xtention
IT with care.

Informationssicherheit in der Abteilung Technik

Die neuen Anforderungen auf den Punkt gebracht

Fachvereinigung Krankenhaustechnik e.V.

UNTERNEHMENSGRUPPE

xtention IT with care. soffico icw xD it for industries*

Agenda

01 Herkunft der Anforderungen

02 Bedeutung der Anforderungen

03 Die Anforderungen

04 Ausblick

Vorstellung

Fridolin Leibetseder, BSc MA

Mitarbeiter Prozess- & Qualitätsmanagement,
Informationssicherheit & Datenschutz

Ausbildung:

- Sichere Informationssysteme (FH Hagenberg) (BSc)
- Information Security Management (FH Hagenberg) (MA)

Zertifizierungen:

- Datenschutzbeauftragter
- ISMS Manager und Auditor nach ISO 27001
- Zusätzliche Prüfverfahrenskompetenz nach §8a (3) BSIG

Tätigkeiten:

- Externer CISO bei vier Krankenhäusern (zwei davon KRITIS-Häuser) und ein internationales Logistik-Unternehmen
- Vielzahl an Kundenprojekten zum ISMS-Aufbau bzw. zur KRITIS-Vorbereitung
- Diverse weitere Kundenprojekte (Datenschutz und Informationssicherheit), Security Awareness, Patch & Schwachstellen Management

01

Herkunft der Anforderungen

Richtlinien, Gesetze und Verordnungen

Herkunft der Anforderungen

Gesetzlicher Hintergrund

Für KRITIS:

1. NIS Richtlinie (EU)

2. IT SIG

3. BSIG

4. B3S

Für alle:

- Patientendaten-Schutz-Gesetz
- Schritt Richtung Digitalisierung
- Änderung des Fünften Buches Sozialgesetzbuch
  - §75c IT-Sicherheit in Krankenhäusern wird eingefügt
  - (1) 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 […]
  - (2) 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, […]
  - (3) 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.

Anforderungen

1.

Einrichten einer Kontaktstelle für das BSI (für KRITIS verpflichtend §8b (3) BSIG)

2.

Aufbau von Meldeprozessen für Störungen oder Ausfälle an das BSI

(für nicht KRITIS freiwillig)

3.

Maßnahmen zur Aufrechterhaltung des Versorgungsniveaus

Angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der VERFÜGBARKEIT, INTEGRITÄT, AUTHENTIZITÄT und VERTRAULICHKEIT ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von Ihnen betriebenen kritischen Infrastrukturen maßgeblich sind.

02

Bedeutung der Anforderungen

Schutzziele, Geltungsbereich und der B3S

Schutzziele

VERFÜGBARKEIT	INTEGRITÄT	AUTHENTIZITÄT	VERTRAULICHKEIT
…von Dienstleistungen, Funktionen eines Informationssystems, IT-Systems, IT-Netzinfrastruktur oder auch von Informationen ist dann gegeben, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.	…bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.	…der Informationen ist sichergestellt, wenn sie von der angegebenen Quelle erstellt wurden.	…stellt den Schutz vor unbefugter Preisgabe von Informationen sicher. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in zulässiger Weise zugänglich sein.

Branchenspezifischer Sicherheitsstandard

Für die Gesundheitsversorgung im Krankenhaus

Ein branchenspezifischer Sicherheitsstandard (B3S) wird innerhalb der jeweiligen Branche entwickelt und soll Sicherheit bei der Umsetzung und bei der Prüfung der Anforderungen gemäß § 8a Absatz 1 BSIG geben.

Zudem vermittelt er Rechtssicherheit, was das BSI im jeweiligen Bereich als "Stand der Technik" ansieht.

DEUTSCHE KRANKENHAUS GESELLSCHAFT

Branchenspezifischer Sicherheitsstandard

Scope / Geltungsbereich

SCOPE / GELTUNGSBEREICH

- Im Sektor Gesundheit repräsentiert die Branche „Medizinische Versorgung“ in den Krankenhäusern, d.h. die (voll-)stationäre Versorgung aus Sicht des Gesetzgebers die zentrale Dienstleistung des Sektors.
- Ausschlüsse aus dem Geltungsbereich sind hinreichend zu beschreiben.
- Beim Scope Lieferanten und Dienstleister nicht vergessen

Branchenspezifischer Sicherheitsstandard

Scope / Geltungsbereich

TECHNISCHE UNTERSTÜTZUNGSPROZESSE IN DER STATIONÄREN VERSORGUNG

- Versorgungstechnische Systeme sind für die Aufrechterhaltung eines geregelten Krankenhausbetriebs unerlässlich und stellen Grundbedürfnisse der Organisation und der Patienten / Mitarbeiter sicher.

- Ohne Bereitstellung bestimmter Leistungen der Versorgungstechnik ist ein Krankenhausbetrieb nicht aufrecht zu erhalten.

03

Die Anforderungen

Kritikalität von Systemen, Assetmanagement, Risikomanagement, ...

B3S

Kritikalität von Systemen

Sollten anhand der Zeitspanne – in der nach Ausfall des Systems – noch keine relevanten Einschränkung der medizinischen Leistungserbringung zu erwarten sein, sind mit Hilfe von TOMs die Störungen und Ausfallzeiten kurz-, mittel- oder langfristig zu überbrücken. Erstellung von Notfallplänen zum Umgang mit Störungen und Ausfällen muss erfolgen. (Abstimmung mit anderen Bereichen!)

1

Systeme der Klasse 1

Höchstens kurzfristig verzichtbar

2

Systeme der Klasse 2

Mittelfristig verzichtbar

3

Systeme der Klasse 3

Längerfristig verzichtbar

B3S

Assetmanagement

Unter Assetmanagement wird die Dokumentation aller Unternehmenswerte verstanden.

ZIEL ist es, eine Übersicht zu haben welche Assets / Werte ich im Unternehmen habe:

- Welche Kritikalität haben diese (siehe Folie davor)
- Werden darauf ggf. personenbezogene Daten oder Gesundheitsdaten verarbeitet?

Das Assetmanagement dient vielen weiteren Maßnahmen als Grundlage.
Diese Übersicht kann in einer Software wie z.B. Wave abgebildet werden oder auch mit Hilfe einer Excelliste.

ERFAHRUNG aus den §8a-Prüfungen:

- Markierung ob innerhalb des Geltungsbereichs oder nicht
- Wie funktioniert Wartung + Nachweise / Protokolle / Berichte
- Ausfallpläne

B3S

Risikomanagement

Mit Hilfe des Risikomanagements können Risiken kontrolliert behandelt und an den notwendigen Entscheidungsträger weiter gegeben werden.
In Kapitel 4 des B3S gibt es eine Beschreibung sowie 37 Anforderungen an das Risikomanagement.

ZIEL ist es, Risiken zu identifizieren und abzufangen bevor diese eintreten und Schaden verursachen können.

Auch für das Risikomanagement gibt es unterschiedliche Softwareunterstützungen, kann jedoch auch mit Excel umgesetzt werden.

Um mit dem Risikomanagement zu beginnen, würde zur Identifizierung ein Brainstorming der jeweiligen Prozess- / System- / Anwendungsverantwortlichen reichen.

ERFAHRUNG aus den §8a-Prüfungen:

Das Risikomanagement des B3S unterscheidet sich von z.B. dem aus der ISO 27005. Die Erfahrung zeigt, dass dies bei den Prüfungen kein Problem ist, solange man den Prozess lebt und es argumentieren kann.

B3S

Beschaffung

Im Zuge der Beschaffung sollten Informationssicherheit und Datenschutz mitberücksichtigt werden.

ZIEL: Bei einer Ausschreibung sollte nicht zu 100% der Preis ausschlaggebend sein, sondern es sollten zum Beispiel auch für die Sicherheit der Systeme Prozente vergeben werden.
Neue Systeme sollten vor der Anschaffung auf ihre Sicherheit etc. überprüft werden bevor diese in Betrieb gehen.

ERFAHRUNG aus den §8a-Prüfungen:

Beispielsweise kann das mit einem Fragebogen – der vor der Anschaffung an den Hersteller gesendet wird und anschließend ausgewertet wird – umgesetzt werden.
Sind Antworten nicht zufriedenstellend können diese in das Risikomanagement aufgenommen werden oder es wird sich nach einem anderen Anbieter umgesehen.
Für die §8a-Prüfung ist die Skizzierung / Beschreibung des Prozesses und das vorzeigen von ausgefüllten Fragebogen meist ausreichend.

B3S

Change Management

Im Zuge des Change Managements werden sämtliche Änderungen innerhalb des Geltungsbereichs abgehandelt. Dabei geht es nicht nur um Änderungen an Konfigurationen, sondern auch um neu Anschaffungen die in die Infrastruktur hinzugefügt werden.

ZIEL ist es, alle Änderungen – abgestimmt von befugtem Personal – kontrolliert und dokumentiert durchzuführen.

Durch Abstimmungen vor der Durchführung von Änderungen sollten die Auswirkungen auf andere Bereiche (insbesondere IT und Medizintechnik) geprüft werden.

ERFAHRUNG aus den §8a-Prüfungen:

- Das Change Management ist meist innerhalb der IT größer bzw. genauer aufgestellt.
- Für die Technik reicht ein monatliches Abstimmen über geplante Änderungen / Wartungen etc. aus.

B3S

Ausfallkonzept

Systeme können ausfallen, daher ist es wichtig einen Ausfall- / Notfallsplan zu haben. Dieser kann unterschiedlich aussehen, wie z.B.

- es wird ein redundantes System betrieben welches bei einem Ausfall übernimmt *(Vorsicht! Ist die Redundanz wirklich durchwegs gegeben?)* ,
- es wird auf den manuellen Betrieb umgeschaltet oder
- es gibt keinen Ausfallsplan da z.B. durch Verträge abgesichert ist, dass innerhalb von kurzer Zeit ein Dienstleister mit einem neuen System vor Ort ist, etc.

ZIEL ist es, für die Systeme im Geltungsbereich / Scope einen Ausfallplan zu haben (beginnend bei Systemen mit hoher Kritikalität).
Falls es schon ein Notfall- oder Business Continuity Management gibt, sollte dieses ausgeweitet/zusammengeführt werden.

ERFAHRUNG aus den §8a-Prüfungen:

Benötigen Pläne zusätzliche Ressourcen – z.B. ein teures System müsste redundant aufgestellt werden – können diese über das Risikomanagement an den richtigen Entscheider herangetragen werden.
Es sollten auch allgemeine Szenarien wie Brand oder Ausfall von Strom / Internet berücksichtigt werden.

B3S

Entsorgung von Geräten

Werden Systeme entsorgt (fehlerhaft oder end of life) ist darauf zu achten, dass diese keine personenbezogenen oder sensiblen Daten beinhalten. Im Idealfall werden jegliche Speicher sicher vernichtet ggf. durch zertifizierten Dienstleister vor Ort im Klinikum.

Idealerweise ist im Assetmanagement markiert bei welchen Systemen bei der Entsorgung auf den Speicher geachtet werden muss. Anschließend können die Speicher z.B. in einer Datentonne gelagert werden, bis der Dienstleister vor Ort zur Vernichtung kommt.

ZIEL ist es, einen praxistauglichen Prozess im Unternehmen zur etablieren der ungewollten Datenabfluss bei der Entsorgung verhindert.

ERFAHRUNG aus den §8a-Prüfungen:
Auch wenn es viele kreative Wege gibt Speicher zu vernichten – abreagieren von Azubis, einmauern in Grundfeste neuer Gebäude – ist grundsätzlich das Hinzuziehen eines zertifizierten Dienstleisters, der die Speicher vor Ort nach den in der DIN vorgegebenen Größen shreddert und das vorgehen Dokumentiert, zu bevorzugen.
Vorsicht! Bei Geräten die unter Wartung stehen oder geliehen sind (wie z.B. Multifunktionsdrucker) können auch diese ggf. Gesundheitsdaten im Speicher enthalten (im Idealfall bei Vertragserstellung berücksichtigen).

B3S

Schwachstellen Scans

Systeme werden manchmal unsicher konfiguriert oder es werden Schwachstellen bekannt, damit solche Lücken gefunden werden können, bevor sie von Angreifern ausgenutzt werden empfehlen sich Schwachstellen Scans oder Penetration Tests.

Penetration Tests und Schwachstellen Scans sollten von externen Unternehmen beauftragt werden, da hierfür viel Know-How notwendig ist. Grundlegend können Schwachstellen Scans aber auch selbst durchgeführt werden.

ZIEL ist es, die eigenen Systeme regelmäßig zu überprüfen, damit Lücken und Angriffsmöglichkeiten entdeckt werden bevor diese von kriminellen ausgenützt werden können.

ERFAHRUNG aus den §8a-Prüfungen:

Egal ob durch Dienstleister oder selbst durchgeführt ist es wichtig, dass dieses Thema regelmäßig betrachtet wird. Bei den §8a-Prüfungen war erfahrungsgemäß IT das Hauptziel.

04

Ausblick

BSI Grundschutz Kompendium

Ausblick

Zwei neue BSI – Bausteine in Arbeit

Ziel ist es, die Bausteine in die kommende Edition 2022 des IT-Grundschutz-Kompendiums aufzunehmen.
Davor ggf. als Community Draft auf der Webseite des BSI veröffentlicht.

INF 13

TECHNISCHE GEBÄUDEMANAGEMENT

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil bei Planung, Umsetzung und Betrieb im Rahmen des technischen Gebäudemanagements zu etablieren.

INF 14

GEBÄUDEAUTOMATION

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil bei Planung, Realisierung und Betrieb von Gebäudeautomation zu etablieren.

Quellen

Name	Beschreibung	Download
BSI Grundschutz Kompendium	Alternative zur ISO 27001, mit besseren Beschreibungen und Bausteinen für Technik (IND und INF – Bausteine)	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2021.pdf;jsessionid=043DB2483EC088829F3B474DB24A5AB8.internet081?__blob=publicationFile&v=6
B3S	Stand der Technik für Krankenhäuser	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
DIN 66399	Definiert Schutzklassen nach denen Datenträger vernichtet werden sollen.	Käuflich zu erwerben Übersicht: https://www.reisswolf.com/leistungsbereiche/akten-und-datenvernichtung/din-66399-schutzklassen/
Projekt Smart Hospitals (Uni München)	In Kapitel 8 Informationen zur Physischen Sicherheit und zur Bildung von Zonen.	https://www.unibw.de/code/smart-hospitals#dokumente
B3S	Branchenspezifischer Sicherheitsstandard für Anlagen oder Systeme zur Steuerung / Bündelung elektrischer Leistung	https://www.bdew.de/media/documents/20210222_BDEW_B3S_Anlagen_zur_Steuerung_und_Bundelung_v1.1_WQNbS5a.pdf

Quellen

Name	Beschreibung	Download
ISO 27001 / 27002	Standard Branchenübergreifend für Informationssicherheit	Käuflich zu erwerben
ISO 27005	Standard zum Informationssicherheits-Risikomanagement	Käuflich zu erwerben
ISO 27019	Standard für Automatisierungstechnik und Energieversorgung	Käuflich zu erwerben
IEC 62443 Familie	Norm zur IT-Sicherheit von Industriellen Automatisierungssystemen	Käuflich zu erwerben

Vielen dank für Ihre Aufmerksamkeit!

Fridolin Leibetseder

Prozess und Qualitätsmanagement

Externer Informationssicherheitsbeauftragter

Tel.: +43 7242 2155-6159

E-Mail: fridolin.leibetseder@x-tention.at

x-tention Informationstechnologie GmbH | Römerstraße 80a, 4600 Wels, Austria