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 II)

Dieser Teil des Aufsatzes widmet sich der Rolle des BSI, geht auf den neuen § 75c SGB V ein und erläutert Anforderungen und mögliche Folgen aus Sicht der Compliance.

3.4 Angebote, Rechte und Pflichten des BSI

Die entsprechenden Inhalte aus den §§ 8a Abs. 3.4 und 8b Abs. 1-4, 6 BSIG wurden bereits im vorigen Abschnitt erläutert.

3.4.1 Maßnahmen zur Wiederherstellung (§ 5a Abs. 1 BSIG)

Handelt es sich bei einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer Stelle des Bundes oder eines Betreibers einer Kritischen Infrastruktur um einen herausgehobenen Fall, so kann das Bundesamt auf Ersuchen der betroffenen Stelle oder des betroffenen Betreibers die Maßnahmen treffen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind.

Die Unterstützung des BSI kann dabei sogar so weit gehen, dass das BSI *vom Hersteller des informationstechnischen Systems verlangen* kann, *an der Wiederherstellung der Sicherheit oder Funktionsfähigkeit mitzuwirken*, *soweit es zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des informationstechnischen Systems erforderlich ist* (§ 5a Abs. 6).

Die hier aufgeführte Option stellt für KRITIS- Betreiber einen deutlichen Vorteil dar, denn sie können die Unterstützung des BSI anfragen, wenn es sich beispielsweise *um einen Angriff von besonderer technischer Qualität handelt oder die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems von besonderem öffentlichem Interesse ist* (§ 5a Abs. 2 BSIG).

3.4.2 Eignungsfeststellung branchenspezifischer Sicherheitsstandards (§ 8a Abs. 2 BSIG)

Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards […] vorschlagen. Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten.

Diese Möglichkeit verankert den kooperativen Ansatz, wie er in der Nationalen Strategie zum Schutz Kritischer Infrastrukturen[38] festgeschrieben wurde. Ziel ist es, dass sich Betreiber Kritischer Infrastrukturen branchenintern zusammenfinden und branchenspezifische Sicherheitsstandards erarbeiten. Das BSI stellt dabei als etablierte Kooperationsplattform zwischen Betreibern und Staat bereits entsprechende Strukturen zur Verfügung. Auch die branchenspezifischen Sicherheitsstandards müssen regelmäßig dem sich weiterentwickelnden Stand der Technik angepasst werden.[39]

Das BSI stellt zu den Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) eine *Orientierungshilfe als Handlungsempfehlung für Autoren, Betreiber und Prüfer* zur Verfügung.[40]

Ein B3S ist typischerweise kein von einer Normungsorganisation wie DIN oder ISO erstellter Standard. Er soll

38 Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). Bundesministerium des Inneren. Stand 17.06.2009.

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

40 Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a (2) BSIG. Handlungsempfehlung für Autoren eines B3S und Sicherheitsthemen für Kritische Infrastrukturen Handlungsempfehlung für Autoren eines B3S und Sicherheitsthemen für Kritische Infrastrukturen. Version 1.0 vom 01.012.2017. Bundesamt für Sicherheit in der Informationstechnik (BSI).

ein Konzept sein, das von Branchenvertretern gemeinsam definiert wurde und dass die Umsetzung von § 8a (1) BSIG bei den Betreibern Kritischer Infrastrukturen unterstützt und geeignete Sicherheitsanforderungen bzw. Sicherheitsvorkehrungen zusammenstellt. […] Eine gesetzliche Pflicht zur Erarbeitung eines solchen branchenspezifischen Sicherheitsstandards besteht nicht. Auch müssen die Betreiber bei vorliegendem B3S diesen nicht zwingend anwenden. Sie können sich auch nur auf Teile des B3S beziehen oder ein komplett eigenes Verfahren wählen. Dies bedeutet, dass es dem Betreiber überlassen bleibt, einen B3S anzuwenden, auf seine individuellen Gegebenheiten anzupassen, ggf. angemessen zu ergänzen – oder auch nicht.[41]

Der B3S der Deutschen Krankenhausgesellschaft, der der Öffentlichkeit über die Webseite der DKG frei zugänglich ist, *orientiert sich an der in der Praxis etablierten Norm ISO 27001, dem „Stand der Technik" sowie der darüberhinausgehenden branchenspezifischen Anforderungen der Norm ISO 27799, als auch der für den Krankenhausbereich relevanten wesentlichen Risiken. Eine Zertifizierung nach ISO 27001 ist für den Nachweis der notwendigen Maßnahmen nicht notwendig. Der B3S dient der Etablierung eines angemessenen Sicherheitsniveaus […] bei gleichzeitiger Wahrung des üblichen Versorgungsniveaus der Patientenversorgung und der Verhältnismäßigkeit der umzusetzenden Maßnahmen.*[42] *Die Umsetzung der geforderten Maßnahmen bedingt Fachwissen und Erfahrung auf dem Gebiet der Informationssicherheit. Sind diese Kenntnisse nicht in ausreichendem Maß vorhanden, empfiehlt sich die Inanspruchnahme qualifizierter Unterstützung.*[43]

3.4.3 Anforderungen an Prüfungen, Nachweise und prüfende Stellen (§ 8a Abs. 5 BSIG)

Das BIS kann zur Ausgestaltung des Verfahrens der Sicherheitsaudits, Prüfungen und Zertifizierungen nach [§ 8a] 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.

Zu diesem Zweck stellt das BSI eine *Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG* zur Verfügung, die *KRITIS-Betreibern und prüfenden Stellen eine Orientierung geben, was in § 8a Absatz 3 BSIG unter „auf geeignete Weise" in Bezug auf eine Prüfung zu verstehen ist und wie die gesetzlichen Anforderungen aus § 8a Absatz 3 BSIG erfüllt werden können. Es beschreibt die Anforderungen an die Beteiligten sowie deren Aufgaben und Zuständigkeiten und liefert Rahmenbedingungen an einen geeigneten Nachweis. Es erläutert den Ablauf der Einreichung von Nachweisen, zu beachtende formale Aspekte und einzuhaltende Fristen.*[44]

Im B3S wird ausführlich zu den folgenden Fragen ausgeführt[45]:

- Wie können KRITIS-Betreiber bei der Erfüllung der Nachweispflicht nach § 8a Absatz 3 BSIG vorgehen? Welche Informationen sollten sie wem bereitstellen?
- Welche Aufgaben haben prüfende Stellen? Was sind geeignete prüfende Stellen?
- Welche Aufgaben hat das Prüfteam und welche Kompetenzen sollte es besitzen?
- Wie sollte die Prüfung durchgeführt werden (Prüfgrundlage, -themen, -methoden, Ergebnisse)?
- Wie werden Nachweisdokumente eingereicht und welche Fristen gibt es zu beachten?

Dem geneigten Leser wird auffallen, dass § 8a Abs. 5 BSIG von *Anforderungen* spricht, das BSI jedoch „nur" eine *Orientierungshilfe* zur Verfügung stellt, die also eine „Hilfe zur Orientierung" geben soll. Auf diesen Unterschied wird nicht zu Zwecken eines semantischen Diskurses hingewiesen, sondern wegen der Tatsache, dass von KRITIS-Betreibern und auch Prüfern immer wieder der Grad der Verbindlichkeit der *Orientierungshilfe* diskutiert und hinterfragt wird. Dies geschieht unter dem Hinweis, dass die *Vertreter der betroffenen Betreiber und der betroffenen Wirtschaftsverbände* zur aktuellen Orientierungshilfe des BSI nicht angehört wurden, wie in § 8a Abs. 5 gefordert.

Unabhängig davon, wie man diese Frage beantwortet, ist aus der praktischen Erfahrung des Verfassers sinnvoll, die Orientierungshilfe des BSI bei der Planung und Durchführung einer Prüfung zu berücksichtigen, um – gerade als Prüfer – Diskussionen mit dem BSI zu einer durchgeführten Prüfung zu vermeiden. Hinzu kommt, dass die Orientierungshilfe aus praktischer Sicht wertvolle Hinweise für die KRITIS-Betreiber und Prüfer enthält.

41 Ebenda.
42 Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus – Gesamtdokument. Version 1.1 vom 22.10.2019. Deutsche Krankenhausgesellschaft. Hier: Seite 10.
43 Ebenda, Seite 11.
44 Orientierungshilfe zu Nachweisen gemäß § 8a (3) BSIG. Version 1.1 vom 21.08.2020. Hier: Seite 5.
45 Empfehlungen eines geprüften Krankenhauses zu den genannten Fragen bei: Plomann R, Becker A, Skerka R-H (2018). Planung und Durchführung einer Prüfung. „Lüner Empfehlung" zur Auswahl einer Prüfenden Stelle für eine Prüfung gem. § 8a (3) BSIG. KU Gesundheitsmanagement. 2018; 87. (12): 53–55.

4. § 75c SGB V

Mit dem Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz – PDSG)[46] wurde in das SGB V[47] eine neuer *§ 75c IT-Sicherheit in Krankenhäusern* eingeführt[48]. Die darin aufgeführten Pflichten gelten nur für solche Krankenhäuser, die nicht als Betreiber Kritischer Infrastruktur Vorkehrungen gemäß § 8a Abs. 1 BSIG zu treffen haben (§ 75c Abs. 3 SGB V).

Hierzu aus der Begründung[49]: *Die fortschreitende Digitalisierung eröffnet neue Potenziale und Synergien in der medizinischen Versorgung. Gleichzeitig wächst in der stationären Versorgung die Abhängigkeit von IT-Systemen. Aber auch das Bedrohungspotenzial wächst durch zunehmend zielgerichtete, technologisch ausgereiftere und komplexere Angriffe. Solche Cyberangriffe richten sich nicht nur gegen große Krankenhäuser mit über 30 000 vollstationären Fällen pro Jahr. Auch in Krankenhäusern mit geringeren Fallzahlen besteht ein großes Bedrohungspotenzial für die dort eingesetzten informationstechnischen Systeme, welches es einzudämmen gilt.*

§ 75c Abs. 1 SGB V verpflichtet Krankenhäuser, ab dem 01.01.2022 *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. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung des Krankenhauses oder der Sicherheit der verarbeiteten Patienteninformationen steht. Die informationstechnischen Systeme sind spätestens alle zwei Jahre an den aktuellen Stand der Technik anzupassen.*

Zunächst fällt auf, dass die Anforderungen nicht auf die stationäre Patientenversorgung eingegrenzt sind, zur Festlegung des individuellen Geltungsbereichs sollte daher der Versorgungsauftrag nach § 108 SGB V unter Berücksichtigung des tatsächlichen Leistungsgeschehens und der für das ISM relevanten Strukturen und Prozesse herangezogen werden.

Da § 75c SGB V Krankenhäuser adressiert, wird hier nicht von kritischer Infrastruktur gesprochen, sondern von *Krankenhäusern*.

Im Gegensatz zu § 8a Abs. 1 BSIG wird hier, ergänzend zu den genannten klassischen Schutzzielen, von *weiteren Sicherheitszielen* gesprochen, ohne diese näher zu benennen. Hierzu zählen jedoch sicher die vorab bereits erläuterten Schutzziele aus dem B3S der DKG *Behandlungseffektivität* und *Patientensicherheit*.

Während in § 8a Abs. 1 BSIG nur von der *Funktionsfähigkeit* (der kritischen Infrastruktur) gesprochen wird, erweitert § 75c Abs. 1 SGB V die Zielgröße auf die Sicherheit der verarbeiteten *Patienteninformationen*. Ob subsummierend damit auch eine Berücksichtigung des Datenschutzes eingebracht werden sollte, bleibt offen und geht auch aus der Begründung zum § 75c SGB V nicht hervor. In Anbetracht der in Deutschland bereits existierenden – zurückhaltend formuliert – umfassenden datenschutzrechtlichen Bestimmungen, wäre dies auch nicht erforderlich gewesen.

Ein mindestens zweijährig vorzulegender geeigneter Nachweis die Erfüllung der Anforderungen betreffend ist – im Gegensatz zu den Betreibern Kritischer Infrastruktur in § 8a Abs. 3 S. 1 BSIG – hier nicht vorgesehen. Spätestens alle zwei Jahre sind die *informationstechnischen Systeme […]* jedoch *an den aktuellen Stand der Technik anzupassen*. Auch hierzu führt die Begründung zu § 75c SGB V nicht aus.

Im Sinne einer nicht abschließenden Nennung wird in § 75c Abs. 2 erläutert, dass die Krankenhäuser die Verpflichtungen aus Abs. 1 erfüllen können, *indem sie einen branchenspezifischen Sicherheitsstandard für die informationstechnische Sicherheit der Gesundheitsversorgung im Krankenhaus in der jeweils gültigen Fassung anwenden, dessen Eignung vom Bundesamt für Sicherheit in der Informationstechnik nach § 8a Absatz 2 des BSI-Gesetzes festgestellt wurde.*

Hier wird also eindeutig auf solche B3S verwiesen, deren Eignung vom BSI festgestellt wurde. In der Begründung zum § 75c SGB V wird hierzu ergänzend festgehalten: *Die Eignung des entsprechenden branchenspezifischen Sicherheitsstandards für die Gesundheitsversorgung im Krankenhaus der Deutschen Krankenhausgesellschaft (B3S) wurde bereits vom Bundesamt für Sicherheit in der Informationstechnik bestätigt. Nach § 8a*

46 Bundesgesetzblatt Jahrgang 2020 Teil I Nr. 46, ausgegeben zu Bonn am 19. Oktober 2020.

47 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.

48 Unverständlich bleibt dabei, warum der neue § 75c im SGB V im vierten Kapitel mit dem Titel „Beziehungen der Krankenkassen zu den Leistungserbringern" und dort im zweiten Abschnitt („Beziehungen zu Ärzten, Zahnärzten und Psychotherapeuten") unter dem ersten Titel *„Sicherstellung der vertragsärztlichen und vertragszahnärztli-chen Versorgung"* eingefügt wurde.

49 Bundestag-Drucksache 19/20708 vom 01.07.2020, Seite 167.

Absatz 2 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik vom Bundesamt für Sicherheit in der Informationstechnik bestätigte branchenspezifische Sicherheitsstandards allgemein wie auch die Standards der Deutschen Krankenhausgesellschaft werden entsprechend dem Stand der Technik angepasst.

Der Verfasser schlussfolgert daraus, dass auch im „Nicht-KRITIS-Bereich" eine Orientierung an oder gar eine Zertifizierung nach DIN EN ISO/IEC 27001 allein nicht ausreichend wäre, wenn ergänzend nicht auch die besonderen Anforderungen, die sich aus der Patientenversorgung ergeben, berücksichtigt werden (siehe dazu vorab in Teil 1 dieses Aufsatzes im JMG 1-2021).

5. Compliance

5.1 Allgemeines

Das systematische Management der Informationssicherheit soll einen effektiven Schutz von Informationen und IT-Systemen in Bezug auf die Schutzziele gewährleisten, zu denen im Krankenhaus zusätzlich auch die Behandlungseffektivität und die Patientensicherheit gehören.

Dieser Schutz ist kein Selbstzweck, sondern dient der Unterstützung von Geschäftsprozessen, der Erreichung von Unternehmenszielen und dem Erhalt von Unternehmenswerten durch eine störungsfreie Bereitstellung und Verarbeitung von Informationen. Dabei gelten die folgenden Leitsätze:

1. Das ISMS mit allen Bestandteilen muss erkennbar eingeführt sein und erkennbar gelebt werden.
2. Daraus folgt, dass in der Organisation bestimmte Merkmale in der dokumentierten und gelebten Praxis feststellbar sind, die für einen externen Beobachter den Unterschied zwischen dieser Organisation und einer Organisation ohne ISMS ausmachen.
3. Ein effektives und effizientes ISMS kann natürlich in bestehende Systeme integriert werden, es muss jedoch als funktionales Managementsystem im Sinne eines „Lenken und Leiten mit Fokus auf Informationssicherheit" erkennbar sein.
4. Es geht bei der Einführung und Aufrechterhaltung des ISMS nicht um die Frage, wie das ISMS mit „möglichst geringstem Aufwand" umgesetzt bzw. in bestehende Systeme integriert werden kann.
5. Einführung und Aufrechterhaltung sollen unter dem Merkmal der „Angemessenheit" betrachtet werden, dabei geht es insbesondere um die Angemessenheit der technischen und organisatorischen Maßnahmen im konkreten Kontext der Organisation, der durch den Geltungs- und Anwendungsbereich abgebildet wird.

Unter Compliance ist die Einhaltung von gesetzlichen Bestimmungen und unternehmensinternen Richtlinien zu verstehen. Interne Richtlinien des Unternehmens können auch von Dritten entwickelte Prinzipien oder Konventionen sein, zu deren Einhaltung sich das Unternehmen selbst verpflichtet hat. Wirkt ein Unternehmen durch angemessene und miteinander verbundene Maßnahmen systematisch und effektiv auf Compliance hin, so spricht man von einem Compliance-Management-System (CMS).

Gemeinsam mit dem Risikomanagementsystem, dem internen Kontrollsystem und der internen Revision bildet das CMS die vier Elemente des „House of Governance". Die sogenannte Corporate oder Good Governance beschreibt die Steuerung und Überwachung von Geschäftsbetrieben mit dem übergeordneten Ziel einer verantwortungsvollen Unternehmensführung.

Die angemessene Beschäftigung mit Compliance oder gar die Einführung und Aufrechterhaltung eines CMS[50] bringt zahlreiche Vorteile mit sich, so zum Beispiel:

- Schafft Vertrauen von Stakeholdern, wie Eigentümern, Vertragspartnern und der Gesellschaft, in die Organisation.
- Motiviert die Organisationsmitglieder durch klare, unmissverständliche Vorgaben.
- Sichert nachhaltig den Wert der Organisation.
- Schützt die Reputation der Organisation.
- Erleichtert oder ermöglicht die Teilnahme an Ausschreibungen und Arbeitsgemeinschaften sowie den Zugang zu Finanzierungen.
- Kann das Risiko der Haftung und Bestrafung der Organisation beziehungsweise ihrer Organe und Mitarbeiter reduzieren.

5.2 Compliance und Informationssicherheit

Das Sicherheitskonzept nach dem BSIG bzw. § 75c SGB V sieht eine Sicherheitskonzeption vor, deren Fundament auf der Sicherstellung eines Mindestniveaus an Informationssicherheit durch angemessene organisatorische und technische Vorkehrungen unter Einhaltung des Stands der Technik basiert. Beide gesetzlichen Vorgaben erwarten eine regelmäßige Anpassung an den

50 Siehe dazu beispielsweise auch: Compliance Management Standards. Management & Dienstleistungen; Praxiskommentar zur ONR 192050, ONR 192051, ISO 19600 und ISO 37001. Herausgeber: Petsche A, Neuper O, Toifl A. 2017, Auflage 1. Auflage.

Stand der Technik, während nur die KRITIS-Betreiber der Nachweis- und Meldepflicht unterliegen.

Zur Erfüllung der sich aus dem BSIG bzw. dem § 75c SGB V ergebenden Anforderungen bedarf es der Einführung eines geeigneten ISMS, welches die medizinische Versorgung absichert und dabei die vielfältigen organisatorischen und thematischen Verknüpfungen berücksichtigt. Hierzu gehören beispielsweise die Medizin- und Gebäudetechnik sowie das CMS und das Risikomanagement. Die Leitungsorgane müssen also erkennen, dass es sich nicht um ein reines IT-Thema handelt. Um eine eindeutige und transparente Organisation der Verantwortlichkeiten und Kompetenzen zu erreichen, sollte die Geschäftsführung eine eindeutige Leitlinie herausgeben, die die Eckpunkte der Informationssicherheit festlegt. Auf Basis dieser Leitlinie werden Verantwortlichkeiten und Kompetenzbereiche der Abteilungen untereinander abgegrenzt und andererseits das erforderliche Miteinander in Fragen der Informationssicherheit geregelt.

5.3 Handlungsempfehlungen für Leitungsorgane

Leitungsorgane von Krankenhäusern sollten prüfen, ob die von ihnen geplanten oder bereits ergriffenen Maßnahmen ausreichen, um die Anforderungen aus dem BSIG oder dem § 75c SGB V zu erfüllen. Dabei sollten auf jeden Fall auch die Beauftragten für den Datenschutz und die Compliance beziehungsweise das CMS einbezogen werden. Der Compliance-Beauftragte sollte hierbei – insbesondere bei der Erstumsetzung des BSI-Gesetzes oder des § 75c SGB V – auf die Erstellung eines Umsetzungsplanes drängen, der bestimmte Zeitpunkte als kritische Messpunkte definiert.

Auch sollte gewährleistet werden, dass die umgesetzten Maßnahmen regelmäßig im Rahmen des internen Auditprogrammes überprüft werden. Audits und Stichprobenkontrollen sind auch deshalb notwendig, weil sie zu den erforderlichen Aufsichtsmaßnahmen im Sinne des § 130 OWiG gehören und so einen Beitrag zum Schutz der Organisationsverantwortlichen leisten können. Ob diese Kontrollmaßnahmen durch das Qualitätsmanagement, die IT-Abteilung, den Informationssicherheits-Beauftragten (ISB) oder den Compliance-Beauftragten (gegebenenfalls auch kombiniert) durchgeführt werden, hängt von den individuellen organisationalen Voraussetzungen des Krankenhauses ab.

5.4 Schadenspotenzial

Eine explizite Rechtspflicht zur Errichtung eines CMS existiert in Deutschland für Krankenhäuser, unabhängig von ihrer Trägerschaft, nicht. Der Begriff der Compliance hat im Krankenhausbereich seit dem Inkrafttreten des Gesetzes zur Bekämpfung von Korruption im Gesundheitswesen im Juni 2016 besondere Aufmerksamkeit erfahren.

Darüber hinaus bestehen für Krankenhäuser weitere Compliance-Risiken, die verschiedene Rechtsgebiete tangieren, beispielhaft seien hier genannt: Behandlungsprozess (Behandlungsfehler, Organisationsmängel), Abrechnung, Infektionsschutz und Krankenhaushygiene, Arbeits- und Sozialversicherungsrecht. Ganz besonders soll hier auch auf die Anforderungen an ein einrichtungsinternes Qualitätsmanagement gemäß der Richtlinie des G-BA hingewiesen werden, die auch wegen der möglichen Folgen der Nichtbeachtung aus der Compliance- Perspektive betrachtet werden muss.

Die zivilrechtliche Haftung für Organisationsmängel führt im Außenverhältnis – das heißt im Verhältnis zur Patientenseite – primär zu einer Haftung des Trägers (respektive der hinter ihm stehenden Haftpflichtversicherung). Im Innenverhältnis (Krankenhausträger zur Geschäftsleitung) ist die Missachtung erforderlicher innerbetrieblicher Organisationsstrukturen ein Mangel der Geschäftsleitung mit den Folgen der Regresspflicht gemäß § 93 Absatz 2 AktG[51], § 43 Absatz 2 GmbHG[52]. Treten in einem Unternehmen Compliance-Verstöße auf, kann dies zu einer ordnungsrechtlichen Außenhaftung führen (§§ 30, 130 OWiG[53]). Daran anknüpfend kann gegen die für die Gesellschaft handelnde Person ein Bußgeld im Rahmen einer Durchgriffshaftung verhängt werden.

Wenn entsprechendes Handeln in der vertikalen personellen Organisationsstruktur bekannt ist und – zumindest – geduldet wird, oder durch diese sogar bedingt ist, ist eine auch strafrechtliche Verantwortung in dieser vertikalen Organisationsstruktur in Form von Beihilfe oder Tatbeteiligung durch mittelbare Täterschaft nicht grundsätzlich zu verneinen. Allerdings stellen sich hinsichtlich der Kausalität und auch des subjektiven Tatbestands erhebliche strafrechtsdogmatische Fragen, deren Darstellung vorliegend zu weit geht. Insgesamt ist jedoch festzustellen, dass strafrechtliche Verantwortung aufgrund grober Mängel der Organisationsstruktur nicht auszuschließen ist.

51 Aktiengesetz vom 6. September 1965 (BGBl. I S. 1089), das zuletzt durch Artikel 15 des Gesetzes vom 22. Dezember 2020 (BGBl. I S. 3256) geändert worden ist.

52 Gesetz betreffend die Gesellschaften mit beschränkter Haftung in der im Bundesgesetzblatt Teil III, Gliederungsnummer 4123-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 16 des Gesetzes vom 22. Dezember 2020 (BGBl. I S. 3256) geändert worden ist.

53 Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 602), das zuletzt durch Artikel 3 des Gesetzes vom 30. November 2020 (BGBl. I S. 2600) geändert worden ist.

Ein primäres, sich direkt aus dem BSI-Gesetz ergebendes Schadenspotenzial ergibt sich aus der Nichteinhaltung der hier darin enthaltenen Vorgaben. Das BSIG sieht in § 14 für das folgende ordnungswidrige Verhalten Bußgelder vor:

- Die in § 8a Absatz 1 BSIG geforderten Maßnahmen werden vorsätzlich oder fahrlässig nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig getroffen. Das Bußgeld kann hier bis zu 50.000 Euro betragen (§ 14 Abs. 1 Nr. 1 BSIG).
- Die vorsätzliche oder fahrlässige Zuwiderhandlung gegen eine Auflage, die das BSI verfügt hat (§ 8a Absatz 3 Satz 5 BSIG), ist mit einem Bußgeld von bis zu 100.000 Euro bedroht (§ 14 Abs. 1 Nr. 2 BSIG).
- Wird die in § 8b Absatz 3 BSIG geforderte Kontaktstelle nicht vorsätzlich oder fahrlässig nicht oder nicht rechtzeitig benannt, so kann ein Bußgeld bis zu 50.000 Euro festgelegt werden (§ 14 Abs. 1 Nr. 3 BSIG).
- Wird eine Meldung über eine erhebliche Störung nach § 8b Absatz 4 Satz 1 Nummer 2 BSIG) vorsätzlich oder fahrlässig nicht unverzüglich über die Kontaktstelle an das BSI gemeldet, so droht ein Bußgeld bis 50.000 Euro (§ 14 Abs. 1 Nr. 4 BSIG).

Die Verwaltungsbehörde ist im Sinne des § 36 Absatz 1 Nummer 1 OWiG das BSI (§ 14 Abs. 3 BSIG).

Als sekundäres Schadenspotenzial, das sich aus der mangelhaften Sicherstellung eines Mindestniveaus an IT-Sicherheit durch angemessene organisatorische und technische Vorkehrungen unter Einhaltung des Stands der Technik ergeben kann, können die folgenden Punkte aufgeführt werden:

- Wird ein Bußgeld nach § 14 BSI-Gesetz verhängt, so besteht aus Sicht des Krankenausgeschäftsführers die Gefahr, dass die Frage seiner möglichen Haftung gegenüber dem Krankenhausträger zumindest geprüft wird.
- Kommt es zu einer Kompromittierung des Datenschutzes im Sinne des Bundesdatenschutzgesetzes, so drohen empfindliche Bußgelder.
- Die Folgen von Sicherheitszwischenfällen können gravierend sein, so berichtete beispielsweise ein deutsches Krankenhaus von Gesamtkosten in Höhe von 1.742.000 Euro, die eine Cyberattacke mit den resultierenden Erlösausfällen und Beratungskosten für IT-Sicherheitsexperten verursachte.
- Ein Reputationsschaden kann für ein Krankenhaus nicht nur durch ein spektakuläres und medienwirksames Ereignis wie eine Cyberattacke entstehen. Ebenso muss sich der daraus unter Umständen resultierende Rückgang von Patientenzahlen und damit auch Erlösen nicht zwangsläufig auf die akute Phase einer Krise beschränken.
- Kommt es in Folge erheblicher Störungen oder gar Ausfällen der stationären medizinischen Versorgung, die durch eine Unterschreitung des im BSI-Gesetz geforderten Mindestniveaus an Informationssicherheit bedingt sind, zu Patientenschäden[54], so ergeben sich hieraus vielfältige Risiken für den Krankenhausträger, seine Organe und auch verantwortliche Mitarbeiter. Diese Risiken können sich im schlimmsten Fall auch im Bereich des Zivil- und sogar Strafrechts bewegen.

Aus § 75c SGB V kann ein direktes Schadenspotenzial nicht abgeleitet werden. Das das SGB V jedoch den sozialrechtlich verbindlichen Standard definiert, könnte die Erfüllung der Verpflichtungen zukünftig eine Rolle bei der Krankenhausvergütung spielen und auch die Einführung einer Nachweispflicht würde nicht überraschen.

In allen Fällen besteht auch ein erhebliches Risiko hinsichtlich der negativen Auswirkungen auf die Kosten für die Haftpflicht- beziehungsweise IT-/Cyber-Versicherung eines Krankenhauses.

5.5 Fazit

Die gemäß BSIG bzw. SGB V einzuhaltenden gesetzlichen Bestimmungen erfordern, dass ein auf den ersten Blick „typisches IT-Thema“ auch und insbesondere unter dem Blickwinkel der Compliance zu betrachten ist.

Werden bestimmte Forderungen nicht rechtzeitig oder nicht vollständig erfüllt, so drohen daraus für KRITIS-Betreiber Bußgelder von bis zu 100.000 Euro.

Resultieren daraus auch Reputationsschäden, Erlösausfälle oder gar Patientenschäden, so bewegen sich die möglichen haftungsrechtlichen Folgenmöglicherweise auch im Zivil- und Strafrecht.

In jedem Fall stellt sich die Frage der Verantwortlichkeit einzelner Personen und auch des Organisationsverschuldens.

Krankenhausgeschäftsführer und deren Beauftragte sind unter präventiven Gesichtspunkten gut beraten, wenn sie prüfen, ob die von ihnen geplanten oder bereits ergriffenen Maßnahmen ausreichen, um die Anforderungen zur Informationssicherheit zu erfüllen.

54 Leider weltweit keine Einzelfälle mehr sind beispielsweise Patientenschäden – bis hin zum Tod – durch externe Angriffe auf Intensivstationen. In Deutschland standen im Jahr 2020 Cyber-Angriffe an zweiter Stelle der Meldungen von KRITIS-Betreibern an das BSI gem. § 8a Abs. 4 BSIG (Quelle: Die Lage der IT-Sicherheit in Deutschland 2020. Bundesamt für Sicherheit in der Informationstechnik (BSI). Stand September 2020, Artikelnummer BSI-LB20/509. Hier: Seite 54).