Dietrich Bonhoeffer Klinikum

Neubrandenburg – Altentreptow – Malchin - Neustrelitz

Informationssicherheit im Krankenhaus

Erfahrungen mit dem KRITIS B3S Audit

Eric Werner

Diakonie Klinikum Dietrich Bonhoeffer GmbH

- 1.000 Betten in 28 Chefarzt geführten Kliniken und Instituten
- 3 Standorte (Neubrandenburg, Altentreptow, Malchin)
- Über 40.000 stationäre Fälle jährlich
- KRITIS-Betreiber nach BSI-KritisV

Quelle: http://dbknb.de/

Planungs-/Gründungsphase

Quelle: http://asyl-vgrd.de/index.php/unsere-arbeitsgruppen

- Initialisierung einer **Arbeitsgruppe**

Teilnehmerkreis:

- Geschäftsführung
- IT
- Medizintechnik
- Bau und Technik
- Qualitätsmanagement
- Datenschutzbeauftragter
- Informationssicherheitsbeauftragter

- **Zielfestlegung** (Nachweisverfahren gemäß B3S, ISMS nach IS0 27001, IT-Grundschutz-Kataloge)

Praktische Umsetzung (1): Orientierung

Quelle: 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/2019-04-02_B3S_KH_v1.0_-_Gesamtdokument.pdf

Praktische Umsetzung (2): Risikomatrix

- Bewertung der kritischen **Systeme, Prozesse** und **Anwendungen**
- Kategorisierung der **Systemklassen** (I, II, III)
- Bewertung der **Schutzziele**
- Identifikation von **Schutzmaßnahmen**
- Verknüpfung zum **Asset-Management**

Quelle: http://www.ibs-ce.de/index.php?id=5

Risikomatrix

1													
2							Schutzziele					Vorabb Geräte Anw	
3	B3S Kürzel	alle Geräte/Systeme/ Anwendungen	Risiko (welches unmittelbar die Sicherheit des Patienten betrifft) ggf. auch Rechtsfolgen, Imageverluste	Erläuterungen, Handlungsbedarf, Begründungen bzgl. Systemklasse und Schutzziele (Freitext)	Prozessverantwortlicher	Risikoeigentümer	Systemklasse 1, 2, 3	Verfügbarkeit (1)	Integrität/ Authentizität (2)	Vertraulichkeit (3)	Patientensicherheit (a)	Behandlungseffektivität (b)	Prozessverantwortlicher (Eintrittswahrscheinlichkeit)
4	1	2	3	4	5	6	7	8	9	10	11	12	13
44	MED02	Massenspektrometer	Erhebliche Einschränkungen bei der Diagnostik zur Behandlung des Patienten	Maldi Microflex LT	MT	LAB	1	3	3	1	2	3	2

1																		
2			chutzziele			Vorabbewertung der Geräte/ Systeme/ Anwendungen					Neubewertung der Geräte/ Systeme/ Anwendungen				Werte			
3	B3S Kürzel	alle Geräte/Systeme/ Anwendungen	Vertraulichkeit (3)	Patientensicherheit (a)	Behandlungseffektivität (b)	Prozessverantwortlicher (Eintrittswahrscheinlichkeit)	Risikoeigentümer (Schadensausmaß)	Risikowert	Maßnahmen und Ergebnisse (Freitext)	Prozessverantwortlicher (Eintrittswahrscheinlichkeit)	Risikoeigentümer (Schadensausmaß)	Risikowert		Patientendaten	Mitarbeiterdaten	Material-/ Finanzdaten	Geräte-/ Anlagendaten
4	1	2	10	11	12	13	14	15	16	17	18	19		20	21	22	23
44	MED02	Massenspektrometer	1	2	3	2	3	6	Ausfallkonzept, Servicevertrag	1	3	3					

Praktische Umsetzung (3): ANF-MN im B3S

AnMnk	Bez	Ar	AnMn10	Bem10	Beschr	St:	Kommentar (ges)
7.02.1	Geschäftsführung / Leitung	1	1	verantw.->MUSS	Die Geschäftsführung MUSS für Bekanntgabe und Durchsetzung entsprechender Ziele der Informationssicherheit (z. B. Informationssicherheitsleitlinie etc.) Sorge tragen.	E	Bezug zu: ALLE (Betrifft alle Mitarbeitenden im Scope) Kommentar: Entwurf ISLL Vers. 1.0 liegt der GF zur Entscheidung vor --> Freigabeprozess Share Center ToDo: Prüfung und Freigabe GF (KW 13) 27.05.19: ISLL freigegeben und ins Share Center eingestellt.
Softwaretests und Freigaben	159	159	0		Wurde die Software abgenommen, MUSS sie danach für die Nutzung freigegeben werden. Die Freigabe der Software ist nachweisbar zu dokumentieren und geeignet zu hinterlegen.	T	Bezug zu: IT,MT Kommentar: Betriebsbereitschaftserklärungen zu eingesetzten Systemen ToDo: Durch IT/MT zu bewerten IT: Aus DA-00778, Richtlinie IT-Vorgaben für Beschaffungsprozesse Endabnahme durch Betriebsbereitschaftserklärung (BBE). MT: Bei der MT sind ausschließlich Service-Protokolle vorhanden. Mit Unterschrift des Service-Protokolls ist die Freigabe erfüllt. Siehe auch ANF-MN 104 und ANF-MN 142.

Nachweisverfahren gemäß § 8a (3) BSIG

- Prüfgrundlage: B3S
- Geltungsbereich: Vollstationäre medizinische Versorgung
- Information an alle Mitarbeitenden
- Voraudit April 2019 (1. Tag)
- Nachweisverfahren Juni 2019 (4. Tage)
- Auditierung aller 3 Standorte

Ergebnis des Nachweisverfahrens

- Keine **Abweichungen**
- Keine **Beanstandungen**
- Lediglich **Hinweise** und **Empfehlungen**
- Benachrichtigung **BSI**

Weiteres Vorgehen

- **Bearbeitung** der **Hinweise** und **Empfehlungen** aus dem Nachweis, fortlaufend durch AG
- Intensivierung der **Mitarbeiterschulungen**
- Erhöhung der Anzahl **interner Audits**
- **Berücksichtigung** von **Informationssicherheit** in sämtlichen Prozessen, Systemen und Anwendungen
- Heranziehen von **Studien**, **Erfahrungsberichten** zum Thema KRITIS, Informationssicherheit etc.

Ausblick

Quelle:
https://www.spenderschrank.de/ausblick/

- **Personelle Ressourcen** steigen
- **Schwellenwerte** sinken
- **Notwendigkeit an Informationssicherheit** und die damit verbundenen **Kosten** steigen
- **Politik** muss verantwortlich handeln (Bereitstellung von Investitionsmitteln, Informationssicherheit und Gesundheitspolitik als Gesamtpaket betrachten)

Vielen Dank für Ihre Aufmerksamkeit!