Journal für Medizin- und Gesundheitsrecht

JMG 1|2021

ISSN 2415-6868
eISSN 2708-6410

Prof. Dr. Andreas Becker

Öffentlich bestellter und vereidigter Sachverständiger für Qualitäts-, Informationssicherheits- und Risikomanagement in Krankenhäusern (IHK zu Köln) / Qualifikation „Spezielle Prüfverfahrens-Kompetenz für § 8a BSIG“.

Anforderungen an die Informationssicherheit in deutschen Krankenhäusern (Teil I)

Das Thema „Informationssicherheit“ spielt in deutschen Krankenhäusern nicht erst seit dem Frühjahr 2016, als die Ransomware „Locky“ in deutschen Krankenhäusern zahlreiche Störungen verursachte, eine wichtige Rolle. Die zunehmende Digitalisierung vieler klinischer und nichtklinischer Prozesse führte dazu, dass die Informationssicherheit an Bedeutung gewonnen hat und die Öffentlichkeit ein angemessenes Maß an Informationssicherheit auch innerhalb der Krankenhäuser fordert.[1]

Der Gesetzgeber folgte diesem Trend und verpflichtete zwischenzeitlich alle Krankenhäuser, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind.

Der vorliegende Aufsatz gibt einen Überblick zu den rechtlichen Grundlagen und den daraus für die Krankenhäuser resultierenden Anforderungen.

1. Qualitätsmanagement-Richtlinie (QM-RL) des Gemeinsamen Bundesausschusses (G-BA)

Die QM-RL[2] *beschreibt die grundsätzlichen Anforderungen für eine erfolgreiche Einführung und Umsetzung von Qualitätsmanagement. Dabei hat der Aufwand in einem angemessenen Verhältnis insbesondere zur personellen und strukturellen Ausstattung zu stehen. Die konkrete Ausgestaltung des einrichtungsinternen Qualitätsmanagements erfolgt spezifisch in jeder Einrichtung*. Die Verpflichtung, ein einrichtungsinternes Qualitätsmanagement in Krankenhäusern einzuführen und weiterzuentwickeln (§ 135a Abs. 2 Nr. 2 SGB V[3]), bezieht sich auf nach § 108 SGB V sogenannte *zugelassene Krankenhäuser*, also Hochschulkliniken, Plankrankenhäuser und Krankenhäuser, die einen Versorgungsvertrag mit den Landesverbänden der Krankenkassen und den Verbänden der Ersatzkassen abgeschlossen haben.

Die Richtlinie (RL) besteht aus einem Teil A mit sektorenübergreifenden Rahmenbestimmungen für die grundsätzlichen Anforderungen an ein einrichtungsinternes Qualitätsmanagement (QM). Im Teil B erfolgen sektorenspezifische Konkretisierungen der Rahmenbestimmungen des einrichtungsinternen QM, dabei beschreibt der Teil B I die für die stationäre Versorgung über die Rahmenbestimmungen hinausgehenden oder konkretisierenden Inhalte des einrichtungsinternen QM.[4]

1 Siehe dazu aktuell: Die Lage der IT-Sicherheit in Deutschland 2020. Bundesamt für Sicherheit in der Informationstechnik (BSI). Stand September 2020, Artikelnummer BSI-LB20/509.

2 Richtlinie des Gemeinsamen Bundesausschusses über grundsätzliche Anforderungen an ein einrichtungsinternes Qualitätsmanagement für Vertragsärztinnen und Vertragsärzte, Vertragspsychotherapeutinnen und Vertragspsychotherapeuten, medizinische Versorgungszentren, Vertragszahnärztinnen und Vertragszahnärzte sowie zugelassene Krankenhäuser (Qualitätsmanagement-Richtlinie/QM-RL) in der Fassung vom 17. Dezember 2015 veröffentlicht im Bundesanzeiger (BAnz AT 15.11.2016 B2) in Kraft getreten am 16. November 2016, zuletzt geändert am 17. September 2020 veröffentlicht im Bundesanzeiger (BAnz AT 08.12.2020 B2) in Kraft getreten am 9. Dezember 2020.

3 Das Fünfte Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung – (Artikel 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477, 2482), das zuletzt durch Artikel 9 des Gesetzes vom 18. Januar 2021 (BGBl. I S. 2) geändert worden ist.

4 Siehe dazu auch in dieser Zeitschrift: Becker A, Wucherpfennig U-B (2017). Die neue QM-Richtlinie für Krankenhäuser in Deutschland: Inhalte und Exkurs zu den möglichen Folgen der Nichtbeachtung (Teil 1). Journal für Medizin- und Gesundheitsrecht. 2017; 2. (2): 105–111 | Wucherpfennig U-B, Becker A (2017). Die neue QM-Richtlinie für Krankenhäuser in Deutschland: Inhalte und Exkurs zu den möglichen Folgen der Nichtbeachtung (Teil 2). Journal für Medizin- und Gesundheitsrecht. 2017; 2. (3): 174–182.

In Teil A § 3 QM-RL werden die sogenannten *grundlegenden Elemente* des QM aufgelistet: Patientenorientierung einschließlich Patientensicherheit, Mitarbeiterorientierung einschließlich Mitarbeitersicherheit, Prozessorientierung, Kommunikation und Kooperation, Informationssicherheit und Datenschutz, Verantwortung und Führung.

Erwähnenswert ist hier, dass zur Informationssicherheit und zum Datenschutz in der RL nicht weiter inhaltlich ausgeführt wird. Da es diesbezüglich für die Krankenhäuser zwischenzeitlich entsprechende gesetzliche Regelungen gibt (siehe nachfolgend), ist das in der RL auch nicht erforderlich. Festzuhalten ist jedoch, dass diese Themenbereiche schon seit der Erstfassung der QM-QL vom 16.11.2016 als Grundelemente des QM definiert und diesem zugeordnet werden.

Weitere Ausführungen in der RL können auch heute noch problemlos auf die Ausgestaltung eines Informationssicherheitsmanagementsystems (ISMS) übertragen werden, so beispielsweise:

> *Unter Qualitätsmanagement ist die systematische und kontinuierliche Durchführung von Aktivitäten zu verstehen, mit denen eine anhaltende Qualitätsförderung im Rahmen der Patientenversorgung erreicht werden soll. Qualitätsmanagement bedeutet konkret, dass Organisation, Arbeits- und Behandlungsabläufe festgelegt und zusammen mit den Ergebnissen regelmäßig intern überprüft werden. Gegebenenfalls werden dann Strukturen und Prozesse angepasst und verbessert. Gleichzeitig soll die Ausrichtung der Abläufe an fachlichen Standards, gesetzlichen und vertraglichen Grundlagen in der jeweiligen Einrichtung unterstützt werden. Die Vorteile von Qualitätsmanagement als wichtiger Ansatz zur Förderung der Patientensicherheit sollen allen Beteiligten bewusstgemacht werden […] Ziele und Umsetzung des einrichtungsinternen Qualitätsmanagements müssen jeweils auf die einrichtungsspezifischen und aktuellen Gegebenheiten bezogen sein.* (Teil A § 1 QM-RL)

> *Qualitätsmanagement ist eine Führungsaufgabe, die in der Verantwortung der Leitung liegt. Dabei erfordert Qualitätsmanagement die Einbindung aller an den Abläufen beteiligten Personen. Qualitätsmanagement ist ein fortlaufender Prozess und von der Leitung an konkreten Qualitätszielen zur Struktur-, Prozess- und Ergebnisqualität auszurichten. Die Festlegung von […] Diese einrichtungsinternen Ziele sollen durch ein schrittweises Vorgehen mit systematischer Planung, Umsetzung, Überprüfung und gegebenenfalls Verbesserung erreicht werden, was auf dem Prinzip des sogenannten PDCA-Zyklus beruht. Durch die Identifikation relevanter Abläufe, ihre sichere Gestaltung und ihre systematische Darlegung sollen Risiken erkannt und Probleme vermieden werden. Um die eigene Zielerreichung im Rahmen des internen Qualitätsmanagements beurteilen zu können, sollten – wo möglich – Strukturen, Prozesse und Ergebnisse der Organisation und Versorgung gemessen und bewertet werden. Kennzahlen und valide Qualitätsindikatoren dienen dazu, die Zielerreichung intern zu überprüfen und somit die individuelle Umsetzung in den Einrichtungen zu fördern.* (Teil A § 2 QM-RL)

Auch das Informationssicherheits-Risikomanagement kann sich an der RL orientieren, denn so die RL in Teil A § 4 Abs. 1: *Risikomanagement dient dem Umgang mit potenziellen Risiken, der Vermeidung und Verhütung von Fehlern und unerwünschten Ereignissen und somit der Entwicklung einer Sicherheitskultur. Dabei werden unter Berücksichtigung der Patienten- und Mitarbeiterperspektive alle Risiken in der Versorgung identifiziert und analysiert sowie Informationen aus anderen Qualitätsmanagement-Instrumenten, insbesondere die Meldungen aus Fehlermeldesystemen genutzt. Eine individuelle Risikostrategie umfasst das systematische Erkennen, Bewerten, Bewältigen und Überwachen von Risiken sowie die Analyse von kritischen und unerwünschten Ereignissen, aufgetretenen Schäden und die Ableitung und Umsetzung von Präventionsmaßnahmen. Ein relevanter Teil der Risikostrategie ist eine strukturierte Risikokommunikation.*

2. Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz –ITSIG)

Das am 17.07.2015 in Kraft getretene ITSIG[5] wurde mit dem Ziel in Kraft gesetzt, diejenigen (*kritischen*) Infrastrukturen zu schützen, die für das Gemeinwesen von zentraler Bedeutung sind. Als sogenanntes Änderungsgesetz sah das ITSIG umfangreiche Änderungen in verschiedenen Gesetzen vor, so auch in dem im nächsten Abschnitt näher erläuterten Gesetz über das Bundesamt für Sicherheit in der Informationstechnik.

Der Vollständigkeit halber ist zu erwähnen, dass die Bundesregierung im Dezember 2020 den *Entwurf eines IT-Sicherheitsgesetzes 2.0* beschlossen hat, welches neue Verpflichtungen auch für die *Betreiber kritischer Infrastrukturen* vorsieht. So sollen diese mit dem ITSIG 2.0

5 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz). Bundesgesetzblatt Jahrgang 2015 Teil I Nr. 31, ausgegeben zu Bonn am 24. Juli 2015.

u.a. verpflichtet werden, Systeme zur Angriffserkennung einzusetzen.[6] Diese Systeme sind im Gesetzentwurf in Artikel 1 definiert als *Systeme zur Angriffserkennung im Sinne dieses Gesetzes sind durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten.*

Weiterhin ist vorgesehen: *Aufgrund veränderter Angriffsszenarien wird der Begriff der Protokollierungsdaten eingeführt und in § 2 Absatz 8a [BSIG] legaldefiniert. […] Protokollierungsdaten dienen der Erkennung, Eingrenzung oder Beseitigung von Störungen oder Fehlern bei der Kommunikationstechnik des Bundes oder der Erkennung, Eingrenzung oder Beseitigung von Angriffen auf die Kommunikationstechnik des Bundes. Inhaltsdaten sind daher regelmäßig keine Protokollierungsdaten. Die Zweckbestimmung schließt das Erstellen von Nutzerprofilen aus. Eine Auswertung von Kommunikationsinhalten von Nutzern ist nicht Gegenstand der Protokollierungsdatenverarbeitung. Mit der Verarbeitung von Protokollierungsdaten lassen sich unter anderem weit verbreitete Trojaner wie etwa die Schadsoftware „Emotet" besser erkennen. […] Die Nutzung von Protokollierungsdaten ist zudem das zweckmäßigste Mittel bei der Erkennung sogenannter Advanced Persistent Threats (APT). Hier handelt es sich um komplexe Angriffe (oftmals von fremden Nachrichtendiensten), deren Spuren regelmäßig nur in den Protokollierungsdaten zu finden sind.*

3. Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)

3.1 Allgemeines

Das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)[7] definiert die Informationssicherheitsanforderungen an Krankenhäuser, die bestimmte Kriterien erfüllen. In den folgenden Abschnitten wird die aktuelle Version des BSIG vom 19.06.2020 berücksichtigt, auf die Darstellung von Vorversionen wird verzichtet.

3.2 Definitionen und Festlegungen

3.2.1 IT-Sicherheit und Informationssicherheitsmanagement

Nach § 2 Abs. 1 BSIG umfasst die Informationstechnik *alle technischen Mittel zur Verarbeitung von Informationen.* In § 2 Abs. 2 BSIG wird die *Sicherheit in der Informationstechnik* definiert als die *Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen 1. in informationstechnischen Systemen, Komponenten oder Prozessen oder 2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen.*

Interessanterweise ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) *zuständig für die Informationssicherheit*[8] *auf nationaler Ebene* (§ 1 BSIG). Die Begriffe Informationssicherheit und Informationssicherheitsmanagement (ISM) werden jedoch im BSIG nicht erläutert, was der Verfasser als Mangel im BSIG betrachtet, denn die im BSIG definierten Anforderungen an die Betreiber Kritischer Infrastrukturen können (und sollen, dazu später mehr) nur durch die Einführung eines ISMS umgesetzt werden.

Üblicherweise verantwortet die IT-Abteilung die Betreuung der IT-Systeme und damit auch deren Sicherheit. Dazu gehören sowohl die Betreuung (zum Beispiel das Benutzer- und Rechtemanagement) als auch der Schutz (zum Beispiel das Patch- und Konfigurationsmanagement) der IT-Systeme beziehungsweise der elektronisch gespeicherten Daten, aber auch die Gewährleistung der Funktionalität, Verfügbarkeit und der Zuverlässigkeit. Das ISMS geht darüber weit hinaus, es beinhaltet zahlreiche Bereiche, wie zum Beispiel Personal, Organisation, Verantwortlichkeiten und physische Sicherheit, aber insbesondere auch die Sicherheit und das Management der IT-Systeme. Einen kontinuierlichen Prozess im ISMS stellen das Identifizieren und Bewerten von Risiken, verbunden mit der Umsetzung von Maßnahmen zur Reduzierung oder sogar Eliminierung dar.

Somit ist die IT-Sicherheit ein Bestandteil der Informationssicherheit. Die Verantwortung für die Informa-

6 Quelle: https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2020/12/it-sig-2-kabinett.html;jsessionid=3757A9B3631663FD7CBC6F0D482855F0.2_cid364 (Zugriff: 22.02.2021).

7 BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 73 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist.

8 Unterstreichung hier und nachfolgend nicht im Original, soweit nicht anders ausgewiesen.

tionssicherheit und das damit verbundene ISMS sollte bei der Geschäftsführung liegen. Da die IT-Abteilung einen wichtigen Teil des gesamten Managementsystems darstellt, sollte sie frühzeitig und intensiv in den Aufbau und den Betrieb des ISMS eingebunden sein.[9]

3.2.2 Kritische Dienstleistung – Kritische Infrastruktur

Die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz[10] (BSI-Kritisverordnung – BSI-KritisV)[11] spielt hier eine zentrale Rolle, denn sie definiert bestimmte Begriffe, legt für die einzelnen Sektoren (so auch für das Gesundheitswesen) fest, worin die *kritischen Dienstleistungen* bestehen, was zu den *Kritischen Infrastrukturen* gehört und, welche Fristen von den Betreibern zu berücksichtigen sind und welche *Schwellenwerte* angelegt werden.

Bei der *kritischen Dienstleistung* handelt es sich – entgegen der auch heute noch anzutreffenden Annahme – nicht um „die IT-Prozesse" eines Krankenhauses. Vielmehr ist darunter *eine Dienstleistung zur Versorgung der Allgemeinheit in den Sektoren […], deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde* zu verstehen (§ 1 Nr. 3 BSI-KritisV).

Im Sektor Gesundheit gehören hierzu (§ 6 Abs. 1 BSI-KritisV):

1. *die stationäre medizinische Versorgung (in den Bereichen Aufnahme, Diagnose, Therapie, Unterbringung/ Pflege und Entlassung nach § 6 Abs. 2 BSI-KritisV);*
2. *die Versorgung mit unmittelbar lebenserhaltenden Medizinprodukten, die Verbrauchsgüter sind;*
3. *die Versorgung mit verschreibungspflichtigen Arzneimitteln und Blut- und Plasmakonzentraten zur Anwendung im oder am menschlichen Körper;*
4. *die Laboratoriumsdiagnostik.*

Um Missverständnissen vorzubeugen, muss hier erwähnt werden, dass sich die Nummern 2 bis 4 nicht auf Krankenhäuser beziehen, sondern beispielsweise auf Medizinproduktehersteller, pharmazeutische Unternehmen oder Großhändler, freie Apotheken und freie Laboratorien. Natürlich werden im Rahmen einer externen Prüfung nach § 8a Abs. 3 BSIG auch Strukturen und Prozesse berücksichtigt, die sich inhaltlich auf die Nummern 2 bis 4 beziehen.

Kritische Dienstleistungen werden von bzw. in *Kritischen Infrastrukturen* erbracht, und dabei handelt es nicht um „die IT" eines Krankenhauses.

Nach § 6 Abs. 6 BSI-KritisV müssen zwei Kriterien erfüllt sein, damit eine sogenannte *Anlage* (oder Teile einer Anlage) als *Kritische Infrastruktur* und ihr Träger somit als KRITIS-*Betreiber* im Sektor Gesundheit eingestuft wird:

1. Es muss sich um eine *Anlage* (oder Teile einer Anlage) handeln, in der eine *kritische Dienstleistung* erbracht wird, die in Anhang 5 Teil 3 Spalte B BSI-KritisV aufgeführt ist und
2. die den zutreffenden Schwellenwert gemäß Anhang 5 Teil 3 Spalte D BSI-KritisV erreicht oder überschreitet.

Für ein Krankenhaus[12] bedeuten diese Kriterien, dass es als *Kritische Infrastruktur* eingestuft wird, wenn es nach § 108 SGB V für die stationäre Patientenversorgung zugelassen ist und den aktuellen Schwellenwert von 30.000 vollstationären Fallen pro Jahr erreicht oder überschreitet. In der Folge wird der Träger des Krankenhauses dann zum *Betreiber einer kritischen Infrastruktur*.

3.2.3. Betreiber oder nicht?

Alle Träger von nach § 108 SGB V für die stationäre Patientenversorgung zugelassenen Krankenhäusern müssen gemäß Anhang 5 Teil 1 Nr. 3 BSI-KritisV jeweils bis zum 31. März des Folgejahres prüfen, ob der Schwellenwert[13] von 30.000 vollstationären Fallen im zurückliegenden Kalenderjahr erreicht oder überschritten wurde.[14]

9 Siehe dazu auch bei: Skerka R-H, Becker A (2017). (K)eine Aufgabe für die IT? Informationssicherheit und ISMS. KU Gesundheitsmanagement. 2017; 86. (5): 58-61.

10 *Kritische Infrastrukturen im Sinne des BSIG sind Einrichtungen, Anlagen oder Teile davon, die 1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und 2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 [BSIG] näher bestimmt.* (§ 2 Abs. 10 BSIG).

11 BSI-Kritisverordnung vom 22. April 2016 (BGBl. I S. 958), die durch Artikel 1 der Verordnung vom 21. Juni 2017 (BGBl. I S. 1903) geändert worden ist.

12 Ein Krankenhaus wird in Anhang 5 Teil 1 Abs. 1 Buchstabe a) BSI-KritisV definiert als: *ein Standort oder Betriebsstätten eines nach § 108 des Fünften Buches Sozialgesetzbuch in der jeweils geltenden Fassung zugelassenen Krankenhauses, der oder die für die Erbringung stationärer Versorgungsleistungen notwendig ist oder sind.*

13 Dieser Schwellenwert, der aktuell von ca. 120 deutschen Krankenhäusern erreicht bzw. überschritten wird, wird zukünftig möglicherweise abgesenkt.

14 Auf spezielle Fragestellungen, wie beispielsweise der Bedeutung von gemeinsamen oder getrennten Bewilligungsbescheiden nach § 108 SGB V im Falle von mehreren Betriebsstätten eines Krankenhauses (konkret: werden Fälle verschiedener Standorte getrennt oder in Summe betrachtet?), wird im Rahmen dieses Aufsatzes nicht eingegangen.

Ist das der Fall, so gilt das Krankenhaus *ab dem 1. April des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den in Teil 3 Spalte D genannten Schwellenwert erstmals erreicht oder überschreitet, als Kritische Infrastruktur* (Anhang 5 Teil 1 Nr. 2 BSI-KritisV) und sein Träger als KRITIS-*Betreiber*.

3.3. Rechte und Pflichten der Krankenhausträger als KRITIS-Betreiber

Krankenhausträger als Betreiber einer *Kritischen Infrastruktur* unterliegen verschiedenen Verpflichtungen und haben auch Rechte, die nachfolgend aufgeführt werden:

3.3.1 Organisatorische und technische Vorkehrungen – Stand der Technik – Angemessenheit (§ 8a Abs. 1 BSIG)

Betreiber Kritischer Infrastrukturen sind verpflichtet […] 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. (§ 8a Abs. 1 BSIG)

Die zu treffenden organisatorischen und technischen Vorkehrungen sollen also Störungen von informationstechnischen Systemen, Komponenten oder Prozesse (Zielobjekte) vermeiden. Die Störungen werden dabei über die sogenannten Schutzziele definiert. Dabei geht es jedoch nur um solche Zielobjekte, die für die Funktionsfähigkeit der betriebenen Kritischen Infrastrukturen maßgeblich sind. Maßgeblich sind dabei zunächst solche Zielobjekte, die in unmittelbarem Zusammenhang mit der stationären Patientenversorgung stehen, dies ergibt sich aus der Definition der *Kritischen Dienstleistung*, wie später noch zu erkennen ist.

Das Erfordernis, angemessene organisatorische und technische Vorkehrungen zu treffen, besteht auch dann, wenn der Betreiber der Kritischen Infrastruktur seine IT durch einen externen Dienstleister betreiben lässt.[15]

Eine in der Praxis für die Krankenhäuser relevante Frage lautet, ob eine bestimmte organisatorische oder technische Vorkehrung dem *Stand der Technik* entspricht, denn dieser soll eingehalten werden. Der Versuch einer Definition des Begriffs Stand der Technik kann nur unter Berücksichtigung verschiedener Quellen (annähernd) gelingen, denn er ist als *unbestimmter Rechtsbegriff auch im Kontext der Informationssicherheit nicht abschließend definiert*, wie die Deutsche Krankenhausgesellschaft (DKG) im Dokument *Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus* (B3S) feststellt.[16]

Die *TeleTrusT – Bundesverband IT-Sicherheit e.V.*[17] führt zu dem Begriff wie folgt aus: *Der Technologiestand „Stand der Technik" muss von den begrifflich ähnlich lautenden Technologieständen wie den „allgemein anerkannten Regeln der Technik" […] und dem „Stand der Wissenschaft und Forschung" […] inhaltlich und messbar voneinander abgegrenzt werden. Diese Unterscheidung ist die wesentliche Grundlage für die Bestimmung des geforderten Technologiestandes. Wie viele Beispiele aus der Praxis zeigen, werden diese drei Begriffe gleichermaßen in der Rechtsprechung und in der Öffentlichkeit vermischt oder gar verwechselt.*

Eingeführt wurden diese drei Begriffe mit der Kalkar-Entscheidung des Bundesverfassungsgerichts im Jahr 1978[18] *und der damit einhergehenden „Drei-Stufen-Theorie". Das Technologieniveau „Stand der Technik" ist angesiedelt zwischen dem innovativeren Technologiestand „Stand der Wissenschaft und Forschung" und dem bewährten Technologiestand „allgemein anerkannten Regeln der Technik". Diese drei Technologiestände werden von den Kategorien „allgemeine Anerkennung" und „Bewährung in der Praxis" flankiert. Aufgrund der Systematik der Gesetze ist eine eindeutige Unterscheidung zwischen subjektiven und objektiven Tatbestandsmerkmalen erforderlich. Das Merkmal „Stand der Technik" ist rein objektivtechnisch zu verstehen. Die subjektiven Aspekte berücksichtigen die Gesetze im konkreten Tatbestand; sie betreffen aber nicht den Definitionsgehalt des „Standes der Technik" selbst.*

Somit kann der Stand der Technik als die im Waren- und Dienstleistungsverkehr verfügbaren Verfahren, Einrichtungen oder Betriebsweisen, deren Anwendung die Erreichung der jeweiligen gesetzlichen Schutzziele am wirkungsvollsten gewährleisten kann, bezeichnet werden.

Verkürzt lässt sich sagen: Der Stand der Technik bezeichnet die am Markt verfügbare Bestleistung eines Subjekts zur Erreichung eines Objekts. Subjekt ist die IT-Sicherheitsmaßnahme; Objekt das gesetzliche IT-Sicherheitsziel.

15 Bundestag-Drucksache 18/4096 vom 25.02.2015, Seite 26.

16 Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus – Gesamtdokument. Version 1.1 vom 22.10.2019. Deutsche Krankenhausgesellschaft; hier: Seite 10.

17 Handreichung zum „Stand der Technik" im Sinne des IT-Sicherheitsgesetzes (IT¬SIG). TeleTrusT – Bundesverband IT-Sicherheit e.V. Berlin. Ausgabe 2021, Version 1.8_2021-02 DE. Hinweis des Verfassers: aus fachlicher Sicht sehr zu empfehlen, wenn man sich zum Stand der Technik des „who is who" technischer und organisatorischer Maßnahmen (TOM) informieren möchte.

18 BVerfG 2. Senat, Beschluss 08.08.1978 – 2 BvL 8/77.

Fortschrittsbedingt kann eine Verschiebung über die einzelnen Technologiestände beobachtet werden („innovationsbedingte Verschiebung"): 1. Eine Maßnahme wird in ihrem Ursprung zunächst das Technologieniveau „Stand der Wissenschaft und Forschung" erreichen; 2. mit der Markteinführung geht sie den „Stand der Technik" über; 3. und mit zunehmender Verbreitung und Anerkennung am Markt wird sie irgendwann den „allgemein anerkannten Regeln der Technik" zugeordnet.

Das BSI selbst gibt mittlerweile *Hinweise zur Umsetzung der Kriterien des § 8a Absatz 1 BSIG für die Beurteilung der Informationssicherheit bei Betreibern Kritischer Infrastrukturen*[19]. In einem ebenfalls dem interessierten Leser sehr zu empfehlenden Dokument gibt das BSI Betreibern Kritischer Infrastrukturen (KRITIS-Betreiber) und auch prüfenden Stellen (siehe dazu später) eine *Konkretisierung der Anforderungen des § 8a Absatz 1 BSIG. Zudem stellt der Anforderungskatalog den prüfenden Stellen geeignete Kriterien für eine sachgerechte Prüfung der eingesetzten Sicherheitsvorkehrungen vor, um die geforderten Nachweise gemäß § 8a Absatz 3 BSIG erbringen zu können.* Mit diesem Anforderungskatalog *soll den KRITIS-Betreibern und prüfenden Stellen ein besseres Verständnis über die Sichtweise des BSI ermöglicht werden. Das Dokument stellt einen sachgerechten Ausgangspunkt dar, um die Anforderungen gemäß §8a Absatz 1 BSIG zu konkretisieren.* Auch wenn *dieser Anforderungskatalog kein verbindliches Kriterium im Sinne des § 8a Abs. 5 BSIG* darstellt, so enthält er doch ausführliche Darstellungen zu unterschiedlichen Anforderungen, so beispielsweise an das ISMS, das Asset Management, die Risikoanalysemethode, die technische Informationssicherheit etc.

In der Begründung[20] zum IT-Sicherheitsgesetz wird dazu ausgeführt: *Bei der Bestimmung des Standes der Technik sind insbesondere einschlägige internationale, europäische und nationale Normen und Standards heranzuziehen, aber auch vergleichbare Verfahren, Einrichtungen und Betriebsweisen, die mit Erfolg in der Praxis erprobt wurden. Die Verpflichtung zur Berücksichtigung des Stands der Technik schließt die Möglichkeit zum Einsatz solcher Vorkehrungen nicht aus, die einen ebenso effektiven Schutz wie die anerkannten Vorkehrungen nach dem Stand der Technik bieten.*

Weitere Ausführungen sind auch zu finden im *Handbuch der Rechtsförmlichkeit. Empfehlungen zur Gestaltung von Rechtsvorschriften nach § 42 Absatz 4 der Gemeinsamen Geschäftsordnung der Bundesministerien vom 22.08.2008* (hier: Abschnitt 4.5. Bezugnahmen auf technische Regeln).

Die KRITIS-Betreiber nach § 8a Abs. 1 BSIG sind nur zu solchen organisatorischen oder technischen Vorkehrungen verpflichtet, die sich im Sinne eines weiteren Kriteriums durch *Angemessenheit* auszeichnen. Dies ist dann der Fall, *wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.*

Hier soll also durch den Betreiber eine Prüfung erfolgen, bei der Aufwand[21] gegen mögliche Folgen abgewogen werden soll. Auch wenn eine solche Vorgehensweise aus dem Risikomanagement grundsätzlich bekannt ist[22], so besteht im Kontext der Kritischen Infrastruktur „Krankenhaus" zunächst Klärungsbedarf hinsichtlich der Operationalisierung des Begriffs *Folgen*.

Bei den möglichen *Folgen eines Ausfalls oder einer Beeinträchtigung der Kritischen Infrastruktur* kann eine quantitative und eine qualitative Komponente gesehen werden. Für die qualitative Komponente nennt das BSIG das Schutzziel der *Verfügbarkeit*, während als Besonderheit der Kritischen Infrastruktur „Krankenhaus" für die Qualität die Schutzziele des BSIG um die Schutzziele *Behandlungseffektivität* und *Patientensicherheit* zu ergänzen sind. Im B3S der DKG werden diese Schutzziele nachvollziehbar definiert[23] und bei einer Vielzahl von Maßnahmen im Rahmen des Informationssicherheits-Risikomanagements und auch bei informationstechnischen Systemen, Komponenten oder Prozessen als Kriterien aufgeführt, so u. a. bei der geforderten Festlegung der Kritikalität, bei der Festlegung der Strategien zur Risikobehandlung, dem Krankenhausinformationssystem (KIS), dem Laborinformationssystem (LIS), dem Radiologieinformationssystem (RIS), Systemen der Versorgungstechnik, Medizinprodukten etc.

Zum LIS wird beispielsweise wie folgt erläutert (Seite 50 f.): *Das LIS eines Krankenhauses hat insbesondere in*

19 Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 BSIG umzusetzenden Maß-nahmen. Hinweise zur Umsetzung der Kriterien des § 8a Absatz 1 BSIG für die Beurteilung der Informationssicherheit bei Betreibern Kritischer Infrastrukturen. („Anforderungskatalog zur Konkretisierung der Kriterien des § 8a Absatz 1 BSIG"). Version 1.0, Stand 28.02.2020; hier: Seite 4.

20 Bundestag-Drucksache 18/4096 vom 25.02.2015, Seite 26.

21 Aufwand mit „Kosten" zu übersetzen, ist hier naheliegend.

22 Beispielsweise bei der Abwägung der Angemessenheit von Maßnahmen zur Risikobewältigung.

23 Die DKG definiert im B3S vom 22.10.2019 (Seite 15) wie folgt: *Patientensicherheit als die Freiheit von unvertretbaren Risiken einer physischen Verletzung oder eines Schadens an der Gesundheit von Menschen. Dies schließt auch die Vermeidung einer nachhaltigen psychischen Belastung ein. Behandlungseffektivität stellt die wirksame Behandlung des Patienten unter Benutzung von Informationen und wirksamen Therapiemaßnahmen, ggf. auf Basis eines Informationsaustausches zwischen unterschiedlichen verantwortlichen Organisationseinheiten, sicher.*

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-Order-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.

Genaugenommen fordert § 8a Abs. 1 BSIG bei den *Folgen* also nur die Berücksichtigung der Auswirkungen, nicht jedoch der Eintrittswahrscheinlichkeiten. Zur Prüfung der Angemessenheit der Umsetzung oder Nichtumsetzung einer bestimmten organisatorischen oder technischen Vorkehrung durch eine Betreiberin wird empfohlen, den Aufwand, die Behandlungseffektivität, die Patientensicherheit und auch die weiteren Schutzziele in Form von Skalen festzulegen[24]. Hierbei handelt es sich um typische Festlegungen, die zu den Rahmenbedingungen eines Informationssicherheits-Risikomanagements oder auch eines Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten, gehören und sinnvollerweise von der Unternehmensleitung in einer Richtlinie festgeschrieben werden müssen. Hierzu geben beispielsweise die DIN EN ISO/IEC 27001[25], die DIN ISO 31000[26] oder auch die DIN EN 80001-1[27] weiterführende Informationen.

Hierzu auch in der Begründung[28] zum IT-Sicherheitsgesetzt: *Bei der Frage der Angemessenheit ist der bei dem Betreiber erforderliche Aufwand, insbesondere die von ihm aufzuwendenden Kosten, zu berücksichtigen. Um die Umsetzung der Mindestanforderungen zu dokumentieren, ist es sachgerecht, dass diese von den Betreibern in entsprechende Sicherheits- und Notfallkonzepte aufgenommen werden.*

3.3.2 Nachweispflicht (§ 8a Abs. 3 BSIG)

Nach § 8a Abs. 3 S. 1 BISG haben die Betreiber Kritischer Infrastrukturen *mindestens alle zwei Jahre die Erfüllung der Anforderungen nach [§ 8a] Absatz 1 [BSIG] auf geeignete Weise nachzuweisen.*

Wird beispielsweise erstmals mit Wirkung ab dem 01.04.2021 der Status als KRITIS-Betreiber festgestellt, so muss der Nachweis spätestens bis zum 31.03.2023 erbracht werden. Der Terminus *mindestens* bedeutet dabei, dass ein Prüfnachweis auch häufiger erbracht werden kann. So könnte eine Prüfung jährlich durchgeführt und so in die interne Auditplanung eines Krankenhauses im Rahmen des Qualitäts- und/oder Risikomanagements integriert und folglich auch in den Managementbewertungen berücksichtigt werden.

Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen (§ 8a Abs. 3 S. 2 BISG).

Zur näheren Ausgestaltung wird an späterer Stelle in diesem Aufsatz näher ausgeführt[29]. Hier wird jedoch bereits darauf hingewiesen, dass eine Zertifizierung nach DIN EN ISO/IEC 27001 nur dann *als Bestandteil eines Nachweises gemäß § 8a Absatz 3 BSIG verwendbar* ist, sofern weitere Anforderungen eingehalten werden, denn u. a. gilt gemäß BSI[30]:

Bei einer ISO 27001-Zertifizierung ist nicht automatisch der gesamte, für den Nachweis nach § 8a BSIG relevante Geltungsbereich erfasst. Der Geltungsbereich des Nachweises muss die Kritische Infrastruktur bzw. die kritische Dienstleistung (kDL) vollständig umfassen (Prozess-Sicht).

Zudem ist der Informationssicherheitsprozess bzgl. der kritischen Dienstleistung mit der „KRITIS-Brille" zu betrachten. Die Vermeidung von Versorgungsengpässen in der kritischen Dienstleistung ist im Kontext von KRITIS von sehr hoher Bedeutung. Daher muss die kritische Dienstleistung mit dem Fokus der Vermeidung von Versorgungsengpässen der Bevölkerung betrachtet werden.

Die KRITIS-Schutzziele (z. B. die Verfügbarkeit der kritischen Dienstleistung) sind in die eigene

24 Natürlich vervollständigt durch die Festlegung einer Skala für die Eintrittswahrscheinlichkeiten.

25 DIN EN ISO/IEC 27001. Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen (ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015); Deutsche Fassung EN ISO/IEC 27001:2017.

26 DIN ISO 31000. Risikomanagement – Leitlinien. Fassung Oktober 2018.

27 DIN EN 80001-1. 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.

28 Bundestag-Drucksache 18/4096 vom 25.02.2015, Seite 26.

29 Erfahrungsbericht zur ersten in einem Krankenhaus durchgeführten Prüfung bei: Skerka R-H, Becker A, Plomann R (2018). Erfahrungsbericht zum IT-Sicherheitsgesetz. Erstes Klinikum durchläuft Prüfung nach §8a BSIG. KU Gesundheitsmanagement. 2018; 87. (8): 65–67.

30 Orientierungshilfe zu Nachweisen gemäß § 8a (3) BSIG. Version 1.1 vom 21.08.2020. Bundesamt für Sicherheit in der Informationstechnik (BSI).

Risikobetrachtung aufzunehmen und durchgängig in allen Prozessen und Maßnahmenumsetzungen zusätzlich zu betrachten („KRITIS-Brille").

Daraus folgt, dass im Rahmen eines (Re-) Zertifizierungsaudits nach DIN EN ISO/IEC 27001 auch die KRITIS-Anforderungen berücksichtigt werden müssen, die über die Anforderungen der Norm hinausgehen, wenn die (Re-) Zertifizierung auch als Nachweis der Erfüllung des § 8a Abs. 3 BISG verwendet werden soll. Ebenso ist denkbar, dass eine bestehende Zertifizierung nach DIN EN ISO/IEC 27001 bei einer unterjährigen KRITIS-Prüfung als Eingabe für die aus der *KRITIS-Sicht* von der Norm abgedeckten Themen berücksichtigt wird.

Die Betreiber übermitteln dem Bundesamt die Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Das Bundesamt kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen (§ 8a Abs. 3 S. 3/4 BISG).

Der sogenannte Prüfbericht bzw. die zugrunde liegende Dokumentation wird nicht von einer prüfenden Stelle an das BSI übermittelt, sondern durch den KRITIS-Betreiber selbst.

Es kann bei Sicherheitsmängeln im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen (§ 8a Abs. 3 S. 4 BISG).

Auch wenn es bei der Verpflichtung zum Nachweis der Erfüllung der Anforderungen kein „Durchfallen" gibt, so sollte beachtet werden, dass gemäß § 8a Abs. 3 S. 1 der *Nachweis der Erfüllung* gefordert wird. In der Praxis bedeutete das bisher, dass das BSI ggf. geeignete Nachweise zur Behebung von Sicherheitsmängeln gemäß dem von dem KRISTIS-Betreiber vorzulegenden Maßnahmenplan angefordert hat. Dem Verfasser ist bezogen auf Krankenhäuser und auch freie medizinische Laboratorien bisher kein Fall bekannt, bei dem das BSI eine Sicherheitsmängelbeseitigung unter Einbeziehung einer Aufsichtsbehörde verlangen musste.

Der Nachweis dient der Kontrolle und Überprüfung der von den Betreibern getroffenen Maßnahmen und damit der Einhaltung eines angemessenen Sicherheitsniveaus durch die Betreiber. Die Ausgestaltung der Sicherheitsaudits, Prüfungen und Zertifizierungen soll nicht im Detail gesetzlich vorgegeben werden, da die Ausgestaltung von den gegebenenfalls erarbeiteten branchenspezifischen Sicherheitsstandards, den in den Branchen vorhandenen technischen Gegebenheiten und bereits bestehenden Auditierungs- und Zertifizierungssystemen abhängt. Generell soll geprüft werden, ob der Betreiber die für seine Branche und Technologie geeigneten und wirksamen Maßnahmen und Empfehlungen befolgt, etwa ein Information Security Management (Sicherheitsorganisation, IT-Risikomanagement etc.) betreibt, kritische Cyber-Assets identifiziert hat und managt, Maßnahmen zur Angriffsprävention und -erkennung betreibt, ein Business Continuity Management (BCM) implementiert hat und darüber hinaus die branchenspezifischen Besonderheiten (zum Beispiel den jeweiligen branchenspezifischen Sicherheitsstandard, sofern ein solcher erstellt und anerkannt wurde) umsetzt.[31]

3.3.3 Verpflichtung zur Kooperation (§ 8a Abs. 4 BSIG)

Das Bundesamt kann beim Betreiber Kritischer Infrastrukturen die Einhaltung der Anforderungen nach Absatz 1 überprüfen; es kann sich bei der Durchführung der Überprüfung eines qualifizierten unabhängigen Dritten bedienen (§ 8a Abs. 4 BSIG).

In diesem Fall hat der Betreiber einer Kritischen Infrastruktur *[…] dem Bundesamt und den in dessen Auftrag handelnden Personen zum Zweck der Überprüfung das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten und auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren* (ebenda).

Dem Verfasser ist bezogen auf Krankenhäuser und auch freie medizinische Laboratorien bisher kein Fall bekannt, bei dem das BSI eine solche Prüfung durchgeführt hat.

3.3.4 Kontaktstelle (§ 8b Abs. 3 BSIG)

Die Betreiber Kritischer Infrastrukturen haben dem Bundesamt […] eine Kontaktstelle für die von ihnen betriebenen Kritischen Infrastrukturen zu benennen. Die Betreiber haben sicherzustellen, dass sie hierüber jederzeit erreichbar sind (§ 8b Abs. 3 BSIG).

Dazu das BSI auf seiner Webseite[32]: *Die Angabe eines ein Funktionspostfachs – d. h. keine persönliche*

31 Bundestag-Drucksache 18/4096 vom 25.02.2015, Seite 26 f.

32 Siehe https://www.bsi.bund.de (Zugriff 24.02.2021; auf die Angabe des vollständigen Links wird verzichtet, da die Webseiten des BSI regelmäßig geändert werden).

E-Mail-Adresse eines einzelnen Mitarbeiters – wird empfohlen, um die jederzeitige Erreichbarkeit zu gewährleisten. Das BSI versteht unter der Formulierung „jederzeit erreichbar" gemäß § 8b Absatz 3 BSIG, dass Betreiber über die registrierte Kontaktstelle rund um die Uhr (24/7) in der Lage sind, BSI-Produkte zur Warnung und Information von KRITIS-Betreibern, (BSI-Produkte: Cyber-Sicherheitswarnungen, Lageinformationen etc.) entgegenzunehmen, unverzüglich zu sichten und zu bewerten (Bearbeitung der Informationen auf Zuruf). In der Regel werden BSI-Produkte während der üblichen Geschäftszeiten versendet. Es ist jedoch nicht auszuschließen, dass das BSI in Ausnahmefällen dringende Warnungen auch außerhalb der üblichen Geschäftszeiten, also an Feiertagen, Wochenenden oder nachts, versendet. Das BSI gestaltet die Cyber-Sicherheitswarnungen so, dass Dringlichkeit und (potenzieller) Handlungsbedarf aus der E-Mail-Betreffzeile (automatisiert) herausgelesen werden können. Somit können bereits existierende dauerhaft erreichbare Stellen in der Institution, z. B. Pforte, Werkschutz oder sonstige Bereitschaftsdienste, akuten Handlungsbedarf erkennen und ggf. eine Alarmierung bzw. Weiterleitung an geeignete Ansprechpartner vornehmen. Geeignete Ansprechpartner verfügen über die fachliche Kompetenz zur Beurteilung des konkreten Vorfalls und sind in die Organisation und Prozesse zur Vorfallsbewältigung eingebunden. Gesteigerte Anforderungen an die Verfügbarkeit einer Kontaktstelle des Betreibers ergeben sich nach einer Meldung einer IT-Störung gegenüber dem BSI. Um eine reibungslose Vorfallsbewältigung in Zusammenarbeit mit dem BSI zu gewährleisten, sollen interne (Weiterleitungs-)Prozesse eingerichtet werden, die eine Alarmierung geeigneter Ansprechpartner nach Eingang der Information auch außerhalb der üblichen Geschäftszeiten sicherstellen. Dies gilt insbesondere, wenn Sie eine IT-Störung an das BSI gemeldet haben und mit Rückfragen des BSI zu rechnen ist.

Die Meldung der Kontaktstelle erfolgt mit der Meldung als KRITIS-Betreiber im *Melde- und Informationsportal* des BSI.

Ergänzend ist hier zu erwähnen, dass die Kontaktstelle nicht nur Meldungen des BSI entgegennimmt, sondern auch Meldungen an das BSI übermitteln kann bzw. soll. Daraus folgt, dass der Betreiber auch interne Kommunikationsprozess sicherstellen muss, über Mitarbeiter und auch Dienstleister und Lieferanten Informationen an den Betreiber übermitteln können, die dann intern analysiert und hinsichtlich ihres Handlungs- und Meldebedarfs bewertet werden müssen. Im Rahmen des ISMS sollte die Kontaktstelle also als Bestandteil interner Melde- und Kommunikationsprozesse gesehen werden, die auch über Anknüpfungspunkte zum betrieblichen Kontinuitätsmanagement[33] verfügen sollen. In der Regel sind bereits entsprechende Alarm- und Kommunikationspläne innerhalb eines Krankenhauses vorhanden, so dass diese genutzt und angepasst werden können, um auch die Anforderungen des BSIG zu erfüllen.

3.3.5 Meldepflicht (§ 8b Abs. 4 BSIG)

Betreiber Kritischer Infrastrukturen haben die folgenden Störungen unverzüglich über die Kontaktstelle an das Bundesamt zu melden:

1. Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben,

2. erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können.

Die Nennung der *kritischen Dienstleistung* (sprich: stationäre Patientenversorgung) ist in § 8b Abs. 4 BSIG nicht erforderlich, da sich die *Störungen* oder *erheblichen Störungen* auf die Funktionsfähigkeit der *Kritischen Infrastrukturen* (potenziell) – mithin also auf die Funktionsfähigkeit des Krankenhauses – auswirken müssen. Ist dies der Fall, so ist die stationäre Patientenversorgung ebenfalls mindestens potenziell gefährdet.

Die Meldungen müssen unverzüglich nach Erkennung der Störung erfolgen, d. h. ohne schuldhaftes Zögern. Alle Erkenntnisse, die zum Zeitpunkt der Meldung vorliegen, müssen an das BSI gemeldet werden.

Eine *Störung* wird in der Begründung[34] des IT-Sicherheitsgesetzes wie folgt definiert: *Eine Störung im Sinne des BSI-Gesetzes liegt daher vor, wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken. Dazu zählen insbesondere Fälle von Sicherheitslücken, Schadprogrammen und erfolgten, versuchten oder erfolgreich abgewehrten Angriffen auf die Sicherheit in der Informationstechnik so-*

33 Hierzu gehören auch ggf. auszulösende Notfall- und Wiederanlaufpläne.

34 Bundestag-Drucksache 18/4096 vom 25.02.2015, Seite 27 f.

wie außergewöhnliche und unerwartete technische Defekte mit IT-Bezug (zum Beispiel nach Softwareupdates oder ein Ausfall der Serverkühlung).

Zu den Definitionen der hier wichtigen Termini erhebliche Störung, Ausfall, erhebliche Beeinträchtigung sowie möglicher Ausfall bzw. mögliche erhebliche Beeinträchtigung wird an dieser Stelle auf die Webseite des BSI verwiesen[35].

In der Praxis kommt immer wieder vor, dass Betreiber unsicher sind, ob eine Störung meldepflichtig ist oder nicht. Hier verfolgt das BSI[36] einen aus Sicht und Erfahrung des Verfassers pragmatischen und für die Betreiber hilfreichen Ansatz, denn die folgenden Fragen können *eine zusätzliche Hilfestellung bieten, ob die Störung zu melden ist: Hätte es mir geholfen, wenn ich Warnungen über diese Art von Vorfall von einem anderen Betreiber bekommen hätte? Ist die (mögliche) Einschränkungen relevant für die Versorgungslage? Im Zweifelsfall suchen Sie den Kontakt zum BSI. Die Mitarbeiter und Mitarbeiterinnen unserer Meldestelle werden Sie gerne hinsichtlich der Meldepflicht beraten.*

Ergreift das BSI in Folge einer Meldung Maßnahmen zur Beseitigung oder Vermeidung einer entsprechenden zukünftigen Störung, so kann es *Soweit erforderlich […] vom Hersteller der betroffenen informationstechnischen Produkte und Systeme die Mitwirkung an der Beseitigung oder Vermeidung einer Störung nach Absatz 4 verlangen* (§ 8a Abs. 6 BSIG).

3.3.6 Recht auf Unterrichtung (§ 8b Abs. 2 Nr. 4 lit. a) BSIG)

Das BSI hat als *zentrale Meldestelle* (§ 8b Abs. 1 BSIG*) die Betreiber Kritischer Infrastrukturen über sie betreffende Informationen zu unterrichten* (§ 8b Abs. 2 Nr. 4 lit. a) BSIG).

Dabei handelt es gemäß sich um § 8b Abs 2 Nr. 1–3 BSIG um

1. *die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik wesentlichen Informationen […], insbesondere Informationen zu Sicherheitslücken, zu Schadprogrammen, zu erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und zu der dabei beobachteten Vorgehensweise,*
2. *deren potentielle Auswirkungen auf die Verfügbarkeit der Kritischen Infrastrukturen in Zusammenarbeit mit den zuständigen Aufsichtsbehörden und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe […],*
3. *das Lagebild bezüglich der Sicherheit in der Informationstechnik der Kritischen Infrastrukturen […]*

Die KRITIS-Betreiber leisten durch die Meldungen nach § 8b Abs. 4 BSIG einen eigenen Beitrag und bekommen dafür, da sie auch von den Meldungen der anderen Betreiber an das BSI und der Bewertung dieser Meldungen durch das BSI profitieren, im Gegenzug ein Mehrfaches an Informationen und Know-how zurück[37].

35 Dort unter: *Fragen und Antworten für Betreiber Kritischer Infrastrukturen zur Meldepflicht nach dem IT-Sicherheitsgesetz.*

36 Ebenda.

37 Bundestag-Drucksache 18/4096 vom 25.02.2015, Seite 27.