetechnik durch
- Maßnahmen im Patch-und Änderungsmanagement erfolgen immer wieder verzögert
- Kapazitätsengpässe bei der Speicherung von immer stärker zunehmender Datenmengen sind ein Problem

[1]https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KRITIS/Studie_Informationssicherheit_stationaere_med_Versorgung.pdf, abgerufen 15. Juni 2021

TÜVRheinland®
Genau. Richtig.

Agenda

Kapitel	Thema	Dauer	Referent	Seite
1	Informationssicherheit im Krankenhaus			
2	Rechtsgrundlagen			
3	Was ist B3S			
4	Die Anforderungsfelder des B3S			
5	TÜV Rheinland Klinikservices			
6	Die Leistungen der TÜV Rheinland i-sec GmbH			

TÜVRheinland®
Genau. Richtig.

Informationssicherheit in der stationären medizinischen Versorgung

Rechtsgrundlagen und Qualitätsanforderungen

- Die Qualitätsanforderungen ergeben sich hauptsächlich aus
  - Patientenrechtegesetz (BGB §§ 630a-g) „Behandlungsvertrag“ sowie Änderungen/Ergänzungen des SGB 5 und der Patientenbeteiligungsverordnung (2013)
  - (2017) EU-Medizinprodukteverordnung (Medical Device Regulation), dem Medizinproduktegesetz (MPG), Medizinprodukte-Betreiberverordnung (MPBetreibV)
  - weitere Regelungen, die sich auf die Qualität der Leistungen beziehen wie Sozialgesetzbuch (SGB) oder Industrienormen (Stand der Technik)
  - Krankenhauszukunftsgesetz KHZG (2020)

TÜVRheinland®
Genau. Richtig.

Informationssicherheit in der stationären medizinischen Versorgung

Krankenhauszukunftsgesetz (KHZG), Krankenhauszukunftsfond (KHZF), Patientendaten-Schutz-Gesetz (PDSG)

- Das KHZG soll die Digitalisierung der Krankenhäuser vorantreiben
- Der KHZF des Bundesamt für Soziale Sicherung (BAS) werden Projekte mit einem Gesamtvolumen von bis zu 4,3 Milliarden Euro (Bund 3 Mrd. + Länder 1,3 Mrd.) gefördert
- Das PDSG stellt klare Regeln für Datenschutz, Datensicherheit und datenschutzrechtliche Verantwortlichkeit auf

TÜVRheinland®
Genau. Richtig.

Informationssicherheit in der stationären medizinischen Versorgung

Patientendaten-Schutz-Gesetz (PDSG)

- Das PDSG verpflichtet alle Krankenhäuser gem. §75c SGB 5 IT-Sicherheit in Krankenhäusern 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

- Erfüllung durch „ 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“

TÜVRheinland®
Genau. Richtig.

Agenda

Kapitel	Thema	Dauer	Referent	Seite
1	Informationssicherheit im Krankenhaus			
2	Rechtsgrundlagen			
3	Was ist B3S			
4	Die Anforderungsfelder des B3S			
5	TÜV Rheinland Klinikservices			
6	Die Leistungen der TÜV Rheinland i-sec GmbH			

TÜVRheinland®
Genau. Richtig.

Informationssicherheit in der stationären medizinischen Versorgung

Was ist B3S

- B3S ist ein sog. **Branchenspezifischer Sicherheitsstandard** des Bundesamt für Sicherheit in der Informationstechnik
- Der Branchenspezifische Sicherheitsstandard kann z.B. von Branchen- oder Berufsverbänden erarbeitet werden.
- Der Branchenspezifische Sicherheitsstandard wird durch das BSI geprüft und akkreditiert, d.h. ist der vorliegende Standard aus Sicht des BSI geeignet

TÜVRheinland®
Genau. Richtig.

Informationssicherheit in der stationären medizinischen Versorgung

Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus

Branche	Medizinische Versorgung
Sektor	Gesundheit
Scope	Branche "Medizinische Versorgung"
Antragsteller	Deutsche Krankenhausgesellschaft e.V. (DKG)
Ansprechpartner	Deutsche Krankenhausgesellschaft e.V. Herr Markus Holzbrecher-Morys Wegelystraße 3 10632 Berlin
Dokument	Der B3S kann auf der DKG-Website heruntergeladen werden.
Gültigkeit	Gültig bis August 2021

https://www.bsi.bund.de/SharedDocs/Textbausteine/DE/KRITIS/B3S/Gesundheit/2021_August_Gesundheit.html?nn=126610, abgerufen 15. Juni 2021

TÜVRheinland®
Genau. Richtig.

Agenda

Kapitel	Thema	Dauer	Referent	Seite
1	Informationssicherheit im Krankenhaus			
2	Rechtsgrundlagen			
3	Was ist B3S			
4	Die Anforderungsfelder des B3S			
5	TÜV Rheinland Klinikservices			
6	Die Leistungen der TÜV Rheinland i-sec GmbH			

TÜVRheinland®
Genau. Richtig.

Informationssicherheit in der stationären medizinischen Versorgung

Die Anforderungsfelder des B3S

Die gute Nachricht vorweg :

Eine Zertifizierung nach ISO 27001 ist für den Nachweis der notwendigen Maßnahmen nicht notwendig !

Ob und inwieweit dies für die Zukunft gilt, bleibt abzuwarten

https://www.dkgev.de/fileadmin/default/Mediapool/2_Themen/2.1_Digitalisierung_Daten/2.1.4._IT-Sicherheit_und_technischer_Datenschutz/2.1.4.1._IT-Sicherheit_im_Krankenhaus/B3S_KH_v1.1_8a_geprueft.pdf, S.10, abgerufen 15. Juni 2021

TÜVRheinland®
Genau. Richtig.

Informationssicherheit in der stationären medizinischen Versorgung

Die Anforderungsfelder des B3S

Maßnahmen zur Aufrechterhaltung des Versorgungsniveaus

„angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der **VERFÜGBARKEIT, INTEGRITÄT, AUTHENTIZITÄT und VERTRAULICHKEIT**

https://www.dkgev.de/fileadmin/default/Mediapool/2_Themen/2.1_Digitalisierung_Daten/2.1.4._IT-Sicherheit_und_technischer_Datenschutz/2.1.4.1._IT-Sicherheit_im_Krankenhaus/B3S_KH_v1.1_8a_geprueft.pdf, S.10, abgerufen 15. Juni 2021

TÜVRheinland®
Genau. Richtig.

Informationssicherheit in der stationären medizinischen Versorgung

Die Anforderungsfelder des B3S

Risiko-Management als Kernkomponente mit derzeit 37 definierten Anforderungen

- Organisation des Risikomanagements
- Ermittlung der Risikoobjekte und Risiko-Eigentümer
- Festlegung der Kritikalität (nach vorgegebenem Muster)
- Risikoidentifikation
- Risikobewertung
- Risikobehandlung
- Risikokommunikation und -überwachung

TÜVRheinland®
Genau. Richtig.

Informationssicherheit in der stationären medizinischen Versorgung

Die Anforderungsfelder des B3S

Definition des Geltungsbereichs mit Vorgaben branchenspezifischer Technik und Software

- 6.4.1 Krankenhausinformationssystem (KIS)Ermittlung der Risikoobjekte und Risiko-Eigentümer
- 6.4.2 Laborinformationssystem (LIS)Risikoidentifikation
- 6.4.3 Radiologieinformationssystem (RIS)
- 6.4.4 Picture Archive and Communication System (PACS)
- 6.4.5 Dokumenten-Management-System / Enterprise-Content-Management
- 6.4.6 Medizintechnik
- 6.4.7 Transportlogistik
- 6.4.8 Versorgungstechnik
- 6.4.9 Versorgungsdienste
- 6.4.10 Sonder- und Spezial-Softwarelösungen

TÜVRheinland®
Genau. Richtig.

Informationssicherheit in der stationären medizinischen Versorgung

Die Anforderungsfelder des B3S

Definition des Geltungsbereichs mit Vorgaben zu kritischen Dienstleistung (kDL)

- 6.5.1 Informationstechnik (16 Subkategorien)
- 6.5.2 Kommunikationstechnik (4 Subkategorien)
- 6.5.3 Versorgungstechnik (14 Subkategorien)
- 6.5.4 Medizintechnik/-produkte (6 Subkategorien)
- 6.5.5 kritische branchenspezifische Anwendungssysteme (10 Subkategorien)

TÜVRheinland®
Genau. Richtig.

Informationssicherheit in der stationären medizinischen Versorgung

Die Anforderungsfelder des B3S

Informationssicherheits-Managementsystem (ISMS)
Mit derzeit **168 Anforderungen** aus den klassischen Bereichen der Informationssicherheit und Zusatzanforderungen

- Organisation (27 Anforderungen)
- Meldepflichten nach § 8b Absatz 4 BSI-Gesetz (3 Anforderungen)
- Betriebliches Kontinuitätsmanagement (12 Anforderungen)
- Asset Management (9 Anforderungen)
- Robuste/resiliente Architektur (9 Anforderungen)
- Physische Sicherheit (4 Anforderungen)

TÜVRheinland®
Genau. Richtig.

Informationssicherheit in der stationären medizinischen Versorgung

Die Anforderungsfelder des B3S

Informationssicherheits-Managementsystem (ISMS)
Mit derzeit **168 Anforderungen** aus den klassischen Bereichen der Informationssicherheit und Zusatzanforderungen

- Vorfallerkennung und Behandlung (6 Anforderungen)
- Überprüfungen im laufenden Betrieb (8 Anforderungen)
- Externe Informationsversorgung und Unterstützung (2 Anforderungen)
- Lieferanten, Dienstleister und Dritte (5 Anforderungen)
- Technische Informationssicherheit (76 Anforderungen)

TÜVRheinland®
Genau. Richtig.

Informationssicherheit in der stationären medizinischen Versorgung

Die Anforderungsfelder des B3S

Informationssicherheits-Managementsystem (ISMS)
Mit derzeit **168 Anforderungen** aus den klassischen Bereichen der Informationssicherheit und Zusatzanforderungen

- Die Technische Informationssicherheit bedarf einer Einzelfallbetrachtung bezogen auf die branchenspezifische Technik und Software sowie der kritischen Dienstleistungen (kDL)

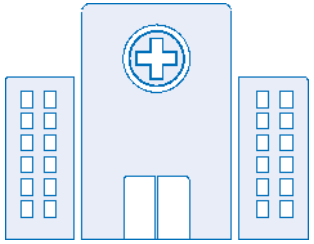
TÜVRheinland®
Genau. Richtig.

Agenda

Kapitel	Thema	Dauer	Referent	Seite
1	Informationssicherheit im Krankenhaus			
2	Rechtsgrundlagen			
3	Was ist B3S			
4	Die Anforderungsfelder des B3S			
5	TÜV Rheinland Klinikservices			
6	Die Leistungen der TÜV Rheinland i-sec GmbH			

TÜVRheinland®
Genau. Richtig.

TÜV Rheinland Klinikservice - Überblick



Zuverlässigkeit und Sicherheit von Gebäuden und technischen Einrichtungen
- Bestandsaufnahmen und Prüfungen der Gebäude-, Betriebs- und Bautechnik
- Medizintechnisches Gerätemanagement
- Hygieneinspektionen (VDI 6022)
- Inspektionen und Prüfungen nach Legionellenverordnung (42. BImSchV)
- Dienstleistungen rund um den Brandschutz

Digitalisierung, Daten- und Informationssicherheit
- Beratung zu Managementsystemen und technologischen Themen
- Überwachung der Informationssicherheit
- Unterstützung bei der Auswahl und Bereitstellung von Hardware und Software
- Kontinuierliche Systemüberwachung
- Planung und Unterstützung bei Digitalisierungsinitiativen (z. B. Krankenhaus 4.0)

Umweltschutz und Nachhaltigkeit von Gebäuden
- Gefahrstoffmanagement
- Umwelt- und Ressourcenmanagement
- Energieaudits gemäß Energiedienstleistungsgesetz und Energie-management ISO 50001
- Nachhaltiges Bauen und Green Building-Zertifizierungen

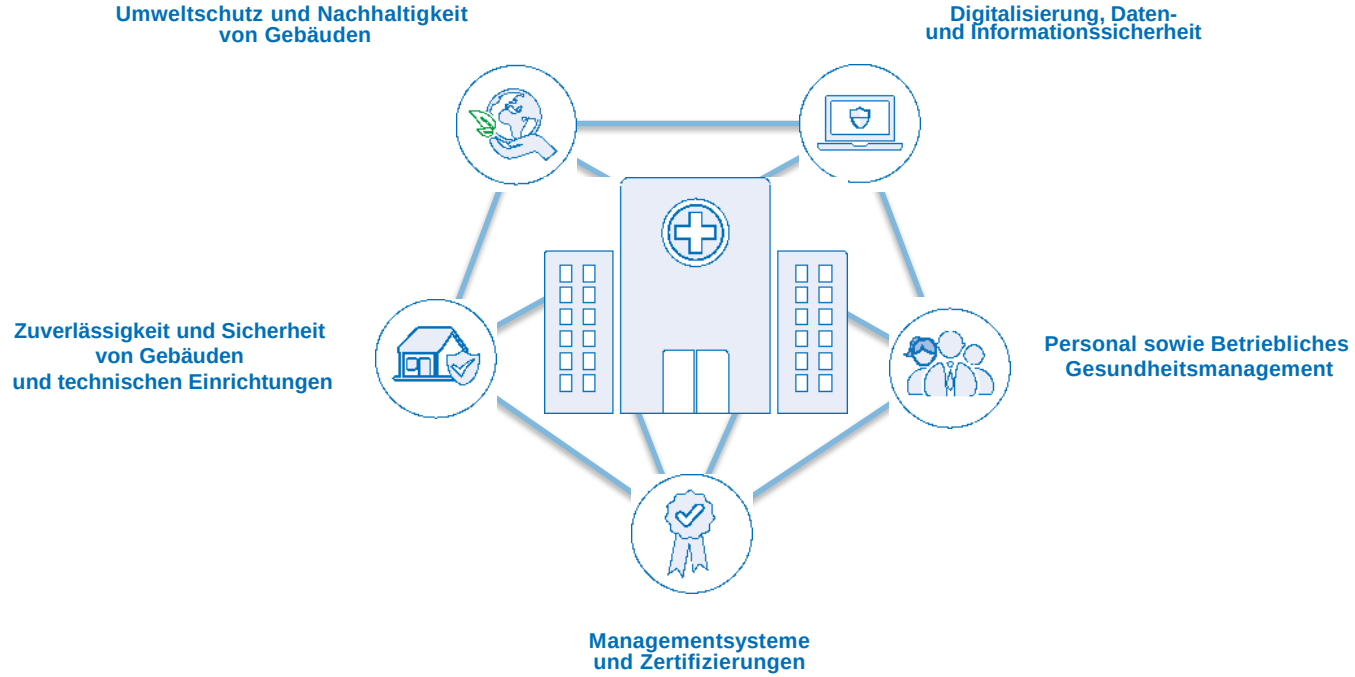
Personal sowie Betriebliches Gesundheitsmanagement
- Aus- und Weiterbildung
- Beauftragtenwesen
- Arbeitsmedizinische Betreuung
- Arbeitssicherheitstechnische Betreuung
- Betriebliches Gesundheitsmanagement

Managementsysteme und Zertifizierungen
- Zertifizierung von Managementsystemen für Akut- und Rehakliniken
- Auditierung von fachspezifische Standards für klinische Einrichtungen
- Zertifizierung der Zentralen Sterilgutversorgung nach EN ISO 13485

TÜVRheinland®
Genau. Richtig.

TÜV Rheinland Klinikservice

Vernetzte Dienstleistungen aus einer Hand



TÜVRheinland®
Genau. Richtig.

Agenda

Kapitel	Thema	Dauer	Referent	Seite
1	Informationssicherheit im Krankenhaus			
2	Rechtsgrundlagen			
3	Was ist B3S			
4	Die Anforderungsfelder des B3S			
5	TÜV Rheinland Klinikservices			
6	Die Leistungen der TÜV Rheinland i-sec GmbH			

TÜVRheinland®
Genau. Richtig.

Leistungsspektrum der TÜV Rheinland i-sec - Umsetzungsunterstützung

- Durchführung einer B3S Gap-Analyse
  - Bewertung des IST-Zustands gemessen am Stand der Technik, Empfehlungen konkreter Maßnahmen, Unterstützung bei der Umsetzung der Maßnahmen
- Verbesserung der IT-Sicherheit
  - Aufbau eines nachhaltigen Information Security Management Systems (ISMS)
  - Gestaltung Ihrer Systeme für Risikomanagement, ISMS, IKS und IT im Hinblick auf Governance, Risk und Compliance-Anforderungen
  - Einführung eines Business Continuity Management Systems (BCMS) zur sicheren Fortführung kritischer Geschäftsprozesse in Not- und Schadensfällen
  - Ganzheitliche Lösungen in den Bereichen Datenschutz und IT Compliance
  - Erstellung von Prozessen und Verfahren sowie notwendigen Dokumentationen
- Tool-Unterstützung Risiko- und Asset-Management zur effizienten und zielgerichteten Dokumentationserfüllung

TÜVRheinland®
Genau. Richtig.

Digital Enterprise. Protected.

Our Cyber Security Portfolio .

Portfolio Categories:	Portfolio Lines:		Delivery Types::
Mastering Risk & Compliance	Governance & Strategy	Business Continuity Management	**Consulting Services**
	Risk & Compliance Management	Data Privacy	**Testing Services**
	Information Security Management Systems		**Managed Services**
Advanced Cyber Defenses	Identity & Access Management	IoT Security	
	Network Security	Industrial Security	
	Application Security	Security Analytics & Detection	
	Endpoint Security	Incident Response	
	Data Protection		
Secure Cloud Adoption	Cloud Security		
	Enterprise Cloud Adoption		
	Hybrid Infrastructure		

TÜVRheinland®
Genau. Richtig.

Ihre Ansprechpartner:

Frank Kümpel
Principal Consultant
Frank.Kuempel@i-sec.tuv.com

Naomi Bals
Key Account Managerin
Naomi.Bals@i-sec.tuv.com

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Köln

www.tuv.com/informationssicherheit

TÜVRheinland®
Genau. Richtig.