DEUTSCHE KRANKENHAUS GESELLSCHAFT

Bundesverband der Krankenhausträger in der Bundesrepublik Deutschland

Krankenhäuser als kritische Infrastrukturen - Umsetzungshinweise der Deutschen Krankenhausgesellschaft

Identifikation betroffener Einrichtungen, Anforderungen an Betreiber und Umsetzung der Maßnahmen nach § 8b Abs. 3 und 4 BSI-Gesetz

19. Dezember 2017

Version: 0.9

Postfach 12 05 55
10595 Berlin
Wegelystraße 3
10623 Berlin

c/o HOPE
Avenue Marnix 30
1000 Brüssel
Telefon +32 2 540 25 50

Commerzbank AG
IBAN DE63 1004 0000 0788 4141 00
BIC COBADEFFXXX
UST-IdNr. DE119355528

www.dkgev.de

Inhalt

1 Management Summary

Mit Veröffentlichung des IT-Sicherheitsgesetzes am 25.06.2015 hat der Gesetzgeber Betreiber so genannter kritischer Infrastrukturen in die Pflicht genommen, sich den Herausforderungen zum Schutz dieser für das Allgemeinwohl wichtigen Einrichtungen im Kontext zunehmender Digitalisierung zu stellen. Auch eine Reihe von Krankenhäusern wird künftig die Anforderungen, die an diese kritischen Infrastrukturen gestellt werden, erfüllen müssen, um die aus Sicht des Gesetzgebers zentrale Dienstleistung der Krankenhäuser - die stationäre Versorgung von Patienten - auch in Zeiten sich ändernder Sicherheitsanforderungen, insbesondere mit Blick auf die wachsende Bedrohung durch Cyberkriminalität, dauerhaft und stabil erbringen zu können.

Das vorliegende Dokument soll Krankenhäuser dabei unterstützen, indem es zunächst die Kriterien erläutert, die zur Identifikation als kritische Infrastruktur im Sinne des BSI-Gesetzes herangezogen werden. Weiter wird auf die umzusetzenden Maßnahmen sowie hierbei geltende Fristen eingegangen. Dabei spielen insbesondere die sofort umzusetzenden Verpflichtungen hinsichtlich eines Meldewesens (Einrichtung einer Kontaktstelle bis 30.12.2017, ab diesem Zeitpunkt Meldung von Störungen an das BSI) bei kritischen Vorfällen eine zentrale Rolle.

Die Hinweise zu meldepflichtigen Vorfällen greifen die Handlungsempfehlungen des Verbandes der Universitätsklinika Deutschlands (VUD) zur IT-Sicherheit, hier insbesondere „Allgemeine Grundsätze und Empfehlungen zum Meldewesen nach dem BSI-Gesetz“ vom 30.11.2017 auf und wurden um Aspekte, die auch für den nichtuniversitären Klinikbetrieb relevant sein können, ergänzt.

Die vorliegenden Umsetzungshinweise nehmen dabei den derzeit in der Entwicklung befindlichen Entwurf eines sog. „branchenspezifischen Sicherheitsstandards (B3S)“ nicht vorweg, sie werden nach dessen Veröffentlichung entsprechend ergänzt.

2 Krankenhäuser als Kritische Infrastrukturen

Mit dem Inkrafttreten des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz – ITSiG) am 25.06.2015 wurden eine Reihe von Anforderungen an Betreiber so genannter „kritischer Infrastrukturen“ definiert, deren Ausfall oder Beeinträchtigung *„aufgrund ihrer Bedeutung für das staatliche Gemeinwesen […] nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen*[1]“ nach sich ziehen würde. Für den Sektor „Gesundheitsversorgung“ enthielt die zum 30.6.2017 in Kraft getretene 1. Änderungsverordnung zur BSI-Kritisverordnung (BSI-KritisV) die notwendigen Festlegungen hinsichtlich der Anlagekategorien, Bemessungskriterien und Schwellenwerte, nach denen künftig „kritische Infrastrukturen“ in der Branche „Medizinische Versorgung“ identifiziert werden. Im Zentrum steht dabei die kritische Dienstleistung der Branche - die stationäre Versorgung von Patienten im Krankenhaus.

Zur Erbringung dieser für das Allgemeinwesen wichtigen und daher „kritischen“ Dienstleistung 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. Für das Jahr 2017 hat diese Meldung bis spätestens zum 30.12.2017 zu erfolgen. 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.

Für Krankenhäuser, welche die identifizierenden Kriterien kritischer Infrastruktur zwei Jahre in Folge erfüllen, entsteht darüber hinaus eine Nachweispflicht zur Umsetzung geeigneter organisatorischer und technischer Vorkehrungen zur Vermeidung von Störungen der informationstechnischen Systeme. Das BSI-Gesetz sieht hierzu die Möglichkeit der Erstellung so genannter „branchenspezifischer Sicherheitsstandards“ vor. Die Deutsche Krankenhausgesellschaft bringt sich in den Diskussionsprozess hierzu aktiv ein, im Kontext zunehmender Digitalisierung im Krankenhaus stellt die Verbesserung der IT-Sicherheit - neben der Sicherstellung notwendiger organisatorischer und finanzieller Rahmenbedingungen - einen Handlungsschwerpunkt dar. Mit den vorliegenden Umsetzungshinweisen sollen IT-Sicherheitsverantwortlichen in den Krankenhäusern ein Überblick über die notwendigen Vorbereitungen und Maßnahmen im laufenden Betrieb gegeben werden sowie Krankenhäuser bei Aufbau- und Ablauforganisation des geforderten Meldeprozesses unterstützt werden. Ziel ist es, die Meldepflichten über IT-Störungen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) quantitativ und qualitativ sicherzustellen. Aufgrund der

[1] Nationale Strategie zum Schutz kritischer Infrastrukturen (Kritis-Strategie), Bundesministerium des Innern, 2009

heterogen ausgeprägten IT-Landschaft in den Krankenhäusern greift der Ansatz, meldepflichtige Vorfälle konkret und abschließend zu nennen, zu kurz. Vielmehr ist im Einzelfall zu entscheiden, welche Ursache und Auswirkungen eine Störung der informationstechnischen Systeme konkret hat bzw. haben kann. Ein erfolgreich abgewehrter Angriff auf die Krankenhaus-Informationstechnik mag daher im Einzelfall keine Beeinträchtigung der kritischen Dienstleistung (stationäre Versorgung) nach sich ziehen. Besteht jedoch Grund zur Annahme, dass die zugrunde liegende Ursache relevant oder gar zeitkritisch für eine Neubewertung des Lagebildes des BSI sein könnte, sollte eine Meldung an das BSI erwogen werden, um den Informationsaustausch zur Gefahrenabwehr aktiv zu unterstützen. Umgekehrt mag sich aus einer Funktionsstörung eines technisch defekten Endgerätes eine (meldepflichtige) Beeinträchtigung der kritischen Dienstleistung ergeben, bei der jedoch zunächst die Wiederherstellung der Behandlungsabläufe im Vordergrund stehen würde, ehe eine Meldung an das BSI abgesetzt wird.

Wesentliches Ziel der im IT-Sicherheitsgesetz festgelegten Informationspflichten ist der Austausch von für IT-Sicherheit relevanten Informationen zwischen den Betreibern kritischer Infrastrukturen und den zuständigen Behörden, hier insbesondere dem BSI. Es ist daher mit Augenmaß und Sachverstand im Einzelfall zu bewerten, wie mit Vorfällen im Bereich der IT-Sicherheit umgegangen wird und ob eine Meldung sinnvoll oder sogar notwendig ist. Dabei werden die Beteiligten lernen und ggf. notwendige Anpassungen vornehmen, um gemeinsame zu einer schrittweisen Verbesserung der IT-Sicherheit in den kritischen Infrastrukturen Deutschlands zu kommen. Es wird daher im Folgenden beispielhaft auch auf Vorkommnisse eingegangen, die im Einzelfall zu einer Meldepflicht geführt hätten, um den Beteiligten eine Hilfestellung bei der Einordnung und Bewertung konkreter Vorfälle zu geben. Darüber hinaus können aus anderen gesetzlichen oder normativen Anforderungen (z. B. Datenschutz) noch weitere Meldepflichten für den Betreiber entstehen. Diese sind aktuell nicht Gegenstand der vorliegenden Umsetzungshinweise.

Da zum gegenwärtigen Zeitpunkt die konkrete Ausgestaltung des branchen-spezifischen Sicherheitsstandards noch nicht vorliegt, können an dieser Stelle etwaige Anforderungen noch nicht detailliert aufgegriffen werden. Es ist jedoch vorgesehen, das vorliegende Dokument um Hinweise zur Umsetzung entsprechender Maßnahmen zur Verbesserung der IT-Sicherheit in den Krankenhäusern zu ergänzen.

3 Rechtliche Grundlagen

3.1 IT-Sicherheitsgesetz

Das IT-Sicherheitsgesetz (ITSiG) änderte bzw. ergänzte als Artikelgesetz im Juni 2015 eine Reihe von Rechtsvorschriften des Bundes, insbesondere das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz). § 8a BSI-Gesetz normiert Anforderungen an die Sicherheit in der Informationstechnik kritischer Infrastrukturen, insbesondere stehen dabei „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse“ im Mittelpunkt. § 8b BSI-Gesetz weist dem BSI die Funktion einer zentralen Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen zu. Hierzu erhält das BSI weitreichende Befugnisse zur Erhebung und Verarbeitung von Meldungen über IT-bedingte Störungen kritischer Infrastrukturen, umgekehrt sollen Betreiber kritischer Infrastrukturen durch das BSI rund um die Uhr über akute Ereignisse oder Warnmeldungen frühzeitig über potenzielle Gefährdungen informiert werden können. Die Konkretisierung der betroffenen kritischen Infrastrukturen erfolgte im Wege nachgelagerter Verordnungen. Mit dem Gesetz zur Umsetzung der europäischen Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie) am 29.06.2017 hat der Gesetzgeber den bestehenden Rechtsrahmen des ITSiG an die Vorgaben zur Informationssicherheit auf europäischer Ebene angepasst.

3.2 Angemessene organisatorische und technische Vorkehrungen

Insbesondere die Änderungen des BSI-Gesetzes (BSIG) sind für Betreiber kritischer Infrastrukturen relevant. Gemäß § 8a Absatz 1 BSIG sind Betreiber kritischer Infrastrukturen verpflichtet, „spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 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.“

Absatz 2 derselben Vorschrift stellt es Betreibern kritischer Infrastrukturen sowie deren Branchenverbänden frei, „branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1“ vorzuschlagen. Das BSI „stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten.“ Die Feststellung erfolgt dabei im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe sowie im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde. Insbesondere für Krankenhausstrukturen, die nicht (nur) dem zuständigen Gesundheitsministerium auf Landesebene unterstellt sind, sondern im Falle von Universitätsklinika auch noch dem für Wissenschaft und Forschung zuständigen Ressort dürften hier umfangreiche Abstimmungsprozesse zur Bewertung eines entsprechenden Sicherheitsstandards erforderlich werden.

Zum Nachweis der Erfüllung der Anforderungen nach § 8a Absatz 1 haben Betreiber kritischer Infrastrukturen nach Absatz 3 „mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Art nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel.“ Das Bundesamt kann „die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde“ und darüber hinaus „bei Sicherheitsmängeln im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel“ verlangen.

Das BSI kann nach Absatz 5 „zur Ausgestaltung des Verfahrens der Sicherheitsaudits, Prüfungen und Zertifizierungen nach Absatz 3 Anforderungen an die Art und Weise der Durchführung, an die hierüber auszustellenden Nachweise sowie fachliche und organisatorische Anforderungen an die prüfende Stelle nach Anhörung von Vertretern der betroffenen Betreiber und der betroffenen Wirtschaftsverbände festlegen.“

3.2.1 Informationsaustausch zwischen BSI und Betreibern kritischer Infrastrukturen

Zur Abwehr von Gefahren für kritische Infrastrukturen wird ein konstruktiver, gelebter Informationsaustausch zwischen dem BSI und den Betreibern kritischer Infrastrukturen als sinnvoll und notwendig erachtet. Hierzu wird dem BSI nach § 8b Absatz 1 BSIG die Funktion einer zentralen Meldestelle für Betreiber kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik zugewiesen. Zur Wahrnehmung dieser Aufgabe erhält das BSI umfangreiche Befugnisse, es kann beispielsweise die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik wesentlichen Informationen sammeln und auswerten, „insbesondere Informationen zu Sicherheitslücken, zu Schadprogrammen, zu erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und zu der dabei beobachteten Vorgehensweise“. Darüber hinaus ist vorgesehen, die potentiellen Auswirkungen entsprechender Angriffe auf die Verfügbarkeit der Kritischen Infrastrukturen in Zusammenarbeit mit den zuständigen Aufsichtsbehörden und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe „zu analysieren, das Lagebild bezüglich der Sicherheit in der Informationstechnik der Kritischen Infrastrukturen kontinuierlich zu aktualisieren“ und Betreiber kritischer Infrastrukturen, die zuständigen Aufsichtsbehörden des Bundes und der Länder oder zentral als Kontaktstellen benannten Behörden soweit notwendig und zur Erfüllung ihrer jeweiligen Aufgaben zu unterrichten.

Der Informationsaustausch ist dabei explizit bilateral verankert.

Nach § 8b Absatz 3 BSIG haben Betreiber kritischer Infrastrukturen dem BSI eine Kontaktstelle für die Übermittlung von Informationen durch das BSI zu benennen. Die Betreiber haben sicherzustellen, dass sie hierüber jederzeit erreichbar sind.

Für den Fall einer „erheblichen 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 kritischen Infrastrukturen führen können oder geführt haben“ sind Betreiber nach Absatz 4 verpflichtet, dies über die Kontaktstelle unverzüglich an das BSI zu melden. Die Meldung muss dabei „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.

Darüber hinaus können Betreiber eines Sektors auch so genannte „gemeinsame übergeordnete Ansprechstellen" benennen, um den Informationsaustausch zwischen den Kontaktstellen und dem BSI abzubilden.

3.2.2 Verpflichtung zur Mitwirkung durch Hersteller

In vielen Fällen, insbesondere im Bereich der Medizinprodukte, aber auch bei Software-Produkten, stehen Betreiber und Hersteller in einem besonderen Spannungsfeld aus Kostensenkungsdruck, rasantem technologischen Fortschritt sowie steigenden regulatorischen Anforderungen bei gleichzeitig schwierigen Investitionsbedingungen. Dabei spielen heute im Krankenhausbereich die Entwicklungsgrundsätze „Security by design" bzw. „Privacy by design" herstellerseitig noch eine eher untergeordnete Rolle. Hersteller müssen Betreiber beim Einsatz ihrer Produkte über den gesamten Lebenszyklus ausreichend unterstützen, insbesondere bei der Beseitigung von Schwachstellen, die im laufenden Betrieb auftreten. Dies wurde in der Vergangenheit nicht immer zufriedenstellend umgesetzt. Der Gesetzgeber hat auf diesen Umstand reagiert, das BSI kann „soweit erforderlich" nach § 8b Absatz 6 vom Hersteller der betroffenen informationstechnischen Produkte und Systeme „die Mitwirkung an der Beseitigung oder Vermeidung einer Störung […] verlangen."

3.2.3 Ziele des Informationsaustauschs

Das BSI hat in den gemeinsamen Beratungen immer wieder betont, dass die Meldung von Sicherheitsvorfällen und Störungen der Weiterentwicklung des Lagebildes, Gefahrenabwehr und Unterstützung der kritischen Infrastrukturen dienen solle. Eine vertrauensvolle Zusammenarbeit zwischen Wirtschaft und Staat, wie sie seit vielen Jahren im Rahmen des Umsetzungsplans Kritische Infrastrukturen (UP KRITIS) erfolgreich gelebt wird, sei dabei die Grundlage erfolgreichen Handelns, da „die Herausforderungen nur von Staat und Wirtschaft gemeinsam angenommen werden können."

§ 8b Absatz 7 BSIG stellt in diesem Zusammenhang klar, dass „*Soweit im Rahmen dieser Vorschrift personenbezogene Daten erhoben, verarbeitet oder genutzt werden, […] eine über die vorstehenden Absätze hinausgehende Verarbeitung und Nutzung zu anderen Zwecken unzulässig [sei]*." Hiermit soll nicht nur explizit dem Datenschutz Rechnung getragen werden, es wird auch jedwede andere Verwendung der in diesem Kontext erhobenen Informationen ausgeschlossen.

3.3 BSI-Kritisverordnung (BSI-KritisV)

Mit Veröffentlichung der „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV)" im Mai 2016 legte der Verordnungsgeber ein Rahmenwerk zur Identifikation kritischer Infrastrukturen vor, das ein abstraktes Vorgehensmodell basierend auf folgenden Grundannahmen beschreibt:

Ausgehend von einer Betrachtung der kritischen Versorgungsdienstleistung der jeweiligen Branche in den Sektoren des UP KRITIS wurden Anlagenkategorien,

Bemessungsgrundlagen und Schwellenwerte definiert, die eine Identifikation der konkreten „Anlagen“ kritischer Infrastrukturen ermöglichen soll. Dabei steht die gesamtgesellschaftliche Relevanz, d.h. der Versorgungsgrad der kritischen Infrastruktur im Mittelpunkt. An dieser Stelle werden zur Identifikation kritischer Infrastrukturen weder Substitutionen (Redundanzen in der Versorgung) noch Interdependenzen (Abhängigkeiten Kritischer Infrastrukturen untereinander) betrachtet. Davon unbenommen ist eine Betrachtung möglicher Substitutionen oder Abhängigkeiten auf Ebene der Maßnahmen zum Schutz der Kritischen Infrastrukturen.

Die BSI-KritisV wurde aufgrund der Komplexität inhaltlich aufgeteilt. Sie enthielt in der im Mai 2016 veröffentlichten Fassung („Korb 1“) zunächst grundsätzliche Regelungen zum Vorgehen und konkrete Vorgaben für die Sektoren Energie, Wasser, Ernährung sowie Informationstechnik und Telekommunikation. Die noch ausstehenden Festlegungen u.a. für den Sektor Gesundheit („Korb 2“) wurden im Juni 2017 mit der 1. Änderungsverordnung zur BSI-KritisV aufgegriffen.

3.4 1. Änderungsverordnung zur BSI-KritisV

Die noch ausstehenden Vorgaben zur Identifizierung kritischer Infrastrukturen um die notwendigen Anlagenkategorien, Bemessungskriterien und Schwellenwerte in den Sektoren Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr wurden mit Veröffentlichung der 1. Änderungsverordnung zur BSI-KritisV am 29.6.2017 bekannt gegeben.

Im Vorfeld hatte das Bundesministerium des Innern im Rahmen der Verordnungsgebung den betroffenen Branchen und Sektoren die Möglichkeit eingeräumt, den legislativen Prozess durch Expertenmeinungen hinsichtlich der Erfordernisse einer praktischen Umsetzbarkeit zu unterstützen. Für die Branche „medizinische Versorgung“ wurde in der Änderungsverordnung die vollstationäre Krankenhausbehandlung als „Kritische Dienstleistung“ festgelegt. Dabei wurde klargestellt, dass Anforderungen an den Krankenhausbereich ausschließlich in dieser Branche definiert werden und mit Blick auf entsprechende Sicherheitsstandards keine Abhängigkeiten zu anderen Branchen (beispielsweise Arzneimittel oder Labordienstleistungen) entstehen sollen. Etwaige Vorgaben eines branchenspezifischen Sicherheitsstandards eine Krankenhaus-Apotheke betreffend müssen daher in den Festlegungen zum Krankenhausbereich aufgenommen werden.

Die Erbringung der Kritischen Dienstleistung wird nach Maßgabe der Änderungsverordnung bei Aufnahme, Diagnose, Therapie, Unterbringung/Pflege und Entlassung erbracht. Als „Anlage“ i. S. d. Verordnung gelten „Standort oder Betriebsstätten eines nach § 108 SGB V zugelassenen Krankenhauses, die für die Erbringung stationärer Versorgungsleistungen notwendig sind.“

Als Bemessungskriterium wurde die Anzahl vollstationärer Krankenhausbehandlungen festgelegt. Ein Krankenhaus ist dann als kritische Infrastruktur gemäß BSI-Gesetz einzustufen, wenn an diesem planungsrechtlich ausgewiesenen Standort mindestens 30.000 vollstationäre Behandlungsfälle pro Jahr erbracht werden (siehe hierzu auch Abschnitt 4.5 Definition des Anlagenbegriffs)

4 Identifikation Kritischer Infrastrukturen

Die Identifikation einer Anlage (hier: Krankenhaus) als kritische Infrastruktur im Sinne des BSI-Gesetzes erfolgt grundsätzlich als Eigenerklärung des Betreibers. Ein zentrales Register der kritischen Infrastrukturen wird hierbei nicht geführt. Die Prüfung, ob ein Krankenhaus als kritische Infrastruktur zu identifizieren ist, bedarf keiner gesonderten Aufforderung durch das BSI. Es wird jedoch erwartet, dass Krankenhäuser, die ausweislich der öffentlich zugänglichen Informationen ihrer Fallzahlen (Qualitätsberichte) eine Überschreitung des Schwellenwertes vermuten lassen, bei Nichtmeldung seitens des BSI kontaktiert und um Aufklärung gebeten werden. Kommen Krankenhäuser ihrer Pflicht zur Meldung als kritische Infrastruktur nicht nach, kann dies als Ordnungswidrigkeit geahndet werden.

4.1 Kritische Dienstleistung in der Branche „Medizinische Versorgung“

Als kritische Dienstleistung im Sinne des BSI-Gesetzes wird in der Branche „Medizinische Versorgung“ derzeit ausschließlich die vollstationäre medizinische Versorgung von Patienten betrachtet. Diese wird in den Bereichen Aufnahme, Diagnose, Therapie, Unterbringung/Pflege und Entlassung erbracht.

Eine Berücksichtigung ambulanter Leistungserbringung bzw. des vertragsärztlichen Bereichs erfolgt derzeit nicht, da der Gesetzgeber hier derzeit keine gesamtgesellschaftliche Relevanz einzelner Leistungserbringer sieht.

4.2 Bemessungskriterium und Schwellenwert zur Identifikation

Um die Identifikation Kritischer Infrastrukturen im Krankenhausumfeld handhabbar zu gestalten und gleichzeitig eine Strategieanfälligkeit zu vermeiden, hat sich der Gesetzgeber hierfür allein auf die Anzahl vollstationär erbrachter Behandlungsfälle konzentriert. Dieses Bemessungskriterium erscheint aufgrund der Historie geeignet, die kritische Versorgungsdienstleistung hinreichend zu beschreiben. Im Rahmen der Kernteamberatungen zur Erstellung der BSI-KritisV wurden umfangreiche Betrachtungen möglicher Parameter, Gewichtungsfaktoren und Berechnungs-vorschriften erörtert. Diese haben jedoch den oben genannten Anforderungen des Gesetzgebers an eine nachvollziehbare und vor allem unstreitige Möglichkeit der Identifikation nicht genügt.

Die Einschränkung auf die Anzahl vollstationär erbrachter Behandlungen spiegelt die Kernaufgabe der Krankenhäuser wider. Da der ambulante Behandlungskontext aufgrund der kleinteilig organisierten niedergelassenen Versorgung (Arztpraxen) bezogen auf den einzelnen Leistungserbringer nicht als versorgungskritisch eingeschätzt wird, erschien es nicht sachgerecht, die ambulante Leistungserbringung im Krankenhaus zur Identifikation der kritischen Infrastrukturen heranzuziehen. Mit Blick auf die vom Gesetzgeber identifizierten kritischen Prozessschritte Aufnahme, Diagnose, Therapie, Unterbringung/Pflege und Entlassung entfällt für die Identifikation (Fallzählung“) der kritischen Infrastrukturen neben den ambulanten Behandlungsfällen auch die Betrachtung teilstationärer, sowie vor- und nachstationärer Behandlungsfälle.

4.3 Hinweise zum Schwellenwert

Mit der Festlegung von 30.000 vollstationären Behandlungsfällen als Schwellenwert werden voraussichtlich 5 - 10% aller Krankenhäuser in Deutschland betroffen sein. Mit der absehbaren Weiterentwicklung der gesetzlichen Grundlage und dem allgemeinen Ziel, bei zunehmender Digitalisierung die IT-Sicherheit in allen Bereichen des gesellschaftlichen Lebens zu verbessern, wird eine künftige Absenkung des Schwellenwertes erwartet.

4.3.1 Bemessungsgrundlage, Stichtagsregelung und Datengrundlage

Als Bemessungsgrundlage für die Erhebung der vollstationären Behandlungsfälle sind die, auch im Rahmen der Datenübermittlung nach § 21 KHEntgG ohnehin zu erhebenden, vollstationären Behandlungsfälle des Vorjahres zugrunde zu legen. Jeweils bis zum 31.3. eines Jahres hat der Betreiber zu prüfen, ob der festgelegte Schwellenwert erreicht oder überschritten wird. Ist dies der Fall, gilt das Krankenhaus ab dem Folgetag (1.4.) als kritische Infrastruktur im Sinne des BSIG.

4.3.2 Maßnahmen bei Überschreitung des Schwellenwertes

Für Krankenhäuser wird künftig die strategische Planung der Informationssicherheit als Teil einer IT-Strategie immer wichtiger werden, um auch künftig auf die Herausforderungen einer stetig zunehmenden Digitalisierung vorbereitet zu sein. In diesem Zusammenhang ist eine Erhebung des Status quo der eingesetzten Systeme, Prozesse und Verfahren empfehlenswert, da mit Überschreitung des Schwellenwertes und der daraus folgenden Erklärung gegenüber dem BSI sofort die Anforderungen nach den §§ 8a und 8b BSIG hinsichtlich der Meldepflichten, Erreichbarkeiten und Maßnahmen zum Schutz der informationstechnischen Systeme greifen.

Ein Übergangszeitraum ist ausdrücklich nicht vorgesehen.

Stellt der Betreiber eines Krankenhauses zum 31.3. eines Jahres fest, dass die Anzahl der vollstationären Behandlungsfälle aus dem Vorjahr den festgelegten Schwellenwert erreicht oder überschritten hat, sind die folgenden Schritte notwendig:

- Registrierung als kritische Infrastruktur und Einrichtung einer Kontaktstelle (siehe hierzu Abschnitt 5.1)
- Meldung von IT-Störungen an das BSI (siehe hierzu Abschnitt 5.3)
- Umsetzung von Maßnahmen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse

Die vorgenannten Schritte sind sofort umzusetzen, diese gelten nach dem Wortlaut der §§ 8a und 8b BSIG ab dem 1.4. des Jahres, das auf die Überschreitung des Schwellenwertes folgt. Der Nachweis der Umsetzung entsprechender Maßnahmen ist dann spätestens 2 Jahre nach Feststellung der Schwellenwertüberschreitung zu erbringen. Künftig kann hierzu ggf. der branchenspezifische Sicherheitsstandard („B3S“) genutzt werden.

Die Verpflichtung zum Nachweis gemäß § 8a Abs. 1 BSIG entsteht unabhängig von der Verfügbarkeit eines B3S. Der Nachweis muss geeignet erbracht werden, hierzu stellen B3S lediglich ein Angebot dar.

4.4 Unterschreitung des Schwellenwertes - Handlungsbedarf prüfen

Die Verbesserung der IT-Sicherheit ist grundsätzlich für alle Krankenhäuser relevant, die Sicherheit des Patienten und auch seiner (Behandlungs-)Daten ist nicht nur zentrales Element heutiger Versorgungsprozesse, sondern leitet sich bereits aus anderen gesetzlichen Verpflichtungen u.a. zum Datenschutz ab. Es ist inzwischen unbestritten, dass IT-Störungen des Krankenhausbetriebs negative Auswirkungen auf die Versorgung der Patienten haben können. Diese reichen von vermeidbaren Unannehmlichkeiten bis hin zur - zumindest temporären - Abmeldung des Krankenhauses von der Notfallversorgung. Auch diejenigen Krankenhäuser, welche nicht unter die Vorgaben des BSI-Gesetzes fallen, da sie den definierten Schwellenwert nicht erreichen, sollten daher prüfen, ob angemessene Maßnahmen zum Schutz der informationstechnischen Systeme getroffen wurden. Zwar entsteht für diese Krankenhäuser keine Verpflichtung zur Meldung von IT-Störungen oder zum Nachweis angemessener Schutzmaßnahmen, mit Blick auf die Verantwortung des Krankenhauses gegenüber dem Patienten sollte das Thema IT-Sicherheit jedoch eingehend bewertet und angemessen umgesetzt werden.

Insbesondere in den Fällen, in denen der Schwellwert nur knapp unterschritten wurde, sollten unbedingt vorbereitende Maßnahmen getroffen werden, um bei Schwellen-wert-überschreitung im Folgejahr die dann sofort greifende Verpflichtung zur Umsetzung entsprechender Maßnahmen realisieren zu können. Diese treten mit der Identifikation als kritische Infrastruktur ein, in den Folgejahren ist hierfür keine Umsetzungsfrist mehr vorgesehen. Lediglich der Nachweis zur Umsetzung entsprechender Maßnahmen ist erst zu führen, wenn das Krankenhaus zwei Jahre in Folge als kritische Infrastruktur im Sinne des BSI-Gesetzes gilt.

In den Fällen, in denen ein Krankenhaus, das bisher als kritische Infrastruktur galt, den Schwellenwert im Vorjahr unterschreitet, entfallen die Nachweis- und Meldepflichten sofort. Eine Nachweispflicht entsteht danach auch frühestens wieder nach zwei Jahren als kritische Infrastruktur. Es wird jedoch empfohlen, die etablierten Verfahren und Prozesse zur IT-Sicherheit (z. B. ISMS) weiterhin aufrecht zu erhalten.

4.5 Definition des Anlagenbegriffs

Bei der Identifikation Kritischer Infrastrukturen kommt der Definition des Anlagenbegriffs - insbesondere bei Krankenhäusern mit mehreren Standorten oder Betriebsstellen - zentrale Bedeutung zu. Allerdings obliegt die Planung der stationären Versorgung den hierfür zuständigen Behörden auf Ebene der Länder. Daher ist die Landeskrankenhausplanung in Deutschland föderal differenziert ausgestaltet. Zudem war zum Zeitpunkt der Verordnungsgebung der Standortbegriff nach § 2a KHG in Verbindung mit dem Verzeichnis dieser Standorte nach § 293 Abs. 6 SGB V noch nicht zwischen den Partnern der Selbstverwaltung konsentiert bzw. vereinbart, auf eine einheitliche Definition für Standorte oder Betriebsstätten eines Krankenhauses unter Berücksichtigung z. B. regionaler Standortgegebenheiten konnte daher noch nicht zurückgegriffen werden.

Zur Definition der Anlagenkategorie wird daher auf die kritische Versorgungsdienstleistung Bezug genommen: Anlagen im Sinne der BSI-KritisV sind „Standort oder Betriebsstätten eines nach § 108 SGB V zugelassenen Krankenhauses, die für die Erbringung stationärer Versorgungsleistungen notwendig sind.“

Die Begründung zur 1. Änderungsverordnung führt ergänzend hierzu aus:

„Der Krankenhausbegriff ist im Sinne der Landeskrankenhauspläne zu verstehen, welche die zugelassenen Krankenhäuser, teilweise differenziert nach Betriebsstätten oder Standorten, ausweisen. Dabei sind räumlich getrennte Standorte oder Betriebsstätten eines Krankenhauses als eine Anlage anzusehen, wenn sie aus planungsrechtlicher Sicht, etwa aus organisatorischen, technischen, medizinischen oder sicherheitsbezogenen Aspekten als Einheit betrachtet werden."

Die Definition zum Anlagenbegriff beinhaltet im Ergebnis zwei alternative Tatbestände:

1. Ein Krankenhaus ist der Standort eines nach § 108 SGB V zugelassenen Krankenhauses.
2. Ein Krankenhaus sind die Betriebsstätten eines nach § 108 SGB V zugelassenen Krankenhauses.

Im Falle von Nummer 2 sind alle Betriebsstätten, die im Sinne des (jeweiligen) Landeskrankenhausplans als ein Krankenhaus behandelt werden (Feststellungsbescheid), in Anwendung der Verordnung als eine Anlage zu betrachten. Erfolgt daher ausweislich des Landeskrankenhausplans eine Zusammenfassung mehrerer Betriebsstätten zu einem „einheitlichen Krankenhaus" oder zu einem „Verbundkrankenhaus", sind diese als Einheit zu betrachten. In diesem Fall sind die vollstationären Fälle der einzelnen Betriebsstätten zu summieren.

Enthält der Landeskrankenhausplan keine Angaben zur Zusammenfassung mehrerer Betriebsstätten, ist aus dem Umstand, dass ein Feststellungsbescheid für mehrere Standorte ergangen ist, nicht zwangsläufig abzuleiten, dass diese planungsrechtlich als Einheit zu betrachten sind, da in der Regel der Träger des Krankenhauses auch bei räumlich getrennten Standorten nur einen einzigen Feststellungsbescheid erhält. Vielmehr ist im Einzelfall zu prüfen, ob sich aus dem Feststellungsbescheid Anhaltspunkte ergeben die eine planungsrechtliche Eigenständigkeit der einzelnen Betriebsstätten rechtfertigen könnten. Hierfür ist zum Beispiel zu berücksichtigen, ob im Feststellungsbescheid mehrere Standorte mit unterschiedlichen Adressen ausgewiesen sind oder ob die Fachabteilungsplanung jeweils unabhängig für die einzelnen Betriebsstätten erfolgt. In diesen Fällen sind diese räumlich getrennten Standorte oder Betriebsstätten nicht als Einheit im Sinne der Identifikation kritischer Infrastrukturen zu betrachten, sodass keine Zusammenfassung der an den einzelnen Standorten ausgewiesenen vollstationären Fallzahlen erfolgt.

Werden dagegen im Feststellungsbescheid die Adressen der unterschiedlichen Standorte nicht gesondert ausgewiesen oder geht aus dem Feststellungsbescheid hervor, dass die Fachabteilungsplanung für mehrere Betriebsstätten übergreifend erfolgt, sind diese als planungsrechtliche Einheit anzusehen.

Ziel der mit dem IT-Sicherheitsgesetz und der BSI-KritisV verbundenen Initiative des Gesetzgebers war die Verbesserung der Informationssicherheit in den für die Versorgung der Bevölkerung wesentlichen Infrastrukturen. Dabei wurde eine einfache, möglichst nicht strategieanfällige, Grundlage für die Identifikation der kritischen Infrastrukturen angestrebt. Der Schwellenwert soll dabei in Verbindung mit dem Anlagenbegriff sicherstellen, dass in jedem Falle diejenigen Anlagen identifiziert werden können, die aufgrund ihrer Dimension in Bezug auf die kritische Versorgungsdienstleistung wesentlich für das Gemeinwesen sind.

Darüber hinaus können Betreiber räumlich getrennte Standorte zusammenfassen, wenn dies aus organisatorischen, technischen, medizinischen oder sicherheitsbezogenen Aspekten mit Blick auf die Intention des Gesetzgebers sinnvoll erscheint.

5 Anforderungen an kritische Infrastrukturen

Identifiziert der Betreiber das Krankenhaus als kritische Infrastruktur, ist dies dem BSI gemäß BSI-KritisV zu melden. Hierfür hält das BSI einen Registrierungsprozess vor, der jedoch zuvor notwendige Anpassungen der internen Organisationsstruktur sowie den Aufbau einer entsprechenden IT-Sicherheitsmanagementstruktur bedingt. U. a. sollten die notwendigen Zuständigkeiten und Verantwortlichkeiten geklärt sein, damit im Ernstfall alle notwendigen Schritte definiert und bekannt sind.

5.1 Meldung kritischer Infrastrukturen, Einrichtung einer Kontaktstelle

Der Betreiber der kritischen Infrastruktur hat die organisatorischen und personellen Vorkehrungen zu treffen, um eine Kontaktstelle gemäß § 8b Absatz 3 BSI-Gesetz einzurichten. Die Benennung gegenüber dem BSI erfolgt mit der Registrierung unter:

https://mip.bsi.bund.de/register

Das BSI betreibt für die namentliche Meldung der kritischen Infrastrukturen sowie für die Meldung von IT-Störungen ein webbasiertes Portal („Meldeportal“). Nach der Registrierung einer kritischen Infrastruktur versendet das BSI ein Informationspaket, bestehend aus einer Zugangsbeschreibung zum Meldeportal sowie dreier Hardware Token für eine 2-Faktor-Authentifizierung. Da die Meldepflicht für IT-Störungen bereits mit der Registrierung entsteht, sind bis zur Einrichtung des Zugangs am Meldeportal ggf. auftretende IT-Störungen via Telefon an das BSI zu übermitteln.

5.2 Art, Aufgabe und Erreichbarkeit der Kontaktstelle

Um die gesetzlichen Aufgaben der Kontaktstelle wahrnehmen zu können, ist eine jederzeitige Erreichbarkeit sicherzustellen. Dabei steht die Fähigkeit der kritischen Infrastruktur im Vordergrund, auf Meldungen des BSI reagieren zu können. Sollten sich aus dem Lagebild z. B. Anhaltspunkte für einen gezielten Angriff auf bestimmte Infrastrukturen ergeben, könnte das BSI diese ggf. direkt und zeitnah kontaktieren. Das BSI wird hierzu in der Regel über die ihm bekannten elektronischen Kontaktadressen (E-Mail) informieren.

Eine telefonische Erreichbarkeit rund um die Uhr ist nicht gefordert.

Es wird die Einrichtung eines Funktionspostfaches empfohlen. Die Erreichbarkeit dieses Funktionspostfaches ist dabei jederzeit sicherzustellen. Weiterhin ist zu gewährleisten, dass eingehende Nachrichten in angemessener Zeit vom jeweils zuständigen Verantwortlichen gesichtet und eventueller Handlungsbedarf identifiziert wird. Dies setzt eine entsprechende fachliche Qualifikation des jeweils Verantwortlichen zur Ersteinschätzung des Sachverhaltes voraus.

Die Weiterleitung bzw. der Abruf der im Funktionspostfach eingehenden Nachrichten ist jederzeit so sicherzustellen, dass eine qualifizierte Bearbeitung der Meldung in angemessener Zeit beginnen kann.

Intention des Gesetzgebers für die „jederzeitige“ Erreichbarkeit der kritischen Infrastrukturen für Meldungen des BSI war insbesondere die schnelle Reaktionsfähigkeit im Krisenfall. Auf eine konkrete Zeitangabe hat der Gesetzgeber hierbei verzichtet, in der Regel ist hierbei von einer Bearbeitung „ohne schuldhaftes Verzögern“ auszugehen. Während zu üblichen Geschäftszeiten z. B. der IT-Anwendungsbetreuung in

Krankenhäusern werktags von 8:00 - 17:00 Uhr mit einer zügigen Bearbeitung in der Regel innerhalb weniger Stunden ausgegangen wird, ist außerhalb dieser Zeiten (insbesondere an den Wochenenden) mit einer ggf. längeren Bearbeitungsdauer zu rechnen.

Es wird empfohlen, auch außerhalb der regulären Geschäftszeiten mindestens alle 24 Stunden eine Sichtung des Funktionspostfaches sicherzustellen.

Die Kontaktstelle („Funktionspostfach“) wird seitens des BSI sowohl für eventuelle Rückfragen zu IT-Störungsmeldungen verwendet (z. B. zur Einschätzung von Vorfällen oder zum Bearbeitungsstatus), als auch zum Zustellen von IT-Sicherheitsinformationen (Sicherheitslagebild). Es wird daher empfohlen, die Kontaktstelle in die vorhandene Infrastruktur für IT-Störungen (z. B. ein Ticketsystem) einzubinden, um eingehende Meldungen des BSI optimal erfassen, nachverfolgen und bearbeiten zu können.

5.3 Verpflichtung zur Meldung von IT-Sicherheitsvorfällen

5.3.1 Wer muss melden?

Die Meldepflicht gemäß § 8b Absatz 4 BSI-Gesetz betrifft Betreiber Kritischer Infrastrukturen, die anhand der in der BSI-KritisV festgesetzten Schwellwerte als Kritische Infrastrukturen im Sinne des BSI-Gesetzes identifiziert wurden. Für die Medizinische Versorgung sind dies Krankenhäuser, die mindestens 30.000 vollstationäre Fälle pro Jahr aufweisen.

5.3.2 Was muss gemeldet werden?

Grundsätzlich sind IT-Störungen zu melden, die zu einem Ausfall oder der Beeinträchtigung der Versorgungsdienstleistung geführt haben oder hätten führen können. Damit soll dem BSI die Möglichkeit eröffnet werden, die seinerseits vorgesehenen Informationspflichten, insbesondere die Erstellung eines aktuellen Lagebildes, durch direkte Informationen aus den Kritischen Infrastrukturen qualitativ erheblich zu verbessern. Hieraus ergeben sich sowohl inhaltliche als auch zeitliche Anforderungen an das Meldewesen. Der Betreiber hat organisatorische Vorkehrungen zu treffen, die im Falle einer auftretenden Anomalie zunächst die Einschätzung erlauben, ob es sich hierbei um einen Ausfall oder eine Störung der Versorgungsdienstleistung handelt und ob dieses Ereignis meldepflichtig ist. Dabei kann auch ein gestuftes Meldesystem - bestehend aus einer Erst- und einer Folgemeldung (ggf. auch Abschlussmeldung) - infrage kommen. Das BSI spricht sich insgesamt für ein proaktives Meldeverhalten aus, nach dem Grundsatz „Besser eine IT-Störung mehr melden, als eine zu wenig!“

Zunächst ist jedoch zu beschreiben, was unter dem Ausfall oder der Beeinträchtigung der Versorgungsdienstleistung zu fassen ist. Da gerade zu Beginn der Umsetzung sowohl auf Seiten der betroffenen Kritischen Infrastrukturen als auch der zuständigen Behörden Erfahrungswerte im Umgang mit entsprechenden Meldungen erst gesammelt werden müssen, enthält beispielhafte Konstellationen, die, ohne Berücksichtigung von weiteren Umständen des Einzelfalls, zu einer Meldung hätten führen müssen.

5.3.3 Wann muss gemeldet werden?

Die Meldung an das BSI hat „ohne schuldhaftes Verzögern“ zu erfolgen. Da im Falle einer Störung der Versorgungsdienstleistung zunächst die Wiederherstellung der kritischen Dienstleistung (vollstationäre Patientenversorgung),im Mittelpunkt steht, kann im Einzelfall (nach einer Erstmeldung) auch eine längere Zeitspanne bis zur ausführlichen Meldung an das BSI infrage kommen.

5.3.4 Wohin muss gemeldet werden?

Meldungen an das BSI sind an das Meldeportal (siehe 5.3.4) zu übermitteln. Stehen die üblichen Meldewege - beispielsweise aufgrund einer größeren IT-Störung - nicht zur Verfügung, kann eine Meldung auch telefonisch an das BSI übermittelt werden (siehe Abschnitt 7.2).

5.4 Maßnahmen zum Schutz der informationstechnischen Systeme

Überschreitet eine Kritische Infrastruktur den Schwellenwert in zwei aufeinanderfolgenden Jahren, hat der Betreiber nachzuweisen, dass er die notwendigen „angemessenen organisatorischen und technischen Vorkehrungen“ zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse getroffen hat, „die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind“.

Der Nachweis ist gegenüber dem BSI zu führen. Dabei kommen Audits, Zertifizierungen o.ä. infrage. Der Gesetzgeber hat hierzu die Möglichkeit branchenspezifischer Sicherheitsstandards vorgesehen. Diese können von der Branche erarbeitet und dem BSI auf Antrag zur Eignungsprüfung vorgelegt werden. Bestätigt das BSI die Eignung und weist der Betreiber im Rahmen eines Audits die Umsetzung dieses B3S nach, wird die Erfüllung der gesetzlichen Anforderungen angenommen.

Der Betreiber kann den Nachweis auch auf anderem Wege führen, allerdings ist in diesem Fall der Prüfmaßstab mit dem BSI abzustimmen, was sich im Einzelfall sehr aufwendig gestalten kann.

Generell wird der Aufbau eines Informationssicherheitsmanagementsystems (ISMS) als Basis für die Umsetzung notwendiger Maßnahmen angesehen.

5.5 Ausgestaltung der Meldung von Sicherheitsvorfällen

Das BSI informiert im Rahmen der Benennung einer Kontaktstelle über die möglichen Kommunikationswege zur Meldung von Sicherheitsvorfällen an das BSI. In der Regel soll hierzu das Melde- und Informationsportal des BSI genutzt werden. In Ausnahmefällen können Meldungen auch elektronisch per E-Mail oder telefonisch übermittelt werden. Das BSI hat ein Muster des Meldeformulars erstellt (siehe Anhang Abschnitt 7.3)

5.6 Empfehlungen zur Aufbauorganisation

Um den steigenden Anforderungen an IT-Sicherheit gerecht zu werden, wird Krankenhäusern eine wirksame und effiziente Aufbauorganisation hierzu notwendiger Strukturen empfohlen. Die Benennung eines Informationssicherheitsbeauftragten (ISB), die Vorgabe von Leit- und Richtlinien zur Informationssicherheit und der Aufbau eines Informationsmanagement-Teams nach Abbildung 1 Aufbauorganisation IT-Sicherheit werden hierfür als Grundvoraussetzung angesehen.

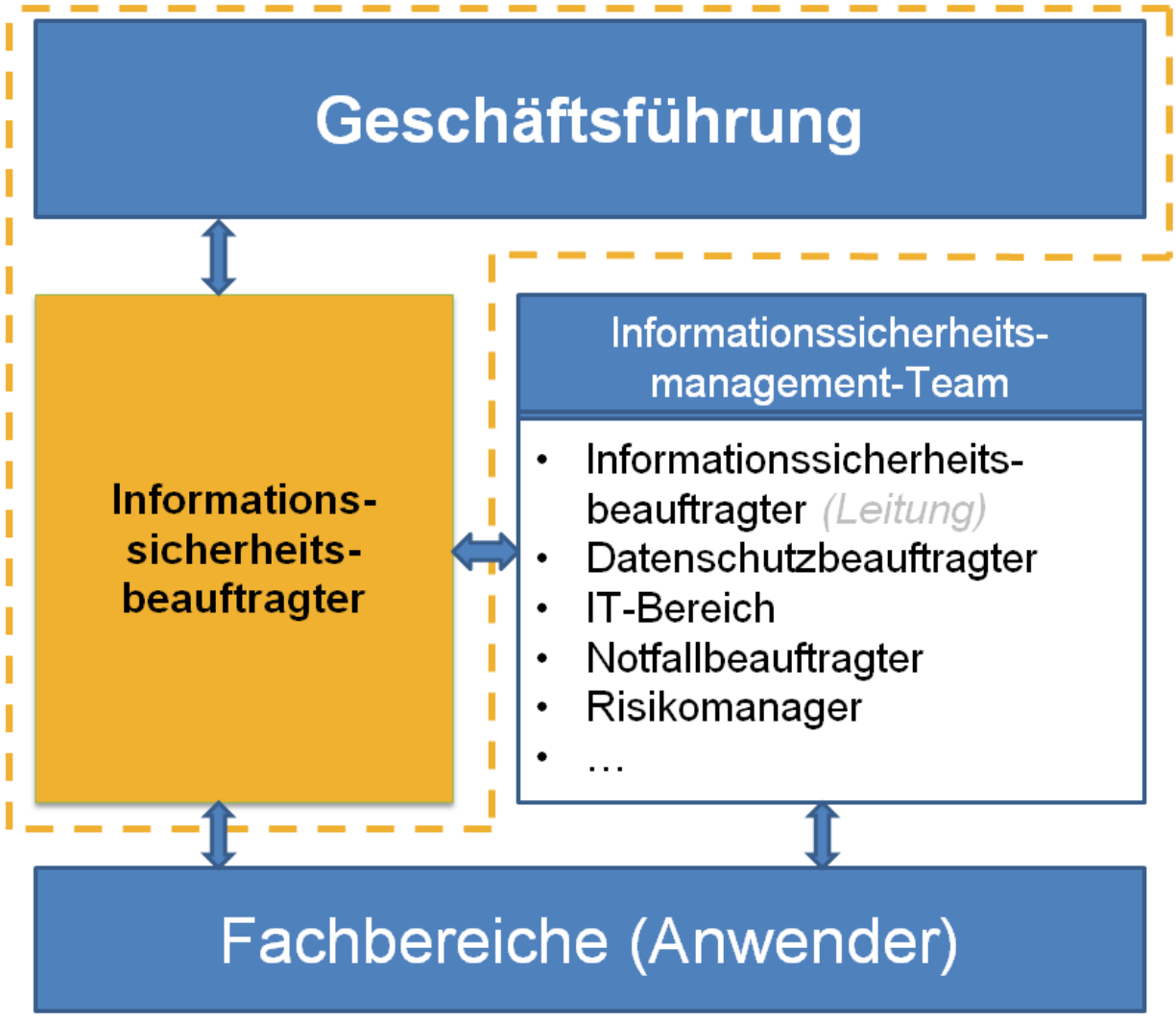


Abbildung 1 Aufbauorganisation IT-Sicherheit

Weiterhin sollten interne Organisationsregelungen [2]für das Auftreten von IT-Störungen definiert werden. Dabei sind insbesondere Fragen zur Zuständigkeit bzw. Verantwortlichkeit und einzuhaltenden Melde- und Entscheidungswegen in Notfallsituationen (gerade auch außerhalb üblicher Geschäftszeiten) zu regeln.

Beispiele hierfür sind u.a.

- „IT-Notfallhandbuch“
- „Richtlinie zum Umgang mit kritischen Vorfällen“

[2] Hinweise hierzu enthält der BSI-Grundschutz-Baustein B 1.6

Schulungsmaßnahmen der Mitarbeiter im Krankenhaus erhöhen die Awareness gegenüber möglichen Angriffsmethoden und sollten daher regelmäßig durchgeführt werden.

5.7 Einrichtungsübergreifende Organisation der Meldeverpflichtungen (SPOC / GÜAS)

Betreiber kritischer Infrastrukturen können neben der Kontaktstelle eine gemeinsame übergeordnete Ansprechstelle (GÜAS) benennen. Hierzu müssen sich einerseits die geplante GÜAS beim BSI registrieren und andererseits die Betreiber, die diese GÜAS nutzen wollen, dies in ihrer Benennung der Kontaktstelle angeben.

Bei der Benennung von GÜAS sind folgende Punkte zu beachten:

- Eine GÜAS kann nur von Betreibern benannt werden, die dem gleichen Sektor angehören.
- Die Aufgabe der GÜAS ist es, die vom BSI versandten Informationen stellvertretend für den Betreiber entgegenzunehmen sowie die Meldung des Vorfalls nach § 8b BSIG im Auftrag der Betreiber an das BSI zu melden.
- Wenn eine GÜAS benannt wurde, erfolgt der Informationsaustausch zwischen dem BSI und dem Betreiber in der Regel über diese. Daher ist hier aus Eigeninteresse der Betreiber nur eine GÜAS zu benennen, der seitens der Betreiber volles Vertrauen entgegengebracht wird.
- Die GÜAS muss eine sogenannte "Traffic Light Protocol“ (TLP) Erklärung unterzeichnen, da sie entsprechend eingestufte Dokumente zur Weiterleitung an die angeschlossenen Betreiber erhalten wird.
- Die GÜAS leiten die vom BSI erhaltenen Informationen nur an Betreiber einer Kritischen Infrastruktur im Sinne von § 2 Absatz 10 BSIG weiter.

Durch die Benennung einer GÜAS ist es möglich, IT-Störungen **pseudonymisiert** an das BSI zu melden. Dazu entfernt die GÜAS alle betreiberidentifizierenden Informationen aus der Vorfallsmeldung. Eine mögliche Rückverfolgbarkeit muss durch die GÜAS sichergestellt werden.

5.8 Nachweise von Maßnahmen zum Schutz der Informationstechnischen Systeme - vorbereitende Maßnahmen

Zur Sicherstellung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von informationstechnischen Systemen und Prozessen hat sich der Aufbau so genannter Informationssicherheitsmanagementsysteme (ISMS) etabliert. Es wird erwartet, dass Aufbau und Betrieb eines ISMS auch wesentlicher Kern des branchenspezifischen Sicherheitsstandards wird, dessen (geprüfte) Einhaltung nach Abstimmung und Eignungsfeststellung durch das BSI als Nachweis geeigneter Maßnahmen i. S. d. § 8a Abs. 1 BSIG anerkannt wird.

Als Vorbereitung werden die folgen Maßnahmen empfohlen:

- organisatorische Festlegung der Verantwortlichkeiten für die IT-Sicherheit im Krankenhaus (Bestellung eines Informationssicherheitsbeauftragten)
- Erhebung des Status quo hinsichtlich der eingesetzten Verfahren, Prozesse und Systeme mit Blick auf die kritische Versorgungsdienstleistung der vollstationären Behandlung von Patienten

- Übersicht der im Krankenhaus etablierten Informationsinfrastrukturen, einschließlich einer Übersicht der hier eingesetzten Netzwerkstrukturen und Medizinprodukte, deren Ausfall oder Beeinträchtigung für die Erbringung der kritischen Versorgungsdienstleistung relevant sind
- Organisation eines übergreifenden Risikomanagements, das neben medizinischen und wirtschaftlichen Risiken auch Risiken aus den Bereichen IT-Sicherheit und Datenschutz berücksichtigt

In Vorbereitung der Umsetzung eines ISMS wird die Erstellung der folgenden Leit- und Richtlinien empfohlen („A 0 Dokumente“ gemäß Liste der BSI-Referenzdokumente):

- Leitlinie zur Informationssicherheit
- Richtlinie zur Risikoanalyse
- Richtlinie zur Lenkung von Dokumenten und Aufzeichnungen
- Richtlinie zur internen ISMS-Auditierung
- Richtlinie zur Lenkung von Korrektur- und Vorbeugungsmaßnahmen

5.9 Unterstützung durch das Lagezentrum des BSI

Gemäß § 8b Abs. 4 lit. a BSIG hat das BSI die Betreiber kritischer Infrastrukturen unverzüglich über sie betreffende Informationen zu folgenden Sachverhalten zu unterrichten.

- Informationen zu Sicherheitslücken, zu Schadprogrammen, zu erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und zu der dabei beobachteten Vorgehensweise,
- deren potentielle Auswirkungen auf die Verfügbarkeit der Kritischen Infrastrukturen
- relevanten Änderungen des Lagebildes bezüglich der Sicherheit in der Informationstechnik der Kritischen Infrastrukturen

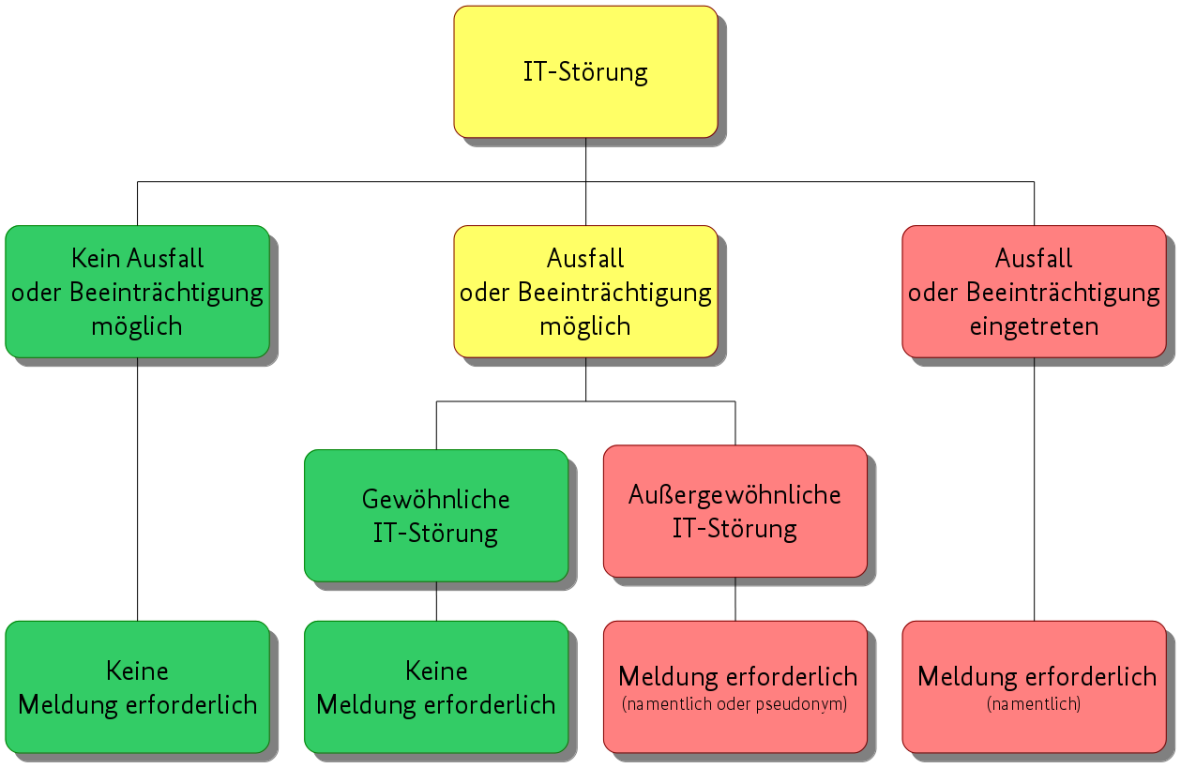
Aus Sicht der Krankenhäuser wäre eine zeitnahe Bewertung von Sicherheitsvorfällen oder akuten Gefährdungen sowie eine entsprechende Information an die Kontaktstelle wünschenswert. In der Vergangenheit haben sich an dieser Stelle jedoch häufig Informationsdefizite (teilweise aufgrund von Nachrichtensperren aufgrund laufender polizeilicher Ermittlungen) offenbart, teilweise waren Informationen in der einschlägigen Fachpresse früher verfügbar, als im Rahmen der Kommunikation an die Betreiber kritischer Infrastrukturen durch das BSI.

Ziel des bilateralen Informationsaustauschs sollte sein, dass Krankenhäuser bei beobachteten Angriffsszenarien rechtzeitig und substanziell mit verfügbaren Informationen aus dem operationalen Lagebild versorgt werden, um ggf. spezifische Schutzmaßnahmen ergreifen zu können.

6 Meldepflichtige Vorfälle (IT-Störungen)

Ausweislich der Begründung des ITSIG bzw. der BSI-KritisV wird von einer eher weiten Auslegung des Störungsbegriffs durch den Gesetzgeber ausgegangen. Eine Meldung ist immer erforderlich, wenn es bereits zu einem Ausfall oder zu einer Beeinträchtigung der betriebenen Kritischen Infrastruktur gekommen ist. Ist ein Ausfall oder eine Beeinträchtigung zwar möglich, aber (noch) nicht eingetreten, so ist eine Meldung nur erforderlich, wenn es sich um eine außergewöhnliche IT-Störung handelt.

Die folgende grafische Übersicht des BSI stellt die Klassifikation von Meldungen im Meldeprozess dar:



Quelle: *Bundesamt für Sicherheit in der Informationstechnik*

6.1 Gewöhnliche IT-Störungen

IT-Störungen werden als gewöhnlich bezeichnet, wenn sie mit den nach "Stand der Technik" umgesetzten technischen bzw. organisatorischen Maßnahmen abgewehrt wurden und ohne nennenswerte Folgen für die Versorgungsdienstleistung oder ohne erhöhten Ressourcenaufwand bewältigt wurden.

Zu Beispielen für gewöhnliche IT-Störungen siehe Abschnitt 7.1.1.

6.2 Außergewöhnliche IT-Störungen

IT-Störungen werden als außergewöhnlich bezeichnet, wenn sie nicht im Rahmen der üblichen Maßnahmen zum Schutz der Systeme, ggf. bereits automatisiert, abgewehrt

werden können, sondern nur mit erheblichem bzw. deutlich erhöhtem Ressourcenaufwand (z. B. erhöhtem Koordinierungsaufwand, Einbeziehung zusätzlicher, ggf. externer Experten, Nutzung einer besonderen Aufbauorganisation, Einberufung eines Krisenstabs) bewältigt werden können.

Zu Beispielen für außergewöhnliche IT-Störungen siehe Abschnitt 7.1.2.

6.3 Beeinträchtigung bzw. Ausfall informationstechnischer Systeme

Nach allgemeinem Verständnis im Kontext der Informationssicherheit (vgl. DIN ISO 27001) entsteht aus dem Aufeinandertreffen einer Bedrohung (z.B. Ransomware) auf eine Schwachstelle (z. B. nicht ausreichend abgesicherte Systeme) eine Gefährdung (z. B. Ausfall oder Beeinträchtigung der Versorgungsdienstleistung). Diese Gefährdung kann sich auf die angebotene Dienstleistung der kritischen Infrastruktur auswirken. Ob jedoch im Einzelnen von einer Beeinträchtigung oder dem Ausfall der Dienstleistung ausgegangen werden muss, hängt von vielen unterschiedlichen Faktoren ab.

Entsteht beispielsweise in der Dienstleistung der Sterilgutversorgung eine Störung, in deren Folge die Chargendokumentation fehlerhaft ist bzw. deren Korrektheit nicht sichergestellt werden kann, kann diese Charge eventuell nicht für den weiteren Prozess freigegeben werden. Können in der Folge Operationen nicht durchgeführt werden, ist ein Ausfall der Dienstleistung festzustellen.

Führt dieselbe Störung dazu, dass lediglich die Chargendokumentation nicht elektronisch (weiter-)verarbeitet werden kann, eine manuelle Chargenfreigabe jedoch möglich bleibt, sich in der Folge lediglich der Durchsatz freigegebener Chargen reduziert und ggf. nicht alle geplanten Operationen durchgeführt werden können, wird von einer Beeinträchtigung der kritischen Dienstleistung ausgegangen.

Das BSI definiert den **Ausfall der Funktionsfähigkeit** der kritischen Infrastruktur als einen Zustand, in dem die betroffene Anlage (in diesem Fall das Krankenhaus) aufgrund einer Störung der Informationstechnologie nicht mehr in der Lage ist, den von ihm erbrachten Anteil an der Erbringung der kritischen Dienstleistung (hier: stationäre Versorgung), zu leisten.

Die **Beeinträchtigung der Funktionsfähigkeit** wird seitens des BSI allgemein definiert als ein Zustand, in dem die betroffene kritische Infrastruktur aufgrund einer Störung der Informationstechnologie nicht mehr in der Lage ist, den von ihr erbrachten Anteil an der Erbringung der kritischen Dienstleistung voll umfänglich, also in der erwarteten Quantität (Menge pro Zeit) zu erbringen.

Das Kriterium der Beeinträchtigung tritt dann ein, wenn die Quantität (Leistung bzw. versorgte Personen) der erbrachten kritischen Dienstleistung der Anlage um mindestens 50 % der im Durchschnitt erbrachten Leistung oder versorgten Personen gemindert ist. Geplante Ausfallzeiten (z.B. durch Wartung, Baumaßnahmen) sind davon ausgenommen.

Letztere allgemeine Definition stößt im Rahmen der Patientenversorgung an Grenzen, da eine Quantifizierung der Patientenversorgung im Vergleich einem Produktionsbetrieb nicht sachgerecht erscheint.

7 Anhang

7.1 Beispielkonstellationen von IT-Sicherheitsvorfällen

Die nachfolgenden Beispiele greifen die Handlungsempfehlungen des Verbandes der Universitätsklinika Deutschlands (VUD) zur IT-Sicherheit, hier insbesondere „Allgemeine Grundsätze und Empfehlungen zum Meldewesen nach dem BSI-Gesetz“ vom 30.11.2017 auf und wurden um Aspekte, die auch für den nichtuniversitären Klinikbetrieb relevant sein können, ergänzt. Die Beispiele sind nicht abschließend formuliert, zudem werden mit Beginn der Meldepflicht ggf. Ergänzungen und Anpassungen des Verfahrens die erwartete „Lernkurve“ aller Beteiligten widerspiegeln. Ziel der vorliegenden Beispiele ist es, an konkreten Fallkonstellationen die differenzierte Betrachtung von IT-Störungen im Einzelfall darzustellen.

7.1.1 Beispiele für gewöhnliche IT-Störungen (in der Regel nicht meldepflichtig)

Ungerichtete Angriffe auf IT-Systeme gehören zum Tagesgeschäft aller IT-Infrastrukturen. Maßnahmen zur Erkennung und Abwehr entsprechender Angriffsversuche (Denial of Service-Angriffe, Schadsoftware) sind daher auch für Krankenhäuser unverzichtbar. Zwar verändert sich auch hier die Bedrohungslage und Angriffsszenarien entwickeln sich immer weiter, der Großteil der ungerichteten Angriffsversuche wird jedoch von den Abwehrmaßnahmen erfolgreich abgewehrt. Der Erkenntnisgewinn aus der Meldung einer einzelnen SPAM-Nachricht wird seitens der Anwender als gering eingeschätzt und steht in den meisten Fällen in keinem angemessenen Verhältnis zum Aufkommen dieser Begleiterscheinung elektronischer Kommunikation. Allerdings könnte der Hinweis auf eine neue SPAM-Methode tatsächlich als Beitrag zur Ergänzung des Lagebildes hilfreich sein. Es gilt daher, diejenigen Ereignisse zu erkennen, die für eine Meldung an das BSI infrage kommen. Der seitens des BSI vertretenen Auffassung „Besser eine Meldung zu viel, als eine zu wenig!“ steht der notwendige Arbeits- und Abstimmungsaufwand zur Meldung entgegen. Die folgenden Beispiele sollen daher gewöhnliche IT-Störungen umreißen, die in der Regel nicht meldepflichtig[3] sind. Ihnen gemein sind das tägliche Aufkommen sowie die geübten Abläufe um Umgang mit entsprechenden Störungen:

- bekannte, bereits veröffentlichte Sicherheitslücken, z. B. über das Warn- und Informationsportal des BSI (WID) verteilt, die bereits in der betroffenen Infrastruktur bearbeitet wurden
- Spam, der als unbedenklich bewertet wurde
- ungezieltes Phishing (bspw. mit generischen Themen, allgemein formulierter Anrede)
- „übliche“ Schadprogramme, die in der Regel durch Antivirensoftware erkannt werden
- technische Defekte im üblichen Rahmen (bspw. Festplattenfehler, Ausfall von Hardwarekomponenten)
- Ausfall eines Systems durch Hardwarefehler, dessen Funktion durch ein redundantes System weiterhin voll gegeben ist

[3] Im Einzelfall, z. B. bei Vorliegen einer hieraus resultierenden IT-Störung, welche die Versorgungsdienstleistung beeinträchtigt, können diese jedoch meldepflichtig werden.

- Verlust / Diebstahl von einzelnen Endgeräten, wenn kein entscheidendes Risiko zur Offenlegung von Daten vorliegt, z.B. bei Einsatz einer nach BSI-Vorgaben hinreichenden Verschlüsselungstechnologie, oder wenn das Endgerät keine schutzwürdigen Daten enthält, inkl. möglicher zwischengespeicherter Daten (Cache)
- durch eine Firewall abgewehrte Angriffsversuche, wenn es zu keiner nennenswerten Beeinträchtigung der übrigen Funktionalität der Firewall kam

7.1.2 Beispiele für außergewöhnliche IT-Störungen (meldepflichtig)

Im Gegensatz zu kritischen Infrastrukturen, die z. B. im Bereich der Produktion vergleichsweise einfach zu messende Parameter (z. B. „Tagesproduktion“) zur Ermittlung einer „Meldeschwelle“ heranziehen können, ist eine vergleichbare „Messbarkeit“ der kritischen Dienstleistung „stationäre Patientenversorgung“ nicht ohne weiteres gegeben. Die Identifikation außergewöhnlicher Störungen wird daher insbesondere von der Erfahrung und Qualifikation der hiermit betrauten Mitarbeiter in den Krankenhäusern abhängen.

Die nachfolgend dargestellten Szenarien kommen aus Sicht des VUD grundsätzlich für eine Meldung infrage, wobei im Kern die gravierende Abweichung vom IT-Normalbetrieb in Bezug auf Auslastung von Ressourcen oder in Bezug auf das Auftreten von unerwünschten Ereignissen steht:

- neue Angriffswege („Vektoren“) bzw. gezielte Ausnutzung von Sicherheitslücken, zu denen noch keinen Patch verfügbar ist
- erfolgreiches Überwinden einer Sicherungsmaßnahme (z. B. explizite Separierungstechnologie, Kapselungs- / Sandboxing-Technologie, Virenscanner etc.)
- außergewöhnliche (D)DoS-Angriffe, die zunächst nicht mit den vorhandenen proaktiven Maßnahmen (Mitigationsmaßnahmen) abgewehrt werden können
- erfolgte, versuchte oder erfolgreich abgewehrte gezielte IT-Angriffe (Advanced Persistent Threats - APT)
- außergewöhnliche und unerwartete technische Defekte mit IT-Bezug, die trotz Absicherung (z.B. Redundanzen) aufgetreten sind
- Spear-Phishing (Merkmale sind z. B. spezifische Themen auf den Empfänger zugeschnitten)
- Diebstahl / Offenlegung von Patientendaten
- Infektion von medizintechnischem Gerät mit Schadsoftware
- Softwarefehler in Systemen mit Patientendatenverarbeitung, wenn diese zu einer falschen Diagnostik bzw. Gefährdung des Therapieerfolgs führen oder führen könnten (z. B. Falschzuordnung von Befunden, Zeitverluste in kritischen Behandlungsfällen usw.)

Darüber hinaus kommen ggf. die folgenden Beispiele für eine Meldung an das BSI infrage:

- auffällige Anzahl von Account-Deaktivierungen im Activ Directory
- auffälliger Anstieg der abgewiesenen SPAMs/ Zeiteinheit
- auffällige Häufung von Meldungen zu Trojanerbefall oder Virus-Meldungen mit dem Status „nicht entfernbar“

- Auftreten von „Schadsoftware“ mit besonders aggressivem Verhalten in Bezug auf Datenverschlüsselung, Datenlöschung, Systemstörung, Systemdeaktivierung, Verbreitung im Netz, Ressourcenauslastung, Backupsystematik
- IT-Störungen mit besonders langer Wiederanlaufzeit

7.1.3 Beispiele für eine Beeinträchtigung oder einen Ausfall der Funktionsfähigkeit (meldepflichtig)

Insbesondere der Ausfall oder die Beeinträchtigung zentraler KH-Infrastrukturkomponenten (Netzwerk, Telefon, E-Mail, Kühlung, Heizung, Wasserversorgung usw.) bzw. der Ausfall oder die Beeinträchtigung von für die kritische Dienstleistung besonders wichtiger Organisationseinheiten (z.B. IT-Abteilung, Apotheke, Labor, Radiologie, Blutbank) stellt ein meldepflichtiges Ereignis dar. In den folgenden Fällen wird in der Regel von einer Meldepflicht des Ereignisses ausgegangen, wenn das zugrunde liegende Ereignis durch eine IT-Störung hervorgerufen wurde:

- Abmeldung einer Klinik von der Notfallversorgung
- Schließung von Stationen
- Ausfall oder Beeinträchtigung der Zentralsterilisation einer Klinik, wenn in der Folge Operationen abgesagt oder verschoben werden müssen
- Ausfall oder Beeinträchtigung der Radiologischen Diagnostik
- Ausfall oder Beeinträchtigung der Stromversorgung, Klimatisierung, Gebäude-steuerung (u.a. Beleuchtung, Fahrstuhl, Zutrittskontrollsystem), wenn dies zu nennenswerten Auswirkungen auf die Versorgung stationärer Patienten führte oder hätte führen können
- Nichtverfügbarkeit oder nicht gesicherte Integrität elektronischer Patientenakten
- Ausfall oder Beeinträchtigung der Lebensmittel-, Hilfsmittel- oder Medikamenten-versorgung
- Ausfall oder Beeinträchtigung der für die Dienstplanung genutzten elektronischen Systeme, wenn dies zu einer Beeinträchtigung der kritischen Dienstleistung geführt hat oder hätte führen können
- Ausfall oder Beeinträchtigung der zur Diagnose / Therapie genutzten elektronischen Systeme (z. B. Laborinformationssystem) oder der hierfür genutzten Informations-infrastruktur (z. B. infolge von Einschränkungen der Netzwerkperformance), so dass in der Folge durch manuelle Verarbeitung die Versorgungsqualität der Patienten beeinträchtigt wurde
- Ausfall oder Beeinträchtigung der Zentralsterilisationssoftware nach einem Update, (z. B. Ausfall der elektronischen Datenanbindung zu den Sterilisatoren), durch Umstellung auf einen manuellen Notbetrieb können nur noch weniger als 50 % der sonst üblichen Leistung erbracht werden, es müssen unkritische Operationen abgesagt oder verschoben werden
- die Patientenakten sind nicht valide oder es wurden Systemparameter / Metadaten zu Untersuchungen verändert, z.B. Bestrahlungsparameter manipuliert oder Patienten-Diagnose-Zuordnungen verändert.

- durch Ausfall oder Beeinträchtigung der Informationstechnik hervorgerufene Patientengefährdung an vernetzten Medizinproduktesystemen
- Ausfall von vernetzten Medizinprodukten oder medizinproduktenahen Systemen aufgrund von IT-Sicherheitsvorfällen, die sich auf IT-technische Designmängel zurückführen lassen (auch bei verfügbaren Redundanzsystemen und ohne akute Gefährdung der Patientenversorgung)

7.2 Kontaktdaten des BSI

Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189

Postfach 20 03 63

53133 Bonn

E-Mail: bsi@bsi.bund.de

KRITIS Büro

erste Anlaufstelle für:

- Registrierung Kontaktstelle
- Auslegung der BSI-KritisV
- Fragen zur Umsetzung ITSiG

Telefon: +49(0)228 99 9582 6166 (Montag-Freitag 08:00-15:30 Uhr)

E-Mail: kritis-buero@bsi.bund.de

BSI Lagezentrum / Meldestelle

falls online nicht möglich:

Telefon:

09:00-16:00 Uhr: +49(0)228 99 9582 6171

16:00-09:00 Uhr: +49(0)170 459 5627

7.3 Musterformular für Meldungen nach § 8b Abs. 4 BSIG

Das Muster des Meldeformulars nach § 8b Abs. 4 BSIG wird auch unter folgender Adresse bereitgestellt:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/Meldeformular_BSIG8b_Muster.pdf?__blob=publicationFile&v=3