

Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus

Gesamtdokument

18.12.2018

Status: Entwurf

TLP-Klassifikation: WHITE

Kategorie: öffentlich

Version: 0.86

Verteiler: Fachausschuss „Daten-Information und -Kommunikation“

Branchenarbeitskreis „Medizinische Versorgung“

Bundesamt für Sicherheit in der Informationstechnik

Inhaltsverzeichnis

1	Vorwort.....	6
1.1	Der „Umsetzungsplan kritische Infrastrukturen“ (UP KRITIS).....	7
1.2	IT-Sicherheitsgesetz	8
1.3	Branchenspezifische Sicherheitsstandards (B3S)	8
1.4	Kritische Infrastrukturen in der Branche „Medizinische Versorgung“	8
2	Methodik zur Erstellung des B3S	9
3	Branchenspezifischer Sicherheitsstandard (B3S) für die medizinische Versorgung	10
3.1	Grundlegendes zur Anwendung des B3S.....	11
3.2	Anforderungen an Betreiber Kritischer Infrastrukturen	11
3.2.1	Maßnahmen zur Aufrechterhaltung des Versorgungsniveaus.....	11
3.2.2	Einrichten einer Kontaktstelle für das BSI.....	11
3.2.3	Aufbau von Meldeprozessen für Störungen oder Ausfälle an das BSI.....	11
3.3	Dokumentenstruktur des B3S.....	12
3.4	Empfohlene Schritte zur Umsetzung des B3S	13
3.5	Fortschreibung des B3S.....	15
4	Risikomanagement in der Informationssicherheit.....	16
4.1	Standard-Risikomanagement-Prozessmodell.....	17
4.2	Management-Anforderungen für die Implementierung eines Informations- Risikomanagements	17
4.2.1	Ermittlung der Risikoobjekte und Risiko-Eigentümer	19
4.2.2	Festlegung von Kritikalität.....	19
4.2.3	Risikoidentifikation.....	20
4.2.4	Risikobewertung	20
4.2.5	Risikobehandlung	22
4.2.6	Risikokommunikation und -überwachung.....	23
4.3	IT-Systemlandschaft in Krankenhäusern nach Kritikalität.....	23
4.3.1	Systeme der Klasse 1	24
4.3.2	Systeme der Klasse 2	24
4.3.3	Systeme der Klasse 3	24
5	Allgemeine Hinweise zur Definition des Geltungsbereichs	25
5.1	Branchenspezifischer Geltungsbereich.....	25

5.2	Ergänzende Regelungen zum Geltungsbereich	27
5.2.1	Übersicht der Kernprozesse und Funktionszuordnung innerhalb des Geltungsbereichs.....	27
5.2.2	Technische Unterstützungsprozesse in der stationären Versorgung	31
5.2.3	Kritische branchenspezifische Anwendungssysteme	36
5.3	Festlegung der spezifischen Ziele und Anforderungen an die Informationssicherheit.....	42
5.4	Leitlinie zur Informationssicherheit	42
6	Branchenspezifische Gefährdungslage	44
6.1	Bedrohungsszenarien.....	45
6.1.1	Allgemeine Bedrohungen	45
6.1.2	IT-spezifische Bedrohungen	45
6.2	Schwachstellen.....	46
6.3	Branchenspezifische Gefährdungen.....	46
6.4	Gefährdungen kritischer branchenspezifischer Technik und Software.....	47
6.4.1	Krankenhausinformationssystem (KIS)	47
6.4.2	Laborinformationssystem (LIS)	48
6.4.3	Radiologieinformationssystem (RIS)	49
6.4.4	Picture Archive and Communication System (PACS).....	49
6.4.5	Dokumenten-Management-System / Enterprise-Content-Management.....	50
6.4.6	Medizintechnik	50
6.4.7	Transportlogistik.....	50
6.4.8	Versorgungstechnik.....	51
6.4.9	Versorgungsdienste.....	51
6.4.10	Sonder- und Spezial-Softwarelösungen	51
6.5	kDL-relevante IT-Systeme und Komponenten.....	52
6.5.1	Informationstechnik.....	52
6.5.2	Kommunikationstechnik.....	53
6.5.3	Versorgungstechnik.....	53
6.5.4	Medizintechnik/-produkte.....	53
6.5.5	kritische branchenspezifische Anwendungssysteme.....	54
7	Angemessene Maßnahmen zur Umsetzung	55
7.1	Informationssicherheitsmanagementsystem (ISMS).....	56

7.2	Organisation der Informationssicherheit.....	56
7.2.1	Geschäftsführung / Leitung.....	56
7.2.2	Beauftragter für Informationssicherheit (ISB, CISO).....	58
7.2.3	Prozess- /Anwendungsverantwortlicher.....	60
7.3	Meldepflichten nach § 8b Absatz 4 BSI-Gesetz.....	61
7.4	Betriebliches Kontinuitätsmanagement.....	61
7.5	Asset Management.....	63
7.6	Robuste/resiliente Architektur.....	64
7.7	Physische Sicherheit.....	65
7.8	Personelle und organisatorische Sicherheit.....	66
7.9	Vorfallerkennung und Behandlung.....	67
7.10	Überprüfungen im laufenden Betrieb.....	68
7.11	Externe Informationsversorgung und Unterstützung.....	69
7.12	Lieferanten, Dienstleister und Dritte.....	69
7.13	Technische Informationssicherheit.....	70
7.13.1	Netz- und Systemmanagement (Netztrennung und Segmentierung).....	70
7.13.2	Absicherung Fernzugriffe.....	70
7.13.3	Härtung und sichere Basiskonfiguration der Systeme und Anwendungen.....	71
7.13.4	Schutz vor Schadsoftware.....	71
7.13.5	Intrusion Detection / Prevention.....	72
7.13.6	Identitäts- und Rechtemanagement.....	72
7.13.7	Sichere Authentisierung.....	73
7.13.8	Kryptographische Absicherung (data in rest, data in motion).....	74
7.13.9	Mobile Sicherheit, Sicherheit Mobiler Zugang und Telearbeit (ggf. „bring your own device“ BYOD).....	75
7.13.10	Vernetzung von Medizingeräten.....	76
7.13.11	Datensicherung, Datenwiederherstellung und Archivierung.....	76
7.13.12	Ordnungsgemäße IT-Administration.....	77
7.13.13	Patch- und Änderungsmanagement.....	78
7.13.14	Beschaffungsprozesse.....	78
7.13.15	Protokollierung.....	79
7.13.16	Umgang mit Datenträgern, Austausch von Datenträgern.....	80
7.13.17	Sicheres Löschen und Entsorgung von Datenträgern.....	81

7.13.18	Softwaretests und Freigaben	82
7.13.19	Datenschutz	83
8	Übersicht der referenzierten Normen und Standards	84
9	Glossar	85

Aus Gründen der leichteren Lesbarkeit wird in den Beschreibungen auf eine geschlechtsspezifische Differenzierung, wie z. B. Teilnehmer/Innen, verzichtet. Es wird durchgängig die männliche Form benutzt. Im Sinne des Gleichbehandlungsgesetzes sind diese Bezeichnungen als nicht geschlechtsspezifisch zu betrachten und gelten gleichermaßen für beide Geschlechter.

1 Vorwort

Die zunehmende Digitalisierung ist auch im Gesundheitswesen heute allgegenwärtig. Sie bietet viele Chancen, Patientenversorgung zu verbessern, birgt aber auch Gefahren, die mit der wachsenden Durchdringung der Abläufe und Prozesse mit Informationstechnik einhergehen. Mit dem IT-Sicherheitsgesetz will der Gesetzgeber wirksame Schutzmechanismen für die so genannten kritischen Infrastrukturen in Deutschland festschreiben.

Die Nutzung informationstechnischer Systeme (IT-Systeme) und insbesondere deren Vernetzung sind allgegenwärtig. Moderne Medizin wäre ohne den Einsatz zum Teil hochkomplexer IT-Systeme nicht mehr denkbar, Informationstechnik stellt für einen optimalen Krankenhausbetrieb schon heute eine Grundvoraussetzung dar. In gleichem Maße steigen jedoch die Auswirkungen, die mit dem Ausfall oder der Beeinträchtigung ebensolcher Systeme verbunden sind. IT unterstützt heute den reibungslosen Ablauf vieler Prozesse im Klinikalltag. Dabei ist nicht nur der Einsatz medizinischer IT-Systeme relevant. Angefangen bei der Gebäudeleittechnik über Wäschereidienste bis hin zur Speiseversorgung der Patienten steuert, unterstützt und überwacht Informationstechnik wichtige Prozesse der Patientenversorgung. Die Verbesserung der Resilienz, d.h. der Widerstandsfähigkeit der IT gegen mögliche Störungen, Fehlfunktionen oder auch gezielte Manipulationen stellt dabei einen wichtigen Ansatz zur Verbesserung der IT-Sicherheit dar.

Dabei ist nicht nur die Sicherheit der IT-Systeme, sondern auch die Sicherheit der hiermit verarbeiteten Informationen in der Gesundheitsversorgung von besonderer Bedeutung. Um diese zu schützen, bedarf es neben der Umsetzung technischer und organisatorischer Vorkehrungen auch eines bewussten Umgangs mit diesen Informationen seitens der hiermit betrauten Mitarbeiter. Überall dort, wo sensible Informationen erhoben, verarbeitet oder gespeichert werden, greifen schon heute die unterschiedlichsten Regelungen zum Datenschutz im Gesundheitswesen. Datenschutz und Datensicherheit gemeinsam sind Bestandteile dessen, was man heute unter „Informationssicherheit“ versteht. Internationale Normen, wie bspw. die ISO 27001, geben den Rahmen für Informationssicherheits-Managementsysteme (ISMS) vor. Diese Systeme werden mit dem Ziel eingesetzt, ein angemessenes Schutzniveau der unternehmenskritischen Informationen sicherzustellen. Durch Sicherstellung der in der Informationssicherheit wesentlichen Schutzziele „Verfügbarkeit“, „Integrität“, „Authentizität“ und „Vertraulichkeit“ kann ein ISMS wesentlich zur Einhaltung unternehmensinterner sowie gesetzlicher Anforderungen, Standards und Regeln beitragen, um Informationssicherheit als integralen Bestandteil zu etablieren.

Der Schutz von Daten und Ressourcen, die Einhaltung von Maßnahmen zum Schutz vor Angriffen sowie - auch im Notfall - die Gewährleistung nachvollziehbarer Abläufe und Prozesse sowie schließlich die Einhaltung von Vertragsbeziehungen tragen dazu bei, die Aufrechterhaltung des gesellschaftlich etablierten Versorgungsniveaus zu gewährleisten.

1.1 Der „Umsetzungsplan kritische Infrastrukturen“ (UP KRITIS)

Auf Ebene des Bundes wurde mit dem „Nationalen Plan zum Schutz der Informationsinfrastrukturen“ schon im Jahr 2005 begonnen, auf die wachsenden Herausforderungen in diesem Bereich zu reagieren. Die Betrachtung der Informationsinfrastrukturen des Bundes wurde zwei Jahre später aus dem „Nationalen Plan zum Schutz der Informationsinfrastrukturen“ herausgelöst und wird seither separat entwickelt. Der „Nationale Plan zum Schutz der Informationsinfrastrukturen - Umsetzungsplan KRITIS“ (UP KRITIS) bildet seit 2007 im Wege einer „Public-private-Partnership“ die Basis für übergreifende Maßnahmen zum Schutz der kritischen Infrastrukturen. Bund und Länder unterscheiden 9 Sektoren Kritischer Infrastrukturen. Davon sind acht in der Plattform UP KRITIS organisiert, die jeweils noch einmal in einzelne Branchen unterteilt werden:

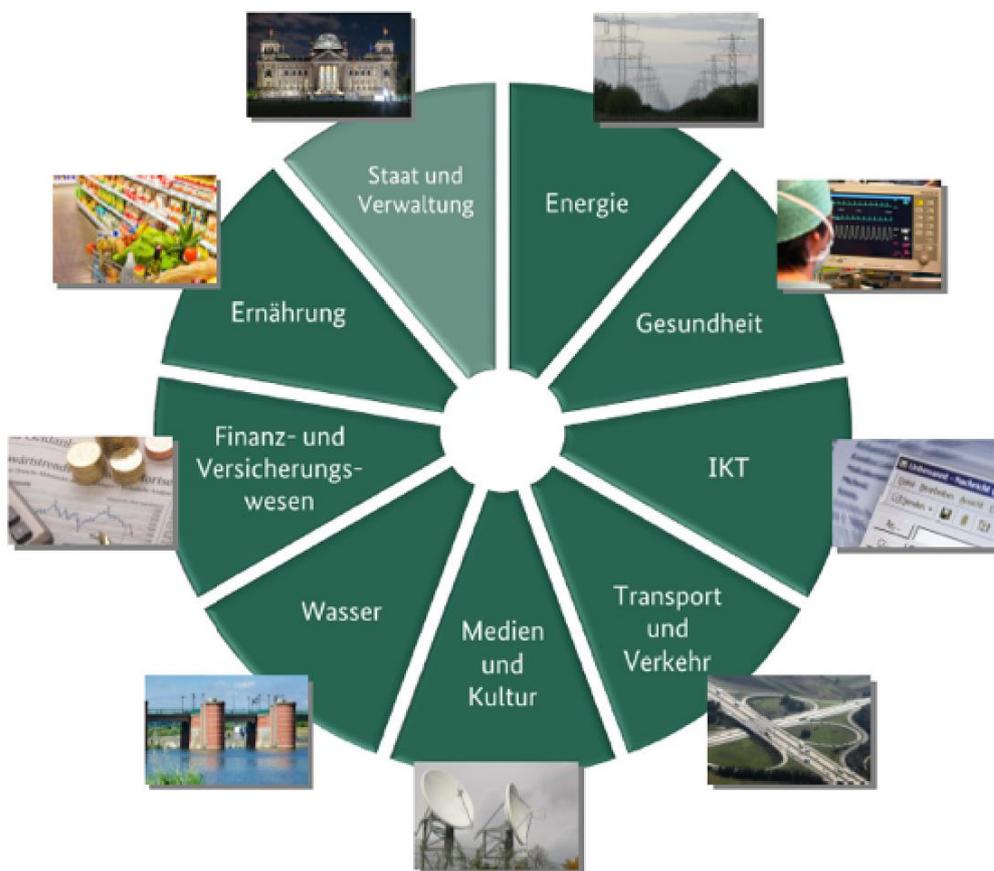


Abbildung 1 Die Sektoren des UP KRITIS (Quelle: BSI)

Im Sektor Gesundheit werden nach den Vorgaben des „Umsetzungsplans kritische Infrastrukturen (UP KRITIS)“ drei Branchen unterschieden:

- Medizinische Versorgung
- Arzneimittel und Impfstoffe
- Labore

1.2 IT-Sicherheitsgesetz

Zur Verbesserung der IT-Sicherheit in den kritischen Infrastrukturen Deutschlands hat der Gesetzgeber Regelungsbedarf in den Sektoren des UP KRITIS erkannt. Diesem Regelungsbedarf wurde mit der Verabschiedung des IT-Sicherheitsgesetzes im Jahr 2015 Rechnung getragen. Danach sind sektorspezifische Maßnahmen zur Verbesserung der IT-Sicherheit zu etablieren, um den Ausfall oder wesentliche Beeinträchtigungen der kritischen Infrastrukturen zu verhindern. Hierzu wurde eine Reihe gesetzlicher Änderungen auf den Weg gebracht, z.B. die im BSI-Gesetz neu verankerte Forderung nach „angemessenen, organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse“, welche der Betreiber einer kritischen Infrastruktur sicherzustellen hat.

1.3 Branchenspezifische Sicherheitsstandards (B3S)

Welche konkreten Maßnahmen innerhalb eines Sektors bzw. einer spezifischen Branche geeignet sein können, um die im BSI-Gesetz abstrakt formulierten Anforderungen umzusetzen, wird dabei weder in der entsprechenden Rechtsnorm noch der korrespondierenden Rechtsverordnung („BSI-KritisV“) geregelt. Die Branchen selbst können durch das Erarbeiten sog. branchenspezifischer Sicherheitsstandards (B3S) die für ihren Bereich sinnvollen und notwendigen Maßnahmen zusammenfassen und dem BSI zur Prüfung der Eignung bei der Erfüllung der im IT-Sicherheitsgesetz formulierten Ziele vorlegen. Dabei hängt der Aufwand zur Implementierung und Aufrechterhaltung geforderter Maßnahmen maßgeblich vom Grad der IT-Durchdringung sowie den nach bisherigen, rechtlichen und normativen Anforderungen, etablierten Maßnahmen ab. Die Aufrechterhaltung des Versorgungsniveaus der kritischen Infrastruktur steht dabei im Mittelpunkt, hierfür sollte u. a. ein Informationssicherheits-Managementsystem (ISMS) etabliert und aufrechterhalten werden. Das vorliegende Dokument stellt einen iterativen Ansatz zur Umsetzung eines entsprechenden branchenspezifischen Sicherheitsstandards für die Branche „Medizinische Versorgung“ vor.

1.4 Kritische Infrastrukturen in der Branche „Medizinische Versorgung“

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. Aufgabe der medizinischen Versorgung ist insbesondere die (Wieder-)Herstellung der Gesundheit der Bevölkerung. Die Perspektive des Gesetzgebers ist dabei der Schutz der Gesamtbevölkerung des Landes, so dass vergleichsweise hohe Maßstäbe an das Funktionieren des Allgemeinwesens geknüpft sind. Die einzelne Arztpraxis und auch kleinere Krankenhäuser oder medizinische Versorgungszentren fallen daher nicht unter die verpflichtenden Regelungen des BSI-Gesetzes. Zudem wurde bei der Formulierung der BSI-KritisV der ambulante Versorgungsbereich aus dem Regelungsbereich der Verordnung genommen.

Zur Erbringung der für das Allgemeinwesen wichtigen und daher „kritischen“ Dienstleistung der vollstationären Versorgung wurde die Anlagekategorie „Krankenhaus“ und als Bemessungskriterium die Anzahl vollstationärer Krankenhausbehandlungen im

Bezugszeitraum (Vorjahr) definiert. Der Schwellenwert zur Identifikation kritischer Infrastrukturen wurde auf 30.000 vollstationäre Behandlungsfälle festgelegt. Gemäß BSI-KritisV haben Krankenhäuser künftig jeweils zum 31. März zu prüfen, ob sie diesen Schwellenwert erreichen oder überschreiten. In diesem Fall übermitteln sie eine entsprechende Meldung an das Bundesamt für die Sicherheit in der Informationstechnik (BSI), das Krankenhaus gilt ab dem Folgetag (1. April) als kritische Infrastruktur i. S. d. BSI-Gesetzes. Mit der Meldung an das BSI ist ein Meldeprozess für IT-Störungen (IT-Sicherheitsvorfälle) zu organisieren, der einen beiderseitigen Informationsaustausch zwischen BSI und kritischen Infrastrukturen sicherstellen soll. Darüber hinaus sind geeignete organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der informationstechnischen Systeme insbesondere mit Blick auf die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der IT-Systeme und Daten zu treffen. Hierzu soll der vorliegende B3S genutzt werden können.

2 Methodik zur Erstellung des B3S

Der vorliegende B3S orientiert sich in seiner Methodik insbesondere an folgenden Quellen:

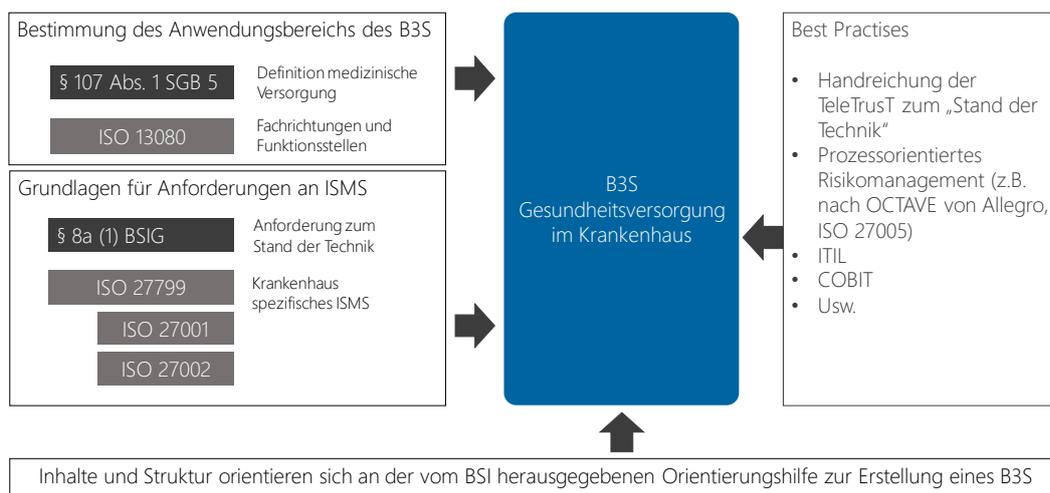


Abbildung 2: Rahmenbedingungen und Quellen zur Erstellung des B3S

Die Erstellung des B3S erfolgte in den folgenden Schritten:

1. Informationssicherheitsmanagement (ISMS) nach ISO 27001 als „Kern“ des B3S
2. Abgrenzung des Gültigkeitsbereichs
 - a. Ermittlung der kritischen Dienstleistungen (kDL) auf Basis der Funktionsbereiche und Funktionsstellen z. B. nach DIN ISO 13080
 - b. Festlegung des für den branchenspezifischen Sicherheitsstandard (B3S) geltenden Anwendungsbereichs mit Blick auf die kritische Dienstleistung (kDL)
 - c. Erläuterung zur Festlegung des für den Anwender des B3S spezifischen Geltungsbereichs
3. Erhebung der Anforderungen an ein Informationssicherheitsmanagementsystem (ISMS) nach ISO 27001 und ISO 27799

-
4. Identifikation der relevanten gesetzlichen Anforderungen zu den kDL im B3S-Anwendungsbereich
 5. Identifikation ggf. anwendbarer Sicherheitsstandards mit Bezug zur IT- und Informationssicherheit (Stand der Technik)
 6. Klassifikation der erhobenen Anforderungen
 - a. Ermittlung der branchenspezifischen Bedrohungen mit Wirkung auf die kritischen Prozesse und deren maßgeblichen IT-Systeme und sonstige Komponenten. Gemäß den in der Orientierungshilfe des BSI dargestellten Bedrohungs- und Schwachstellen-Kategorien
 - b. Interpretation der normativen Anforderungen mit Blick auf die medizinische Versorgung und branchenspezifische Risiken
 7. Anpassung von Inhalt und Strukturierung B3S gemäß B3S-Orientierungshilfe

3 Branchenspezifischer Sicherheitsstandard (B3S) für die medizinische Versorgung

Der vorliegende B3S orientiert sich an der in der Praxis etablierten Norm ISO 27001, dem „Stand der Technik“ sowie der darüberhinausgehenden branchenspezifischen Anforderungen der Norm ISO 27799, als auch der für den Anwendungsbereich relevanten wesentlichen Risiken. Für den vorliegenden B3S wurden nur die für die Zielgruppe dieses branchenspezifischen Sicherheitsstandards relevanten Aspekte übernommen. Eine Zertifizierung nach ISO 27001 ist für den Nachweis der notwendigen Maßnahmen nicht notwendig.

Der B3S dient der Etablierung eines angemessenen Sicherheitsniveaus i.S.v. § 8a (1) BSIG bei gleichzeitiger Wahrung des üblichen Versorgungsniveaus der Patientenversorgung und der Verhältnismäßigkeit der umzusetzenden Maßnahmen.

„Stand der Technik“ ist als unbestimmter Rechtsbegriff auch im Kontext der Informationssicherheit nicht abschließend definiert. Maßgeblich ist jedoch, dass ein B3S ausschließlich Vorgaben zur Ausgestaltung informations(sicherheits)technischer Prozesse und Maßnahmen machen kann, nicht aber etwa den „Stand der Technik“ der eingesetzten Medizinprodukte beschreibt.

Die heterogene Systemlandschaft in den Krankenhäusern stellt eine der Herausforderungen in der Umsetzung eines Sicherheitsstandards im Krankenhaus dar, da eine durchgängige Standardisierung der eingesetzten Systeme nicht vorausgesetzt werden kann. In der Folge kann derzeit (noch) nicht auf einen allgemein anerkannten „Stand der Technik“ in der Branche „Medizinische Versorgung“ referenziert werden. Zur Bestimmung des „Stand der Technik“ bietet es sich an, die für den B3S relevanten existierenden Sicherheitsstandards aus anderen Bereichen der Informationsverarbeitung sowie in der Praxis erfolgreich etablierte Methoden und Verfahren heranzuziehen.

3.1 Grundlegendes zur Anwendung des B3S

Die Umsetzung der geforderten Maßnahmen bedingt Fachwissen und Erfahrung auf dem Gebiet der Informationssicherheit. Sind diese Kenntnisse nicht in ausreichendem Maß vorhanden, empfiehlt sich die Inanspruchnahme qualifizierter Unterstützung.

Die Anwendung des vorliegenden B3S ist grundsätzlich freiwillig, sie bietet dem Anwender jedoch eine geeignete Prüfgrundlage zum Umsetzungsnachweis der erforderlichen Maßnahmen. Weist der Betreiber kritischer Infrastrukturen die Umsetzung eines durch das BSI als „geeignet zur Umsetzung der Anforderungen nach § 8b Abs. 4 BSI-Gesetz“ anerkannten B3S nach, wird von der Einhaltung der gesetzlich vorgeschriebenen Maßnahmen ausgegangen. Ziel ist die Sicherstellung und Aufrechterhaltung der kritischen Versorgungsdienstleistung und der hierfür benötigten Geschäftsprozesse.

Darüber hinaus wird der vorliegende Sicherheitsstandard Krankenhäusern zur Orientierung empfohlen, um ein hohes Maß an Sicherheit im Kontext moderner Informationsverarbeitung zu gewährleisten.

3.2 Anforderungen an Betreiber Kritischer Infrastrukturen

3.2.1 Maßnahmen zur Aufrechterhaltung des Versorgungsniveaus

Das BSI-Gesetz schreibt eine Reihe von Maßnahmen zur Verbesserung der IT-Sicherheit in Deutschland vor. Betreiber kritischer Infrastrukturen haben gemäß § 8a BSI-Gesetz u. a. „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. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Infrastruktur steht.“ Die Aufrechterhaltung des im jeweiligen Krankenhaus etablierten Versorgungsniveaus steht im Mittelpunkt der Betrachtung. Dieses kann abhängig vom Versorgungsauftrag, der jeweils verfügbaren Ressourcen sowie weiteren Einflussfaktoren unterschiedlich ausgeprägt sein.

3.2.2 Einrichten einer Kontaktstelle für das BSI

Darüber hinaus haben, gemäß § 8b Abs. 3, Betreiber Kritischer Infrastrukturen dem BSI eine Kontaktstelle für die Kommunikationsstrukturen nach § 3 Absatz 1 Satz 2 Nummer 15 zu benennen. Die Betreiber haben sicherzustellen, dass sie hierüber jederzeit erreichbar sind. Die Übermittlung von Informationen durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt an diese Kontaktstelle.“

3.2.3 Aufbau von Meldeprozessen für Störungen oder Ausfälle an das BSI

Weiterhin sind gemäß § 8b Abs. 4 durch den Betreiber kritischer Infrastrukturen „erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen kriti-

schen Infrastrukturen 1. führen können oder 2. geführt haben, über die Kontaktstelle unverzüglich an das Bundesamt zu melden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zur Branche des Betreibers enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der kritischen Infrastruktur geführt hat.“

3.3 Dokumentenstruktur des B3S

Die einzelnen Dokumente und deren Zielsetzung werden in der nachfolgenden Tabelle erläutert:

Nr	Abschnitt	Zielsetzung	Verweis Orientierungshilfe B3S des BSI
01	Rahmendokument	Grundsätzliche Darstellung der Zielsetzung des B3S sowie zur Anwendung der B3S-Abschnitte	Teil I
02	Risikomanagement	Anforderungen an die Umsetzung eines Informationssicherheits-Risikomanagements innerhalb des individuellen ISMS	
03	Geltungsbereich und Schutzziele	Herangehensweise zur Festlegung der individuellen Grenzen des durch den B3S geforderten Informationssicherheits-Managementsystems (ISMS) für die kDL und den damit verbundenen Schutzziele (Leitlinie zur Informationssicherheit)	
04	Gefährdungslage	Darstellung der branchenspezifischen Gefährdungslage	
05	Maßnahmenempfehlungen	Allgemeine Maßnahmenempfehlungen zur Behandlung der in 03 dargestellten Gefährdungslage.	Teil II
06	Nachweis der Umsetzung	Anforderungen an die Nachweisführung der Erfüllung der Anforderungen gemäß § 8a (1) und (3) BSIg	Teil III

Tabelle: Struktur des B3S

3.4 Empfohlene Schritte zur Umsetzung des B3S

Für die Umsetzung der Anforderungen wird die folgende, an der Priorisierung der erforderlichen Maßnahmen orientierte Schrittfolge vorgeschlagen.

Nr.	Ziele und Tätigkeiten	Verweis
1.	<p><u>Ziel</u></p> <p>Kontext des ISMS definieren</p> <p><u>Kerntätigkeiten</u></p> <p>Anwendungsbereich des ISMS und strategische Ziele der Informationssicherheit definieren</p> <ul style="list-style-type: none"> • Informationssicherheitspolitik entwickeln (Leitlinie) • Ermittlung relevante Compliance-Anforderungen 	Kapitel 5
2.	<p><u>Ziel:</u></p> <p>Managementstruktur für ISMS definieren</p> <p><u>Kerntätigkeiten:</u></p> <p>Entwicklung und Inkraftsetzung folgender Richtlinien / Standards:</p> <ul style="list-style-type: none"> • Sicherheitsorganisation und Verantwortlichkeiten • Vorgehen zur Informationssicherheitsrisikobeurteilung • Meldung und Behandlung von Sicherheitsvorfällen • Schulung und Bewusstseinsbildung • Lenkung von dokumentierten Informationen • Klassifizierung von Informationen • Sicherer IT-Betrieb • Interne Audits zur Wirksamkeitsprüfung • Vorbeuge- und Korrekturmaßnahmen • Steuerung von Lieferanten und Unterauftragnehmern (UAN) 	Kapitel 4 Kapitel 7 Risikomanagement in der Informationssicherheit
3.	<p><u>Ziel:</u></p> <p>Grundsätzliche Maßnahmen umsetzen</p> <p><u>Kerntätigkeiten:</u></p> <p>Implementierung der Sicherheitsorganisation, Entwicklung und in Kraftsetzung folgender Verfahren:</p> <ul style="list-style-type: none"> • Definition von Kriterien zur Bewertung und Klassifizierung von Informationen • Klassifizierung von Informationen • Verwaltung der Werte • Steuerung von Lieferantenbeziehungen • Handhabung von Informationssicherheitsvorfällen • Lenkung von dokumentierten Informationen 	Siehe Ergebnisse Nr. 2
4.	<p><u>Ziel:</u></p> <p>Bestandsaufnahme, Risikoeinschätzung und Konzeption</p> <p><u>Kerntätigkeiten:</u></p> <ul style="list-style-type: none"> • Werte und deren Eigentümer im Kontext der kDL (des Geltungsbereichs des ISMS) identifizieren 	Kapitel 4 Kapitel 6

Nr.	Ziele und Tätigkeiten	Verweis
	<ul style="list-style-type: none"> • Bedrohungen und Schwachstellen identifizieren • Eigentümer der Risiken identifizieren • Bewertung der aktuell umgesetzten technischen und organisatorischen Maßnahmen zur Informationssicherheit (GAP-Analyse, Reifegradanalyse) • Bewertung von Auswirkungen und Eintrittswahrscheinlichkeiten • Entscheidung über nicht akzeptable Risiken (Schutzbedarf vs. Risiko) • Risikobehandlung für jedes nicht akzeptable Risiko definieren; Maßnahmen auswählen und Restrisiko abschätzen • Ziele für ausgewählte Maßnahmen / Sicherheitsprozesse definieren • Bericht zu Risikoeinschätzung und -behandlung schreiben; Restrisiken genehmigen durch oberste Leitung 	
5.	<p><u>Ziel:</u></p> <p>Umsetzung der Maßnahmen (von detailliertem Plan zur Risikobehandlung)</p> <p><u>Kerntätigkeiten:</u></p> <p>Umsetzung der Maßnahmen gemäß definierter Richtlinien, Prozesse und Verfahren:</p> <ul style="list-style-type: none"> • Organisation der Informationssicherheit (z.B. Mobile Endgeräte) • Personelle Sicherheit • Management von Werten (Strukturanalyse) • Zugangskontrolle • Kryptografie • Physische- und Umgebungssicherheit • Betriebssicherheit • Kommunikationssicherheit • Systembeschaffung, Entwicklung und Wartung • Beziehungen zu Lieferanten • Umgang mit Informationssicherheitsvorfällen • Sicherstellung des Geschäftsbetriebs für die kDL 	Siehe Ergebnisse Nr. 4
6.	<p><u>Ziel:</u></p> <p>Projektbegleitende Trainings, Ausbildung und Awareness</p> <p><u>Kerntätigkeiten:</u></p> <ul style="list-style-type: none"> • Schulungsbedarf ermitteln • Zeitplan für Schulungsmaßnahmen definieren • Schulung und Sensibilisierung der Mitarbeiter und Führungskräfte (Awareness) 	Kapitel 7
7.	<p><u>Ziel:</u></p> <p>Evaluierung der Effektivität des ISMS</p> <p><u>Kerntätigkeiten:</u></p> <p>Monitoring & Überwachung</p> <ul style="list-style-type: none"> • Validierbare Evaluierung der Effizienz der Maßnahmen • Korrektive/präventive Maßnahmen definieren (nach Bedarf) <p>Planung und Durchführung interner Audits</p> <ul style="list-style-type: none"> • Auditoren auswählen und trainieren • Internes Audit durchführen und dokumentieren • Bericht über korrektive und präventive Maßnahmen erstellen 	06 Nachweis der Umsetzung (wird nachgereicht)

3.5 Fortschreibung des B3S

Das BSI stellt die Eignung eines B3S in der Regel für zwei Jahre fest, danach ist dieser für eine fortbestehende Aussage über seine Eignung dem BSI erneut vorzulegen. Für den hier vorgelegten B3S wird demgemäß eine turnusgemäße Überprüfung spätestens alle zwei Jahre angestrebt. Bis zu einer Aktualisierung behält die jeweils aktuelle Fassung des B3S ihre Gültigkeit.

4 Risikomanagement in der Informationssicherheit

Informationssicherheit muss zu einem Geschäftserfordernis werden.

In diesem Kapitel werden die grundlegenden Anforderungen an die umzusetzenden Abläufe des übergreifenden Risikomanagements beschrieben. Die konkreten und allgemeingültigen Gefährdungen bzw. Schwachstellen der kDL werden in Kapitel 6 beschrieben.

Ziel der „Informationssicherheit“ ist es, sowohl die Informationen selbst als auch die Prozesse, Anwendungen, Systeme, Services, Kommunikation und Einrichtungen zu schützen, welche die Informationen enthalten, verarbeiten, speichern, transportieren oder liefern.

Zur Aufrechterhaltung der Funktionsfähigkeit der kritischen Dienstleistung ist ein angemessenes und wirksames Risikomanagement zur Informationssicherheit zu betreiben und aktiv zu fördern

Die Umsetzung des B3S fokussiert gemäß B3IG § 8a insbesondere auf die Aufrechterhaltung der Funktionsfähigkeit der kritischen Dienstleistung „Stationäre medizinische Versorgung“. Zur Erfüllung der damit verbundenen organisationsspezifischen Sicherheits- und Geschäftsziele müssen Sicherheitsmaßnahmen eingeführt, überwacht, überprüft und bei Bedarf verbessert werden. Zudem bedarf es hierbei einer ganzheitlichen, koordinierten Betrachtung der Risiken für alle Informationswerte die innerhalb des B3S-Anwendungsbereichs genutzt werden und die eine Auswirkung auf deren Funktionsfähigkeit und somit der Informationssicherheit haben könnten.

Siehe im Standard ISO/IEC 27001 die Abschnitte 6.1.2, 6.1.3, 8.2 und 8.3

Für die Einschätzung und die Behandlung von Informationsrisiken ist eine Methodik zur einheitlichen Ermittlung von Bedrohungen, Schwachstellen und Risiken sowie Maßnahmen zu deren Behandlung und Steuerung festzulegen sowie eine Aussage zum akzeptablen Risikoniveau zu treffen.

Für den B3S-Anwendungsbereich erfolgt die Risikoeinschätzung entsprechend der Anforderungen folgender Normen:

ISO 27002 enthält allgemeine Umsetzungsempfehlungen

→ Informationssicherheit - allgemein: DIN ISO/IEC 27001 „Informationssicherheits-Managementsysteme - Anforderungen“

ISO 27799 enthält Umsetzungsempfehlungen für das Gesundheitswesen

→ Informationssicherheit von Medizingeräten in IT-Netzwerken: DIN EN 80001-1 „Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten - Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten“

Die wesentlichen Punkte des Risikomanagements in der Informationssicherheit werden in den nachfolgenden Abschnitten beschrieben.

4.1 Standard-Risikomanagement-Prozessmodell

Zur Umsetzung eines Standard-Risikomanagement-Prozesses haben sich die folgenden Teilprozesse bewährt:

1. Werte (Risikoobjekte) und Verantwortliche (Risiko-Eigentümer) ermitteln
2. Kritikalität der Werte festlegen
3. Risikokriterien festlegen
4. Bedrohungen und Schwachstellen identifizieren (potentielle und vorhandene)
5. Risiken bewerten (Eintrittswahrscheinlichkeit und Schadenspotenzial)
6. Risiken behandeln (akzeptieren, vermeiden, transferieren oder reduzieren)
7. Risiken kommunizieren und überwachen

Im Folgenden werden zunächst allgemeine Anforderungen an die Umsetzung des Risikomanagements (Management-Rahmen) definiert. Anschließend werden die Teilprozesse des Standard-Risikomanagement-Prozesses im Einzelnen dargestellt.

4.2 Management-Anforderungen für die Implementierung eines Informations-Risikomanagements

Es ist eine angemessene und wirksame Organisation zum Betrieb des Informationssicherheits-Risikomanagements zu etablieren, im Folgenden nur ISMS-Risikomanagement genannt.

ANF-RM 1 Die Krankenhausleitung MUSS die mit dem ISMS-Risikomanagement verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege definieren und aufeinander abstimmen sowie hierfür angemessene Risikosteuerungs- und -controllingprozesse einrichten und diesbezügliche Berichtspflichten definieren.

Das Informations-Risikomanagement ist vollständig, wenn es beispielsweise alle notwendigen Elemente der ISO/IEC 27005 enthält.

ANF-RM 2 Die Rahmenbedingungen zum ISMS-Risikomanagement MÜSSEN in einer Richtlinie zum ISMS-Risikomanagement festgelegt werden, welches den folgenden Zielen dient:

- a. Festlegung einer Organisationsstruktur mit den notwendigen Rollen (insbesondere des **Risikomanagers**), die dafür verantwortlich sind, sicherzustellen, dass der in diesem B3S geforderte ISMS-Risikomanagementprozess durchgeführt wird.
- b. Methode zur Ermittlung der Unternehmenswerte in der Informationstechnik und deren Verantwortlicher (Werteverantwortliche)
- c. Durchführung einer Schutzbedarfsfeststellung für die ermittelten Werte
- d. Festlegungen einer Risikomanagementmethode beim Einsatz von

Medizinprodukten in einem IT-Netzwerk innerhalb des B3S-Anwendungsbereichs gemäß DIN EN 80001-1.

- e. Ermittlung der für den B3S-Anwendungsbereich relevanten Bedrohungen und Schwachstellen
- f. Bewertung der sich aus den Bedrohungen und Schwachstellen ergebenden Risiken anhand von Eintrittswahrscheinlichkeiten und Schadenspotenzial
- g. Integration des ISMS-Risikomanagements in das bestehende, übergreifende Risikomanagement, insbesondere durch Ermittlung der aggregierten Risiken der Informationssicherheit
- h. Methode zur geeigneten Behandlung der Informationssicherheitsrisiken
- i. Anforderungen an Dokumentation und Kommunikation der Informationssicherheits-Risiken inklusive der Restrisiken und des Maßnahmenplans und der Bewertung durch das Management
- j. Regelungen zur Steuerung und Überwachung der Informationssicherheitsrisiken

ANF-RM 3 Die Informations-Risikorichtlinie MUSS explizit in Kraft gesetzt und allen Beschäftigten und ggf. relevanten Geschäftspartnern bekanntgegeben werden.

ANF-RM 4 Eine standardisierte Risiko-Methodik MUSS zur Ermittlung der Risikobewertungen (insbesondere im Hinblick auf die Schutzziele Verfügbarkeit, Integrität/Authentizität, Vertraulichkeit) festgelegt werden, um die Konsistenz der Bewertung der Risiken nachvollziehbar sicherstellen (ggf. auch Teil von ANF-RM 2).

ANF-RM 5 Es MUSS festgelegt werden, wer die Ergebnisse der Risikobewertung und -behandlung dokumentiert sowie alle nachfolgenden Überprüfungen zur Risikobewertung und -behandlung durchführt (ggf. auch Teil von ANF-RM 2).

ANF-RM 6 Zum Betrieb von als kritisch bewerteten Systemen (vernetzt, nicht vernetzt) aus den Bereichen Medizingeräte, IT-Systeme, IT-Netzwerke, IT-Anwendungen MUSS eine Freigabe auf Basis einer verbindlichen Risikobewertung vorliegen.

4.2.1 Ermittlung der Risikoobjekte und Risiko-Eigentümer

ANF-RM 7 Es MUSS ein Verantwortlicher festgelegt werden, der die Werte des Risikomanagements der Informationssicherheit ermittelt, dokumentiert und verwaltet.

ANF-RM 8 Ein Risikoeigentümer MUSS festgelegt werden, der die Ergebnisse der Risikoanalyse und -behandlung verantwortet sowie alle nachfolgenden Überprüfungen zu Risikoanalysen und -behandlungen durchführt.

ANF-RM 9 Grundsätzlich SOLLTE der Verantwortliche des Informationssystems als Risikoeigentümer der Information auch die Informationsrisiken ermitteln.

4.2.2 Festlegung von Kritikalität

ANF-RM 10 Für alle kritischen Werte (Informationen, IT-Systeme, Funktionen und Anwendungen) MÜSSEN die wesentlichen Anforderungen (Eigenschaften) der Verfügbarkeit, Integrität/Authentizität und Vertraulichkeit (Schutzziele) erhoben werden:

- a. VERFÜGBARKEIT: Die Verfügbarkeit von Werten ist gegeben, wenn diese von den Anwendern innerhalb definierter Rahmenbedingungen genutzt werden können.
- b. INTEGRITÄT/AUTHENTIZITÄT: Die Integrität/Authentizität ist gegeben, wenn die Korrektheit (Unversehrtheit), Echtheit und Vertrauenswürdigkeit von Informationen und der korrekten Funktionsweise von Systemen gewahrt wird.
- c. VERTRAULICHKEIT: Die Vertraulichkeit schützt Informationen vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.

ANF-RM 11 Die Bewertung der Schutzziele SOLLTE folgende Faktoren der Patientensicherheit und Behandlungseffektivität mit einbeziehen:

- a. PATIENTENSICHERHEIT: Freiheit von unvermeidbaren Risiken einer physischen Verletzung oder eines Schadens an der Gesundheit von Menschen oder eines Schadens an Eigentum oder der Umwelt
- b. BEHANDLUNGSEFFEKTIVITÄT: Wirksame Behandlung des Patienten unter Benutzung ausgetauschter Informationen sowie die Anwendung wirksamer Gesundheitsmaßnahmen, durch die verantwortliche Organisation aufgrund des Informationsaustausches

ANF-RM 12 Es MUSS eine Definition nicht akzeptabler Auswirkungen von Risiken, z. B. Gefährdung von Menschenleben, nicht akzeptable wirtschaftliche Schäden,

erfolgen. Wird ein Risiko identifiziert, dessen Auswirkungen die hier festgelegten Grenzwerte erreichen oder überschreiten, so DARF dieses System NICHT betrieben bzw. der Prozess so nicht umgesetzt werden.

ANF-RM 13 Für alle Werte MÜSSEN einzelne Personen oder Personengruppen als Verantwortliche festgelegt werden.

4.2.3 Risikoidentifikation

ANF-RM 14 Zur Identifizierung von Bedrohungen und Schwachstellen SOLLTEN Bedrohungsprofile, nach Möglichkeit auf Basis eines All-Gefahrenansatzes¹, erhoben werden, z. B.:

- a. Personen mit Netzzugang: Die Bedrohungen in dieser Kategorie stellen Bedrohungen für die Informationen über die technische Infrastruktur durch Personen dar. Dies kann durch Fehlhandlungen oder Vorsätzen von internen Personen sowie von externen Personen entstehen.
- b. Personen mit physischem Zugang: Die Bedrohungen in dieser Kategorie stellen Bedrohungen für die Informationen über physische Zugriffe dar. Dies kann durch Fehlhandlungen oder Vorsätzen von internen Personen sowie von externen Personen entstehen.
- c. Technische Bedrohungen: Die Bedrohungen in dieser Kategorie wirken auf die Systeme eines Unternehmens. Beispiele hierfür sind Hardwarefehler, Softwarefehler, Malware, Fehler einer USV und andere systembedingte Probleme.
- d. Weitere Bedrohungen: Die Bedrohungen in dieser Kategorie sind Probleme oder Situationen, die außerhalb der Kontrolle einer Organisation liegen. Zu dieser Kategorie von Bedrohungen gehören Kommunikationsstörungen, Stromausfälle und Naturkatastrophen (z. B. Überschwemmungen oder Erdbeben).

ANF-RM 15 Es SOLLTEN bereits etablierte Maßnahmen zu den erkannten Risiken erfasst und bei der Risikobewertung berücksichtigt werden.

4.2.4 Risikobewertung

Für alle Risikoobjekte sind die Eintrittswahrscheinlichkeiten und Schadenspotenziale so zu bewerten, als wenn sich ein entsprechendes Risiko materialisieren würde. Hierbei ist zu prüfen, welche Auswirkungen der Verlust eines Schutzziels (siehe ANF-RM 10) für das betrachtete Informationssystem darstellen könnte. Dies sind zum Beispiel Schäden finanzieller und anderer Art, direkte Schäden und Folgeschäden sowie der Aufwand

¹ Der All-Gefahrenansatz des BSI berücksichtigt die Elementaren Gefährdungen des IT-Grundschutz-Kompodiums

und die Dauer, um die Schäden zu beheben.

ANF-RM 16 Die Krankenhausleitung MUSS die Kriterien zur Bewertung von Risiken auf Basis von Eintrittswahrscheinlichkeiten und Schadenspotenzialen (ANF-RM 23) vorgeben (ggf. auch Teil von ANF-RM 2).

Statistische Ergebnisse sind
prinzipiell mit Unsicherheiten
behaftet

ANF-RM 17 Die Risikobewertung SOLL sich hinsichtlich einer Priorisierung an der Kritikalität der Werte entsprechend der Klassifizierung in Kapitel 4.3 (IT-Systemlandschaft in Krankenhäusern nach Kritikalität) orientieren.

ANF-RM 18 Risiken MÜSSEN anhand von Schadensklassen zu ihren qualitativen Schadensauswirkungen in Risikoklassen eingestuft und in eine Risikomatrix (Wahrscheinlichkeit gegen Auswirkung) eingeordnet werden.

ANF-RM 19 Risiken, die einer qualitativ hohen Schadensklasse zugeordnet wurden, MÜSSEN auch zu ihren quantitativen Schadensauswirkungen eingestuft werden.

ANF-RM 20 Die Schadensklassen MÜSSEN in mehreren Stufen, z. B. von „gering“ (geringe Schäden, keine Auswirkungen auf das Sicherheitsniveau) bis „gravierend“ (sehr hohe bis Existenz bedrohende Schäden), aufgeteilt werden.

ANF-RM 21 Die Eintrittswahrscheinlichkeit/Schadenshäufigkeit eines Risikos MUSS durch geeignetes Fachpersonal eingeschätzt werden, dies SOLLTE auf Basis geeigneter statistischer Erfassungen und Erfahrungen erfolgen.

ANF-RM 22 Zur Bestimmung der Eintrittswahrscheinlichkeiten SOLLTEN die folgenden Faktoren berücksichtigt werden:

- a. Schadenshäufigkeit: Sind neue Vorfälle oder Schäden durch Erfahrungswerte zu erwarten?
- b. Schwachstellenentdeckung: Wie leicht ist die Schwachstelle zu erraten?
- c. Fähigkeit des Angreifers: Welche technischen Fähigkeiten setzt ein erfolgreicher Angriff voraus?
- d. Exposition der kritischen Komponente: In welchem Maß ist das System durch seine räumliche Lage einer potenziellen Bedrohung durch ein natürliches Ereignis ausgesetzt?
- e. Güte der Maßnahmen zur Angriffsentdeckung: Wie schnell kann ein Angriff entdeckt werden?

ANF-RM 23 Anhand der erwarteten Eintrittswahrscheinlichkeiten (ANF-RM 22) und Schadenshöhen gem. der Schadensklassen (ANF-RM 20) SOLLTEN nachvollziehbar Risikoklassen gebildet werden.

4.2.5 Risikobehandlung

Die Risiko-Eigentümer legen für ihre Werte/Risiko-Objekte eine Strategie fest, wie mit den Risiken umzugehen ist (Risikobehandlungsplan).

ANF-RM 24 Der Risikobehandlungsplan MUSS im Rahmen eines formalen Prozesses freizugeben und dessen Umsetzung gesteuert und überwacht werden.

ANF-RM 25 Die Krankenhausleitung MUSS die Kriterien zur Behandlung und Akzeptanz von Risiken auf Basis der Risikoklassen (ANF-RM 23) vorgeben.

ANF-RM 26 Die Strategien zur Risikobehandlung SOLLTEN folgende Optionen² enthalten:

- a. Risikominderung: Auswahl von zusätzlichen Sicherheitsmaßnahmen. Die Auswahl erfolgt sowohl auf Basis der Abwägung des Nutzen-Kosten-Verhältnisses als auch der Sicherstellung der Funktionsfähigkeit (Verfügbarkeit) der kritischen Dienstleistung.
- b. Risikovermeidung: Durch Beendigung einer Geschäftsaktivität, welches dieses Risiko verursacht, jedoch nicht die Funktionsfähigkeit (Verfügbarkeit) der kritischen Dienstleistung in nicht vertretbarem Rahmen beeinflusst.
- c. Risikoakzeptanz: Risiken können akzeptiert werden, sofern die Wahl anderer Risikobehandlungsoptionen unverhältnismäßig ist und mögliche Auswirkungen insbesondere auf die Erbringung der kritischen Versorgungsdienstleistung sowie die Patientensicherheit als vertretbar eingeschätzt werden (Restrisiko). Die Entscheidung hierüber MUSS durch die Geschäftsführung erfolgen.

ANF-RM 27 Es SOLLTE eine Erklärung zur Anwendbarkeit der Sicherheitskontrollen gemäß Anhang A der DIN ISO/IEC 27001 erstellt und fortgeschrieben werden:

- a. Welche Sicherheitskontrollen für den B3S-Anwendungsbereich zutreffen und welche nicht
- b. Rechtfertigung für diese Entscheidungen und ob diese Sicherheitskontrollen implementiert werden oder nicht

ANF-RM 28 Die Freigabe der Erklärung zur Anwendbarkeit sowie die Anerkennung sämtlicher Restrisiken MUSS durch die Geschäftsführung bzw. gemäß den vorgegebenen Risikokompetenzregelungen erfolgen.

² Die Übertragbarkeit oder Verlagerung eines Risikos auf einen Dritten ist im KRITIS-Kontext nicht anwendbar [Diskussion mit BSI notwendig].

4.2.6 Risikokommunikation und -überwachung

Die Risiken müssen in geeigneter Form innerhalb des Krankenhauses kommuniziert und berichtet werden. In jedem Fall müssen die Entscheidungsträger im B3S-Anwendungsbereich in die Kommunikation mit einbezogen werden.

ANF-RM 29 Die Krankenhausleitung MUSS sich in angemessenen Abständen über die Risikosituation berichten lassen:

- a. Ergebnisse der Überwachung
- b. Akzeptierte Restrisiken
- c. Veränderungen an der Risikosituation

ANF-RM 30 Die Risikoberichterstattung MUSS in nachvollziehbarer, aussagefähiger Art und Weise verfasst werden und hat für wesentliche Risiken mindestens halbjährlich und für die sonstigen Risiken mindestens jährlich zu erfolgen.

ANF-RM 31 Die nach verbindlichen Kriterien (z.B. anhand von Risikoklassen nach ANF-RM 23) ermittelten Restrisiken MÜSSEN der Krankenhausleitung bekanntgegeben werden, um ggf. im Einzelfall weitere Maßnahmen umzusetzen.

ANF-RM 32 Die Krankenhausleitung MUSS festlegen, welche Überwachungsmaßnahmen für die definierten Risikoklassen (ANF-RM 23) durchzuführen sind.

ANF-RM 33 In die Risikoberichterstattung MUSS die aktuelle Risikosituation, eine zukunftsorientierte Risikoeinschätzung und bei Bedarf auch Handlungsvorschläge, z.B. zur Risikoreduzierung, aufgenommen werden.

ANF-RM 34 Die Berichterstattung SOLLTE das jeweilige Risiko, die Ursachen, die möglichen Implikationen sowie ggf. bereits getroffene Gegenmaßnahmen umfassen.

ANF-RM 35 Der Risikobericht MUSS durch die Krankenhausleitung nachweislich zur Kenntnis genommen werden.

ANF-RM 36 Bei Änderungen von kritischen Werten (Informationssysteme, Netzwerke, Medizintechnik) MUSS eine Überprüfung der Risikobewertung erfolgen.

4.3 IT-Systemlandschaft in Krankenhäusern nach Kritikalität

Die Bewertung der Kritikalität eines Systems erfolgt zunächst auf Grundlage der Zeitspanne, in der nach Ausfall des Systems noch keine relevante Einschränkung der medizinischen Leistungserbringung zu erwarten ist. Das Krankenhaus muss hierzu über geeignete organisatorische Notfallmaßnahmen verfügen, um Ausfallzeiten kurz-, mittel- oder längerfristig zu überbrücken. Die Erstellung von Ausfallkonzepten ist Teil des Notfallmanagements und soll die Aufrechterhaltung wesentlicher basaler Ablaufverfahren auch ohne IT-Unterstützung durch Prozesswerkzeuge sicherstellen. Die Verantwortung für die Erstellung und regelmäßige Überprüfung entsprechender Notfall-

pläne obliegt den Fachrichtungen und Funktionsstellen des Krankenhauses. Notfallpläne basieren in der Regel auf gestaffelten, technischen, papiergebundenen und organisatorischen Ersatzverfahren sowie alternativen Kommunikationslinien (alternativ zu „IT“). Sie werden durch das Management veranlasst, durch die Fachrichtungen oder Funktionsstellen bei Bedarf aktiviert, durchgeführt und nach Behebung der Störung beendet. Im Rahmen der Notfallkonzepte ist sowohl die Aufrechterhaltung des laufenden Betriebes als auch die Wiederanlaufplanung (z. B. Nachbearbeitung von Dokumentationen) zu berücksichtigen.

- Klasse 1: Ausfall der Systeme kann nur kurzfristig kompensiert werden
- Klasse 2: Ausfall der Systeme kann mittelfristig kompensiert werden
- Klasse 3: Ausfall der Systeme kann längerfristig kompensiert werden

Für diese Systemklassen sollen differenzierte Anforderungen entsprechend der individuellen Kritikalität definiert werden. Die Kritikalität wird hier nach der Zeit bemessen, innerhalb derer ein System nach einer Störung oder einem Ausfall wiederhergestellt sein muss, bevor sich maßgebliche Einschränkungen bis hin zum Ausfall des Versorgungsprozesses für die Behandlung von Patienten ergeben. Hierbei sind im Rahmen der Angemessenheit die Grenzen technischer Maßnahmen (z. B. Ausweichsysteme) zu berücksichtigen. Die Zuordnung der Systeme zu den entsprechenden Klassen obliegt dem Betreiber. In Betriebsmodellen mit zentralen RZ-Strukturen kann ein einheitlich hohes Absicherungsniveau sinnvoll sein, wenn eine Unterscheidung nach Systemklassen organisatorisch und wirtschaftlich aufwendiger wäre.

4.3.1 Systeme der Klasse 1

Die Störung eines Systems der Klasse 1 führt bereits nach kurzer Zeit zu relevanten Mehrbelastungen der Organisationseinheiten, einer Einschränkung der medizinischen Leistungserbringung. Darüber hinaus ist bei einem längeren Ausfall mit einer Beeinträchtigung der kritischen Dienstleistung zu rechnen. Die konkrete Zeitspanne ist im Einzelfall den Gegebenheiten vor Ort angemessen anzupassen. höchstens kurzfristig verzichtbar:

4.3.2 Systeme der Klasse 2

Mittelfristig verzichtbar

Systeme, deren Störung über einen mittleren Zeitraum durch die Organisation (Notfallkonzepte) beherrscht werden können, ohne dass eine relevante Einschränkung der medizinischen Leistungserbringung zu befürchten ist, werden als Systeme der Klasse 2 bezeichnet.

4.3.3 Systeme der Klasse 3

Längerfristig verzichtbar

Die Einordnung als System der Klasse 3 erfolgt für diejenigen Systeme im Krankenhaus, für die längere Störungszeiten durch die Organisation ohne relevante Einschränkung der medizinischen Leistungserbringung beherrschbar sind.

5 Allgemeine Hinweise zur Definition des Geltungsbereichs

Der Definition und Abgrenzung des Geltungs- bzw. Anwendungsbereichs eines B3S kommt entscheidende Bedeutung bei der Umsetzung der Maßnahmen zur Sicherstellung der Informationssicherheit zu. Der Geltungsbereich ist eindeutig zu benennen, insbesondere wenn nur ein Teil der vorgehaltenen Systeme in die Betrachtungen zum B3S einfließen. In heterogenen Strukturen, wie sie im Krankenhaus-Umfeld alltäglich sind, kann dies regelmäßig der Fall sein. Im Kern steht die (voll-)stationäre Versorgung von Patienten im Fokus, sie ist als kritische Versorgungsdienstleistung (kDL) Grundlage der Einschätzung als kritische Infrastruktur.

Es ist zu dokumentieren und zu begründen, welche Bereiche, Prozesse oder Systeme nicht unmittelbare Berücksichtigung finden. Aufgrund der Komplexität der Anforderungen kann auch ein gestuftes Realisierungskonzept infrage kommen, welches den Geltungsbereich zunächst abschließend beschreibt, für die Umsetzung jedoch eine iterative, einer Priorisierung folgende Vorgehensweise beschreibt.

Das vorliegende Dokument beschreibt insbesondere ein Vorgehensmodell zur Identifikation für die kDL kritischer Bereiche und Prozesse der Krankenhäuser. Der B3S definiert dabei explizit keine allgemeingültigen Festlegungen zum Geltungsbereich, da sich diese einrichtungsabhängig unterscheiden können. Die Prüfung der sachgerechten Definition des Geltungsbereichs hat einrichtungsindividuell im Rahmen der Prüfung / Auditierung gemäß § 8a BSIG zu erfolgen.

Zur Unterstützung bei der Abgrenzung des kritischen Geltungsbereiches enthält das Dokument abstrakte Beschreibungen der für die stationäre Versorgung wichtigen Funktionsbereiche, Prozesse und technischen Unterstützungsprozesse eines Krankenhauses in generalisierter Form, sowie Fallbeispiele zum besseren Verständnis der Bewertungsanforderungen im angestrebten Vorgehensmodell.

5.1 Branchenspezifischer Geltungsbereich

Der vorliegende B3S adressiert insbesondere diejenigen Krankenhäuser, die gemäß BSI-KritisV als kritische Infrastruktur gelten. Nach der Rechtsverordnung kann der Geltungsbereich eines B3S die kritische Dienstleistung, Teile davon (z.B. einzelne Prozessschritte), eine KRITIS-Branche, einen Teil einer Branche oder für die kritische Dienstleistung relevante (Typen von) „Einrichtungen, Anlagen oder Teile[n] davon“ umfassen. Daher ist zunächst der jeweils individuelle Geltungsbereich (im Folgenden auch „B3S-Anwendungsbereich“ genannt) abzugrenzen. Dabei kann es sich um einzelne Betriebsstätten, Krankenhausstandorte oder auch mehrere Standorte (z. B. Trägerverbände) handeln. Auch innerhalb der Standorte bzw. Betriebsstätten kann der B3S-Anwendungsbereich auf diejenigen Strukturelemente beschränkt werden, die für die Erbringung der kritischen Dienstleistung (stationäre medizinische Versorgung) notwendig sind. Aufgrund der heterogenen Organisationsformen der identifizierten Einrichtungen wird zur Beschreibung der inneren Struktur auf allgemeingültige Funktionsbereiche und Funktionsstellen Bezug genommen (nach DIN 13080).

Siehe ISO/IEC 27001, Abschnitt 4.3

Liste rechtlicher, vertraglicher und sonstiger Anforderungen

Als Verfahrensvorgabe wird ein risikobasierter Ansatz für den Betreiber vorgesehen, der den Fokus auf diejenigen Bereiche, Prozesse und Systeme legt, welche für die Erbringung der kritischen Dienstleistung notwendig sind.

Für den B3S-Anwendungsbereich der Branche „Medizinische Versorgung“ wurden die folgenden Annahmen getroffen:

- Abgrenzung des B3S-Anwendungsbereichs auf Krankenhäuser nach § 107 Abs. 1 SGB V, die nach § 108 SGB V zugelassen sind
- Strukturierung der Funktionsbereiche und -stellen nach DIN 13080:2016-06.

Der Betreiber hat die für die Erbringung der kritischen Versorgungsdienstleistung notwendigen Informationen und sonstigen Werte zu erheben. Hieraus ergeben sich die Abhängigkeiten informationsverarbeitender Einrichtungen und Systeme, die ebenfalls in direktem Zusammenhang mit der Funktionsfähigkeit der kritischen Infrastruktur zur Erbringungen der kritischen Versorgungsdienstleistung stehen.

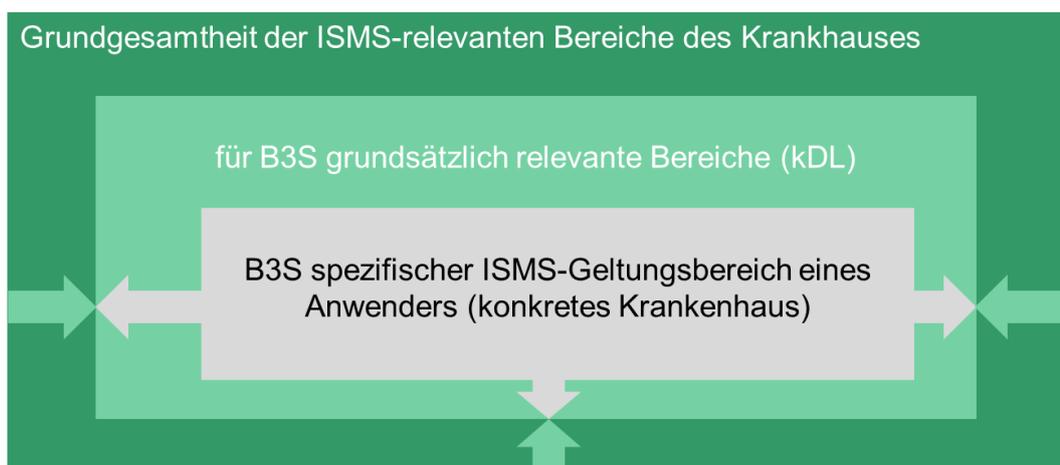
Bestandsaufnahme und Analyse aller notwendigen Informationen, Werte und Prozesse, die für den sicheren Betrieb der KDL notwendig sind

Der B3S zielt vorrangig auf die Sicherstellung der Verfügbarkeit kritischer Informationen der medizinischen Versorgung ab.

Der Schutz der Informationen erstreckt sich daher sowohl auf die für den Betrieb der kritischen Dienstleistung benötigten Informationen, die innerhalb des Krankenhauses als auch außerhalb des Krankenhauses erhoben, verarbeitet, übertragen oder archiviert werden, solange diese dem B3S-Anwendungsbereich zugeordnet werden können. Dies schließt eine Datenverarbeitung im Auftrag ausdrücklich mit ein.

Informationen sind dabei über ihren gesamten Lebenszyklus zu betrachten: von der Erstellung, Verarbeitung, Speicherung, Übermittlung bis zur Löschung. Besonderes Augenmerk gilt dabei eventuellen Ausschlüssen aus dem B3S-Anwendungsbereich, diese sind hinreichend zu beschreiben.

Der für die Umsetzung des B3S in einem konkreten Krankenhaus spezifische Geltungsbereich leitet sich ab aus den grundsätzlich für einen B3S infrage kommenden Bereichen der kritischen Dienstleistung. Diese wiederum sind in der Regel ebenfalls ein Teilbereich aller im Krankenhaus bestehenden Bereiche:



Alle im B3S-Anwendungsbereich vorhandenen Werte und Prozesse die explizit nicht (auch temporär) im ISMS berücksichtigt werden sollen, sind genau zu benennen. Die

Gründe für einen Ausschluss müssen nachvollziehbar dokumentiert werden, insbesondere darf durch deren Ausschluss das Sicherheitsniveau der kDL nicht abgesenkt werden.

5.2 Ergänzende Regelungen zum Geltungsbereich

Da die stationäre Versorgung sämtliche Prozesse und Aufgaben, die der Erhaltung und Wiederherstellung der Gesundheit des Patienten dienen, umfasst, berücksichtigt der vorliegende B3S die Bereiche Labore („Klinisches Labor“) und Arzneimittel („Krankenhausapotheke“), soweit diese den primären Aufgaben des Krankenhauses in Erfüllung der kritischen Dienstleistung „Medizinische Versorgung“ zuzurechnen sind. Die in den entsprechenden Branchen „Labore“ und „Arzneimittel“ separat zu definierenden Anforderungen entfalten für die Branche „Medizinische Versorgung“ keine Wirkung. Für den Krankenhausbereich sollten auch die Prozesse und Systeme in den zentralen Notfallambulanzen und -aufnahmen in die Überlegungen, hinsichtlich der Umsetzung des B3S, mit einbezogen werden, da ein Teil der Patienten über diesen Zugang in die stationäre Versorgung aufgenommen wird.

5.2.1 Übersicht der Kernprozesse und Funktionszuordnung innerhalb des Geltungsbereichs

Im Folgenden werden die Prozessschritte dargestellt, die üblicherweise bei der stationären Behandlung von Patienten im Krankenhaus durchlaufen werden. Im weiteren Verlauf des Dokumentes werden die für die jeweiligen Prozessschritt in der Regel im Krankenhaus vorgehaltenen Informationssysteme beschrieben.

Die identifizierten Prozesse und Systeme werden hinsichtlich ihrer Kritikalität für die Erbringung der kDL bewertet, dabei wird insbesondere auf die Sicherstellung der stationäre medizinische Versorgung unter Berücksichtigung der Aspekte PATIENTENSICHERHEIT und BEHANDLUNGSEFFEKTIVITÄT fokussiert. Im Ergebnis werden diejenigen Funktionsbereiche und Funktionsstellen identifiziert, die von wesentlicher Relevanz für die Aufgabenerfüllung im Kontext stationärer Versorgung sind.

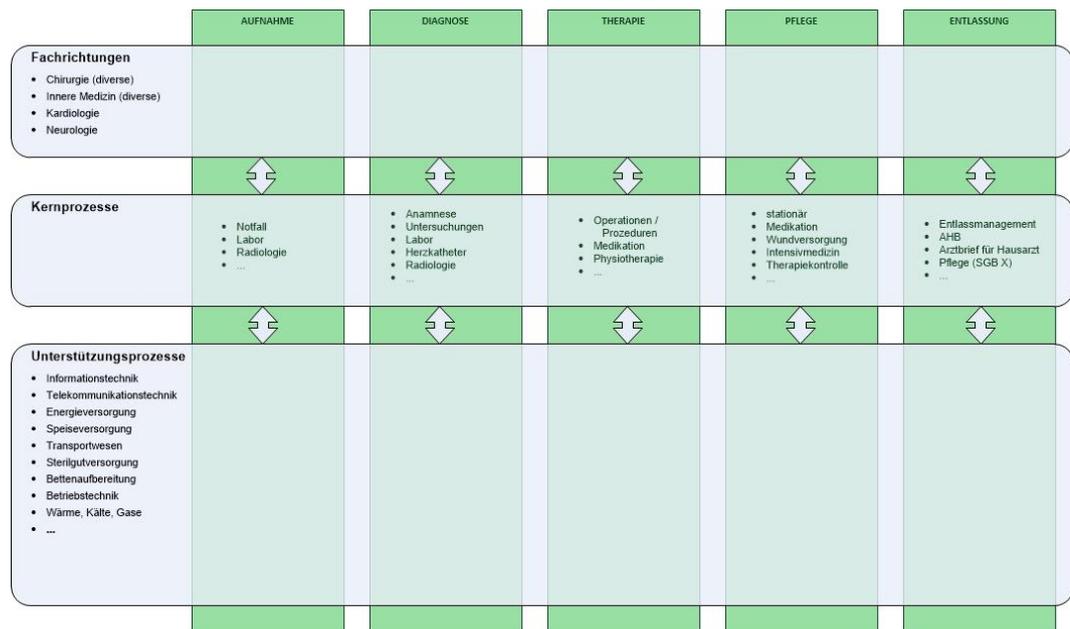


Abbildung 3: Prozessschritte der stationären medizinischen Versorgung

Bei der Betrachtung der für die stationäre Versorgung kritischen Systeme und Prozesse können die Funktionsbereiche und Funktionsstellen der DIN 13080 als „Raster“ zur Strukturierung herangezogen werden, um ein einheitliches Vorgehensmodell sicherzustellen.

Im Sinne einer prinzipienorientierten Vorgehensweise soll die folgende Einteilung daher als „Blaupause“ für die Erhebung kritischer Prozesse dienen, hierauf aufbauend kann eine „Prozesslandkarte“ als Unterstützung für die Definition des Geltungsbereichs genutzt werden.

5.2.1.1 Vorbereitung/Aufnahme

Abhängig davon, ob die Notwendigkeit stationärer Krankenhausbehandlung aus einer Notfallsituation heraus oder aufgrund einer elektiven (geplanten) Maßnahme erfolgt, können bereits im Vorfeld der Aufnahme Versorgungsleistungen anfallen (z. B. im Rahmen vorstationärer Untersuchungen, radiologische Befunderhebung etc.). Die Übernahme von Informationen im Rahmen dieser Versorgungsleistungen, aber auch aus künftig flächendeckend verfügbaren Lösungen für Patientenakten stellt aufgrund häufig fehlender standardisierter Schnittstellen eine besondere Herausforderung dar. Dies ist bei der Abgrenzung des B3S-Anwendungsbereichs zu berücksichtigen. Diese können im Einzelfall vom Einlesen optischer Datenträger (CD, DVD), der elektronischen Belegübermittlung bis hin zur perspektivisch erwarteten Kommunikation von Leistungserbringern über die Telematikinfrastruktur und deren Komponenten reichen.

Elektive Aufnahmen stellen dabei heute den überwiegenden Anteil stationärer Krankenhausbehandlung dar, über die Notaufnahme kommen durchschnittlich 45% der

Patienten in die stationäre Versorgung³.

Bei elektiven Aufnahmen beginnt der Versorgungsprozess üblicherweise mit dem Erreichen der Pflegestation, die für den Patientenaufenthalt vorgesehen ist. Im Vorfeld des stationären Aufenthalts erfolgen die administrativen Prozesse der „Aufnahme“ (Datenerhebung auf Basis der elektronischen Gesundheitskarte, Abschluss des Behandlungsvertrags, etc.) in der Regel bereits über die Organisationseinheit „Aufnahme“ des Krankenhauses. Bei Überleitungen aus der „Notfallaufnahme“ wird der Behandlungsvertrag i.d.R. nachträglich erstellt.

Administrative Prozesse der Aufnahme erfüllen überwiegend organisatorische oder rechtliche Anforderungen (Behandlungsvertrag, Leistungsabrechnung), die mit Blick auf die medizinische Patientenversorgung zunächst keine kritischen Prozesse darstellen.

Werden jedoch in diesem Schritt für die Versorgung wichtige Informationen erhoben, die zwingend für die nachgelagerten Behandlungen oder die Patientenversorgung benötigt werden, sind die diesbezüglichen Aktivitäten der Aufnahme dem Geltungsbereich der kritischen Dienstleistung zuzuordnen. Hierzu können beispielsweise die Erfassung des MRSA-Status, von Arzneimittelunverträglichkeiten oder das Vorhandensein anderer nach Infektionsschutzgesetz relevanter Informationen zählen.

Zu den wichtigen Informationen zählen beispielsweise die eindeutige Identifikation des Patienten („Fallnummer“) oder Angaben zu Allergien oder sonstige lebenswichtige Hinweise („CAVE-Hinweise“, Herzschrittmacher etc.).

5.2.1.2 Diagnostik

Die Diagnostik liefert die Grundlage für alle weiteren behandlungsrelevanten Schritte der Patientenversorgung. Sie stellt den ersten von drei Primärbereichen stationärer Patientenversorgung dar. Dabei steht die Diagnostik am Anfang des stationären Versorgungsprozesses und wird insbesondere in der Notfallaufnahme, aber auch durch den allgemeinen Arztendienst von medizinischen Fachrichtungen wie Chirurgie, Kardiologie, Innere Medizin, Orthopädie, Gynäkologie, Geburtshilfe, Pädiatrie u.v.m. erbracht. Ergänzt werden diese Leistungen um die Funktionsdiagnostik wie Endoskopie, Labormedizin, bildgebende Diagnostik und interventionelle radiologische Verfahren, Nuklearmedizin und Pathologie. Häufig werden in den Funktionsstellen hochspezialisierte oder hochtechnisierte diagnostische Einheiten vorgehalten. Auch der Prozess der Anamnese (einschließlich Medikamentenanamnese) fällt in den Bereich der Diagnostik.

Die Dienstleistung „Medizinische Versorgung“ ist in ihren Prozessschritten „Diagnose“ und „Therapie“ abhängig vom Einsatz labormedizinischer Verfahren und Geräte, vom Einsatz von Diagnose- und Untersuchungsgeräten (z.B. Blutdruck- und Blutgasmessgeräte, CTs), von der Verfügbarkeit von Medizinprodukten, die Verbrauchsgüter sind

³ Quelle: Angaben des Statistischen Bundesamtes (destatis)

(z.B. Verbandsmaterialien, Spritzen, Rollstühlen, Brillen), Arzneimitteln, von der Verfügbarkeit von Organen, Blut- und Plasmaderivaten, sowie vom Einsatz von Operationstechnik (z.B. OP-Tische, Endoskope, Knochenfräsen, Bohrer). Stehen medizintechnische Systeme, die für diagnostische Zwecke genutzt werden, nicht zur Verfügung, kann die Erbringung der eigentlichen Versorgungsleistung gestört oder behindert sein. Dabei ist zu berücksichtigen, dass medizintechnische Anlagen bereits heute hohen Auflagen durch das Medizinproduktegesetz (MPG) sowie ergänzenden Verordnungen (u.a. Medizinproduktebetriebsverordnung) unterliegen, um deren Funktionsfähigkeit zu gewährleisten.

5.2.1.3 Therapie

Die Therapie repräsentiert nach der Diagnostik den zweiten Primärbereich des Krankenhauses. Die Behandlung von Krankheiten und Linderung von Beschwerden ist Kernaufgabe der Krankenhäuser. Diagnose und Therapie erfolgen dabei häufig unter ähnlichen technischen Rahmenbedingungen, einzelne diagnostische Verfahren sind bereits für therapeutische Interventionen – teilweise während der Diagnostik – ausgelegt (Beispiel: Herzkatheters bzw. Angiografie). In diesen Fällen finden sich fließende Übergänge von Diagnostik zu Therapie.

Typische therapeutische Einheiten sind: Arztdienst, Funktionsdiagnostik, Endoskopie, Angiografie, interventionelle radiologische Verfahren, Nuklearmedizin/Strahlentherapie, Operationen und Eingriffe sowie unterstützende Behandlungen, z.B. Physiotherapie.

Stehen medizintechnische Anlagen oder notwendige Versorgungstechnik nicht zur Verfügung, wären Therapie und unterstützende Pflege möglicherweise eingeschränkt oder behindert. Die Therapie als Kern der stationären Patientenversorgung würde unter Umständen massiv eingeschränkt, wenn z.B. die Bereitstellung relevanter Therapiestrukturen (OP-Saal, Sterilgutversorgung, Klima & Wärme, Desinfektion u.v.m.) nicht sichergestellt werden kann. Auch für therapeutische Verfahren und Systeme gilt, dass medizintechnische Anlagen hohen Auflagen durch das Medizinproduktegesetz (MPG) und die zugehörigen Verordnungen unterliegen.

5.2.1.4 Unterbringung und Pflege

Während der medizinischen Behandlung stellt die Pflege der Patientinnen und Patienten im Krankenhaus deren Versorgung sicher und bildet damit den dritten Primärbereich der Patientenversorgung. Von der täglichen Stationspflege, der Umsetzung diagnostischer Kontrollmaßnahmen (Point of Care Testing, POCT) über die Sicherstellung medikamentöser Therapien bis hin zu komplexen pflegerischen Situationen im intensivmedizinischen Bereich hängt der Behandlungserfolg auch von der Verfügbarkeit der Pflege ab.

Im Rahmen der Pflegeanamnese werden bereits zu Beginn der Versorgung Informationen über den Pflegestatus des Patienten erhoben, dies erfolgt häufig werkzeuggestützt bzw. im Rahmen definierter Pflegeprozesse. Im weiteren Verlauf der Behand-

lung kann die Verfügbarkeit relevanter Informationen aus Sicht der Pflege wesentliche Unterstützungsleistungen erbringen. Stehen pflegerelevante Informationen nicht oder nicht rechtzeitig zur Verfügung, kann dies negative Auswirkungen auf die Behandlungsqualität haben, im intensivmedizinischen Bereich bestehen ggf. zeitkritische Anforderungen an die Verfügbarkeit entsprechender Informationen eines Patientendatenmanagementsystem (PDMS).

5.2.1.5 Entlassung

Am Ende des stationären Versorgungsprozesses steht die Entlassung des Patienten aus dem Krankenhaus.

Der Entlassungsprozess ist zur Erbringung der kritischen Dienstleistung nicht relevant

Die gesetzlichen Anforderungen an ein Entlassmanagement sind in § 39 Abs.1a SGB V geregelt und umfassen neben dem Recht des Versicherten auf einen sog. Entlassbrief auch den Auftrag, den Informationsaustausch mit den an der Anschlussversorgung des Patienten beteiligten Leistungserbringern sicherzustellen. Der Entlassbrief ist derzeit nicht in elektronischer Form vorgeschrieben. Der Versicherte hat gegenüber der zuständigen Krankenkasse ein Recht auf Unterstützung des Entlassmanagements, dabei kann das Krankenhaus in diese Unterstützungsleistungen eingebunden sein. Ab dem 1.1.2019 können Unterstützungsleistungen der Krankenkasse für den Patienten im Rahmen der Datenübermittlung nach § 301 Abs. 1 SGB V angefordert werden.

Stehen für das Entlassmanagement benötigte Informationen nicht oder nicht rechtzeitig zur Verfügung, kann der Versorgungsprozess (z.B. bei Patienten mit erhöhtem Pflegegrad) u.U. beeinträchtigt sein, der Patient könnte ggf. nicht entlassen werden.

5.2.2 Technische Unterstützungsprozesse in der stationären Versorgung

Die folgende Übersicht dient dem Verständnis der üblichen - oder häufig auftretenden - Organisationsformen der technischen Unterstützungsprozesse im Krankenhaus. Dabei bestehen in den Krankenhäusern höchst unterschiedliche Zuordnungen der Verantwortungsbereiche. Es finden sich daher Verantwortlichkeiten (z.B. Diensttelefonie) unter Umständen in mehreren Organisationseinheiten. Die tatsächliche Organisationsstruktur eines Krankenhauses lässt sich nur durch direkte Erhebung ermitteln. Die technischen Unterstützungsprozesse bilden in der Regel eine wesentliche Voraussetzung für die kritische Dienstleistung (kDL) „Medizinische Versorgung“. Jedoch sind nicht alle betreuten oder bereitgestellten Einzeltechnologien zwingend Voraussetzung für die Verfügbarkeit der medizinischen Versorgung. Auch können Zuständigkeiten für Systeme und Prozesse im Einzelfall anderen oder mehreren Bereichen zugeordnet werden, eine disjunkte Betrachtung ist aufgrund der zunehmenden Durchdringung mit Informationstechnologie (z. B. in der Medizintechnik, aber auch Versorgungstechnik) in vielen Fällen kaum mehr möglich.

5.2.2.1 Informationstechnik (IT)

Informationstechnische Systeme bilden die Basis fast aller technischen Unterstützungsprozesse im Krankenhaus. Dabei steht die Bereitstellung von Infrastruktur für

den Einsatz informationstechnischer Systeme (Hard- und Software) im Mittelpunkt. In der klassischen Aufteilung und Wahrnehmung zeichnet die IT damit verantwortlich für Datennetzwerke, PC-Arbeitsplätze, Server & Storage-Systeme, Sicherheitseinrichtungen wie Firewall und Malware-Schutz, Anwendungsverfahren (Software), technische und logische Integration von Lösungen und Modalitäten (Medizintechnik) über Schnittstellen und Datennetze. Infolge der stetig zunehmenden Digitalisierung verschmelzen früher getrennte Zuständigkeitsbereiche heute zunehmend.. Kommunikationstechnik basiert inzwischen immer häufiger auf IP-Technologie, Gebäudeleittechnik wird digitalisiert, Daten der Videoüberwachung werden über IP-Datennetze transportiert, dezentrale Untersuchungsgeräte nehmen ein immer breiteres Feld ein (z. B. Point-of-Care Testing). „Klassische IT“ ist daher heute kaum noch eindeutig abzugrenzen und führt zu diversen Mischformen in der Krankenhaus-Organisation. Zur Vermeidung von unklaren Zuständigkeiten sollte eine regelmäßige Überprüfung und ggf. Anpassung der organisatorischen Verantwortlichkeiten erfolgen. Historisch bedingt zeichnet die IT in der Regel nicht verantwortlich für medizintechnische Anlagen (zuständig: Medizintechnik), Schnittstellen ergeben sich hier aber durch physikalische und logische Integration der Medizinprodukte in die bestehende IT-Infrastruktur. Hierzu zählen insbesondere Fernwartungsverfahren für allgemeine technische Anlagen (Versorgungstechnik, Medizintechnik) sowie die Bereitstellung typischer IT-Systeme wie Datennetze oder Anwendungslösungen.

Mindestens die folgenden Aufgaben und Systeme MÜSSEN für die Sicherstellung der kDL in die Risikobetrachtung der Informationstechnik aufgenommen werden:

- Arbeitsplatzsysteme, z.B. PC-Arbeitsplätze, Notebooks, Tablets, Smartphones (über deren Lebenszyklus)
- Serversysteme (Anwendungen, Datenbanken, Basisdienste, z. B. Verzeichnisdienste, DNS, DHCP)
- Storage-Systeme (SAN, NAS)
- IP-Netzwerke (WAN, LAN, WLAN, VLAN)
- Virtualisierung (Anwendungen, Server, Clients, Netzwerk)
- Softwaresysteme (Lebenszyklus von Betriebs- und Anwendersystemen)
- Peripherie-Geräte (Monitore, Befundarbeitsplätze, Drucker, Scanner, Zubehör)
- Sicherheitsgateways (Firewall, DMZ, VPN)
- Sicherheitskomponenten (Malware-Schutz, Spamabwehr, Überwachungssysteme)
- Rechenzentrumsbetrieb
- USV-Betrieb
- Backup und Wiederherstellung
- Fernwartungsbetrieb
- IP-basierte Aufgabenfelder
 - Telekommunikation
 - Videoüberwachung
 - Netzbereitstellung für Versorgungstechnik (Anlagentechnik wie Fahrstuhl-anlagen, Zugangssysteme, Schrankensysteme, GLT)
 - Netzbereitstellung (i.d.R. Kopplung) für Medizintechnik (physikalische und logische Integration von medizintechnischen Anlagen)

5.2.2.2 Kommunikationstechnik (KT)

Die Kommunikationstechnik umfasst die Bereitstellung von Kommunikationsleistungen im Krankenhaus. Dabei ist zwischen Rufsystemen, der Diensttelefonie und der Patiententelefonie zu unterscheiden. Die Kommunikationstechnik liefert darüber hinaus i.d.R. die Grundlagendienste für die Festnetztelefonie, die Patiententelefonanlage (sofern noch vorhanden) sowie den Mobilfunkbereich und die Fax-Technik. Zusätzliche Aufgaben können sich z. B. aus dem gemeinsamen Betrieb von Patiententelefonie und Patientenfernsehen (TV) in einem gemeinsamen Leistungsangebot ergeben. In bestimmten Fällen können sich Zuständigkeitsbereiche auch überschneiden und damit auch mehrere „Betreiber“ infrage kommen können. Zum Aufgabengebiet der Kommunikationstechnik können zudem Satelliten-Empfangsanlagen oder Kabeleinspeisungen gehören. Zudem können sich bedingt durch den technischen Fortschritt Änderungen in bestehenden Verantwortlichkeiten ergeben, ein Beispiel hierfür ist die zu beobachtende Ablösung bisheriger Fax-Technologie durch Multi-Funktionsgeräte (All-in-One). Telekommunikationstechnik hat heute häufig umfangreiche Schnittstellen zur Informationstechnik, klassische TK-Anlagen werden im Kontext der Digitalisierung (All-IP-Umstellung) zunehmend verdrängt. „Voice over IP (VoIP)“ dominiert heute die Telefonesysteme, IP-Netze stellen immer häufiger die technische Grundlage dieser Leistungsangebote dar. Moderne Alarmierungssysteme basieren auf einer zentralen Alarmserver-Architektur. Diese setzen definierte Alarmierungsketten unter Rückgriff auf unterschiedliche Kommunikationsmittel um.

Organisatorisch ist die Kommunikationstechnik selten eine eigenständige Einheit. Häufig ist sie der Versorgungstechnik zugeordnet, die sich im Gegensatz zur technischen Entwicklung im Bereich der Telekommunikation eher an klassischen Anlagentechniken orientiert. Bedingt durch einen höheren Digitalisierungsgrad hat die Kommunikationstechnik einen erheblichen Vorsprung (VoIP seit Ende der 90er) gegenüber der Versorgungstechnik, die heute eher auf betriebliche technische Anlagen (Energieversorgung, Gas, Wasser, Sanitär, Transportanlagen, Wärme, Kälte) fokussiert. In vielen Fällen ist die Kommunikationstechnik inzwischen Bestandteil der Informationstechnik.

Mindestens die folgenden Aufgaben und Systeme MÜSSEN für die Sicherstellung der kritischen Dienstleistung in die Risikobetrachtung aufgenommen werden:

- Rufsysteme, Diensttelefonie/Festnetzapparate (Endgeräte, Schwerpunkt VoIP-Telefone mit Netzversorgung oder Energieversorgung PoE (Power over Ethernet), DECT/GSM, TK-Anlagenserver)
- Diensttelefonie/Mobil (Endgeräte, z. B. Mobiltelefonie / Smartphones)
- Fax-Betrieb (ggf. Faxserver, klassische Fax-Anlagen, Multifunktionsgeräte)
- Wechselsprechtechnik (Redundanz-Konzept für Störfälle, z. B. Mobiltelefonie, Zugangslösungen, z. B. Klingel- und Sprechanlagen für geschlossene Bereiche)

5.2.2.3 Medizintechnik (MT)

Medizintechnische Systeme sind für die Erbringung der kDL häufig unerlässlich und unterstützen den Diagnose- und Therapieprozess wesentlich. Sie bergen infolge der

häufig direkten Einwirkung auf Patienten jedoch auch ein besonderes Gefährdungspotenzial. Daher gelten hier besondere rechtliche Anforderungen, die beispielsweise im Medizinproduktegesetz bzw. einer Reihe von Verordnungen geregelt sind. Neben der reinen „Untersuchungstechnik“ werden medizintechnische Systeme heute immer häufiger durch informationstechnische Komponenten ergänzt und untereinander vernetzt. Die Systeme der Medizintechnik sind dabei in der Regel als geschlossene (gekapselte) Systeme konzipiert, die nur unter bestimmten Bedingungen mit anderen informationstechnischen Komponenten gekoppelt werden dürfen. Insbesondere bei der Integration von Medizinprodukten in IT-Netzwerke bestehen normative Anforderungen an einen Risikomanagementprozess (DIN EN 80001-1:2011). Medizintechnik-Anlagen entsprechen mit Blick auf Informationssicherheit häufig noch nicht dem aktuellen Stand der Technik aus IT-Sicht. Regulatorische Anforderungen aus dem Bereich der Medizinprodukte sind vielfach nicht mit der gelebten Praxis aus den Bereichen der Informationstechnik in Einklang zu bringen, (z. B. Freigabe von Software-Updates durch den Hersteller eines Medizinproduktes). Häufig kommen eingebettete Betriebssysteme („embedded systems“) zur Anwendung, die weitgehend gekapselt betrieben werden. Antiviren-Programme gehören i.d.R. nicht zum Standard medizintechnischer Anlagen. Demgegenüber finden sich auch eine Reihe von Systemen aus dem medizintechniknahen Bereich, die nicht den Regelungen des Medizinprodukterechts unterfallen, jedoch für Dokumentationszwecke, Qualitätssicherung etc. notwendig werden (z. B. PACS).

Medizintechnische Anlagen können sowohl einzelne Geräte sein, als auch Anlagenkonglomerate, wie es zum Beispiel ein CT oder ein MRT darstellt. CT-Anlagen bestehen aus technischen Betriebskomponenten, dem Untersuchungsgerät selbst (inkl. der Gantry (Röhre)) sowie Bedien- und Befundkonsolen für die Datenverarbeitung. Auf Grund der hohen gesetzlichen Anforderungen werden medizintechnische Anlagen i.d.R. über Serviceverträge durch den jeweiligen Hersteller instandgehalten. Dabei kommt der Präventivwartung (Fernwartung) eine besondere Bedeutung zu.

Auch nicht vernetzte Medizinprodukte müssen bei der Risikoanalyse berücksichtigt werden, da auch diese Systeme grundsätzlich beeinträchtigt werden können. In der Regel bestehen hier andere Risiken (Infektion mit Schadsoftware z. B. über USB anstelle einer Infektion über das Netzwerk) und auch die zur Absicherung zu treffenden Maßnahmen unterscheiden sich, für den Versorgungsprozess sind sie in vielen Fällen jedoch notwendig und müssen daher entsprechend betrachtet werden.

Die Nutzung von telemedizinischen Systemen sowie Telemetrie-Systemen an der Schnittstelle zwischen Medizintechnik und Informationstechnik nimmt gegenwärtig an Bedeutung stark zu, über Alarmierungsmechanismen wirken diese bis in den Bereich der Kommunikationstechnik. Sie erhöhen die Freiheitsgrade der Patientenversorgung und können in Verbindung mit Alarmsystemen den optimalen Personaleinsatz unterstützen. Alarmierungssysteme werden sowohl in der intensivmedizinischen Überwachung als auch bspw. in psychiatrischen Einrichtungen zur Notfallalarmierung in Bedrohungssituationen eingesetzt.

An die Versorgung von Patienten im intensivmedizinischen Bereich werden besonde-

ren Anforderungen insbesondere hinsichtlich der Verfügbarkeit und Integrität der für die medizinische Versorgung notwendigen Informationen gestellt. Bei dem verstärkten Einsatz von Patientendatenmanagementsystemen (PDMS) im intensivmedizinischen Bereich übernehmen Systeme der Medizintechnik und Informationstechnik gemeinsam Verantwortung für die Versorgungsdienstleistung, ein Ausfall könnte hier zu einem sofortigen Wegfall von Kapazitäten führen, was Auswirkungen auf die Versorgung haben kann.

Mindestens die folgenden Aufgaben und Systeme MÜSSEN für die Sicherstellung der kritischen Dienstleistung in die Risikobetrachtung aufgenommen werden:

- Patientendatenmanagementsystemen (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 Alarmerungssysteme (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.)

Hinweis: Im Rahmen des B3S werden die auf ein konkretes Medizinprodukt einwirkenden IT-Risiken aufgrund seiner Vernetzung erhoben und bewertet. Die gerätespezifischen Risiken werden durch die zuständige Medizintechnik-Organisation, auf Basis der Medizinprodukteverordnung verantwortet.

5.2.2.4 Versorgungstechnik (VT)

Bei der Aufrechterhaltung der kDL kommt auch der Versorgungstechnik (auch: Krankenhaus-technik, Haustechnik, technische Betriebsorganisation, Gebäudeschutz o.ä.) eine wesentliche Bedeutung zu. Hierzu zählen insbesondere Basisinfrastruktur-Dienste, die in einer komplexen technischen Gebäudestruktur, wie einem Krankenhaus, von Bedeutung sind. Versorgungstechnische Systeme sind für die Aufrechterhaltung eines geregelten Krankenhausbetriebs unerlässlich und stellen Grundbedürfnisse der Organisation und der Patienten / Mitarbeiter sicher. Die Versorgungstechnik stellt den Betrieb von Gebäuden, Ver- und Entsorgungseinrichtungen, technischen Anlagen und sämtlichen benötigten Servicediensten zur Aufrechterhaltung des laufenden Betriebs sicher. Ohne Bereitstellung bestimmter Leistungen der Versorgungstechnik ist ein Krankenhausbetrieb nicht aufrecht zu erhalten. Durch die Vielzahl möglicher Organisationsformen in Krankenhäusern kann die Versorgungstechnik auch für Anlagen, wie die Sterilgut-Aufbereitung verantwortlich zeichnen. Für den Geltungsbereich des B3S muss das (vorhandene) übergeordnete und übergreifende Business-Continuity-Management (BCM) der Organisation beachtet und Maßnahmen zum Schutz der

Versorgungstechnik - soweit diese sich aus dem B3S ergeben - in das übergeordnete BCM integriert werden.

Mindestens die folgenden Aufgaben und Systeme MÜSSEN für die Sicherstellung der kritischen Dienstleistung in die Risikobetrachtung aufgenommen werden:

- Energieversorgung, Elektroversorgung (Netzversorgung (Einspeisung), Ersatzversorgung, Notstromdiesel)
- Klimatisierung/Kühlung (z.B. OPs, technische Anlagen)
- Videoüberwachung (Schnittstelle: IT)
- Digitale Zugangs- und Schließsysteme
- Zufahrts- und Schrankensysteme
- Gebäudeleittechnik, Gebäudeautomatisierungstechnik

Die folgenden Aufgaben und Systeme sind in aller Regel bereits in einem übergeordneten BCM-System aufgenommen und können ggf. im Rahmen der Risikobetrachtung zusätzlich aufgenommen werden:

- Wasserversorgung (Frisch- und Abwasser von hoher Bedeutung für Sterilprozesse, Hygiene und Entsorgung)
- sanitäre Anlagen
- Wärme/Heizung (z.B. Patienten- und Untersuchungsräume)
- Lichttechnische Systeme
- Gase (u.a. Beatmung, MRT u.ä.)
- Transportanlagen (primär Fahrstuhl-Anlagen)
- Versorgung und Entsorgung
- Bau und Instandhaltung

5.2.3 Kritische branchenspezifische Anwendungssysteme

HL7
Standard zum Austausch von Gesundheitsdaten zwischen Informationssystemen.

DICOM
Offener Standard zur Speicherung und zum Austausch von medizinischen Bilddaten.

IHE
Offener, prozessbasierter Schnittstellenstandard der die Nutzung von SSt wie HL7 oder DICOM im Rahmen definierter Prozesse vorgibt. Gewinnt an Bedeutung.

Neben Standardsoftware und -technik wie Fileserver, E-Mail-System und Software zur Bürokommunikation werden in Krankenhäusern BRANCHENSPEZIFISCHE SYSTEME eingesetzt, die in der Regel über die Schnittstellen HL7 und DICOM (eventuell als Bestandteil einer IHE-Struktur) kommunizieren. Bei der Risikoklassifikation und Gefährdungsanalyse ist es daher wichtig, nicht einzelne Hardware- und Software-Komponenten zu betrachten, sondern die für die KDL relevanten Informationssysteme, also einen für die medizinische Versorgung prozessrelevanten Informationsverbund aus Hardware, Software und menschlicher Interaktion insgesamt. Nachfolgend werden die i.d.R. für die medizinische Versorgung wichtigen Hauptinformationssysteme im Krankenhausbereich aufgeführt, sowie die branchenspezifische Gefährdungslage für diese Hauptinformationssysteme im Überblick dargestellt. Über diese allgemein im Krankenhauskontext eingesetzten Informationssysteme hinaus sind je nach Ausprägung des vom Betreiber ermittelten Geltungsbereiches für den B3S weitere, zur Erbringung der medizinischen Versorgung wichtigen Informationssysteme zu identifizieren und in Bezug auf die Gefährdungslage zu bewerten.

5.2.3.1 Krankenhausinformationssystem (KIS)

Als Krankenhausinformationssystem (KIS) wird die zentrale Arbeitskomponente für den Prozess der medizinischen Versorgung des Patienten definiert. Es handelt sich dabei häufig nicht um ein monolithisches System, sondern vielmehr um eine Sammlung von Werkzeugen, teilweise nebeneinander, die in der Regel von einem oder mehreren Herstellern bezogen wird. Im Schwerpunkt bedient das KIS die Grundstruktur des Behandlungsprozesses von der Aufnahme bis zur Entlassung. KIS werden nahezu immer durch weitere, spezialisierte Systeme („Subsysteme“) ergänzt. Die Kommunikation zwischen den Systemen wird zunehmend über Standardschnittstellen (HL7) abgebildet. Darüber hinaus nimmt das System unter Umständen Aufgaben der Abrechnung und ERP-Funktionen (Materialwirtschaft) wahr. KIS werden kontextabhängig auch als klinische Arbeitsplatzsysteme (KAS) bezeichnet, hierbei stehen in der Regel jedoch Komponenten mit medizinischem Schwerpunkt (z.B. Endoskopie oder andere Untersuchungsarten), im Mittelpunkt. Das KIS führt in vielen Krankenhäusern die zentrale Patientenakte (elektronische Patientenakte, ePA), in der in der Regel Befunddaten, Untersuchungsergebnisse, Verordnungen und Therapieentscheidungen, die Dokumentation der Behandlung (OP-Bericht etc.) sowie der Pflege (inkl. Medikation und Vitalparameterdokumentation) enthalten sind.

Neben Standardlösungen kommen auch im Bereich der KIS Individuallösungen zum Einsatz, dabei variieren Umfang und Ausprägung der vom KIS bereitgestellten Funktionen stark. Das KIS bietet häufig Funktionen für Order/Entry-Systeme und übermittelt teilweise Anforderungen an Subsysteme (z.B. RIS, LIS, weitere).

5.2.3.2 Laborinformationssystem (LIS)

Für die Anforderung, Verarbeitung und Bereitstellung labordiagnostischer Untersuchungen stellt das LIS in vielen Krankenhäusern eine unverzichtbare Komponente für die medizinische Versorgung dar. Weiter werden Prozesse aus dem Bereich der klinischen Chemie, Mikrobiologie (Hygiene) sowie Aufgaben der Qualitätssicherung in vielen Bereichen über das LIS sichergestellt (z. B. Transfusionsmedizin, POCT-Geräte, wie Blutzuckeranalyse). Umfangreiche Dokumentationsanforderungen, z. B. entsprechend der Richtlinien der Bundesärztekammer (RiLiBÄK) stellen immense Anforderungen an die Chargen- und Untersuchungsdokumentation, die ebenfalls durch Funktionalitäten im LIS abgebildet werden. Auch externe Organisationsbereiche (z.B. MVZ, Kooperationspartner) sind zum Teil tief in das LIS integriert.

5.2.3.3 Radiologieinformationssystem (RIS)

Das RIS stellt ein Spezialsystem des Krankenhauses (oder von Radiologischen Instituten) dar. Es bedient die spezifischen Anforderungen, die sich im Wesentlichen aus der Röntgenverordnung (RöV) im Rahmen von Dokumentationspflichten ergeben. Darüber hinaus dient es der Terminplanung und der Befunderstellung für die Rückübermittlung an die zentrale elektronische Akte des KIS (ePA). Das RIS stellt zudem häufig die Verbindung zwischen Patientendaten und Bilddaten der Untersuchungen dar. Im Rahmen der radiologischen Untersuchung entstehen Bilddaten, die aus Einzelbildern

(Durchleuchtung) oder Serienaufnahmen (Schnittbilder wie CT und MRT) bestehen können und in der Regel nach dem DICOM-Standard (mit weltweit einheitlicher Kennzeichnung) verarbeitet werden.

5.2.3.4 Picture Archive and Communication System (PACS)

Das PACS stellt in der Regel das zentrale klinische Bildarchivierungssystem dar, dessen Kernaufgabe die Speicherung und Bereitstellung von Bilddaten z. B. radiologischer Untersuchungen (auch Nuklearmedizin/Strahlentherapie), Aufnahmen des CT und MRT (Schnittbilder), Ultraschall (US) oder Angiografie (Gefäße) und Herzkatheterarbeitsplätzen bildet. Der Austausch von Bilddaten erfolgt meist mittels der internationalen Standardschnittstelle DICOM.

Häufig wird über das PACS die krankenhauseitige Bereitstellung von Bilddaten sichergestellt. Dabei kann es sich um „abgesetzte“ Befundarbeitsplätze entsprechend RÖV handeln (siehe RIS). Das PACS stellt ein Archiv- und Kommunikationssystem dar. Insbesondere für Anwendungen im Rahmen telemedizinischer Leistungen stellt die Kommunikation zwischen PACS heute eine Standardfunktion moderner Systeme dar.

Bezüglich der PATIENTENSICHERHEIT ist das Risiko einer Schädigung von Personen nicht auszuschließen, wenn es zu einem Integritätsverlust bei der Zuordnung von bildgebenden Diagnosedaten, Patientenstammdaten und Befundungsinformationen kommt.

Für Diagnose und Therapie werden an die VERFÜGBARKEIT und INTEGRITÄT der Daten des PACS somit hohe Anforderungen gestellt, darüber hinaus ist gesetzlichen Vorgaben Rechnung zu tragen. Besonders kritisch können bildgebende Verfahren in zeitkritischen Behandlungsprozessen (oft während einer Operation) sein, da diese für Diagnose und Therapieentscheidungen herangezogen werden.

Auch hier bilden die zu schützenden Informationen eine Grundlage für Diagnosefindung und Therapieentscheidungen und tragen daher maßgeblich zur BEHANDLUNGSEFFEKTIVITÄT bei.

5.2.3.5 Dokumenten-Management-System (DMS/ECM)

DMS oder ECM-Systemen kommt im Krankenhaus eine stetig wachsende Bedeutung zu. Die elektronische Verwaltung von Dokumenten oder digitalisierten Patientenakten unterstützt dabei den medizinischen Versorgungsprozess in mehrfacher Hinsicht. Bereits zu Beginn der Behandlung werden häufig Vorbehandlungsdaten, z.B. Befunde des behandelnden Hausarztes, in die IT-Systeme des Krankenhauses (KIS, DMS/ECM) übernommen. Zwischen Subsystemen werden Informationen zum Teil dokumentenbasiert ausgetauscht (z. B. Anästhesieprotokoll als PDF-Dokument).

Darüber hinaus können DMS/ECM-Systeme als redundantes Archiv (Backup) zur elektronischen Akte im KIS genutzt werden, um bei Störungen des KIS oder wichtiger Subsysteme (z.B. Medikation) Informationen auf diesem Wege bereitzustellen. Auch

die Bereitstellung von digitalisierten Papierakten erfolgt i.d.R. über DMS/ECM-Systeme. Die Relevanz des digitalen Archivsystems wächst mit dem Grad der Digitalisierung eines modernen Krankenhauses.

Neben den gesetzlichen Vorgaben hinsichtlich der Vorhaltung der Behandlungsdokumentation, müssen die im DMS/ECM-System abgelegten Daten oftmals während des Diagnose- und Therapieprozesses verfügbar sein. Als begleitender Bestandteil der Diagnosefindung und Ausgangspunkt folgender medizinischer Entscheidungen, trägt die Untersuchungsdokumentation von Vorbefunden durch verfügbare Dokumente zur BEHANDLUNGSEFFEKTIVITÄT bei.

Auf Grund der sensiblen und häufig umfangreich vorgehaltenen medizinischen und personenbezogenen Daten im DMS/ECM-Kontext, ist insbesondere Gewährleistung der VERTRAULICHKEIT von hoher Bedeutung.

5.2.3.6 OP-Planungssystem

Die Ressourcenplanung für den Operationsbetrieb stellt zunehmend komplexe Anforderungen an das Management, daher wird in immer mehr Kliniken die OP-Planung heute nur noch IT-gestützt umgesetzt. Da OP-Leistungen einen wesentlicher Bestandteil der kDI der vollstationären Versorgung darstellen, ist die VERFÜGBARKEIT deshalb von hoher Bedeutung.

5.2.3.7 Systeme für Transportlogistik (Patienten-, Proben-, Speisen- und Arzneimitteltransporte)

Logistiksysteme kommen im Krankenhaus für unterschiedliche Einsatzzwecke zur Anwendung. Im Vordergrund steht dabei zumeist der Patiententransport im Rahmen von Diagnostik und Therapie. Jedoch spielt auch der Probentransport, z.B. im Rahmen von Schnellschnitten der Pathologie während laufender Eingriffe/OPs, eine Rolle sowie der Probentransport zum Labor, der zumeist von einem digitalen Anforderungsprozess (anderes Anwendungsverfahren; LIS) begleitet wird. Die Bedienung erfolgt wahlweise über Eingabemasken im KIS oder direkt im Subsystem. Letzteres hat Vorteile bei Störungen.

An die Aufrechterhaltung der unterschiedlichsten logistischen Prozesse im Krankenhausbetrieb werden aufgrund der zahlreichen Abhängigkeiten zu anderen Systemen hohe Anforderungen an die VERFÜGBARKEIT gestellt. Der Ausfall der Logistik kann insbesondere bei zeitkritischen Prozessen die BEHANDLUNGSEFFEKTIVITÄT und ggf. auch die PATIENTENSICHERHEIT maßgeblich negativ beeinflussen (z. B. Ausfall von Fahrstuhlssystemen in mehrstöckigen, bettenführenden Abteilungen).

Auch die Anforderungen an die INTEGRITÄT der für logistische Systeme herangezogenen Informationen werden als hoch eingeschätzt, um den Krankenhausbetrieb aufrecht zu erhalten (z. B. auch die rechtzeitige Verbringung von Patienten an den jeweils notwendigen Ort).

5.2.3.8 Systeme der Versorgungstechnik⁴

Zur Versorgungstechnik werden Infrastrukturkomponenten gezählt, die für die Aufrechterhaltung der ressourcenbezogenen und technischen Rahmenbedingungen des Krankenhausbetriebs notwendig sind. Hierzu zählen z. B. Heizungstechnik, Kältetechnik, Wasser- und Abwassersysteme, Energieversorgungsanlagen, Lichttechnik, Schließsysteme sowie technische Anlagen, wie Fahrstühle oder die Gebäudeleittechnik, die heute in weiten Teilen bereits als Gebäudeautomationstechnik verstanden und betrieben wird.

Die ausfallsichere (VERFÜGBARKEIT) und korrekte (INTEGRITÄT) Funktionsweise der Versorgungstechnik bildet aufgrund zahlreicher Abhängigkeiten zu anderen Systemen eine wesentliche Grundlage zur Aufrechterhaltung des Krankenhausbetriebs. Ohne funktionierende Energie- und Wasserversorgung kommen wesentliche Versorgungsprozesse schon nach kurzer Zeit zum Erliegen. Die PATIENTENSICHERHEIT und BEHANDLUNGSEFFEKTIVITÄT kann in der Folge stark beeinflusst werden.

In der Regel werden hier keine vertraulichen Informationen verarbeitet, es bestehen somit keine besonderen Anforderungen an die VERTRAULICHKEIT. Ausnahmen bestehen für die Zutrittskontrolle von technischen Anlagen der Versorgungstechnik (z. B. kartenbasierte, elektronische Schließsysteme).

5.2.3.9 Systeme der Versorgungsdienste

Unter dem Begriff Versorgungsdienste werden relevante Unterstützungsprozesse in Krankenhäusern subsummiert. Hierzu zählen u. a. die Speisenversorgung, die Hygiene-Dienste (Reinigung, Desinfektion), die Bettenaufbereitung, der Wäschedienst, die Sterilgutversorgung u.v.m. Die meisten dieser Prozesse werden heute digital unterstützt. Im Falle der Speisenversorgung liegt in der Regel ein IT-System für Bestell- und Lieferwesen mit Patientenbezug zugrunde. Zwar ist die Notfallversorgung mit Nahrungsmitteln und Getränken in der Regel auch ohne IT-Unterstützung möglich, erfordert jedoch insbesondere mit Blick auf die Beachtung patientenindividueller Rahmenbedingungen (z. B. Unverträglichkeiten etc.) im Einzelfall einen deutlich höheren Ressourceneinsatz.

Die Anforderungen an die VERFÜGBARKEIT und INTEGRITÄT der für Versorgungsdienste notwendigen Informationen können stark variieren.

Als essentieller Bestandteil der Basisversorgung tragen die Versorgungsdienste maßgeblich zur BEHANDLUNGSEFFEKTIVITÄT bei. Der Ausfall kann zudem - in Bezug auf die Sicherstellung von Hygienevorgaben – unmittelbar negative Auswirkungen auf die PATIENTENSICHERHEIT haben.

⁴ Betrachtung unter dem Vorbehalt der Vernetzung der Systeme bzw. wenn diese seitens der IT benötigt werden (andernfalls in BCM zu betrachten, nicht Gegenstand des ISMS)

5.2.3.10 Medizintechnik/-produkte

Medizintechnische Systeme kommen insbesondere in der Diagnostik und der Therapie zum Einsatz. Hierzu zählen radiologische Anlagen wie Durchleuchtung (Röntgen), Ultraschallsysteme (Farbdoppler, Echokardiographie), medizinische Großgeräte (CT, MRT, Linearbeschleuniger etc.) oder auch kleinere Geräte, wie Infusionspumpen. Medizintechnik beinhaltet häufig Komponenten der Informationstechnik (z. B. Steuerungstechnik). Medizintechnische Systeme können autark betrieben oder (meist IP-basiert) über die Netzwerkinfrastruktur miteinander verbunden sein.

Die Verfügbarkeit des Medizingerätes sowie die für das jeweilige Nutzungsszenario notwendigen (Patienten-)Daten und Informationen (z. B. Dosisangaben, Bestrahlungsintensität etc.) tragen maßgeblich zu einer optimalen Patientenbehandlung bei. Die Anforderungen an die Verfügbarkeit werden i.d.R. als hoch eingestuft.

Ebenso hohe Anforderungen werden an die INTEGRITÄT der Informationen gestellt, auf deren Grundlage die Nutzung der medizintechnischen Systeme erfolgt. Wird die INTEGRITÄT der Informationen durch unbewusste oder absichtlich herbeigeführte Veränderung gestört, besteht u. U. eine starke Gefährdung des medizinischen Behandlungsprozesses sowie in bestimmten Fällen eine unmittelbare Gefährdung der Patientensicherheit.

Bei der Nutzung von Medizintechnik werden in der Regel auch besondere personenbezogene Daten (Gesundheitsdaten) erhoben und verarbeitet, daher ist die Absicherung der VERTRAULICHKEIT ebenfalls von besonderer Bedeutung.

Die Behandlungseffektivität innerhalb der Therapie oder Diagnostik kann durch Fehlfunktionen, Ausfälle der Medizintechnik oder Störung der Schnittstellen zu anderen Medizin- oder IT-Geräten maßgeblich beeinflusst werden.

5.2.3.11 Spezialisierte Anwendungen im klinischen Umfeld

Typisch für das Krankenhausumfeld ist der Einsatz einer Vielzahl von Softwarelösungen. Vielfach kommen Individuallösungen und Eigenentwicklungen zum Einsatz. Viele dieser Lösungen dienen dabei in erster Linie der Erfüllung gesetzlicher Auflagen der Dokumentation, zur Erfüllung von Verordnungen oder der Qualitätssicherung in unterschiedlichsten Fachbereichen sowie zur Unterstützung in besonders spezifischen Behandlungskontexten. Es wird darauf hingewiesen, dass insbesondere eigenentwickelte Software-Produkte hinsichtlich der Anfälligkeit gegenüber Cyberangriffen geprüft werden sollten.

Werden Informationen für Sonder- und Speziallösungen für Prozesse genutzt, die unmittelbar oder mittelbar Prozesse der kDL unterstützen (z. B. Langzeit-Hautkrebsmonitoring-Software), bestehen die gleichen Vorgaben an die VERFÜGBARKEIT und INTEGRITÄT der Informationen sowie an die Kritikalitätseinstufung, wie für die Hauptinformationssysteme zur Unterstützung der stationären, medizinischen Versorgung. Für Systeme, die vorwiegend einer zusätzlichen Dokumentation dienen,

können die Anforderungen an Verfügbarkeit auch niedriger ausfallen.

5.3 Festlegung der spezifischen Ziele und Anforderungen an die Informationssicherheit

Zur Beherrschung der individuellen und dynamischen Anforderungen an den Schutz der Informationen im Geltungsbereich der medizinischen Versorgung ist der Aufbau eines Informationssicherheits-Managementsystems (ISMS), z. B. entsprechend den Anforderungen der Norm ISO 27001, als wirksame Maßnahme allgemein anerkannt. Das ISMS ist dabei angemessen an den Anforderungen des Krankenhausbetriebs auszurichten, um die für den konkreten Betreiber spezifischen Ziele und Anforderungen an die Informationssicherheit umsetzen zu können. Das ISMS ist durch geeignete Maßnahmen aufrechtzuerhalten und fortlaufend zu verbessern.

Informationssicherheit dient dem Schutz von (digitalen und nicht digitalen) Informationen, sie umfasst alle dabei die logische und technische Sicherheit, physische Sicherheit, organisatorische Maßnahmen, Betriebsverfahren, Notfallplanung, Vertragsbeziehungen, inkl. Outsourcing und wichtige Schnittstellen, wie IT-Management, Datenschutz, Risikomanagement und Personal.

Mit dem Ziel, die Sicherheit aller für die Versorgung der Patienten notwendigen Informationen sowie der Informationstechnik, der vernetzten Medizin- und Versorgungstechnik auch unter wirtschaftlichen Aspekten angemessen auszugestalten, sind insbesondere die folgenden Punkte von Bedeutung:

- Das vom Krankenhaus angestrebte Sicherheitsniveau MUSS definiert, umgesetzt und fortlaufend an die aktuellen Bedürfnisse sowie die Gefährdungslage angepasst werden.
- Steuerbare und einfache Strukturen SOLLTEN einer hohen Komplexität, die zu unnötigen Risiken führen kann, vorgezogen werden.
- Alle Mitarbeiter MÜSSEN regelmäßig zur aktiven Umsetzung und Notwendigkeit der Informationssicherheit sensibilisiert und geschult werden.
- Informationssicherheit benötigt Ressourcen und MUSS im Rahmen von Investitions- und Beschaffungsmaßnahmen berücksichtigt werden. Dies erfordert eine möglichst vollständige und risikoorientierte Kosten-Nutzen-Betrachtung, die auch notwendige Kontroll- und Überwachungsmaßnahmen berücksichtigt.

5.4 Leitlinie zur Informationssicherheit

Zur Verankerung eines Informationssicherheits-Managementsystems (ISMS) ist eine Leitlinie von der Geschäftsführung des Krankenhauses vorzugeben. Die Leitlinie enthält die Definition des Zwecks, den Stellenwert der Informationstechnik, der Ziele der Informationssicherheit und der Grundlagen und Grundsätze für das Informationssicherheits-Management und liegt im Verantwortungsbereich der Geschäftsführung.

Siehe ISO 27002, ISO 27799

Die Krankenhausleitung hat den Stellenwert der Informationssicherheit für den B3S-Anwendungsbereich sowie die damit verbundenen Ziele zu nennen sowie allgemeine Vorgaben und Prinzipien zur Erreichung dieser Ziele vorzugeben.

Diese Vorgaben sind durch die Krankenhausleitung als Teil eines übergeordneten Risikomanagements für alle wesentlichen Risiken festzulegen. Sie beschreiben den Umgang mit Risiken, die aus der Geschäftsstrategie resultieren.

Die Leitlinie soll konsistent zur Geschäfts-/Unternehmensstrategie sein und mindestens zu den folgenden Aspekten Aussagen zur Zielsetzung enthalten (die konkrete Ausgestaltung erfolgt in Form von geeigneten Richtlinien und Konzepten):

- Stellenwert der Informationssicherheit und Bedeutung der wesentlichen Informationen, Geschäftsprozesse sowie der Informationstechnik für die Aufgabenerfüllung und Einhaltung der wesentlichen gesetzlichen, regulatorischen und vertraglichen Anforderungen, insbesondere zum Schutz von Gesundheitsdaten
- Sicherheitsziele und Kernelemente der Sicherheitsstrategie für die Geschäftsprozesse und die eingesetzte Informationstechnik mit Bezug zu den Aufgaben und Geschäftszielen des Krankenhauses
- Beschreibung der für die Umsetzung des Informationssicherheitsprozesses zu etablierenden Organisationsstruktur
- Aufforderung der Beschäftigten zur Einhaltung der rechtlichen und ethischen Verantwortlichkeiten zum Schutz von sensiblen Informationen
- Bekenntnis der Geschäftsführung zur Leitlinie und Zusicherung ihrer Durchsetzung

Im Kontext des vorliegenden B3S sollten darüber hinaus folgende Aspekte bei der Erstellung der Leitlinie zu berücksichtigen werden:

- Besonderer Stellenwert des Schutzes der „kritischen Dienstleistung“
- Bedeutung der besonderen Datenschutzanforderungen im Kontext der medizinischen Versorgung
- Technische, personelle und organisatorische Verantwortung zur Sicherstellung der Versorgungsdienstleistung

Die Leitlinie zur Informationssicherheit ist innerhalb der eigenen Organisation den betroffenen Fachrichtungen und Funktionsstellen sowie relevanten Dienstleistern weitgehend nachweislich bekannt zu geben und regelmäßig auf Angemessenheit zu überprüfen.

6 Branchenspezifische Gefährdungslage

Neben den allgemeinen Gefährdungen, denen sich Krankenhäuser - wie Unternehmen anderer Branchen auch - im Rahmen des IT-Betriebes ausgesetzt sehen, bestehen bezüglich der von Einrichtungen der medizinischen Versorgung erbrachten „kritischen Dienstleistung“ eine Reihe weiterer branchenspezifischer Gefährdungsszenarien, die vor allem auf unterstützende IT-Systeme zurückzuführen sind, die eine hohe Relevanz für die Aufgabenerfüllung der medizinischen Versorgung besitzen.

Im Rahmen des vorliegenden B3S werden grundsätzlich nur Gefährdungen in Bezug auf die Verletzung der Schutzziele Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität von unterstützenden IT-Systemen betrachtet. Weiterhin kommt den Aspekten Patientensicherheit und Behandlungseffektivität als Kernelement der medizinischen Versorgung im medizinischen Behandlungsprozess bei der Gefährdungsanalyse besondere Bedeutung zu.

Die branchenspezifische Gefährdungslage soll für die kritische Dienstleistung „stationäre medizinische Versorgung“ anhand des vorliegenden Gefährdungskatalogs mit Blick auf besonders relevante Gefährdungen für die kritische Dienstleistung erhoben werden.

Grundsätzlich beruht das etablierte Verfahren der Gefährdungs- und Risikoanalyse auf einem Mapping von Bedrohungs-Szenarien auf entsprechende Schwachstellen sowie einer Bewertung der Eintrittswahrscheinlichkeit und der sich aus der Gefährdung ggf. ergebenden Folgen für die prozessunterstützenden Informationssysteme in Bezug auf die Schutzziele bzw. die Kernaspekte des medizinischen Behandlungsprozesses. Dem „Allgefahren Ansatz“ folgend, wie er in der Regel vom BSI empfohlen wird, sind sämtliche Gefährdungen, die sich für die kDL ergeben können, zu betrachten. Um diesen Prozess handhabbar zu gestalten, erfolgt eine Zusammenfassung von Gefährdungen und den hieraus abzuleitenden Maßnahmen auf ein angemessenes und branchenspezifisch sinnvolles Abstraktionsniveau.

Eine Fokussierung auf spezifische, informationstechnische Gefährdungsparameter wird aufgrund der heterogenen und sehr dynamischen, informationstechnischen Systemlandschaft an den Krankenhäusern bewusst nicht vorgenommen. Die Ermittlung der spezifischen Gefährdungslage und der Kritikalität der Systeme anhand der katalogisiert aufgeführten Bedrohungs- und Schwachstellenszenarien sowie den branchenspezifischen Gefährdungen und Kritikalitätsklassifikationen umfasst technische Gefährdungsparameter jedoch abstrakt. Es gelten des Weiteren folgende Definitionen:

- VEFÜGBARKEIT von Dienstleistungen, Funktionen eines Informationssystems, IT-Systems, IT-Netzinfrastruktur oder auch von Informationen ist dann vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.
- INTEGRITÄT bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Bei AUTHENTISCHEN

Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden.

- VERTRAULICHKEIT stellt den Schutz vor unbefugter Preisgabe von Informationen sicher. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.
- PATIENTENSICHERHEIT ist der Freiheit von unververtretbaren Risiken einer physischen Verletzung oder eines Schadens an der Gesundheit von Menschen, wie einer nachhaltigen psychischen Belastung, oder eines Schadens an Eigentum oder der Umwelt
- BEHANDLUNGSEFFEKTIVITÄT stellt die wirksame Behandlung des Patienten unter Benutzung von Informationen sowie die Anwendung wirksamer Gesundheitsmaßnahmen, aufgrund des Informationsaustausches zwischen den unterschiedlichen, behandelnden Organisationen sicher.

6.1 Bedrohungsszenarien

Für die branchenspezifische Gefährdungsanalyse sollten folgende Primärbedrohungsszenarien - gegliedert nach allgemeinen Bedrohungen und IT-spezifischen Bedrohungen - betrachtet werden:

6.1.1 Allgemeine Bedrohungen

- BED 1 Höhere Gewalt und Elementarschadensereignisse
- BED 2 Abhängigkeiten von Dienstleistern und Herstellern (Ausfall externer Dienstleister, unberechtigter Zugriff, versteckte Funktionen in Hard- und Software)
- BED 3 Ausfall von Basisinfrastrukturen mit direktem Bezug zur IT (Sekundäreffekte, z. B. Strom und TK)
- BED 4 Manipulation, Diebstahl, Verlust, Zerstörung von IT oder IT-relevanten Anlagen und Anlagenteilen
- BED 5 Beschädigung oder Zerstörung verfahrenstechnischer Komponenten, Ausrüstungen und Systeme
- BED 6 Terroristische Akte (physisch mit Wirkung auf die IT oder direkt IT-bezogen)

6.1.2 IT-spezifische Bedrohungen

- BED 7 Hacking und Manipulation
- BED 8 Schadprogramme / Ransom-Ware
- BED 9 System Missbrauch (Innentäter) und unbefugter Zugriff
- BED 10 Gezielte Störung / Verhinderung von Diensten, z. B. distributed denial of service (DDoS), gezielte Systemabstürze, u. ä.
- BED 11 Social Engineering

BED 12 Identitätsmissbrauch (Phishing, Skimming, Zertifikatsfälschung)

BED 13 Advanced Persistent Threat (APT)

BED 14 E-Mail-Account-Übernahme / Spamming

6.2 Schwachstellen

In Bezug auf die branchenspezifische Gefährdungsanalyse werden folgend Schwachstellenszenarien als generalisierbar angenommen:

SWS 1 Organisatorische Mängel

SWS 2 Technische Schwachstellen in Software, Firmware und Hardware

SWS 3 Technisches Versagen von IT-Systemen, Anwendungen oder Netzen (sowie Verlust von gespeicherten Daten)

SWS 4 Menschliche Fehlhandlungen, menschliches Versagen

SWS 5 Infrastrukturelle Mängel (baulich, Versorgung mit Strom etc.)

SWS 6 Verwendung ungeeigneter Netze/ Kommunikationsverbindungen, sonstige Schwächen in der Kommunikationsarchitektur

SWS 7 Verkopplung von Diensten (Beeinträchtigung eines Dienstes durch Störung anderer Dienste)

6.3 Branchenspezifische Gefährdungen

Aus den Bedrohungen und Schwachstellen werden die folgenden branchenspezifischen Gefährdungen abgeleitet:

GEF 1 Nichtverfügbarkeit wichtiger, medizinisch relevanter Daten im Diagnose-Prozess

GEF 2 Nichtverfügbarkeit wichtiger medizinisch relevanter Daten im Therapie-Prozess

GEF 3 Nichtverfügbarkeit wichtiger medizinisch relevanter Daten im Versorgungs-Prozess

GEF 4 Nichtverfügbarkeit wichtiger medizinisch relevanter Daten im Entlassungs-Prozess

GEF 5 Nichtverfügbarkeit von für den Behandlungsprozess wichtiger Prozess- und Freigabeinformationen

GEF 6 Nichtverfügbarkeit von behandlungsprozessrelevanten IT-Systemen

GEF 7 Nichtverfügbarkeit von behandlungsrelevanten Logistikketten

GEF 8 Inkonsistenzen in für den Behandlungsprozess relevanten Datenbeständen

GEF 9 Inkonsistenzen bei der Übertragung von für den Behandlungsprozess relevanten Datenbeständen

GEF 10 Manipulation von medizinisch relevanten Daten im Diagnose-Prozess

GEF 11 Manipulation von medizinisch relevanten Daten im Therapie-Prozess

-
- GEF 12 Manipulation von medizinisch relevanten Daten im Versorgungs-Prozess
 - GEF 13 Manipulation von medizinisch relevanten Daten im Entlassungs-Prozess
 - GEF 14 Unterbrechung von behandlungsrelevanten Kommunikationsabläufen.
 - GEF 15 Vertraulichkeitsverlust bei besonders sensiblen Patienten- und Behandlungsinformationen.
 - GEF 16 Verlust der Datenauthentizität
 - GEF 17 Fremdsteuerung/Manipulation von medizinische relevanten IT-Systemen
 - GEF 18 Fremdsteuerung/Manipulation von netzangebundenen Medizingeräten
 - GEF 19 Fremdsteuerung/Manipulation von relevanten Infrastrukturkomponenten

6.4 Gefährdungen kritischer branchenspezifischer Technik und Software

Neben Standardsoftware und -technik wie Fileserver, E-Mail-System und Software zur Bürokommunikation werden in Krankenhäusern BRANCHENSPEZIFISCHE SYSTEME eingesetzt, die in der Regel über die Schnittstellen HL7 und DICOM (eventuell als Bestandteil einer IHE-Struktur) kommunizieren. Bei der Risikoklassifikation und Gefährdungsanalyse ist es daher wichtig, nicht einzelne Hardware- und Software-Komponenten zu betrachten, sondern die für die kDL relevanten Informationssysteme, also einen für die medizinische Versorgung prozessrelevanten Informationsverbund aus Hardware, Software und menschlicher Interaktion insgesamt. Nachfolgend werden die i.d.R. für die medizinische Versorgung wichtigen Hauptinformationssysteme im Krankenhausbereich aufgeführt, sowie die branchenspezifische Gefährdungslage für diese Hauptinformationssysteme im Überblick dargestellt. Über diese allgemein im Krankenhauskontext eingesetzten Informationssysteme hinaus sind je nach Ausprägung des vom Betreiber ermittelten Geltungsbereiches für den B3S weitere, zur Erbringung der medizinischen Versorgung wichtigen Informationssysteme zu identifizieren und in Bezug auf die Gefährdungslage zu bewerten.

HL7
Standard zum Austausch von Gesundheitsdaten zwischen Informationssystemen.

DICOM
Offener Standard zur Speicherung und zum Austausch von medizinischen Bilddaten.

IHE
Offener, prozessbasierter Schnittstellenstandard der die Nutzung von SSt wie HL7 oder DICOM im Rahmen definierter Prozesse vorgibt. Gewinnt an Bedeutung.

6.4.1 Krankenhausinformationssystem (KIS)

Die Krankenhausinformationssysteme (KIS) in ihren unterschiedlichen Ausprägungen sind das organisatorische Steuerungs- und Dokumentationsrückgrad der stationären, medizinischen Versorgung. Störungen an zentralen KIS-Infrastrukturkomponenten oder an angebundene IT-, Medizintechnik- oder Abteilungssystemen können schnell dazu führen, dass der medizinische Behandlungsprozess empfindlich verlangsamt und gestört wird. Störungen des KIS können hierbei von der Nichtverfügbarkeit von Hardwarekomponenten über Software-Fehler in KIS- Funktionsmodulen, fehlerhafte oder korrumpierte Datenschnittstellen bis hin zu akuten Angriffen auf die Integrität der im KIS vorgehaltenen Daten und Informationen verursacht werden. Der Absicherung des KIS mit dessen vielfältigen Schnittstellen und Kommunikationsverbindungen kommt im Krankenhaus somit besondere Bedeutung zu.

Gefährdungen ergeben sich, neben den KIS-systemimmanenten Gefährdungen insbesondere auch im erweiterten KIS-Client-Kontext. Extern über Datenträger oder auf anderem Wege eingebrachte, elektronische Patientendaten (z.B. elektronische Radiologie-Bilder und Arztbriefe), E-Mail-Kommunikation und die Nutzung von Web- bzw. Internet-Verbindungen im KIS-Nutzungskontext bergen dieselben Informationssicherheitsrisiken, welche generell bei der Nutzung elektronischer Kommunikations- und Datenaustauschlösungen auftreten können. Die Möglichkeiten für Gefährdungen des KIS-Betriebes sind – vor allem bei zunehmender Vernetzung von Krankenhäusern untereinander sowie mit niedergelassenen Ärzten, Patienten und Dienstleistern – vielfältig. Gefährdungen können sich insbesondere auf die allgemeinen Schutzziele: Verfügbarkeit, Integrität und Vertraulichkeit beziehen, jedoch ist das Gefährdungspotential im KIS-Betrieb zunehmend auch in Bezug auf die Aspekte der direkten Patientenbehandlung, wie BEHANDLUNGSEFFEKTIVITÄT und PATIENTENSICHERHEIT von Bedeutung. Aufgrund des für den Personenzugang weitgehend offenen Charakters eines Krankenhauses, ist weiterhin dem Zutrittsschutz, dem Zugang zu den Clientsystemen und – vor dem Hintergrund der hohen Vertraulichkeitsanforderungen – dem Zugriffsschutz auf (Behandlungs-)Daten ein besonderes Gewicht bei der Gefährdungsanalyse beizumessen.

6.4.2 Laborinformationssystem (LIS)

Das LIS eines Krankenhauses hat insbesondere in Bezug auf die Behandlungsaspekte BEHANDLUNGSEFFEKTIVITÄT und PATIENTENSICHERHEIT eine herausragende, medizinische Prozessbedeutung, da durch dieses Informationssystem im stationären Versorgungskontext elementare Diagnostikdaten verarbeitet und zur Verfügung gestellt werden. Eine mangelnde Verfügbarkeit des oder der LIS-Systeme eines Krankenhauses kann den Behandlungsprozess empfindlich verlangsamen und stören. Die fehlende Verfügbarkeit von Labor- oder Entry-Informationen erhöht u.a. das Risiko, dass Laborproben nicht zeitgerecht verarbeitet werden oder es zu Verwechslungen von Probenmaterial kommen könnte. Datenintegritätsverluste bei der Übermittlung von Laborwerten können zu diagnostischen oder therapeutischen Fehlentscheidungen mit direkter Relevanz in Bezug auf die BEHANDLUNGSEFFEKTIVITÄT und die PATIENTENSICHERHEIT führen. Gefährdungen in der Labornetz-Außenanbindung sind – neben den Gefährdungen, die sich durch den Einsatz elektronischer Kommunikations- und Informationsmedien generell ergeben können – insbesondere bei der Übertragung von Labordaten an netzexterne Empfänger sowie ggf. vielfältigen Wartungszugängen zu sehen. Besondere Gefährdungen können sich aus der oftmals ungenügenden, IT-sicherheitstechnischen Absicherung von netzgebundenen Laboranalysegeräten mit oder ohne direkter LIS-Anbindung ergeben, die – ähnlich den netzgebundenen Medizingeräten – bei nicht ausreichenden Absicherungs- bzw. Netzabgrenzungsmaßnahmen anfällig für die Verbreitung von Schadsoftware sein können und damit ein erhebliches Schadensausmaß erwarten lassen. Auch sind Angriffe auf Krankenhauslaborsysteme denkbar, die ungenügend geschützte Laborsysteme als „Einfallstor“ für die Ausspähung von Daten oder als Zutrittsmöglichkeit zu Fernwartungsnetzen von Laborsystemhersteller adressieren

6.4.3 Radiologieinformationssystem (RIS)

Beeinträchtigung der Verfügbarkeit eines RIS hat in Bezug auf die bildgebende Diagnostik, welche durch RIS/PACS-Unterstützt wird, eine hohe Relevanz für die kDL, da sämtliche auf diese Form der Diagnostik angewiesenen Behandlungsprozesse bei Nicht-Verfügbarkeit erheblich gestört werden. Datenintegritätsverluste im Kontext der bildgebenden Diagnostik haben ggf. eine Patientengefährdung durch fehlerhafte Behandlung oder Fehlparametrisierung zur Folge. Authentizitätsverlust bei Freigabeprozessen im RIS können haftungstechnische Folgen nach sich ziehen, soweit nach Röntgenverordnung nicht autorisierte Diagnostik erfolgt. Die IT-Gefährdungen im RIS-Bereich sind ähnlich denen im KIS-Bereich, jedoch wesentlich stärker im direkten Diagnostik-Kontext zu sehen.

6.4.4 Picture Archive and Communication System (PACS)

Das PACS (oder die PACS-Systeme) ist vor allem durch die Risiken elektronischer Kommunikation und Informationsgewinnung auf Clientsystemen und durch die vielfältigen Schnittstellen zu netzgebundenen Medizin- und Bilderfassungsgeräten bzw. anderen DICOM-Knoten im LAN- oder WAN-Netzverbund gefährdet. Unter anderem sind PACS-Systeme z.B. im Kontext von Telemedizin- und Teleradiologie-Vereinbarungen sowie die Wartungszugänge von Medizintechnikfirmen mit externen Netzwerken verbunden. Zudem werden im Kontext PACS/RIS oftmals externe Patientendaten eingelesen. Netzgebundene, bildgebende Modalitäten verfügen in der Regel nicht über eine Schadsoftware-Abwehr, aufgrund der Qualitätssicherungsanforderungen an Medizinprodukte weisen diese jedoch häufig nicht zeitgerecht zu schließende Software-Schwachstellen auf. Ein PACS-Informationsverbund ist in der Folge einem relativ hohen Gefährdungspotential ausgesetzt. Zudem können Integritätsverluste bei der Einbindung des PACS in den KIS- und RIS-Kontext erhebliche Folgen für die BEHANDLUNGSEFFEKTIVITÄT und PATIENTENSICHERHEIT haben. Der Einfluss von Schadsoftware oder der Integritätsverlust bei diagnostischen Bilddaten wirkt sich jedoch nicht zwingend unmittelbar auf das PACS selbst aus, sondern wirkt indirekt über die Bilddatenverteilungsfunktion dieses Informationssystems.

Werden Modalitäten und Software-Systeme in der diagnostischen Bildgebung kompromittiert, können sich durch Offenlegung von Patientendaten erhebliche Folgen in Bezug auf die Verletzung von Persönlichkeitsrechten der Patienten aus Sicht des Datenschutzes ergeben. In diesem Kontext sind insbesondere auch Telemedizin- und Tumorboard-Schnittstellen und Radiologie-Portale mit externer Beteiligung besonders sorgfältig in Bezug auf mögliche Gefährdungen der Vertraulichkeit zu bewerten. Besonders hervorzuheben ist zudem die IT-Gefährdungproblematik bei als Medizin-geräten deklarierten, vernetzten, bildgebenden Modalitäten und IT-Systemen, inkl. der ggf. vorhandenen Offline-Schnittstellen (z.B. USB). Im Bereich der interventionellen Radiologie sind IT-Systemstörungen der Verfügbarkeit und technischen Systemintegrität im Kontext der an das PACS-angebundenen Modalitäten ggf. sogar unmittelbar patientengefährdend. Eine detaillierte Gefährdungsanalyse wird in diesem Medizingerätekontext i.d.R. über ein Risikomanagement nach DIN EN 80001 gewährleistet.

6.4.5 Dokumenten-Management-System / Enterprise-Content-Management

EMC/DMS-Systeme sind, wie alle IT-Systeme, die flächendeckend im Krankenhaus eingesetzt werden, insbesondere auch durch IT-Angriffsformen (ATP, Trojaner) gefährdet, die auf das Abgreifen von Informationen fokussieren. Des Weiteren können derartige Systeme u.a. Schadsoftware im gesamten Krankenhaus weiter verteilen (z.B. kompromittierte Office oder PDF-Dokumente), ohne selbst signifikant beeinträchtigt zu werden. Eine unerlaubte oder unbewusste Veränderung (INTEGRITÄT) der Informationen kann den medizinischen Behandlungsprozess beeinflussen.

6.4.6 Medizintechnik

Medizingeräte (auch netzgebunden) unterliegen den besonderen Regularien der Medizinproduktegesetzgebung. Die für eine Zulassung des Medizinproduktes nötigen Qualitätssicherungsmaßnahmen und Gefährdungsanalysen beziehen sich jedoch i.d.R. auf das Medizingerät selbst und nicht auf die Absicherung eines im Netzwerk betriebenen, ggf. heterogenen Medizingeräte-Verbundes. Als besonderer Gefährdungsschwerpunkt ist die oftmals noch ungenügende, IT-sicherheitstechnische Absicherung von Medizingeräten mit ihrer diagnostischen oder therapeutischen Fokussierung, sowie die aufgrund der Medizingerätezulassungsregelungen nur verzögert behebbaren Schwachstellen an den IT- und Software-Komponenten der Medizingeräte zu sehen.

Medizingeräte mit oder ohne direkter Netz-Anbindung lassen so – ähnlich wie bei netzgebundenen Laborsystemen – bei nicht ausreichenden Absicherungs- bzw. Netzabgrenzungsmaßnahmen z.B. im Falle von sich „wurmartig“ verbreitender Schadsoftware ein erhebliches Schadensausmaß erwarten. Auch sind Angriffe auf Medizingeräte i.d.R. unmittelbar in Bezug auf die Behandlungsqualität und die Patientensicherheit von Bedeutung. Unzureichend abgesicherte Medizingeräte können zudem als „Einfallstor“ für die Ausspähung von Daten im Netzwerkbereich des Krankenhauses oder als Zutrittsmöglichkeit zu Fernwartungsnetzen von Medizingeräteherstellern ausgenutzt werden. Das Schadenspotenzial ist sowohl mit Blick auf mögliche Patientengefährdungen als auch auf finanzielle Auswirkungen, z. B. infolge eines Datenschutzverstößes erheblich.

Aufgrund der hohen Behandlungsrelevanz, der potentiell erheblichen Patientengefährdung und der besonderen rechtlichen Gegebenheiten, ist insbesondere die Netz-anbindung und die Absicherung des netzgebundenen Betriebs im Sinne eines speziellen, die medizinischen Risiken fokussierenden Risikomanagement- und Gefährdungsanalyseprozesses nach DIN EN 80001-1 eine Grundanforderung an das Informationssicherheitsmanagement eines Krankenhauses.

6.4.7 Transportlogistik

Während des Transports von Patienten, Proben oder Informationen auf Datenträgern sind diese häufig einem erhöhten Risiko ausgesetzt (z. B. Verlust von Datenträgern bzw. Offenbarung von Gesundheitsdaten). Die Anforderungen an die VERTRAULICH-

KEIT können variieren, werden jedoch in der Regel als hoch eingeschätzt. Logistiksysteme sind generell allen IT-Risiken bzw. Gefährdungen ausgesetzt, denen auch andere Informationssystemen des Krankenhauses ausgesetzt sind. Ein besonderes Risiko ergibt sich in diesem Kontext jedoch ggf. durch das Outsourcing von Logistikprozessen an Dienstleister u.ä.

6.4.8 Versorgungstechnik

Die Systeme der Versorgungstechnik am Krankenhaus sind oftmals auf IT-Systeme angewiesen, die älter sind oder aber für Betriebskontexte entworfen wurden, die eine moderne Netzwerkintegration in offene Netze nicht vorsehen. Auf der anderen Seite ist gerade die Gebäudeautomatisations- und Versorgungstechnik einem erheblichen Innovationsdruck in Bezug auf den Einsatz von IoT-Systemen und Cloud-Anbindungslösungen ausgesetzt. Während die Gebäudeautomatisierung und die Versorgungstechniksysteme im Idealfall bisher in einem geschlossenen, vom IT-Kommunikationsnetzwerk getrennten Netzwerksegment betrieben wurden, öffnen sich diese technischen Betriebsnetze zunehmend. Das Gefährdungspotential dieser Mischung an Geräte- und IT-Technik-Mischung ist erheblich. Durch externe Netzzugänge und ggf. nicht ausreichend abgesicherte Gebäudeautomatisierungssystemen, ist im Falle von gezielt hierauf fokussierten IT-Angriffen mit erheblichem Schadenspotential zu rechnen

6.4.9 Versorgungsdienste

IT-Systeme der Versorgungsdienste sind allen IT-Risiken und Gefährdungen des üblichen IT-Betriebes eines Krankenhauses ausgesetzt. Ein besonderes Gefährdungspotential liegt zum einen in der Störung der Versorgungsprozessflüsse sowie in der Störung der Datenintegrität bei der Qualitätssicherung von Hygienemaßnahmen im medizinischen Prozessunterstützungskontext, z.B. bei der Sterilgutaufbereitung. Dies gilt des Weiteren auch insbesondere im Kontext der Speisezubereitung und -versorgung. Auch im Rahmen der Versorgungsdienstleistungen kommen in den Krankenhäusern i.d.R. IT-Systeme zum Einsatz, die aufgrund ihrer sehr speziellen Fokussierung in einem relativ kleinen Marktsegment oftmals Sicherheitslücken aufweisen können. Sie können daher vergleichsweise einfach angegriffen und gestört werden, sobald ein Angreifer den Netzwerk- und Client-Schutz eines Krankenhausnetzwerks überwunden hat. Neben hauseigenen Versorgungsdiensten ist in Bezug auf die Gefährdungsanalyse weiterhin die elektronische Kommunikation mit ggf. dienstleistenden Unternehmen besonders zu betrachten.

6.4.10 Sonder- und Spezial-Softwarelösungen

Bezüglich der PATIENTENSICHERHEIT ist ein unmittelbarer Schaden an Personen nur dann zu erwarten, wenn Daten der Sonder- und Spezialsoftware unmittelbar diagnostische und therapeutische Entscheidungen beeinflussen können. In Bezug auf eine Gefährdungsanalyse sind insbesondere die Systeme zu betrachten, die somit direkten Einfluss auf die BEHANDLUNGSEFFEKTIVITÄT und ggf. die PATIENTENSICHERHEIT haben.

Sondersysteme und Spezialsoftware im Krankenhauskontext haben aus der IT-Sicherheitsicht oftmals ein besonderes Gefährdungspotential. Die spezialisierte Software ist i.d.R. eher an den direkten Funktionsanforderungen der medizinischen Behandlung oder der adressierten Dokumentationsfragestellung orientiert, als an einem sicheren Software-Design. Oftmals weist derartige Software daher auch Entwicklungs- bzw. Sicherheitsmängel auf und wird vom Hersteller nur zeitverzögert aktualisiert oder gar nicht mehr gepflegt. Diese Software kann jedoch aufgrund der hoch spezifischen, medizinisch notwendigen Funktionalität nicht einfach ersetzt werden. Während das Risiko einer Verfügbarkeitsstörung dieser Software i.d.R. als gering anzusehen ist, stellen derartige Systeme jedoch ein „Trittbrett“ für Schadsoftware oder Hacker dar, die entsprechende Software-Lücken ausnutzen. Auch ist das Risiko des Datenabflusses und somit ein Verlust von Datenvertraulichkeit in Kontext der Sondersysteme und Eigenentwicklungen ggf. als besonders hoch zu bewerten. Eine Gefährdungsanalyse muss daher in sinnvollem Rahmen die Auswirkung einer möglichen Störung eines solchen Systems für die kDL im betroffenen Informationsverbund betrachten.

6.5 kDL-relevante IT-Systeme und Komponenten

Grundlage der Gefährdungsanalyse sollten die im Dokument „Geltungsbereich und Schutzziele“ erfassten technischen Unterstützungsprozesse sowie die kritischen, branchenspezifische Anwendungssysteme bilden, die im Wesentlichen auf folgende, branchenspezifischen Systeme und Komponenten wirken und für den Behandlungsprozess (und damit die kDL) elementar sind.

6.5.1 Informationstechnik

- IT 1 Arbeitsplatzsysteme, z.B. PC-Arbeitsplätze, Notebooks, Tablets
- IT 2 Serversysteme (Anwendungen, Datenbanken, Virtualisierung)
- IT 3 Stagesysteme (z B. SAN)
- IT 4 IP-Datennetzwerke (WAN, LAN, WLAN, VLAN)
- IT 5 Softwaresysteme (Lebenszyklus von Betriebs- und Anwendersystemen)
- IT 6 Peripherie-Geräte (Monitore, Befundarbeitsplätze, Zubehör)
- IT 7 Drucker (Netzwerkbetrieb, Bereitstellung, Instandhaltung)
- IT 8 Security (Firewall, DMZ, VPN, Malware-Schutz, Spamabwehr usw.)
- IT 9 Rechenzentrumsbetrieb
- IT 10 Betrieb von Unterverteilungen des IP-Datennetzwerks (Verteilerräume)
- IT 11 USV-Betrieb
- IT 12 Fernwartungsbetrieb
- IT 13 Telekommunikationssysteme (IP-basiert)
- IT 14 Videoüberwachung (IP-basiert)
- IT 15 Versorgungstechnik (IP-basierte Anlagentechnik: Fahrstuhl Anlagen, Zugangs-

systeme, Schrankensysteme, GLT)

IT 16 Netzbereitstellung (i.d.R. Kopplung) für Medizintechnik (physikalische und logische Integration von medizintechnischen Anlagen)

6.5.2 Kommunikationstechnik

KT 1 Rufsysteme, Diensttelefonie/Festnetzapparate (Endgeräte, Schwerpunkt VoIP-Telefone mit Netzversorgung oder Energieversorgung PoE (Power over Ethernet), DECT/GSM, TK-Anlagenserver, IP-Netze)

KT 2 Diensttelefonie/Mobil (Endgeräte, z. B. Mobiltelefonie / Smartphones)

KT 3 Fax-Betrieb (ggf. Faxserver, klassische Fax-Anlagen, Multifunktionsgeräte)

KT 4 Wechselsprechtechnik (Redundanz-Konzept für Störfälle, z. B. Mobiltelefonie, Zugangslösungen, z. B. Klingel- und Sprechanlagen für geschlossene Bereiche)

6.5.3 Versorgungstechnik

VT 1 Energieversorgung, Elektroversorgung (Netzversorgung (Einspeisung), Ersatzversorgung, Notstromdiesel)

VT 2 Wasserversorgung (Frisch- und Abwasser von hoher Bedeutung für Sterilprozesse, Hygiene und Entsorgung)

VT 3 sanitäre Anlagen

VT 4 Wärme/Heizung (z.B. Patienten- und Untersuchungsräume)

VT 5 Klima/Kühlung (z.B. OPs, technische Anlagen)

VT 6 Lichttechnische Systeme

VT 7 Gase (u.a. Beatmung, MRT u.ä.)

VT 8 Transportanlagen (primär Fahrstuhl-Anlagen)

VT 9 Versorgung und Entsorgung

VT 10 Videoüberwachung (Schnittstelle: IT)

VT 11 Zugangs- und Schließsysteme

VT 12 Zufahrts- und Schrankensysteme

VT 13 Gebäudeleittechnik, Gebäudeautomatisierungstechnik

VT 14 Bau und Instandhaltung

6.5.4 Medizintechnik/-produkte

MED 1 Einsatz von Patientendatenmanagementsystemen (PDMS)

MED 2 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

-
- MED 3 Telemedizinische Systeme / Telemetriesysteme zur Überwachung wichtiger Parameter bei Erhöhung von Freiheitsgraden in der Patientenversorgung
 - MED 4 patientengebundene Alarmierungssysteme (häufig gekoppelt mit IT-Komponenten, im Einzelfall auch Teil der Kommunikationstechnik)
 - MED 5 Steuerung der Instandhaltung medizintechnischer Anlagen für Diagnostik und Therapie (herstellerbasierte Leistungserbringung)
 - MED 6 Instandhaltung und Austausch von Einzelgeräten (z. B. "Kleingeräte", wie Infusionspumpen o.ä.)

6.5.5 kritische branchenspezifische Anwendungssysteme

- KBA 1 Krankenhausinformationssystem (KIS)
- KBA 2 Laborinformationssystem (LIS)
- KBA 3 Radiologieinformationssystem (RIS)
- KBA 4 Picture Archive and Communication System (PACS)
- KBA 5 Dokumenten-Management-System / Enterprise-Content-Management
- KBA 6 OP-Planungssystem
- KBA 7 Transportlogistik (Patienten-, Proben-, Speisen- und Arzneimitteltransporte)
- KBA 8 Register (z. B. für Tumorerkrankungen)
- KBA 9 Qualitätssicherung (z. B. für Hygiene, Transfusionsmedizin oder Point-of-Care-Testing (POCT))
- KBA 10 Spezialisierte Anwendungen im klinischen Umfeld

7 Angemessene Maßnahmen zur Umsetzung

Die nachfolgend genannten Maßnahmenempfehlungen richten sich in ihrer Struktur nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik⁵ und orientieren sich an Anhang A der ISO 27001. Sie sollen zur Erreichung der definierten Schutzziele beitragen und im Ergebnis eine sichere und resiliente IT-Infrastruktur zur Sicherstellung der stationären medizinischen Versorgung gewährleisten. Die Maßnahmen richten sich insbesondere an die im Dokument „04 Gefährdungskatalog“ beschriebenen branchenspezifischen Systeme.

Im Einzelfall kann die Berücksichtigung weiterer Systeme für die Sicherstellung des störungsfreien und sicheren Betriebs im Krankenhaus notwendig werden, wenn dies nach erfolgter Risikobetrachtung entsprechend der Vorgaben im Dokument „02 Risikomanagement“ geboten erscheint. Die konkrete Ausgestaltung der Maßnahmenempfehlungen sollte stets der jeweiligen Situation angemessen (risikoorientiert) erfolgen.

Die Formulierung der Maßnahmenempfehlungen erfordert einen gewissen Abstraktionsgrad, um sowohl bestehende Lösungen zur Umsetzung von IT-Sicherheit integrieren zu können, als auch der heterogenen Systemlandschaft in den Krankenhäusern Rechnung zu tragen. Gleichzeitig besteht der Anspruch, die Beschreibung der Maßnahmen hinreichend konkret für eine nachvollziehbare Umsetzung und Prüfung zu fassen. In die regelmäßige Revision des vorliegenden B3S sollen insbesondere hierzu Erfahrungen aus der Praxis aufgenommen werden.

Die zeitgleiche Umsetzung aller vorgeschlagenen Maßnahmen wird in den meisten Fällen weder unter organisatorischen, personellen noch wirtschaftlichen Aspekten realisierbar sein. Der Prozess des Sicherheitsmanagements ist vielmehr - einer Priorisierung folgend - iterativ zu verfeinern und soll im Ergebnis fester Bestandteil aller relevanten, die stationäre Versorgung betreffenden Prozesse im Krankenhaus werden.

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID sowie mit, in Anlehnung an die dem RFC 2119 entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworten MUSS, SOLL, SOLLTE, KANN gekennzeichnet.

„MUSS“: Die Einhaltung der Anforderung ist zwingend für die Umsetzung des B3S.

„SOLL“: Die Einhaltung der Anforderung wird empfohlen, ist jedoch nicht zwingend für die Umsetzung des B3S, sofern hierdurch die Informationssicherheit nicht gefährdet wird. Die Nicht-Umsetzung ist nachvollziehbar zu begründen.

„SOLLTE“: Die Einhaltung der Anforderung wird empfohlen, ist jedoch nicht zwingend für die Umsetzung des B3S.

⁵ Orientierungshilfe „Branchenspezifische Sicherheitsstandards“, Version 1.0

„KANN“: Die Beschreibung eines zulässigen Weges, wie eine Anforderung eingehalten werden kann.

7.1 Informationssicherheitsmanagementsystem (ISMS)

Kern der Umsetzung des vorliegenden B3S ist der Aufbau und Betrieb eines Informationssicherheitsmanagementsystems (ISMS) für den B3S-Anwendungsbereich. Die hier aufgeführten Maßnahmen orientieren sich dabei eng an den Vorgaben der ISO 27001 sowie den zusätzlichen Anforderungen der ISO 27799. In der Gesamtschau sind alle für den B3S-Anwendungsbereich relevanten Strukturen, Prozesse und Abläufe für Planung, Steuerung und Kontrolle des ISMS zu erheben und geeignet zu dokumentieren. Für den B3S-Anwendungsbereich ist eine geeignete Informationssicherheitsstruktur aufzubauen sowie Richtlinien, Konzepte und Verfahren zu erarbeiten, welche die Ausgestaltung der Informationssicherheit schriftlich fixieren. Dies schließt eine geeignete Dokumentenlenkung sowie Aussagen zur Aufbewahrung und Archivierung ein. Regelmäßige Schulungsmaßnahmen (Awareness) der Mitarbeiter zu den geltenden Vorgaben und ein geeignetes Controlling der Umsetzung der Vorgaben sind ebenfalls obligatorisch. Ferner sind die Richtlinien, Konzepte und Vorgaben regelmäßig hinsichtlich ihrer Aktualität zu überprüfen.

7.2 Organisation der Informationssicherheit

Der Betreiber hat die notwendigen organisatorischen und technischen Voraussetzungen für die sachgerechte und angemessene Umsetzung von Informationssicherheit im Krankenhaus zu schaffen. Entscheidend sind hierbei vor allem auch die eindeutige und widerspruchsfreie Zuweisung von Zuständigkeiten sowie die fachliche Eignung der hierfür verantwortlichen Personen. Miteinander in Konflikt stehende Aufgaben und Verantwortungsbereiche müssen angemessen voneinander getrennt definiert werden. Die Zuweisung miteinander in Konflikt stehender Aufgaben und Verantwortlichkeiten an eine Person ist zu vermeiden. Die Erreichung der Schutzziele muss unabhängig von der gewählten Organisationsstruktur gewährleistet werden.

Die den betreffenden Personen / Mitarbeitern zugewiesenen Verantwortungsbereiche sind nachvollziehbar zu dokumentieren, die hierzu gehörenden Informationswerte und Prozesse sind mit Blick auf die Informationssicherheit zu definieren. Dies umfasst auch die Koordination und Kontrolle der Informationssicherheitsaspekte in Lieferantenbeziehungen (z. B. im Bereich der Medizintechnik). Personen mit Verantwortung für Informationssicherheit dürfen Sicherheitsaufgaben im Rahmen ihrer Weisungsbefugnis an andere delegieren. Sie bleiben verantwortlich und müssen in angemessener Form feststellen, ob die übertragenen Aufgaben ordnungsgemäß durchgeführt wurden. Die nachfolgend beschriebenen Rollen haben sich dabei für ein funktionierendes Informationssicherheitsmanagement als notwendig und sinnvoll erwiesen.

7.2.1 Geschäftsführung / Leitung

Die Geschäftsführung trägt die Gesamtverantwortung für das Informationssicherheitsmanagement. Sie stellt durch ihr Handeln sicher, dass ein wirksames Informati-

Informationssicherheitsmanagementsystem aufgebaut und betrieben wird, etwa indem sie entsprechende Ziele der Informationssicherheit in Form von Leit- und Richtlinien bekanntgibt und durchsetzt, Rollen und Verantwortlichkeiten zuweist, notwendige Ressourcen bereitstellt und sowohl im Innen- als auch Außenverhältnis die Bedeutung des Informationssicherheitsmanagements glaubhaft und nachhaltig vermittelt.



Abbildung 4 Management der Informationssicherheit

Die Benennung und Bestellung eines Informationssicherheitsbeauftragten (ISB) zur Organisation des Aufbaus, der Durchführung und Überwachung des Informationssicherheitsmanagements wird dabei als notwendig angesehen. Der Gesetzgeber hat (bisher) die Funktion, Aufgaben und Zuständigkeiten eines Informationssicherheitsbeauftragten im Gegensatz zum Datenschutzbeauftragten nicht festgelegt. Aufgrund ähnlicher Anforderungen im Hinblick auf Kontrollpflichten und Weisungsfreiheit sollte der ISB in vergleichbarer Weise in der Organisation verankert werden.

Beschreibung der im Zusammenhang mit dem Informationssicherheitsmanagement zu erledigenden Aufgaben für alle Rollen

Benennung eines Informationssicherheitsbeauftragten notwendig.

Die Geschäftsführung ist weiterhin verantwortlich für die Überprüfung des Informationssicherheitsmanagements. Die Einrichtung angemessener Kontrollen kann delegiert werden, z. B. an die in den Funktionsbereichen und Funktionsstellen für Informationssicherheit Verantwortlichen. Für die Geschäftsführung bestehen die folgenden Anforderungen und Verantwortlichkeiten:

Siehe ISO 27002, 6.1.1 Informationssicherheitsrollen und -verantwortlichkeiten

ANF-MN 1 Die Geschäftsführung ist verantwortlich für Bekanntgabe und Durchsetzung entsprechender Ziele der Informationssicherheit (z. B. Informationssicherheitsleitlinie etc.).

ANF-MN 2 Die Geschäftsführung ist verantwortlich für die Zuweisung von Rollen und Verantwortlichkeiten sowie der Bereitstellung von notwendigen organisatorischen, personellen und finanziellen Ressourcen zur Umsetzung des Informationssicherheitsmanagements im Krankenhaus. Diese müssen geeignet sein, die Durchsetzung der hierfür notwendigen Maßnahmen zu gewährleisten.

ANF-MN 3 Die Geschäftsführung ist verantwortlich für die glaubhafte und nachhal-

tige Vermittlung der Bedeutung der Informationssicherheit gegenüber Mitarbeitern, Patienten und Dritten (z. B. Aufsichtsbehörden etc.).

- ANF-MN 4 Die Geschäftsführung ist verantwortlich für die Überprüfung eines wirksamen Informationssicherheitsmanagements durch fortlaufende Kontrolle der Zielerreichung.
- ANF-MN 5 Die Geschäftsführung ist verantwortlich für die Sicherstellung eines angemessenen Qualifikationsniveaus (erforderliche Kenntnisse und Erfahrungen) der Mitarbeiter entsprechend ihrer Aufgaben, Kompetenzen und Verantwortlichkeiten.
- ANF-MN 6 Die Geschäftsführung ist verantwortlich für die Sicherstellung der Trennung widersprüchlicher Aufgaben und Verantwortungsbereiche, um das Risiko von Interessenkonflikten sowie unautorisierter oder versehentlicher Änderungen oder Missbrauch von Unternehmenswerten zu minimieren (Beispiel: Informationssicherheitsbeauftragter und IT-Leiter in einer Person birgt Interessenskonflikte).

7.2.2 Beauftragter für Informationssicherheit (ISB, CISO)

- ANF-MN 7 Es MUSS mindestens eine Person als Beauftragter für die Informationssicherheit (Manager-Informationssicherheit, Informationssicherheitsbeauftragter, Chief Information Security Officer) im B3S-Awendungsbereich benannt werden.
- ANF-MN 8 Der Informationssicherheitsbeauftragte SOLLTE der Krankenhausführung direkt unterstellt werden. Er steuert die Umsetzung und Weiterentwicklung des Informationssicherheitsmanagementprozesses.
- ANF-MN 9 Der Informationssicherheitsbeauftragte MUSS durch die Krankenhausleitung, sowie durch die Mitarbeiter ausreichend unterstützt und frühzeitig in alle relevanten Projekte (z. B. auch Beschaffungsprozesse) und Prozesse eingebunden werden, um schon in der Planungsphase sicherheitsrelevante Aspekte berücksichtigen zu können. Dies gilt insbesondere bei der Einführung neuer Technologien.
- ANF-MN 10 Der Informationssicherheitsbeauftragte SOLLTE bei der Organisation des Aufbaus, der Durchführung und Überwachung der für die Sicherstellung der Informationssicherheit notwendigen Maßnahmen durch weitere (interne bzw. externe) Mitarbeiter unterstützt werden (z. B. Bildung eines Informationssicherheitsmanagement-Teams).
- ANF-MN 11 Die definierten Ziele zum Informationssicherheitsmanagement MÜSSEN mit dem Management abgestimmt werden.
- ANF-MN 12 Aufgrund der engen Verzahnung von Informationssicherheit und Datenschutz SOLLTE die Zusammenarbeit des Informationssicherheitsbe-

auftragten mit dem Datenschutzbeauftragten und der IT-Leitung unterstützt werden. Die Definition und Umsetzung der technisch-organisatorischen Maßnahmen (TOM) des Datenschutzes SOLLTE mit dem Datenschutzbeauftragten abgestimmt werden.

- ANF-MN 13 Der Informationssicherheitsbeauftragte ist verantwortlich für Planung, Umsetzung und Steuerung des von der Geschäftsführung initiierten Informationssicherheitsprozesses.
- ANF-MN 14 Der Informationssicherheitsbeauftragte initiiert die Erarbeitung von konkreten Verbesserungsvorschlägen zur Erreichung des angestrebten Informationssicherheitsniveaus durch die operativ verantwortlichen Organisationseinheiten.
- ANF-MN 15 Der Informationssicherheitsbeauftragte ist verantwortlich für die Erarbeitung und jährliche Überprüfung sowie Anpassung der Informationssicherheitsleitlinie.
- ANF-MN 16 Der Informationssicherheitsbeauftragte MUSS die Unternehmensleitung in zentralen Fragen der Informationssicherheit unterstützen.
- ANF-MN 17 Der Informationssicherheitsbeauftragte ist verantwortlich für die Untersuchung informationssicherheitsrelevanter Ereignisse.
- ANF-MN 18 Der Informationssicherheitsbeauftragte ist verantwortlich für Etablierung und Steuerung von Sensibilisierungs- und Schulungsmaßnahmen der Mitarbeiter.
- ANF-MN 19 Der Informationssicherheitsbeauftragte ist Ansprechpartner bei Projekten mit Auswirkungen auf die Informationsverarbeitung. Er MUSS bei der Einführung neuer Software und IT-Systeme (ggf. auch Medizinprodukte) einbezogen werden, um sicherzustellen, dass informationssicherheitsrelevante Aspekte ausreichend beachtet werden.
- ANF-MN 20 Der Informationssicherheitsbeauftragte erstattet der Unternehmensleitung regelmäßig Bericht über den aktuellen Stand der Informationssicherheit im Unternehmen, insbesondere über Risiken und Sicherheitsvorfälle.
- ANF-MN 21 Der Informationssicherheitsbeauftragte ist zentraler Ansprechpartner für Informationssicherheit für Mitarbeiter und Dritte.

siehe Dokument 02 Risikomanagement: Risiko-Berichterstattung

Hinweis: Damit diese Personen Ihre Verantwortung im Bereich Informationssicherheit angemessen ausfüllen, sollten diese Verantwortlichen im Sicherheitsmanagement relevante Berufserfahrung und Kenntnisse zum Betrieb von Informationssicherheits-Managementsystemen nach ISO 27001 nachweisen können. Die regelmäßige Aktualisierung dieser Kenntnisse im Rahmen von Schulungen wird empfohlen.

7.2.3 Prozess- /Anwendungsverantwortlicher

ANF-MN 22 Für jede Abteilung bzw. jeden Prozess im Geltungsbereich SOLL ein Verantwortlicher bestimmt werden, der die Verantwortung für den jeweiligen Prozess bzw. Anwendung sowie für die zugehörigen Informationen (Daten) trägt. Sollte ein Prozessverantwortlicher nicht benannt werden können, so gilt die Geschäftsführung als prozessverantwortlich.

ANF-MN 23 Der Prozess-/Anwendungsverantwortliche MUSS im eigenen Verantwortungsbereich entsprechende technische und organisatorische Maßnahmen planen und umsetzen. Die Umsetzung der erarbeiteten Informationssicherheitsrichtlinien MUSS im Einklang mit dem Informationssicherheitsbeauftragten (ISB) erfolgen.

ANF-MN 24 Der Prozess-/Anwendungsverantwortliche MUSS für eine Einstufung der Schutzbedarfe/Kritikalität der verantworteten Prozesse/Anwendungen hinsichtlich der Schutzziele Verfügbarkeit, Vertraulichkeit, Authentizität und Integrität sowie mit Blick auf die Behandlungseffektivität und Patientensicherheit Sorge tragen. Die Schutzbedarfsfeststellung erfolgt in enger Abstimmung mit dem Informationssicherheitsmanagement (ISB).

ANF-MN 25 Der Prozess-/Anwendungsverantwortliche MUSS Maßnahmen, die aus seiner Sicht zur Verbesserung und Erhaltung der Informationssicherheit im eigenen Verantwortungsbereich ergriffen werden müssen, mit dem Informationssicherheitsbeauftragten abstimmen.

ANF-MN 26 Der Prozess-/Anwendungsverantwortliche MUSS Notfallpläne bzw. Notbetriebsbeschreibungen für die verantworteten Prozesse bzw. Anwendungen erstellen und regelmäßig aktualisieren.

ANF-MN 27 Der Prozess-/Anwendungsverantwortliche MUSS die Umsetzung des Informationssicherheitsrisikomanagements unterstützen durch:

- Analyse und, wenn möglich, quantitative Bewertung der von ihm verantworteten Informationssicherheitsrisiken, auch unter Beachtung des jeweiligen Schutzbedarfs hinsichtlich der Schutzziele (Verfügbarkeit, Vertraulichkeit, Authentizität und Integrität).
- Vorbereitung von Entscheidungen zur Behandlung der Informationssicherheitsrisiken.
- periodische Überprüfung der verantworteten Informationssicherheitsrisiken einschließlich der diesen Risiken zugeordneten Maßnahmen.

Hinweis: Prozesseigentümer können auch die Aufgaben der Anwendungseigentümer bzgl. der zugehörigen Anwendungen übernehmen. Umgekehrt können die Anwendungseigentümer auch die Aufgaben des Prozesseigentümers zum übergeordneten Prozess übernehmen.

7.3 Meldepflichten nach § 8b Absatz 4 BSI-Gesetz

- ANF-MN 28 Betreiber Kritischer Infrastrukturen MÜSSEN nach § 8b Absatz 4 BSI-Gesetz IT-Störungen melden, die zu einem Ausfall oder der Beeinträchtigung der Versorgungssicherheit geführt haben oder hätten führen können. Der Betreiber MUSS ein entsprechendes Meldeverfahren implementieren, welches die Identifikation, Analyse und Entscheidung über eingetretene Vorfälle, die meldepflichtig sind, ermöglicht. Hierzu KANN ein mehrstufiges System, welches eine Erst- und Folgemeldung erlaubt, angewandt werden.
- ANF-MN 29 Bei Eintreten eines meldepflichtigen Vorfalles MUSS das Ereignis ohne schuldhaftes Verzögern an das Melde- und Informationsportal (MIP) des BSI weitergegeben werden. Da im Falle einer Störung oft die Wiederherstellung der Daten und Sicherung der Weiterarbeit Priorität haben, KANN eine ausführliche Meldung zeitlich versetzt erfolgen, sofern dem BSI zuvor eine Erstmeldung übermittelt wurde. Für den Fall, dass eine Störung die digitale Übermittlung verhindert, KANN diese alternativ auch telefonisch vorgenommen werden.
- ANF-MN 30 Betreiber Kritischer Infrastrukturen MÜSSEN dem BSI eine Kontaktstelle benennen, die Meldungen des BSI zu Einschätzungen oder Hinweisen die Informationssicherheit betreffend entgegennimmt. Die durchgängige Erreichbarkeit der Kontaktstelle sowie eine zeitnahe Bearbeitung der dort eingegangenen Meldungen MUSS angemessen sichergestellt werden.

Hinweis: Zu meldepflichtigen Störungen zählen nach derzeitiger Einschätzung des BSI außergewöhnliche Ausfälle und Beeinträchtigungen (IT-Störungen) der kritischen Dienstleistungen, welche nicht ohne nennenswerte Probleme mit den angewandten Maßnahmen abgewehrt werden können. Insbesondere neue, bisher nicht veröffentlichte Sicherheitslücken, unbekannte Schadprogramme, Spear-Phishing oder außergewöhnliche und unerwartete, technische Defekte mit IT-Bezug, z.B. nach erfolgten Updates, sollen an das BSI gemeldet werden.

7.4 Betriebliches Kontinuitätsmanagement

Zur Sicherstellung der vollstationären medizinischen Versorgung („kritische Versorgungsdienstleistung des Sektors“) werden bestimmte Systeme, Komponenten und Prozesse benötigt, die nachfolgend als „kritische Dienstleistung (kDL)“ bezeichnet werden. Diese können im Einzelfall unterschiedlich ausgeprägt sein. Damit nach einer Störung oder dem Ausfall dieser kDL eine schnellstmögliche Wiederherstellung auf ein vordefiniertes Niveau erfolgen kann, sind entsprechende Maßnahmen vorzusehen. Wird ein betriebliches Kontinuitätsmanagement eingesetzt, so sollten die im B3S-Anwendungsbereich liegenden Systeme, Komponenten und Prozesse hierbei berücksichtigt werden.

ISO 27001 Standard, Abschnitt A.17

ISO 22301 Standard, Abschnitte 4.1, 4.3, 5.3, 6.2 und 9.1.1

- ANF-MN 31 Innerhalb des B3S-Anwendungsbereichs MUSS die Aufrechterhaltung

der kritischen Dienstleistungen (kDL) im Störungs- sowie im Notfall sichergestellt und geeignete Maßnahmen zur schnellstmöglichen Wiederherstellung vorgesehen werden. Hierzu KANN ein betriebliches Kontinuitätsmanagementsystem eingesetzt werden.

- ANF-MN 32 Mit der Umsetzung eines betrieblichen Kontinuitätsmanagements KÖNNEN die strategischen Ziele der Organisation verfolgt werden. Die sich hieraus ergebenden spezifischen Ziele SOLLTEN in einer Leitlinie zum betrieblichen Kontinuitätsmanagement vorgegeben werden.
- ANF-MN 33 Wird ein „Betriebliches Kontinuitätsmanagement-System (BKMS)“, z.B. nach ISO 22301, betrieben, SOLLTE zur Aufrechterhaltung der Funktionsfähigkeit der kDL der B3S-Anwendungsbereich hierbei berücksichtigt werden.
- ANF-MN 34 Wird ein BKMS zur Absicherung der kDL betrieben, MUSS dieses von der Geschäftsführung freigegeben werden.
- ANF-MN 35 Wird ein betriebliches Kontinuitätsmanagement für den B3S-Anwendungsbereich vorgesehen, SOLLTE dies in die übergeordnete (organisationsweite) Notfallorganisation integriert werden.
- ANF-MN 36 Es SOLLTE ein Verantwortlicher für die Festlegung der Zielsetzung für das gesamte betriebliche Kontinuitätsmanagement im B3S-Anwendungsbereich und der Methode für die Bewertung der Erreichung dieser Zielsetzung benannt werden.
- ANF-MN 37 Wird ein betriebliches Kontinuitätsmanagements im B3S-Anwendungsbereich eingesetzt, SOLLTE regelmäßig, mindestens jährlich, die Zielerreichung überprüft werden.
- ANF-MN 38 Die Organisation MUSS diejenigen kDL mit hohem Risiko identifizieren und dokumentieren. Für jede dieser kDL MUSS folgendes dokumentiert werden:
- a. eine kurze Beschreibung der kritischen Dienstleistung
 - b. eine Begründung, warum der Prozess ein zentraler Prozess bzw. ein Prozess mit hohem Risiko ist (im Rahmen einer Auswirkungsanalyse sind mögliche Bedrohungen für die kDL im B3S-Anwendungsbereich zu identifizieren und die daraus möglicherweise resultierenden Auswirkungen auf den Geschäftsbetrieb zu bewerten)
 - c. wer für die kDL verantwortlich ist (kDL-Verantwortlicher)
 - d. wie lange ein Ausfall der kDL toleriert werden kann (Maximal tolerierbare Ausfallzeit – MTA). Diese Festlegung SOLL als Grundlage für die im Risikomanagement vorgesehene Kritikalitätsbewertung genutzt werden.

-
- ANF-MN 39 Für diejenigen kDL mit hohem Schadenspotenzial MÜSSEN Geschäftsfortführungspläne verfügbar sein, die Notfall- und Wiederanlaufpläne umfassen, z. B. als „Notfallhandbuch“.
- ANF-MN 40 Die Notfallpläne MÜSSEN allen beteiligten Mitarbeitern zur Verfügung stehen. Sie SOLLTEN Lieferanten, Dienstleistern und Dritten ebenfalls zur Verfügung gestellt werden, wenn dies im Rahmen der Notfallmaßnahmen erforderlich oder sinnvoll ist.
- ANF-MN 41 Die im Notfall zu verwendenden Kommunikationswege (Alarmierungspläne) MÜSSEN festgelegt sein.
- ANF-MN 42 Alarmierungspläne SOLLTEN durch alle beteiligten Mitarbeiter nachweislich zur Kenntnis genommen werden und diesen stets zur Verfügung stehen. Sie SOLLTEN Lieferanten, Dienstleistern und ebenfalls zur Verfügung gestellt werden, wenn dies im Rahmen der Alarmierungspläne erforderlich oder sinnvoll ist.
- ANF-MN 43 Es SOLLTEN regelmäßig Notfallübungen durchgeführt werden. Diese MÜSSEN an der Kritikalität der Prozesse und Systeme ausgerichtet sein.

Notfallpläne müssen gewährleisten, dass im Notfall zeitnah organisatorische, technische oder papierbasierte Ersatzlösungen zur Verfügung stehen. Wiederanlaufpläne müssen innerhalb eines angemessenen Zeitraums die Rückkehr zum Normalbetrieb ermöglichen.

7.5 Asset Management

Unternehmenswerte, die mit Informationswerten oder informationsverarbeitenden Einrichtungen in Zusammenhang stehen, sollten als Grundlage für Risikoanalysen, der Einstufung ihres Schutzbedarfes und der Ableitung von Zugriffsrechten inventarisiert werden. Die grundsätzlichen Anforderungen an ein Risikomanagement werden im Teildokument „02 Risikomanagement“ beschrieben.

A.8.1.1-4
A.8.2.1-3

- ANF-MN 44 Der Lebenszyklus von Werten/Wertegruppen („Assets“) und der Umgang mit diesen Werten muss definiert sein, indem Regelungen zur Inventarisierung, Klassifizierung, Nutzung, Zugang, Änderung, Löschung und Rückgabe aufgestellt und umgesetzt sind.
- ANF-MN 45 Informationswerte und deren Kritikalität für die kDL MÜSSEN in einem Wertinventarverzeichnis dokumentiert werden.
- ANF-MN 46 Abhängigkeiten untereinander MÜSSEN innerhalb der Inventarisierung der Werte erhoben und dokumentiert werden. Dabei MUSS die logische Kette vom Prozess über die Anwendung, dem hierfür verwendeten IT-System und der zugrunde liegenden IT-Infrastruktur berücksichtigt werden.
- ANF-MN 47 Gleichartige Werte SOLLEN innerhalb der Inventarisierung der Werte gruppiert werden.
- ANF-MN 48 Das Wertinventarverzeichnis der Informationswerte, die im Behandlungskontext für die kDL notwendig sind, SOLLTE aktuell gehalten und

BSI-Standard 100-2, Kapitel 4.2 Strukturanalyse

mit anderen Inventarverzeichnissen abgestimmt werden (z. B. IT-Asset-Inventarverzeichnis).

- ANF-MN 49 Gesundheitsdaten und diesbezügliche Werte SOLLTEN mit Blick auf den besonderen Schutzbedarf dieser Informationen innerhalb des Inventarverzeichnisses entsprechend ausgewiesen und ggf. gesondert behandelt werden (z. B. besondere Vorgaben zur Speicherung von Gesundheitsdaten auf mobilen Datenträgern etc.).
- ANF-MN 50 Soweit im Rahmen des Asset-Managements Medizingeräte, welche Gesundheitsdaten verarbeiten, berücksichtigt werden, MÜSSEN diese eindeutig identifizierbar sein, da sie besondere Sicherheitsmaßnahmen in Bezug auf ihre Arbeitsumgebung erfordern können.
- ANF-MN 51 Die Anforderungen an die Nutzung von Informationswerten zur Dokumentation des Umlaufs von Medikamenten (z. B. Systeme zur Arzneimitteltherapiesicherheitsprüfung, Arzneimitteldatenbanken und -Verifikationssysteme, Abgabesysteme) SOLLTEN anhand eines Regelwerkes dokumentiert und festgelegt werden, um die Erreichung der Schutzziele, insbesondere der Integrität und Verfügbarkeit für diese Informationswerte zu gewährleisten.
- ANF-MN 52 Ist zur Erbringung der kDL die Weitergabe von Gesundheitsdaten an Mitarbeiter oder Dritte notwendig (z. B. auf mobilen Datenträgern, elektronische Datenübermittlung), MÜSSEN die Schutzziele der IT-Sicherheit eingehalten werden. Hierzu SOLLTEN geeignete technische und organisatorische Maßnahmen vorgesehen werden, die eine notwendige Weitergabe von Gesundheitsdaten ermöglichen und gleichzeitig eine unerlaubte Weitergabe von Informationen verhindern.
- ANF-MN 53 Gesundheitsdaten MÜSSEN besonders geschützt und angemessen eingestuft werden. Dies gilt insbesondere für mobile Datenträger, die z. B. durch geeignete Verschlüsselung vor Offenbarung von gespeicherten Gesundheitsdaten (z. B. bei Verlust) geschützt werden müssen.

7.6 Robuste/resiliente Architektur

Geräte und Betriebsmittel sind vor Ausfällen schützen und Verfügbarkeitsanforderungen durch angemessene Redundanz zu gewährleisten.

- ANF-MN 54 IT-Systeme und Medizingeräte, die relevant für die Versorgungssicherheit sind, MÜSSEN vor Ausfällen externer Versorgungsdienste (z. B. Stromausversorger, Wasserversorger), welche die eigene kDL beeinträchtigen können, angemessen geschützt werden.

- ANF-MN 55 Die Einhaltung der für den ordnungsgemäßen Betrieb herstellerseitig definierten Umgebungsanforderungen (z. B. Betriebstemperatur etc.) für

Medizingeräte und IT-Systeme, die im Rahmen der kDL eingesetzt werden, MUSS durch angemessene Verfahren (z. B. Klimatechnik) gewährleistet werden.

- ANF-MN 56 Beeinträchtigungen infolge von Wechselwirkungen zwischen Infrastruktureinrichtungen für die kDL und Versorgungseinrichtungen (z. B. Leitungsnetze für Wasser, Strom mit IT-Systemen, kommunikationstechnischen Einrichtungen oder Medizingeräten), SOLLTEN durch angemessene Maßnahmen (z. B. Schutz vor physischen Störungen und Beschädigungen, Vermeidung von potenziellen baulichen Gefahren) vermieden werden.
- ANF-MN 57 IT-Netzwerke und Kommunikationsleitungen SOLLEN in Bereichen mit sensiblen IT-Systemen, in denen hohe Emissionen durch Medizingeräte auftreten können, ausreichend abgeschirmt werden.
- ANF-MN 58 Für die Versorgungssicherheit relevante IT-Systeme und Komponenten, welche direkt oder indirekt und maßgeblich an der kDL beteiligt sind, MÜSSEN angemessen redundant ausgelegt sein. Soweit dies nicht durch die Vorhaltung redundanter Systeme möglich ist (z. B. bei medizinischen Großgeräten), sind angemessene organisatorische und technische Ersatzverfahren vorzusehen.
- ANF-MN 59 Die angemessene Robustheit der Architektur und Funktionalität von Redundanzen sowie Ersatzverfahren SOLLTEN regelmäßig, mindestens jährlich, bewertet werden.

7.7 Physische Sicherheit

Der physische Schutz von Gebäuden, in denen Kernsysteme der kDL untergebracht sind (z. B. Rechenzentrum, medizinische Behandlungsräume bis hin zu Operationseinheiten in Containerbauweise) sollte bereits bei der Konzeption, über die Einrichtung bis hin zur Nutzung Teil des Informationssicherheitskonzeptes sein. Die Integration bestehender Gebäudestrukturen stellt hier eine besondere Herausforderung dar.

A.11.1.1-6

INF.1: Allgemeines Gebäude

- ANF-MN 60 Informationssysteme, die unternehmenskritische Daten verarbeiten, SOLLTEN angemessen vor physischen Schäden (z. B. Hochwasserschutz, wasserführende Leitungen etc.) geschützt werden.
- ANF-MN 61 Der Zutritt zu zentralen Infrastrukturdiensten und -Komponenten (insbesondere Server bzw. Datenbanken), die für die kDL notwendig sind, darf nur durch autorisiertes Personal erfolgen. Es MUSS ein angemessener Zutrittsschutz eingerichtet werden, der eine angemessene Protokollierung mit einschließt.
- ANF-MN 62 Ein Zonenkonzept für unterschiedliche Sicherheitsbereiche SOLLTE entlang der Anforderungen an Kritikalität und Schutzwürdigkeit der verarbeiteten Informationen konzipiert und angewendet werden.

ANF-MN 63 In öffentlich zugänglichen Bereichen des Krankenhaus befindliche IT-Systeme MÜSSEN angemessen durch technische oder organisatorische Maßnahmen vor unbefugtem Zugriff geschützt werden.

7.8 Personelle und organisatorische Sicherheit

Mitarbeiter und Auftragnehmer müssen ihre Verantwortlichkeiten in Bezug auf Informationssicherheit kennen, verstehen und für die jeweilige Tätigkeit geeignet sein. Das Sicherheitskonzept sollte die Phasen der Bewerbung, Einstellung, Sensibilisierung und Beschäftigungsbeendigung begleiten.

ANF-MN 64 Mitarbeiter MÜSSEN nachweislich auf die Geheimhaltung sowie die Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen verpflichtet werden. Den Mitarbeitern MÜSSEN die rechtlichen Rahmenbedingungen ihrer Tätigkeit bekannt sein.

ANF-MN 65 Hintergrundüberprüfungen von Einstellungskandidaten SOLLTEN bei Berufstätigkeiten mit Zulassungserfordernis (z. B. Ärzte) die Prüfung dieser beruflichen Qualifikation einschließen (z. B. Approbationsurkunde).

ANF-MN 66 Bei Mitarbeitern, Auftragnehmern oder freiwilligen Helfern, die (voraussichtlich) Gesundheitsdaten verarbeiten, SOLLTEN zum Zeitpunkt der Bewerbung mindestens die Identität, aktuelle Adresse und frühere Beschäftigungen erfasst werden. Kommt ein Beschäftigungsverhältnis nicht zustande, sind diese Informationen entsprechend der gesetzlichen Fristen zu löschen.

ANF-MN 67 Beschäftigte, die für Aufgaben mit Bezug zur Informationssicherheit eingestellt werden, MÜSSEN über die für die Ausübung dieser Funktion notwendigen Kompetenzen verfügen. Fehlende Kompetenzen sind zeitnah durch Schulungen sicherzustellen.

ANF-MN 68 Bewerber für kritische Positionen mit Bezug zur Informationssicherheit (z. B. IT-Administratoren) SOLLTEN einer Sicherheitsüberprüfung (z. B. durch Vorlage eines polizeilichen Führungszeugnisses) unterzogen werden.

ANF-MN 69 Bei Beschäftigten, die Gesundheitsdaten verarbeiten oder sicherheitsbezogene Rollen/Verantwortlichkeiten ausüben, SOLLTEN in deren Stellenbeschreibungen die sicherheitsrelevanten Tätigkeiten explizit beschrieben und ein Hinweis auf eine ggf. notwendige Sicherheitsüberprüfung aufgenommen werden.

ANF-MN 70 Beschäftigte oder Auftragnehmer MÜSSEN dazu verpflichtet werden, Verstöße gegen die Informationssicherheit und den Datenschutz zu melden.

ANF-MN 71 Alle Beschäftigte und ggf. involvierte Dritte wie Auftragsnehmer,

A.7.1.1-2
A.7.2.1-3
A.7.3.1

Die Einforderung eines polizeilichen Führungszeugnisses kann sinnvoll sein. Im Falle pädiatrischer medizinischer Versorgung sogar eines erweiterten Führungszeugnisses.

Wissenschaftler, Studenten und freiwillige Helfer, die Gesundheitsdaten verarbeiten, MÜSSEN zu Beginn ihrer Tätigkeit hinsichtlich der gültigen Informationssicherheitsrichtlinien informiert werden. Sie SOLLTEN zu möglichen disziplinarischen Maßnahmen im Falle eines Verstoßes geschult und über regelmäßige Aktualisierungen zu den Informationssicherheitsrichtlinien und –maßnahmen informiert werden.

ANF-MN 72 Die nach ANF-MN 71 festgelegten disziplinarische Maßnahmen MÜSSEN im Einklang mit gesetzlichen Bestimmungen stehen und SOLLTEN den, zwischen Vertretern der Arbeitnehmer und Aufsichtsbehörden bzw. Einrichtungen der Selbstverwaltung im Gesundheitswesen getroffenen, Vereinbarungen entsprechen.

ANF-MN 73 Zur Sensibilisierung und Schaffung eines Informationssicherheitsbewusstseins SOLLEN regelmäßig (mindestens jährlich) IT-Sicherheitsschulungen der Mitarbeiter und gegebenenfalls im Informationsverbund tätigen Dienstleistern durchgeführt und entsprechende Schulungsmaterialien angeboten werden.

ANF-MN 74 Nutzer- und aufgabenorientierte Schulungs- und Sensibilisierungsmaßnahmen SOLLTEN in einem übergreifenden Konzept geplant werden.

7.9 Vorfallerkennung und Behandlung

Informationssicherheitsvorfälle sollen möglichst zuverlässig erkannt, konsistent behandelt und im Rahmen der gesetzlichen Vorgaben an die zuständigen Stellen gemeldet werden. Die hierbei gewonnenen Erkenntnisse sollen helfen, die Auswirkungen und Eintrittswahrscheinlichkeiten zukünftiger Vorfälle zu verringern. Der rechtzeitigen und zweckmäßigen Reaktion bei eingetretenen Informationssicherheitsvorfällen kommt dabei eine besondere Bedeutung zu.

A.16.1.1-7

ANF-MN 75 Es MÜSSEN Aufgaben, Verfahren und Verantwortlichkeiten zum Umgang mit Informationssicherheitsvorfällen festgelegt werden (z. B. im Rahmen von Richtlinien). Dies betrifft insbesondere:

- a. Verfahren zur Beobachtung, Identifikation, Analyse und Beurteilung von Informationssicherheitsvorfällen
- b. Dokumentation durchzuführender Maßnahmen, Verantwortlichkeiten und Handlungsanweisungen im Falle eingetretener Sicherheitsvorfälle
- c. Informationen über einen Sicherheitsvorfall an betroffene Personen und ggf. öffentlichen Stellen im Rahmen von Meldeverpflichtungen (entsprechend der gesetzlichen Anforderungen)
- d. Sicherstellung einer nachfolgenden Berichterstattung an die Geschäftsführung

ANF-MN 76 Kritische IT-Systeme SOLLTEN über Logging- und Überwachungs-

funktionalitäten verfügen, die helfen, Informationssicherheitsvorfälle festzustellen und nachzuvollziehen.

- ANF-MN 77 Zur Unterstützung der juristischen Aufarbeitungen von Informationssicherheitsvorfällen KÖNNEN forensische Verfahren zur Beweissicherung (z. B. Protokolldaten, Log-Dateien etc.) implementiert werden. Dies SOLLTE in einer IT-Sicherheitsrichtlinie festgehalten werden.
- ANF-MN 78 Es SOLLTEN Verfahren zur Wiederherstellung der Integrität von Informationen nach einem Informationssicherheitsvorfall implementiert und getestet werden.
- ANF-MN 79 Es SOLLTE ein Verfahren zur Nachverfolgung der Behandlung von Informationssicherheitsvorfällen etabliert werden, welches auch Auskunftsmöglichkeiten zum Bearbeitungsstand für Betroffene enthält.
- ANF-MN 80 Um Krisen- und Notfallmanagementpläne zum geeigneten Zeitpunkt in Kraft zu setzen, SOLL vorab eine Priorisierung der bei einem Informationssicherheitsvorfall einzuleitenden Maßnahmen erfolgen.

7.10 Überprüfungen im laufenden Betrieb

Die Einhaltung von Sicherheitsrichtlinien ist auch im laufenden Versorgungsbetrieb des Krankenhauses zu überprüfen. Um Beeinträchtigungen der kDL durch entsprechende Kontrollen zu vermeiden, sollten die Anforderungen und Aktivitäten, insbesondere die betroffenen Systeme dieser Kontrollen, sorgfältig geplant und mit dem Geschäftsablauf abgestimmt werden. Insbesondere die nach § 8a BSIG vorgesehene Prüfung auf Umsetzung der für die Informationssicherheit erforderlichen Maßnahmen stellt hohe Anforderungen an die Beteiligten. Dabei muss vermieden werden, dass sich aus der Prüfung selbst Störungen für den Betrieb oder die kDL ergeben.

- ANF-MN 81 Die Wirksamkeit von Maßnahmen zur Verbesserung der Informationssicherheit MÜSSEN regelmäßig durch Audits überprüft werden. Hierbei SOLLTEN die im Dokument „06 Nachweis der Umsetzung“ und dessen Anhängen festgelegten Rahmenbedingungen (z. B. zum Prüfumfang, Prüfgrundlage) berücksichtigt werden.
- ANF-MN 82 Das Vorgehen bei Kontrollen, Prüfungen und Audits (auch intern) betriebsrelevanter Systeme sowie Audit-Feststellungen MUSS dokumentiert und ggf. in einen überprüfbaren Maßnahmenplan überführt werden.
- ANF-MN 83 Im Fall einer Kontrolle, Prüfung oder eines Audits MUSS sichergestellt werden, dass keine Änderungen von Daten oder Systemen vorgenommen werden können, die sich störend auf den Betrieb auswirken können (z. B. durch Spiegelung von Systemen).

- ANF-MN 84 Die Durchführung von externen Kontrollen, Prüfungen und Audits MUSS

vertraglich geregelt werden. Dabei MUSS der Sicherstellung der Versorgung (kDL) Priorität eingeräumt werden.

ANF-MN 85 Die unberechtigte Kenntnisnahme von Gesundheitsdaten durch Dritte (z. B. einen externen Prüfer) ist nicht zulässig und MUSS so weit als möglich ausgeschlossen werden. Datenschutzrisiken SOLLTEN darüber hinaus durch organisatorische Maßnahmen reduziert (z. B. auch durch Verpflichtungen entsprechend § 203 StGB).

ANF-MN 86 Die Durchführung der Kontrolle, Prüfung oder des Audits MUSS protokolliert werden.

ANF-MN 87 Nach einem erkannten Sicherheitsvorfall SOLLTE geprüft werden, welche Maßnahmen zur zukünftigen Vermeidung eines entsprechenden Sicherheitsvorfalls getroffen werden können.

ANF-MN 88 Im Rahmen eines Sicherheitsvorfalls ermittelte Schwachstellen SOLLEN entsprechend des definierten Maßnahmenplans zeitnah behoben werden.

7.11 Externe Informationsversorgung und Unterstützung

Bei der Erstellung des Rahmenwerks zur Umsetzung der Informationssicherheit sollten aktuelle Informationen und Entwicklungen berücksichtigt werden.

A.6.1.3-4
A.15.1.3

ANF-MN 89 Es SOLLTEN Informationswege etabliert werden, die den zeitnahen Austausch zu relevanten Informationen bzgl. der Informationssicherheit ermöglichen und damit dem Schutz der eingesetzten Systeme bzw. der Erkennung von Bedrohungen und Schwachstellen dienen können. Dies betrifft z. B. den Austausch mit

- a. hierfür zuständigen Behörden, wie z. B. dem BSI
- b. Informationssicherheitsdienstleistern, Herstellern von Antivirensoftware sowie weiteren Anbietern sicherheitsrelevanter Informationen

ANF-MN 90 Es SOLLTEN mögliche Unterstützungsanforderungen für den Fall eines akuten IT-Sicherheitsvorfalls geklärt werden, wenn die Erkennung, Beseitigung und Wiederanlaufplanung die Kapazitäten der eigenen Organisation (auch kurzzeitig) überschreiten können (z. B. CERTs).

7.12 Lieferanten, Dienstleister und Dritte

ANF-MN 91 Es MÜSSEN Richtlinien für den sicheren Umgang bei einem betrieblichen Datenaustausch mit externen Partnern festgelegt werden (siehe auch ANF-MN 52).

A.13.2.2
A.15.1.-2
A.15.2.1-2

ANF-MN 92 Es MUSS eine allgemeine Risikobewertung für den Zugang Dritter zu Gesundheitsdaten erfolgen, die auch die potenzielle Gefahr des unberechtigten Zugangs zu Systemen, Daten und Gesundheitsinfor-

tionen, die für die Aufrechterhaltung der kDL notwendig sind, durch Lieferanten, Dienstleister und Dritte berücksichtigt. Gegebenenfalls ist das bestehende Sicherheitsniveau und die hierfür verwendete Technik anzupassen.

ANF-MN 93 Im Umgang mit Lieferanten, Dienstleistern und Dritten SOLLEN zum Schutz der Unternehmenswerte Leitlinien zur Aufrechterhaltung der Anforderungen an die eigene Informationssicherheit erstellt, den Lieferanten bekanntgegeben und dies dokumentiert werden.

ANF-MN 94 Lieferanten, Dienstleistern und Dritten SOLL die Informationssicherheitsleitlinie und weitere relevante Regelungen der Informationssicherheit vor Beauftragung (z.B. als Vertragsbestandteil) verbindlich gemacht werden.

ANF-MN 95 Bei der Auslagerung wesentlicher Bereiche, Prozesse oder Systeme, die für die Erbringung der kritischen Dienstleistung notwendig sind, an externe Dienstleister MUSS die Absenkung des Sicherheitsniveaus vermieden werden. Der Auftraggeber MUSS die Einhaltung des für ihn gültigen Sicherheitsniveaus durch geeignete vertragliche und organisatorische Maßnahmen seitens des Dienstleisters sicherstellen.

7.13 Technische Informationssicherheit

7.13.1 Netz- und Systemmanagement (Netztrennung und Segmentierung)

A.13.1.3

ANF-MN 96 Soweit sinnvoll, MUSS eine Trennung verwendeter Netzwerke (Segmentierung) eingerichtet werden, um im Schadensfall mögliche Auswirkungen zu begrenzen. Die Segmentierung KANN sich dabei an den organisatorischen Strukturen des Krankenhauses orientieren und als „Zonenkonzept“ umgesetzt werden.

ANF-MN 97 Die Segmentierung der Netzwerke MUSS Informationssysteme, die für die kDL relevant sind, so in absicherbare Netzwerksegmente aufteilen (z. B. im Rahmen eines Zonenkonzepts), dass die jeweiligen Systeme gegenüber sich ausbreitenden Gefährdungen im Netzwerk möglichst geschützt sind.

7.13.2 Absicherung Fernzugriffe

ANF-MN 98 Fernzugriffe SOLLEN so eingerichtet/gekapselt werden, dass andere IT-Systeme im Informationsverbund, die nicht im Fernzugriffsfokus stehen, nicht negativ beeinflusst werden können.

ANF-MN 99 Fernwartungszugriffe MÜSSEN nachvollziehbar protokolliert werden.

ANF-MN 100 Für Fernzugriffe MÜSSEN sichere Kommunikationsverbindungen

verwendet werden und deren Anforderungen SOLLTEN regelmäßig kontrolliert werden.

ANF-MN 101 Die möglichen Zugänge und Kommunikationsschnittstellen für einen Verbindungsaufbau von außen MÜSSEN auf das notwendige Maß beschränkt werden. Ebenso MÜSSEN alle Kommunikationsverbindungen nach vollzogenem Fernzugriff getrennt werden (Deaktivierung).

ANF-MN 102 Für eine Fernwartung MÜSSEN notwendige Ports ständig bereitgestellt werden.

ANF-MN 103 Es MÜSSEN unter Berücksichtigung des erforderlichen Schutzbedarfes des IT-Systems oder der Anwendung sichere Authentisierungsmechanismen für die Administratoren eingesetzt werden.

7.13.3 Härtung und sichere Basiskonfiguration der Systeme und Anwendungen

ANF-MN 104 Für die Inbetriebnahme von Systemen und Anwendungen MÜSSEN Vorgaben zur sicheren Basiskonfiguration und ggf. Maßnahmen zur Härtung der eingesetzten Systeme festgelegt und angewendet werden. A.12.5.1
A.12.6.1

ANF-MN 105 Es MUSS eine regelmäßige Analyse und ggf. Anpassung der Vorgaben zur sicheren Basiskonfiguration und Härtung im Hinblick auf mögliche technische Schwachstellen durchgeführt werden.

ANF-MN 106 Es MUSS ein Freigabe- und Kontrollverfahren für die Installation von Software auf betriebsrelevanten Systemen implementiert werden.

7.13.4 Schutz vor Schadsoftware

ANF-MN 107 Die Umsetzung der allgemeinen Maßnahmen zum Schutz vor Schadsoftware nach DIN ISO 27799 MUSS geprüft werden, insbesondere die folgenden Maßnahmen: A.12.2.1

- a. Vorgabe einer Richtlinie zum Verbot des Einsatzes nicht autorisierter Software sowie den Risiken, die sich aus der Nutzung von Software aus unbekanntem Quellen ergeben können, sowie möglichen Schutzmaßnahmen
- b. Maßnahmen zur Vermeidung und Erkennung von nicht autorisierter Software sowie zur Vermeidung bekannter oder potenziell verdächtiger Software, E-Mail-Anhänge und Webseiten
- c. Reduzierung möglicher Schwachstellen durch regelmäßige Updates gemäß den vom Hersteller entsprechender Systeme gesetzten Rahmenbedingungen (Freigabe)

ANF-MN 108 Zum Schutz von unternehmenskritischen Informationen MUSS ein

System zur Vorbeugung und Erkennung schädlicher Software eingerichtet werden.

ANF-MN 109 Zum Schutz vor Ausführung von Schadsoftware SOLL die Ausführung von unbekanntem Programmen verhindert werden (Application-Whitelisting). Die Ausführung von Makros in Bürosoftwareprodukten MUSS kontrolliert erfolgen. Kontrollmaßnahmen KÖNNEN u.a. Rückfragen beim Nutzer, signierte Makros der eigenen Organisation sein.

7.13.5 Intrusion Detection / Prevention

ANF-MN 110 Es SOLLTE ein System zur Vorbeugung und Erkennung von nicht autorisierten Zugriffsversuchen auf das Netzwerk und die Systeme des Krankenhauses implementiert werden, das neben dem Verhindern unberechtigter Zugriffsversuche (z. B. durch Firewall) auch den prinzipiell erlaubten Netzwerkverkehr auf gefährliche Inhalte kontrolliert.

ANF-MN 111 Es SOLLTEN regelmäßige Überprüfungen auf Schwachstellen sowohl innerhalb des eigenen Netzes als auch von extern erfolgen (Penetrationstests), um sowohl externe Angriffsmöglichkeiten zu identifizieren, als auch interne Schwachstellen zu erkennen, die aufgrund eines Firewall-Schutzes (derzeit) nicht zu einer direkten Gefährdung führen.

7.13.6 Identitäts- und Rechtemanagement

Die Forderung, ein adäquates Identitäts- und Berechtigungsmanagement in jedem Krankenhaus zu etablieren, wurde schon im Rahmen des technischen Datenschutzes seitens der Aufsichtsbehörden gefordert. Dies gilt nicht nur für Gesundheitsdaten, die besonderen Anforderungen hinsichtlich des Schutzbedarfs sowie der damit verbundenen Informationsverarbeitung unterliegen, auch der Zugriff z. B. auf Administrationsberechtigungen oder Netzwerksysteme muss angemessen geschützt werden. Zugang zu und Zugriff auf entsprechende Informationen darf nur durch berechtigte Nutzer erfolgen. Werden in Notfallsituationen bestehende Zugriffsbeschränkungen temporär aufgehoben, um die medizinische Versorgung sicherzustellen, bestehen besondere Anforderungen an eine nachträgliche Kontrolle dieser Zugriffe.

ANF-MN 112 Das Krankenhaus MUSS ein Rollen- und Berechtigungskonzept erstellen und umsetzen, welches den unbefugten Zugriff auf personenbezogene Daten durch angemessene Maßnahmen verhindert. Der Zugriff auf Gesundheitsdaten im Rahmen vertraglicher und gesetzlicher Verpflichtungen (z. B. Behandlungsvertrag, gesetzliche Übermittlungspflichten) MUSS kontrolliert werden.

ANF-MN 113 Es SOLLTE eine Richtlinie zur Zugriffskontrolle erstellt werden, die Zugriffsrechte und -beschränkungen auf Informationen und Funktionen im Informationsmanagementsystem und dessen Erteilung bzw. Entzug

A.9.1.1-2
A.9.2.1-3
A.9.2.5-6
A.9.4.1-5
A.12.6.2

regelt. Hierbei SOLLTEN insbesondere die folgenden Punkte berücksichtigt werden:

- a. Einheitliche Beschreibung, Dokumentation und Umsetzung des Identitäts- und Berechtigungsmanagements,
- b. Erstellung eines Überblicks über Gruppen und Arten von Identitäten und Berechtigungen, die typischerweise in den verschiedenen Bereichen einer Institution verwaltet werden,
- c. Vorgaben für Beantragung und Vergabe von Zugriffsrechten und deren Änderungen sowie eine nachvollziehbare Dokumentation,
- d. Vorgaben zur Verwaltung von Identitäten, Benutzerkennungen und Berechtigungen,
- e. Umgang mit den Benutzerkennungen, Berechtigungen und Authentisierungsmitteln durch die Benutzer,
- f. Vorgaben zum Umgang mit Kennungen von Administratoren, Notfallbenutzern und anderen privilegierten Benutzern sowie Vorgaben zur Gewährung von zeitlich eingeschränktem Zugriff auf erweiterte Berechtigungen,
- g. Festlegung von Berechtigungsstrukturen, Dokumentation und Genehmigungsverfahren für die Vergabe von Berechtigungen, Festlegen und Einhalten von Administrationsprozessen,
- h. Vorgaben zur Erstellung und restriktiven Zuweisung von Berechtigungen auf den Zielsystemen,
- i. regelmäßige Überprüfung der Berechtigungen nach den Prinzipien Need-to-Know und Least Privileges,
- j. regelmäßige Prüfung aller Berechtigungen auf Aktualität (keine Berechtigungen für inaktive oder gelöschte Benutzer, keine unberechtigte Kumulation von Zugriffsrechten infolge von innerbetrieblichen Aufgabenwechseln oder Ausbildungsprogrammen),
- k. regelmäßige Prüfung aller Berechtigungen, ob diese einem Benutzer unter Umgehung des Identitäts- und Berechtigungsmanagements direkt auf den Zielsystemen zugewiesen wurden

ANF-MN 114 Nach Beendigung des Arbeitsverhältnisses zwischen Personal und Krankenhaus MUSS sichergestellt werden, dass erteilte Zugangsrechte unmittelbar entzogen werden (insbesondere auch bei Studenten, Praktikanten und Aushilfspersonal).

7.13.7 Sichere Authentisierung

Der Zugang zu IT-Systemen und Informationen ist durch ein sinnvolles und risikofokussiertes Authentisierungsverfahren abzusichern.

A.9.2.4
A.9.3.1

ANF-MN 115 Es MUSS ein formaler Prozess zur Vergabe/Zuweisung von Authentisierungsdaten etabliert werden, der

- Nutzer zur Geheimhaltung individueller Authentisierungsdaten verpflichtet
- die erstmalige Übermittlung von (temporären) Authentisierungsdaten zum Nutzer regelt
- Vorgaben für Änderungsintervalle sowie Komplexität von Passwörtern enthält
- Vorgaben für die Änderung temporärer Passwörter nach der ersten Anmeldung an einem Informationssystem enthält
- die Identität eines Nutzers sicherstellt, dessen Authentisierungsdaten geändert werden sollen

ANF-MN 116 Authentifizierungsverfahren SOLLEN so gewählt werden, dass die Zugriffssicherheit auf Daten und IT-System bezogen auf die Erbringung der kDL angemessen umgesetzt wird. Dabei SOLLTEN auch die Einsatzmöglichkeiten einer 2-Faktor-Authentifizierung zur Erhöhung der Sicherheit berücksichtigt werden.

7.13.8 Kryptographische Absicherung (data in rest, data in motion)

Mit Hilfe eines Kryptographiekonzeptes können die Vertraulichkeit, Authentizität oder Integrität von Informationen gewährleistet werden.

ANF-MN 117 Das Krankenhaus SOLLTE ein Kryptographiekonzept erstellen, welches die kryptographischen Verfahren als auch das Schlüsselmanagement der jeweiligen Anwendungsfelder (z.B. WLAN, VPN, SSL für E-Mail und Web) festlegt.

ANF-MN 118 Das Kryptographiekonzept MUSS die technischen und organisatorischen Gegebenheiten des Krankenhauses, insbesondere die eingesetzte Medizintechnik, berücksichtigen. Die Festlegung von Art, Stärke und Qualität des jeweils erforderlichen Verschlüsselungsalgorithmus SOLLTE anhand von Risikoanalysen erfolgen.

ANF-MN 119 Innerhalb des Kryptographiekonzeptes SOLLTEN alle relevanten IT-Technologien und Kommunikationsverbindungen aufgeführt werden. (Reihenfolge tauschen mit ANF-MN-123)

A.10.1.1-2
A.18.1.5

ISO 17090-3
Ausstellung und
Verwendung von digitalen
Zertifikaten im
Gesundheitsbereich

7.13.9 Mobile Sicherheit, Sicherheit Mobiler Zugang und Telearbeit (ggf. „bring your own device“ BYOD)

Es sind unterstützende Sicherheitsmaßnahmen und -richtlinien zu etablieren, um die Risiken und den Schutz von Informationen bei der Nutzung von Mobilgeräten und Fernzugriffen innerhalb einer ungeschützten Umgebung (öffentliche Orte, Verkehrsmittel, Heimarbeitsplätze, etc.) zu steuern. Die Verwendung von privat genutzter Hardware („bring your own device“) ist hierbei explizit zu regeln.

A.6.2.1
A.6.2.2
A.11.2.6

SYS.3.2.2: Mobile Device Management (MDM)

ANF-MN 120 Die Verwendung von mobilen Geräten, Telearbeitsplätzen und mobilen medizinischen Geräten SOLL explizit freigegeben werden.

ANF-MN 121 Nutzer mobiler Geräte und Telearbeitsnutzer MÜSSEN hinsichtlich des Schutzbedarfes mobiler Geräte, Telearbeitsplätze und den hierauf verarbeiteten Daten sensibilisiert und zur Einhaltung der festgelegten Regelungen der Richtlinie(n) verpflichtet werden, insbesondere wenn es sich um den Zugriff oder die Verarbeitung von Gesundheitsdaten handelt.

ANF-MN 122 Neben der Bestimmung der spezifischen Risiken, die sich aus der Nutzung mobiler Technologien im Gesundheitswesen ergeben, SOLLTEN folgende Regelungen für Mobilgeräte und Telearbeitsplätze festgelegt werden:

- Anmeldung, Zugangskontrollen und Authentisierungsmethoden
- Anforderungen an den physischen Schutz des Gerätes, z. B. dass Daten nicht von unberechtigten Personen gelesen werden können, das Gerät niemals unbeaufsichtigt bleiben darf und ggf. bei Nichtbenutzung weggeschlossen werden sollte (Diebstahlschutz sowie unerlaubter Zugriff und Zugang von Dritten)
- Einschränkung von Software-Installationen und Verfahren zur Software- bzw. System-Aktualisierungen
- Schutz vor Schadsoftware (z. B. Firewall, Virenschutz)
- Nutzung drahtloser Verbindungen (z. B. WiFi, Bluetooth) und Internet-Diensten
- Methoden zur Sicherung des Fernzugriffs
- Art der Informationen, die auf den Geräten verarbeitet bzw. lokal gespeichert werden dürfen
- Verschlüsselungsverfahren und Maßnahmen zum Schutz der Daten, insbesondere von Gesundheitsdaten
- Geregelter Backupverfahren/-turnus und Sicherstellung der Einbeziehung dieser mobilen Geräte zu geplanten Backup-Zeiten
- Remotezugriff, Sperrung, Löschung und Deaktivierung des Gerätes sowie Meldeverfahren bei Verlust

-
- Widerruf von Berechtigungen und Zugriffsrechten sowie die Rückgabe von Betriebsmitteln
 - Explizite Trennung von privater und geschäftlicher Nutzung (bei BYOD)
 - Anforderungen an die Genehmigung mobiler oder Tele-Arbeitsplätze

ANF-MN 123 BYOD SOLLTE nur in begründeten Ausnahmefällen zum Einsatz kommen, insbesondere die Nutzung privater (vom Nutzer administrierter) Endgeräte (z. B. Smartphones) MUSS kritisch geprüft werden. Dies schließt Vorgaben für die Speicherung personenbezogener Daten auf privaten Geräten ausdrücklich ein.

ANF-MN 124 Für mobile Geräte (insbesondere Smartphones, Tablets) SOLLTE ein Mobile Device Management implementiert werden.

7.13.10 Vernetzung von Medizingeräten

ANF-MN 125 Für den Einsatz von Medizingeräten in medizinischen IT-Netzwerken SOLLTEN die Anforderungen der DIN EN 80001-1:2011 für das Risikomanagement berücksichtigt werden.

ANF-MN 126 Die Aufrechterhaltung des Betriebs medizintechnischer Anlagen MUSS auch bei Verlust von Kommunikationsverbindungen oder NetzwerkinTEGRATIONEN möglich sein, bzw. über entsprechende organisatorische Ersatzverfahren sichergestellt werden, soweit dies im Verantwortungsbereich des Betreibers der medizintechnischen Anlage liegt.

7.13.11 Datensicherung, Datenwiederherstellung und Archivierung

A.12.3.1

Die im Krankenhaus erhobenen und verarbeiteten Informationen (Gesundheitsdaten, unternehmenskritische Informationen, z. B. auch Konfigurationsdaten), müssen vor Verlust geschützt werden.

ANF-MN 127 Die Vorgaben zur regelmäßigen Prüfung und Anfertigung von Sicherheitskopien von Informationen (Datenbanken, Dateisystemen, Archiven, Konfigurationsdaten), Software und Systemimages MÜSSEN in einem Datensicherungskonzept definiert werden.

ANF-MN 128 Es MUSS ein Datensicherungskonzept mit folgenden Mindestinhalten erstellt werden:

- Festlegung der zu sichernden Daten
- Häufigkeit, Zeitpunkt und Generationenanzahl der Datensicherung (insbesondere zum Zeitraum zwischen zwei Datensicherungen, der im Fall eines Datenverlustes noch akzeptabel ist)
- Einhaltung der Vertraulichkeit der Daten (Verschlüsselung)

-
- Art des Speichermediums
 - Physischer Archivierungsort und Transport, der die klimatischen Bedingungen einer längerfristigen Aufbewahrung erfüllt
 - Umfang des Backups (komplett, inkrementell)
 - Festlegung von Verantwortlichkeiten und Zugriffsrechten auf Datensicherungen
 - Aufbewahrungsfristen und Lösungsverfahren
 - regelmäßige Prüfung auf Vollständigkeit und Aktualität der Backups
 - regelmäßige Prüfung der Wiederherstellbarkeit und Lesbarkeit

ANF-MN 129 Backups, die Gesundheitsinformationen enthalten, MÜSSEN ausreichend gegen unbefugten Zugriff geschützt werden, z. B. durch Verschlüsselung und/oder Lagerung in einer sicheren Umgebung und Trennung von Primär- und Backupdaten.

7.13.12 Ordnungsgemäße IT-Administration

IT-Administratoren stellen die ordnungsgemäß funktionierende IT-Landschaft durch Wartung, Erweiterung und Notfallreaktionen sicher.

OPS.1.1.1: Ordnungsgemäße IT-Administration

ANF-MN 130 IT-Administratoren MÜSSEN über die notwendigen fachlichen Qualifikationen als auch über ausreichende Ressourcen verfügen, um die ihnen übertragenen Aufgaben zuverlässig und sorgfältig erledigen zu können.

ANF-MN 131 Für eine ordnungsgemäße IT-Administration SOLLTEN die Rollen bzw. Arbeitskontexte „IT-Administration“ und „IT-Nutzung“ (E-Mail, Internet, Office etc.) getrennt werden.

ANF-MN 132 Die Überwachung von Administrationstätigkeiten SOLL durch eine personenbezogene Rechtevergabe von Administrationsprivilegien im Logfilemanagement ermöglicht werden. Die Manipulation von Logfiles/Audittrails MUSS durch geeignete organisatorisch-technische Maßnahmen soweit möglich ausgeschlossen werden.

ANF-MN 133 Es MÜSSEN Vertretungsregelungen für administrative Aufgaben und Verantwortlichkeiten getroffen werden.

ANF-MN 134 Nach dem Ausscheiden von IT-Administratoren MÜSSEN deren persönliche Zugänge unmittelbar gesperrt und ihm/ihr bekannte Passwörter geändert werden (z.B. für Router, Master-Kennwörter, Notfall-Kennungen).

7.13.13 Patch- und Änderungsmanagement

A.11.2.4
A.12.1.2

Um Schwachstellen zu vermeiden und kontinuierlich zu schließen, ist ein kontrolliertes und gesteuertes Patch- und Wartungsmanagement nötig. Das Änderungs- und Patchmanagement muss im sensiblen kDL-Kontext mit besonderer Sorgfalt erfolgen, um Risiken für entsprechende medizinische Prozesse zu minimieren.

ANF-MN 135 Es SOLLTE ein formaler Freigabeprozess für Änderungen von Systemen (Hard- und Software) im Anwendungsbereich des B3S implementiert werden, dem eine adäquate Risikobewertung durch die betroffenen Bereiche vorausgeht. Der Freigabeprozess SOLLTE ebenfalls Vorgaben für eine Roll-Back-Planung enthalten.

ANF-MN 136 Die Wartung von Systemen (Hard- und Software) im Anwendungsbereich des B3S durch externes Personal MUSS vertraglich geregelt und die Einhaltung insbesondere von Sicherheitsanforderungen SOLLTE (zumindest stichprobenartig) überprüft werden (z. B. Begleitung von externem Wartungspersonal im Rechenzentrum, Einsatz von durch die Organisation freigegebenen Geräten, Regelungen zum Umgang mit externen Speichermedien).

ANF-MN 137 Die ordnungsgemäße Einhaltung der Freigabeprozesse (z. B. für Patches, Freigabeprozess für Neueinführung von Systemen, Freigabeprozess von Changes) SOLLTE regelmäßig, mindestens jährlich, überprüft werden.

7.13.14 Beschaffungsprozesse

A.14.1.1

Bereits im Kontext der Beschaffung von IT-Systemen und IT-gebundenen Medizinprodukten müssen Anforderungen an die IT-Sicherheit berücksichtigt werden. Für den sicheren und datenschutzkonformen Betrieb von IT-Systemen und IT-gebundenen Medizingeräten kommt dem sicheren Design der Produkte immer höhere Bedeutung zu. Informationssicherheit muss bereits vom Hersteller des Produktes mitgedacht werden, wobei sich aus der Integration von Systemen verschiedener Hersteller auch mangels einheitlicher Schnittstellen besondere Herausforderungen für den Betreiber ergeben.

Die Informationssicherheit ist dabei über den gesamten Lebenszyklus des Produktes / Systems zu betrachten, aus Sicht des Betreibers beginnt dies bereits mit dem Prozess der Beschaffung, der eine kontrollierte und qualitätsgesicherte Bereitstellung von IT-Systemen und IT-gebundenen Medizinprodukten gewährleisten sollte. Die hierfür vom Betreiber festgelegten Anforderungen sollen sich aus den getroffenen Regelungen zur Informationssicherheit ableiten lassen. Sie sollen sich auch im Rahmen von Standardisierungsinitiativen als empfohlene Produkteigenschaften etablieren und mittelfristig zu einer Verbesserung der Verfügbarkeit entsprechender Produkte am Markt beitragen.

ANF-MN 138 Die Berücksichtigung von Anforderungen an Informationssicherheit

SOLLTE für die Bereiche Informationstechnik, Medizintechnik, Kommunikationstechnik und Versorgungstechnik als wesentliches Merkmal / Kriterium für Beschaffungsprozesse etabliert werden.

ANF-MN 139 Der Informationssicherheitsbeauftragte SOLLTE in alle relevanten Beschaffungsprozesse eingebunden werden (vgl. auch ANF-MN 9).

ANF-MN 140 Bei der Beschaffung netzwerkfähiger Medizingeräte SOLLTE das Produkt neben den medizinischen Anforderungen auch die Aspekte der IT- und Datensicherheit berücksichtigen. Ein Risikomanagementprozess nach DIN EN 80001 SOLL mögliche Schwachstellen managen, die bezogen auf die kDL nicht durch den Hersteller abgefangen wurden, wenn das Medizingerät in ein medizinisches IT-Netzwerk integriert wird.

ANF-MN 141 Bei der Beschaffung netzwerkfähiger Medizinprodukte SOLLTE der Betreiber vom Hersteller die notwendigen Informationen, die sich aus dem Risikomanagementprozess nach DIN EN 80001 ergeben, im Rahmen der Ausschreibung anfordern, um eine adäquate Einschätzung des Produktes hinsichtlich des Risikomanagementprozesses vornehmen zu können.

ANF-MN 142 Neue Hard- und Software SOLLTE vor dem Produktivbetrieb innerhalb eines Testsystems getestet und anhand der erwarteten Funktionen überprüft werden.

7.13.15 Protokollierung

Zur Gewährleistung der Nachvollziehbarkeit von sicherheitsrelevanten Aktionen sowie aufgrund gesetzlicher Anforderungen an den Datenschutz muss ein Protokollierungskonzept erstellt werden, welches die Nachvollziehbarkeit z. B. von Störungen, Warnungen, Informationssicherheitsvorfällen, Ausnahmen sowie Datenzugriffen von Benutzern und Administratoren entsprechend der gesetzlichen Vorgaben gewährleisten sollte.

A.12.4.1-4

ANF-MN 143 Es MUSS ein Protokollierungs- und Auswertungskonzept erstellt werden, welches zumindest Festlegungen zu Art, Ablageort und Umfang der protokollierten Informationen sowie zu den Modalitäten der Auswertung der Protokolle enthält. Hierzu zählen insbesondere Anlässe für eine anlassbezogene Auswertung sowie Regelungen für stichprobenartige Auswertungen, Umfang, Verantwortliche und Beteiligte der Auswertungen (ggf. „4-Augen-Prinzip“) sowie Umsetzung der Betroffenenrechte (Informationspflichten).

ANF-MN 144 Protokollierte Ereignisse SOLLTEN nachvollziehbar abgelegt werden und vor dem Zugriff und Manipulation Unbefugter geschützt zu werden.

ANF-MN 145 Protokollierte Aktivitäten der Systemadministratoren MÜSSEN bei Systemen mit erhöhtem Schutzbedarf durch entsprechende Maßnahmen gegen nachträgliche Änderung, Löschung oder Deaktivierung durch die

Systemadministratoren geschützt werden.

ANF-MN 146 Zusätzlich zu sicherheitsrelevanten Ereignissen (Konfiguration der Protokollierung auf System- und Netzebene) SOLLTE eine zentrale Protokollierungsinfrastruktur auch allgemeine Betriebsereignisse protokollieren, die auf einen Fehler hindeuten, z. B. Ausbleiben von Protokollierungsdaten bzw. Nichterreichbarkeit eines protokollierenden IT-Systems, Betriebsereignisse, die auf eine außergewöhnliche Auslastung bzw. Beanspruchung einzelner Dienste hindeuten.

ANF-MN 147 Die Protokollierungsinfrastruktur SOLLTE ausreichend dimensioniert sein, sodass eine Skalierung im Sinne einer erweiterten Protokollierung berücksichtigt werden kann. Falls die Protokollierungsinfrastruktur extern aufgebaut und betrieben werden soll, SOLLTE ein spezialisierter Dienstleister beauftragt werden.

ANF-MN 148 Für eine synchrone Protokollierung aller relevanten Informationssysteme SOLLTE mit einer einzigen Referenzzeitquelle synchronisiert werden.

7.13.16 Umgang mit Datenträgern, Austausch von Datenträgern

Datenträger sind vor Missbrauch, Offenlegung, Verfälschung und unbefugtem Zugriff zu schützen und gemäß einer Informationsklassifizierung zu handhaben.

ANF-MN 149 Es MUSS eine Richtlinie definiert werden, die den ordnungsgemäßen Umgang mit Datenträgern innerhalb und außerhalb des Krankenhauses sowie klare Meldewege bei Verlust/Diebstahl regelt. Folgende Aspekte SOLLTEN dabei berücksichtigt werden:

- a. welche mobilen Datenträger tatsächlich genutzt werden und wer diese einsetzen darf,
- b. welche Daten auf mobilen Datenträgern gespeichert werden dürfen (ebenfalls: Ausschlüsse)
- c. wie die auf mobilen Datenträgern gespeicherten Daten vor unbefugtem Zugriff, Manipulation und Verlust geschützt werden,
- d. wie die Daten auf mobilen Datenträgern gelöscht werden sollen,
- e. ob und wie private Datenträger genutzt werden dürfen,
- f. mit welchen externen Mitarbeitern oder Dienstleistern Datenträger ausgetauscht werden dürfen und welche Sicherheitsregelungen dabei zu beachten sind,
- g. wie verhindert wird, dass mobile Datenträger für die unbefugte Weitergabe von Informationen benutzt werden,
- h. wie der Verbreitung von Schadsoftware über mobile Datenträger vorgebeugt wird.

A.8.3.1
A.8.3.3
A.11.2.5

ANF-MN 150 Gesundheitsdaten, die auf mobilen bzw. Wechseldatenträgern gespeichert sind, MÜSSEN während des Transports verschlüsselt und SOLLTEN diebstahlgeschützt gelagert werden. Dies gilt nicht für Daten, die dem Patientenmitgegeben werden, z. B. Bilddaten auf DVD.

ANF-MN 151 Nicht mehr benötigte Inhalte auf wiederverwendbaren Medien SOLLTEN anhand der Anforderungen in ANF-MN 154 bzw. ANF-MN 158 zur Löschung von Datenträgern und IT-Systemen sicher gelöscht werden.

ANF-MN 152 Befugte Personen oder Kurierdienste, die Datenträger mit Gesundheitsdaten transportieren dürfen, MÜSSEN explizit benannt und nachweislich zum sicheren Umgang verpflichtet werden.

ANF-MN 153 Werden Datenträger außerhalb des Zuständigkeitsbereichs der für IT-Sicherheit im Krankenhaus Verantwortlichen verwendet (z. B. Weitergabe an Mitarbeiter), SOLLTE bei deren Rückgabe eine Informationssicherheitsprüfung (z. B. auf Integrität, Virenbefall) vorgenommen werden.

7.13.17 Sicheres Löschen und Entsorgung von Datenträgern

Es soll die Wiedergewinnung von gezielt vernichteten Informationen auf digitalen und analogen Datenträgern verhindert werden.

A.8.3.2
A.11.2.7

BDSG

ANF-MN 154 Es MUSS eine klare und generelle Vorgehensweise zur Aussonderung und Löschung von Datenträgern und IT-Systemen definiert werden.

ANF-MN 155 Die Regelungen der Institution zum Löschen und Vernichten von Datenträgern SOLLTEN in einer Richtlinie dokumentiert werden. Die Richtlinie SOLLTE allen relevanten Verantwortlichen und Mitarbeitern der Institution bekannt sein und beachtet werden. Es SOLLTEN hierzu stichprobenartig Kontrollen durchgeführt und die Richtlinie regelmäßig aktualisiert werden.

ANF-MN 156 Es SOLLTE ein/e Verantwortliche/r zur Prüfung, Löschung und Entsorgung von Datenträgern benannt werden.

ANF-MN 157 Sofern Betriebsmittel/Geräte entsorgt oder wiederverwendet werden sollen, MUSS überprüft werden, ob diese Speichermedien enthalten. Diese MÜSSEN datenschutzkonform gelöscht werden.

ANF-MN 158 Speichermedien, die sensible Informationen (insbesondere Gesundheitsdaten) enthalten, MÜSSEN vor ihrer Wiederverwendung oder Entsorgung hausintern oder durch einen qualifizierten Entsorger physisch zerstört oder mittels geeigneter Verfahren gelöscht bzw. überschrieben werden, so dass die ursprünglichen Informationen nicht wiederhergestellt werden können. Die Hinweise des BSI (z. B. Maßnahmen zur Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten nach BSI-Grundschutz - M2.433) bzw. die Regelungen entsprechend

DIN 66399 KÖNNEN hierbei beachtet werden.

ANF-MN 159 Die Außerbetriebnahme / Aussonderung von IT-Systemen und Datenträgern SOLLTE geregelt und dokumentiert werden. Dabei SOLLTE sichergestellt sein, dass vor der Aussonderung alle auf einem IT-System oder Datenträger gespeicherten Informationen sicher gelöscht sind (Restinformationen).

ANF-MN 160 Bei der Reparatur oder Entsorgung von medizinischen Geräten, die Daten aufnehmen oder ausgeben, MUSS durch geeignete Maßnahmen die Rekonstruktion von Gesundheitsdaten zuverlässig ausgeschlossen werden.

ANF-MN 161 Die Löschung von Datenträgern mit sensiblen Daten SOLLTE protokolliert werden.

7.13.18 Softwaretests und Freigaben

Zur Sicherstellung des ordnungsgemäßen Produktiveinsatzes von Anwendungen sollten diese durch ein geregeltes Verfahren getestet und freigegeben werden.

ANF-MN 162 Vor dem Einsatz im Produktivbetrieb SOLLTEN angemessene Integrationstests und Systemtests und Freigabetests durchgeführt werden, bei denen die Funktionalität und Sicherheit der Software auf dem Zielsystem geprüft und freigegeben wird.

ANF-MN 163 Wurde die Software abgenommen, MUSS sie danach für die Nutzung freigegeben werden. Die Freigabe der Software ist nachweisbar zu dokumentieren und geeignet zu hinterlegen.

ANF-MN 164 Die Freigabeerklärung SOLLTE dabei die folgenden Informationen umfassen:

- a. Bezeichnung und Versionsnummer der Software und falls erforderlich des IT-Verfahrens,
- b. Bestätigung, dass die Abnahme ordnungsgemäß vorgenommen wurde,
- c. Einschränkungen für die Nutzung (Parametereinstellung, Benutzerkreis)
- d. Freigabedatum, ab wann die Software eingesetzt werden darf sowie
- e. die eigentliche Freigabeerklärung

ANF-MN 165 Entwicklungs-, Test- und Betriebsumgebungen SOLLTEN physisch oder virtuell voneinander getrennt sein.

ANF-MN 166 Reale Gesundheitsdaten SOLLTEN nicht auf Entwicklungs- und Testum-

A.12.1.4
A.14.2.1-9
A.14.3.1

gebungen genutzt oder gespeichert werden. Ist eine Nutzung unvermeidbar, MUSS die Entwicklungs- und Testumgebungen entsprechend gehärtet oder die Daten anonymisiert bzw. pseudonymisiert werden.

ANF-MN 167 Es MUSS ein/e Verantwortliche/r zur Freigabe von Software benannt werden.

ANF-MN 168 Standard- und Individualsoftware SOLLTE geprüft und einem formalen Abnahmeprozess unterstellt werden. Folgende Prüfkriterien SOLLTEN mindestens beachtet werden:

- Software frei von Schadcode
- Kompatibilität der Software zu Betriebssystem und anderen eingesetzten Anwendungen
- Erfüllung der geforderten Funktionalität
- vollständige Dokumentation/Handbücher der Software
- erfolgreicher Abnahmetest anhand geeigneter Testfälle
- Konformität zur Informationssicherheitsleitlinie

ANF-MN 169 Die Integration von Software, welche die kDL beeinflusst, MUSS im Rahmen eines dokumentierten Change-Prozesses erfolgen.

ANF-MN 170 Bei einem Wechsel von Betriebssystemen, Datenbanken oder Middleware-Plattformen SOLLTE überprüft werden, ob Software, welche die kDL beeinflusst, weiterhin ihre erwarteten Funktionen fehlerfrei erfüllt, der Freigabeprozess SOLLTE erneut durchgeführt werden.

7.13.19Datenschutz

Die Berücksichtigung der Anforderungen des Datenschutzes und der gesetzlichen sowie unternehmensinternen Regelungen zum Datenschutz im Informationssicherheitsmanagement ist in der Informationssicherheitsrichtlinie zu fordern und umzusetzen. Ein Informationssicherheitsvorfall kann bei Verletzung der Vertraulichkeit von Gesundheitsdaten immer auch einen Datenschutzverstoß zur Folge haben. Datenschutz und Informationssicherheit sind daher gemeinsam zu betrachten.

A.18.1.4
BDSG

ANF-MN 171 Die Krankenhausleitung MUSS eine Richtlinie zum Schutz personenbezogener Daten entwickeln, implementieren und kommunizieren. Diese Richtlinie SOLLTE mit der Leitlinie zur Informationssicherheit abgestimmt sein.

ANF-MN 172 Das Krankenhaus MUSS den benannten Datenschutzbeauftragten in den Informationssicherheitsprozess einbinden.

8 Übersicht der referenzierten Normen und Standards

Norm	Bezeichnung
DIN ISO/IEC 27001	Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen (ISO/IEC 27001:2013 + Cor. 1:2014)
DIN EN ISO 27799:2016-12	Medizinische Informatik - Informationssicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002 (ISO 27799:2016); Englische Fassung EN ISO 27799:2016 ISO 22301 „Betriebliches Kontinuitätsmanagement-System (BKMS)“
DIN EN 80001-1:2011-11;VDE 0756-1:2011-11	Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten - Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten (IEC 80001-1:2010); Deutsche Fassung EN 80001-1:2011
DIN 66399-1:2012-10	Büro- und Datentechnik - Vernichten von Datenträgern - Teil 1: Grundlagen und Begriffe
DIN 66399-2:2012-10	Büro- und Datentechnik - Vernichten von Datenträgern - Teil 2: Anforderungen an Maschinen zur Vernichtung von Datenträgern
DIN 13080:2016-06	Gliederung des Krankenhauses in Funktionsbereiche und Funktionsstellen

9 Glossar

AIS	Das Anästhesie-Informationssystem (AIS) stellt ein Dokumentationssystem für die Anästhesie im Zuge der Anästhesie und OP-Dokumentation dar, welches primär der Dokumentation dient
AMTS	Arzneimitteltherapiesicherheit (AMTS), Systeme zur (automatischen) Prüfung von Arzneimittelwechselwirkungen als Unterstützungssystem
Audit-Trail	System zur Protokollierung aller Änderungen in einer Datenbank. Es wird aufgezeichnet, welcher Anwender wann was geändert hat. Dieses System dient dazu, Änderungen im Nachhinein nachvollziehen zu können. Der public audit trail ist öffentlich einsehbar.
DMS	Dokumenten-Management-System (DMS) oder Enterprise-Content-Management (ECM) gingen aus der Dokumenten-Archivierung hervor und erfüllen heute Funktionen im Rahmen der Prozesssteuerung von Dokumenten-Workflows sowie als Archive von Bilddaten im Sinne pdf oder jpg. Mischformen zu PACS sind möglich und am Markt vorhanden.
DSGVO	Europäische Datenschutzgrundverordnung
ISMS	Informationssicherheitsmanagementsystems (ISMS)
ITS/IPS	Intrusion Detection System / Intrusion Prevention System
KIS	Ein Krankenhausinformationssystem (KIS) ist definiert als ein einzelnes Software-Anwendungsverfahren, das aus mehreren Software-Komponenten eines Herstellers bestehen kann. Ein KIS dient in erster Linie der Prozessunterstützung von Verwaltung, Medizin und Pflege im Krankenhaus.
LIS	Ein Labor-Informationssystem (LIS) besonderer Bedeutung für die Leistungserbringung im Krankenhaus
OPS	Der Operationen- und Prozedurenschlüssel (OPS) ist die amtliche Klassifikation zum Verschlüsseln von Operationen, Prozeduren und allgemein medizinischen Maßnahmen des Deutschen Instituts für Medizinische Dokumentation und Information (DIMDI)
OPS	OP-Planungs- und Dokumentationssystem, Unterstützungssystem für Planung und Dokumentation von operativen Eingriffen im Krankenhaus, auch genutzt für nachfolgende Berichtspflichten
PACS	Ein Picture Archive and Communication System (PACS) dient der Speicherung und Archivierung von digitalen Bilddaten aus Diagnostik und Therapie sowie der Kommunikation zwischen IT (KIS) und Medizintechnik-Geräten (Diagnostik, Therapie, Pflege). PACS können auch Mischformen

aus PACS, DMS und ECM sein. Ebenso umgekehrt DMS/ECM-Systeme PACS-Funktionen beinhalten.

POCT Point of Care Testing beschreibt Labor-Untersuchungen (primär Blutgas- und Blutzuckermessungen) dezentral und unabhängig von zentraler Labortechnik.

RIS Ein Radiologie-Informationssystem (RIS) ist definiert als einzelnes Software-Anwendungsverfahren. Es dient der Abbildung der Arbeitsabläufe in der Funktionsstelle Radiologie unter spezieller Berücksichtigung der Anforderungen der Röntgenverordnung (RöV).