Prof. Dr. Andreas Becker, Edgar Gärtner

Der neue § 75c SGB V

Anforderungen an die Informationssicherheit in Krankenhäusern

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 durch eine Ergänzung des SGB V alle Krankenhäuser, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zu treffen. Der vorliegende Aufsatz gibt einen Überblick zum neuen § 75c SGB V und den daraus für die Krankenhäuser resultierenden Anforderungen.

Bisheriger Stand: IT-Sicherheitsgesetz und BSI-Gesetz

Das am 17. Juli 2015 in Kraft getretene Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz – ITSIG)[2] wurde mit dem Ziel in Kraft gesetzt, diejenigen 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 im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG)[3].

Das BSIG definiert die Informationssicherheitsanforderungen an Krankenhäuser, die bestimmte Kriterien erfüllen, die in der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz[4] (BSI-Kritisverordnung – BSI-KritisV)[5] festgelegt sind. Die BSI-KritisV 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, welche Fristen von den Betreibern zu berücksichtigen sind und welche Schwellenwerte angelegt werden.

Bei der kritischen Dienstleistung handelt es sich 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 Absatz 1 BSI-KritisV):

1. *die stationäre medizinische Versorgung (in den Bereichen Aufnahme, Diagnose, Therapie, Unterbringung/Pflege und Entlassung nach § 6 Absatz 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 Medizinprodukteherstellen, pharmazeutische Unternehmen oder Großhändler, freie Apotheken und freie Laboratorien. Natürlich werden im Rahmen einer externen Prüfung nach § 8a Absatz 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 Absatz 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[6] 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 Fällen pro Jahr erreicht oder überschreitet. In der Folge wird der Träger des Krankenhauses dann zum *Betreiber einer kritischen Infrastruktur.*

Die an die Krankenhausträger als Betreiber einer Kritischen Infrastruktur gestellten Anforderungen werden im nächsten Abschnitt in der Gegenüberstellung mit dem § 75c SGB V aufgegriffen.

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 u. a. verpflichtet werden, Systeme zur Angriffserkennung einzusetzen[7]. Diese Systeme sind im Gesetzentwurf in Artikel 1 wie folgt definiert: *Systeme zur Angriffserkennung im Sinne dieses Gesetzes sind durch technische Werkzeuge und organisatorische Einbindung unterstützte Pro-*

zesse 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.*

§ 75c SGB V

Mit dem Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz – PDSG)[8] wurde in das SGB V[9] eine neuer § *75c IT-Sicherheit in Krankenhäusern* eingeführt[10]. Die darin aufgeführten Pflichten gelten nur für solche Krankenhäuser, die nicht als Betreiber Kritischer Infrastruktur Vorkehrungen gemäß § 8a Absatz 1 BSIG zu treffen haben (§ 75c Absatz 3 SGB V).

Hierzu aus der Begründung[11]: *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. Auch in Krankenhäusern mit geringeren Fallzahlen besteht ein großes Bedrohungspotenzial für die dort eingesetzten informationstechnischen Systeme, welches es einzudämmen gilt.*

§ 75c Absatz 1 SGB V verpflichtet Krankenhäuser, ab dem 1. Januar 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.*

Übereinstimmungen und Unterschiede

Die §§ 75c Absatz 1 SGB V und 8a Absatz 1 BSIG weisen folgende Übereinstimmungen und Unterschiede auf:

- Nach beiden Paragrafen sind angemessene organisatorische und technische Vorkehrungen (OTV), die dem Stand der Technik entsprechen, zu treffen.
- Die OTV adressieren im BSIG vier Schutzziele, nämlich die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit. Im SGB V dagegen werden nur drei Schutzziele explizit genannt, hier fehlt die Authentizität[12]. Dieser Unterschied ist nicht nachvollziehbar, da Informationssicherheit nach DIN EN ISO/IEC 27000[13] auch die Authentizität berücksichtigen kann, wie es auch in der DIN EN ISO/IEC 27001[14] umgesetzt wird: hier wird die Authentizität zwar nicht bei den primären Schutzzielen eines Informationssicherheitsmanagementsystems (ISMS) aufgeführt (Abschnitt 0.1), jedoch wird sie im Anhang A der Norm unter A.10.1 bei den Schutzzielen von Kryptographischen Maßnahmen genannt. Auch im Branchenspezifischen Sicherheitsstandard (B3S) für die Gesundheitsversorgung im Krankenhaus[15] der Deutschen Krankenhausgesellschaft (DKG) ist die Authentizität als Schutzziel aufgeführt. Möglicherweise wird die Authentizität im § 75c Absatz 1 SGB V unter den hier erwähnten *weiteren Sicherheitszielen* subsumiert, zu denen dann auch die im B3S der DKG sinnvollerweise aufgeführte *Behandlungseffektivität* und *Patientensicherheit* zählen würden.
- Während in § 8a Absatz 1 BSIG nur von der *Funktionsfähigkeit* (der Kritischen Infrastruktur) gesprochen wird, erweitert § 75c Absatz 1 SGB V die Zielgröße auf die *Sicherheit der verarbeiteten Patienteninformationen*. Ob subsumierend damit auch eine Berücksichtigung des Datenschutzes eingebracht werden sollte, bleibt offen und geht auch aus der Begründung[16] zum § 75c SGB V nicht hervor. Auch in Anbetracht der bereits existierenden datenschutzrechtlichen Regelungen (Datenschutz-Grundverordnung/DSG-VO[17]) ist die Motivation zur Ergänzung *Sicherheit der verarbeiteten Patienteninformationen* nicht nachvollziehbar.[18]
- Weiterhin fällt auf, dass die Anforderungen im § 75c Absatz 1 SGB V nicht – wie im KRITIS-Bereich gemäß BSI-Kritisverordnung (BSI-KritisV)[19] – auf die stationäre Patientenversorgung eingegrenzt sind. Daher dürfte hier auch die teilstationäre Behandlung und die ambulante Versorgung zum Regelungsbereich gehören. Die Festlegung des individuellen Geltungsbereichs sollte daher das tatsächliche Leistungsgeschehen und die für das ISMS relevanten Strukturen und Prozesse heranziehen. ▶

- Da § 75c Absatz 1 SGB V Krankenhäuser adressiert, wird hier nicht von Kritischen Infrastrukturen gesprochen, sondern von *Krankenhäusern*.
- Während sich die BSI-KritisV auf *Standorte oder Betriebsstätten eines nach § 108 des Fünften Buches Sozialgesetzbuch in der jeweils geltenden Fassung zugelassenen Krankenhauses* (Anhang 5, Teil 1 Nr. 1) bezieht, sieht § 75c Absatz 1 SGB V die Beschränkung auf nach § 108 SGB V zugelassene Krankenhäuser nicht vor.
- Ein mindestens zweijährig vorzulegender geeigneter Nachweis zur Erfüllung der Anforderungen betreffend ist – im Gegensatz zu den Betreibern Kritischer Infrastruktur in § 8a Absatz 3 S. 1 BSIG – im § 75c SGB V 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 Absatz 2 SGB V erläutert, dass die Krankenhäuser die Verpflichtungen aus Absatz 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 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.*

Die Verfasser schlussfolgern aus dem Hinweis auf B3S der DKG, 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. So ist im KRITIS-Bereich eine Zertifizierung nach DIN EN ISO/IEC 27001 nur dann *als Bestandteil eines Nachweises gemäß § 8a Absatz 3 BSIG verwendbar,* sofern weitere Anforderungen eingehalten werden, denn u. a. gilt gemäß BSI[20]:

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 bezüglich 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 (zum Beispiel die Verfügbarkeit der kritischen Dienstleistung) sind in die eigene 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 Absatz 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.

- Auch die folgenden Verpflichtungen, denen KRITIS-Betreiber unterliegen, treffen auf den „§ 75c-Bereich" nicht zu: Verpflichtung zur Kooperation (§ 8a Absatz 4 BSIG), Benennung einer Kontaktstelle mit jederzeitiger Erreichbarkeit (§ 8b Absatz 3 BSIG), Meldepflicht (§ 8b Absatz 4 BSIG).
- Das Recht auf unverzügliche Unterrichtung durch das BSI über die Betreiber betreffende Informationen (§ 8b Absatz 2 Nr. 4 lit. a) BSIG), wie für *die Abwehr von Gefahren […] wesentlichen Informationen […] insbesondere Informationen zu Sicherheitslücken, zu Schadprogrammen, zu erfolgten oder versuchten Angriffen […] und zu der dabei beobachteten Vorgehensweise, sowie deren potentielle Auswirkungen […]* (§ 8b Absatz 2 Nr. 1-3 BSIG) ist im § 75c SGB V nicht kodifiziert. Die KRITIS-Betreiber leisten durch die Meldungen nach § 8b Absatz 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[21].

Zwischenfazit

Mit dem neuen § 75c SGB V formuliert der Gesetzgeber Informationssicherheitsanforderungen an Krankenhäuser, die nicht zum Kreis der KRITIS-Betreiber gehören und – je nach individueller Ausgangssituation – zur Umsetzung der geforderten Maßnahmen erhebliche Anstrengungen und Aufwände erfordern können. In Anbetracht der – vorsichtig formuliert – komplexen Antragsverfahren zum Krankenhauszukunftsfonds[22] besteht kein Anlass zu ausgeprägtem Optimismus, dass alle Krankenhäuser zumindest eine angemessene finanzielle Unterstützung für die anstehenden Maßnahmen erhalten werden.

Empfohlen wird ein gestuftes Umsetzungskonzept, welches sich angemessen an den strukturellen und prozessualen Gegebenheiten des Krankenhauses orientiert und dabei etablierte Quellen, wie beispielsweise die DIN EN ISO/IEC 27001, das IT-Grundschutz-Kompendium des BSI und natürlich den B3S der

DKG, ebenso angemessen berücksichtigt. Zum Stand der Technik von Maßnahmen werden auch die Handreichung des Bundesverbandes IT-Sicherheit e.V.[23] und die Hinweise zur Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen des BSI[24] empfohlen.

Zur Frage, ob bezüglich der Umsetzung der geforderten Maßnahmen bzw. ihrer Anpassung an den Stand der Technik auch in Zukunft eine Nachweispflicht nicht eingeführt wird, könnte heute nur spekuliert werden. Die Erfahrungen der Vergangenheit sprechen jedoch eher dafür, dass die Krankenhäuser mit einer Nachweispflicht rechnen müssen.

Wünschenswert wäre eine zügige Überarbeitung des § 75c Absatz 1 SGB V hinsichtlich der oben angesprochenen sprachlichen bzw. inhaltlichen Unklarheiten, die sich aus den Textunterschieden zum § 8a Absatz 1 BSIG ergeben.

Compliance

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, dem Erreichen von Unternehmenszielen und dem Erhalt von Unternehmenswerten durch eine störungsfreie Bereitstellung und Verarbeitung von Informationen. Dabei gelten die folgenden Leitsätze:

- Das ISMS mit allen Bestandteilen muss erkennbar eingeführt sein und erkennbar gelebt werden.
- 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.
- 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.
- 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.
- 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[25] 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.

Compliance und Informationssicherheit

Vom 1. Januar 2022 an gilt die Regelung des § 75c SGB V zur Informationssicherheit in Krankenhäusern als unmittelbar geltendes Recht. Die bereits bestehenden rechtlichen Verpflichtungen zum Datenschutzrecht (etwa dem Umgang mit personenbezogenen Daten oder Patientendaten) sowie der technische Datenschutz (etwa Datenschutz-Grundverordnung, DS-GVO; Bundes und Landesdatenschutzgesetze, BDSG und LDSG) werden um die gesetzliche Regelung zur Informationssicherheit ergänzt.

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 basiert. Beide gesetzlichen Vorgaben erwarten eine regelmäßige Anpassung an den 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, das die medizinische Versorgung absichert und dabei die vielfältigen organisatorischen und thematischen Verknüpfungen berücksichtigt. Hierzu gehören beispielsweise die Medizin- und Gebäudetechnik, 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.

Handlungsempfehlungen für Leitungsorgane

Leitungsorgane von Krankenhäusern sollten prüfen, ob die von ihnen geplanten oder bereits ergriffenen Maßnahmen ausreichen, um die Anforderungen aus dem § 75c SGB V zu erfüllen. Dazu ist erforderlich, die vorhandenen technischen Vorkehrungen zur Störungsvermeidung zu analysieren und diese – ggfs. sachkundig beraten – an den aktuellen Stand der Technik iSd § 75c SGB V anzupassen. Dabei sollten auf jeden Fall auch die Beauftragten für den Datenschutz und die Compliance beziehungsweise das CMS einbezogen werden.

Der Compliance-Beauftragte sollte – insbesondere bei der Erstumsetzung des § 75c SGB V – auf einen verbindlichen Umsetzungsplan drängen, der bestimmte Zeitpunkte als kritische Messpunkte definiert.

Auch nach der erstmaligen Anpassung an den aktuellen Stand der Technik bis spätestens 1. Januar 2022 gehört zu den organisatorischen Vorkehrungen des § 75c SGB V eine effektive Pflichtendelegation, den Stand der Technik und seine Weiterentwicklung regelmäßig zu beobachten – aber auch branchenspezifische Risiken, wie etwa gezielte Angriffe auf die IT-Sicherheit anderer Krankenhäuser.

Die Pflichtendelegation setzt selbstredend entsprechende Fach- und Sachkenntnis der Delegierten in der Informationssicherheit voraus. Diese müssen deshalb geschult und ihre Weiterbildungen sollten dokumentiert sein.

Technische oder rechtliche Veränderungen betreffend der Informationssicherheit müssen ebenso erkannt und analysiert werden wie auch aktuelle Risiken, etwa durch bewusste (Cyber-) Angriffe von außen. Nach § 75c Absatz 1 S. 3 SGB V sind die informationstechnischen Systeme bereits kraft Gesetzes alle zwei Jahre an den aktuellen Stand der Technik anzupassen. Ein effektives ISMS muss aber in der Lage sein, auch „unterjährig" zu reagieren, so etwa bei einem identifizierten konkreten Störungsrisiko mit drohenden Auswirkungen auf die Funktionsfähigkeit des Krankenhauses.

Ein funktionierendes ISMS verlangt im Vorhinein festgelegte Melde- und Berichtswege ebenso wie korrespondierende Kompetenzzuweisungen und Vertretungsregelungen. Vielfach gehen mit Störungen in der Informationssicherheit auch datenschutzrechtliche Verstöße einher, so beispielsweise unverzügliche Meldepflichten an den Datenschutzbeauftragen. Die beiden Bereiche des Datenschutzes und der Informationssicherheit sollten deshalb miteinander kooperieren.

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 Informationssicherheitsbeauftragten (ISB) oder den Compliancebeauftragten (gegebenenfalls auch kombiniert) durchgeführt werden, hängt von den individuellen organisationalen Voraussetzungen des Krankenhauses ab.

Die Einrichtung einer effektiven und effizienten Compliance-Struktur dient dazu, die Risiken von Gesetzesverstößen, Missbräuchen und fehlerhaften Handlungen zu verringern. Ganz vermeidbar werden Verstöße aber nicht sein. Die Leitungsorgane und die dafür verantwortlichen weiteren Delegierten sollten deshalb darauf vorbereitet und auch entsprechend geschult sein, dass es zu Störungen in der Informationssicherheit kommen kann, die auch schwerwiegend sein können. § 75c SGB V spricht selbst von *Störungen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind.* Für den Störungsfall sollte deshalb eine Zuständigkeits- und Ablaufregelung vorhanden sein, die aufzeigt, wie damit umzugehen ist.

Zwingend geboten ist, neben der unverzüglichen Beseitigung der Störungsursache, eine Aufklärung der identifizierten Informationssicherheitsstörung sowie deren Dokumentation. Vorhandene Verfahrensanweisungen sind an die gewonnenen Erkenntnisse zur Störungsursache anzupassen und die damit tangierten Mitarbeiter im gestörten Ablaufprozess sind mit den Änderungen vertraut zu machen (zum Beispiel über Attachments oder Schulung).

Die vom neuen § 75c SGB V normierte Informationssicherheit kann effektiv im Krankenhaus nur dann erreicht und verbessert werden, wenn die Leitungsorgane auch die richtigen Konsequenzen nach einem Störungsfall ziehen.

Zeigt die zuvor beschrieben Aufklärung eines Sicherheitsstörfalls das Fehlverhalten eines identifizierten Mitarbeitenden des Krankenhauses, sollte im Rahmen der arbeitsrechtlichen Möglichkeiten darauf reagiert werden. Dabei kann – abhängig von der Schwere des Verstoßes sowie der Schuldform (etwa Vorsatz oder nur leichteste Fahrlässigkeit) auch nach dem bekannten Führungsgrundsatz vorgegangen werden: „Be hard in the issue and soft on the person." Das Selbstverständnis der Krankenhausführung, die Informationssicherheit ernst zu nehmen, wie sie jetzt in § 75c SGB V für die dortigen Krankenhäuser kodifiziert wurde, kommt nirgendwo besser zum Ausdruck als im Umgang mit „non-compliant" handelnden Mitarbeitenden.

Haftungsrisiko

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

Darüber hinaus bestehen für Krankenhäuser weitere Compliance-Risiken, die verschiedene Rechtsgebiete tangieren. Beispielhaft seien hier der Behandlungsprozess (Behandlungsfehler, Organisationsmängel), Abrechnung, Infektionsschutz und Krankenhaushygiene, Arbeits- und Sozialversicherungsrecht genannt. 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.

Beim Haftungsrisiko im Falle eines Verstoßes möchten wir zwischen der (zivilrechtlichen) Haftung des Krankenhauses bzw. des jeweiligen Trägers einerseits und einer (zivilrechtlichen) Haftung der verantwortlichen Leitungsorgane bzw. Mitarbeiter andererseits unterscheiden.

- Die Frage des Haftungsrisikos stellt sich im Falle der Beeinträchtigung der Informationssicherheit im Krankenhaus immer dann, wenn es durch den Störungsfall zu bezifferbaren wirtschaftlichen Schäden gekommen ist.
- Die Folgen von Sicherheitszwischenfällen können gravierend sein; so berichtete beispielsweise ein deutsches Krankenhaus von Gesamtkosten in Höhe von 1 742 000 €, die eine Cyberattacke mit den resultierenden Erlösausfällen und Beratungskosten für IT-Sicherheitsexperten verursachte.[26] Aber auch gegenüber Dritten, vor allem auch gegenüber Patienten können durch Störfälle Haftungen entstehen, wenn das Krankenhaus durch mangelnde Organisation zur angemessenen Behandlung nicht mehr oder nur stark zeitverzögert in der Lage ist.
- Die Schadenskosten trägt primär das Krankenhaus selbst, respektive der dahinterstehende Krankenhausträger. Inwieweit eine Haftpflichtversicherung für solche Schäden regressiert werden kann, hängt vom Vorhandensein einer entsprechenden Versicherung und der Ausgestaltung des jeweiligen Versicherungsvertrages ab. Eine verantwortungsvolle Krankenhausleitung sollte das Inkrafttreten des § 75c SGB V zum Anlass nehmen, den vorhandenen Bestand an Versicherungen auf die Einstandspflichten bei Störungen der Informationssicherheit überprüfen zu lassen.

Für die Leitungsorgane und sonstige verantwortliche handelnde Personen besteht aber im Störfalle stets das weitere Risiko einer eigenen Schadenshaftung gegenüber dem Krankenhausträger. Dabei hilft ein vielfach „wohlgesonnener" Krankenhausträger wenig, sofern eine Haftpflichtversicherung einstandspflichtig ist. Nach § 86 Absatz 1 VVG[27] geht nämlich kraft Gesetzes (cessio legis) *dieser Anspruch auf den Versicherer über, soweit der Versicherer den Schaden ersetzt.*

Die persönliche Eigenhaftung der Leitungsorgane und der anzuwendende Sorgfaltsmaßstab haben im Gesellschaftsrecht bereits seit Längerem gesetzliche Ausprägungen gefunden. Sich diese immer wieder ins Bewusstsein zu rufen, ist hilfreich.

So heißt es in § 43 Absatz 1 GmbHG[28]: *Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden.* Und § 43 Absatz 2 GmbHG begründet die persönliche Haftung der Geschäftsführer mit ihrem Privatvermögen kurz und bündig: *Geschäftsführer, welche ihre Obliegenheiten verletzen, haften der Gesellschaft solidarisch für den entstandenen Schaden.*

Noch deutlicher wird die gesetzliche verankerte Organisationsverpflichtung der Leitungsorgane bei der Aktiengesellschaft. § 91 Absatz 2 AktG[29] lautet dazu: *Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.* Nach § 93 Absatz 1 S. 1 AktG haben auch die *Vorstandsmitglieder bei ihrer Geschäftsführung die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden.* Die persönliche Haftung der Leitungsorgane wird in aller Klarheit in § 93 Absatz 2 AktG festgeschrieben, wenn es heißt: *Vorstandsmitglieder, die ihre Pflichten verletzen, sind der Gesellschaft zum Ersatz des daraus entstehenden Schadens als Gesamtschuldner verpflichtet.*[30]

Zur Absicherung dieser vielfach existenzgefährdenden persönlichen Haftung wird den Leitungsorganen empfohlen, eine evtl. bestehende sogenannte D&O-Versicherung[31] im Hinblick auf den ab 1. Januar 2022 geltenden § 75 c SGB V daraufhin zu überprüfen, ob diese Haftungsrisiken versicherungsvertraglich abgesichert sind. Besteht noch keine D&O-Versicherung, sollte mit dem Arbeitgeber der Abschluss einer solchen (nach-)verhandelt werden.

Straf- und Bußgeldrisiko

Ein primäres, sich direkt aus dem BSI-Gesetz ergebendes Bußgeldrisiko ergibt sich aus der Nichteinhaltung der hier darin enthaltenen Vorgaben. Das BSIG sieht in § 14 für verschiedene ordnungswidrige Verhalten Bußgelder vor, die bis zu 100 000 € betragen können. Verwaltungsbehörde ist hier im Sinne des § 36 Absatz 1 Nummer 1 OWiG das BSI (§ 14 Absatz 3 BSIG). Nach §§ 14 Absatz 1 Nr. 1 in Verbindung mit 8a Absatz 1 S. 1 BSIG ist auch explizit der Verstoß gegen die Verpflichtung der Betreiber Kritischer Infrastrukturen ordnungswidrig, für eine angemessene organisatorische und technische Vorkehrung zur Störungsvermeidung der Informationssicherheit zu sorgen.

Demgegenüber ist die in § 75c Absatz 1 SGB V ab 1. Januar 2022 neu geschaffene Verpflichtung für die übrigen Krankenhäuser nicht bußgeldbelegt, sofern gegen die Verpflichtung verstoßen wird, für angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen für die genannten Sicherheitsziele zu sorgen. § 395 SGB V, der die Bußgeldvorschriften enthält, wurde vom Gesetzgeber nicht angepasst. Eine Begründung hierfür findet sich in den Gesetzesmaterialien nicht.[32] Wenn ein Krankenhaus jedoch, die gesetzliche Verpflichtung aus § 75c SGB V missachtend, keine ausreichenden Vorkehrungen trifft und es kommt zu einer Störung im genannten Umfang (Maßgeblichkeit für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen) kommt, sind damit vielfach andere Straftatbestände verletzt und Ordnungswidrigkeiten verwirklicht.

Zu denken ist aus dem Bereich des Strafrechts etwa an das Ausspähen von Daten nach § 202a StGB[33], die Datenveränderung nach § 303a StGB, die Computersabotage nach § 303b StGB, strafbare Verstöße nach § 42 BDSG[34] und die Verletzung von Privatgeheimnissen nach § 203 StGB, weil in der Regel unweigerlich auch sensible, dem Arztgeheimnis unterfallende Patientendaten tangiert sind. ▶

Aus der Sicht des Ordnungswidrigkeitenrechts sind vielfach Datenschutzverstöße begangen worden, sofern es zu Störfällen in der Informationssicherheit kommt. Zu nennen sind etwa die Bußgeldvorschriften des § 43 BDSG und der entsprechenden LDSG, aber ebenso Artikel 83 DS-GVO[35]. Mit dem Inkrafttreten der DS-GVO wurde gegenüber den vorherigen nationalen datenschutzrechtlichen Vorschriften die Möglichkeit geschaffen, horrende Bußgelder und Sanktionen zu verhängen, die im Höchstmaß nach Artikel 83 Absatz 6 DS-GVO bis zu 20 Mio. € oder bis zu 4 % des weltweiten Jahresumsatzes des betroffenen Unternehmens betragen können. Die Rechtspraxis zeigt, dass die Datenschutzbehörden mit der Verhängung von Bußgeldern in dramatischer Höhe auch tatsächlich ernst machen.[36]

Die Leitungsorgane eines Krankenhauses sind im Bereich des Straf- und Ordnungswidrigkeitenrechts die primären Adressaten der jeweiligen Tatbestände.

Verletzt das verantwortliche Direktoriumsmitglied seine Verpflichtung aus 75c SBG V und kommt es deshalb zu einem Störfall in der Informationssicherheit, die einen Straf- oder Ordnungswidrigkeitentatbestand verwirklicht, so handelt (auch) das Leitungsorgan durch seine (Aufsichts-)Pflichtverletzung nach § 130 Absatz 1 OWiG selbst ordnungswidrig, sofern diese Störung *durch gehörige Aufsicht verhindert oder wesentlich erschwert worden wäre.*

Diese durch die Aufsichtspflichtverletzung begangene Ordnungswidrigkeit kann nach § 130 Absatz 3 S. 1 OWiG mit einer Geldbuße bis zu 1 Mio. € geahndet werden. Dabei ist zu konstatieren, dass dieses Bußgeld nicht vom Arbeitgeber „übernommen“ werden kann, weil die Aufsichtspflichtverletzung im Krankenhaus niemals „im betrieblichen Interesse“ liegen kann. Es gibt auch keine Versicherung, die die Zahlung der Geldbuße übernehmen würde. Das Bußgeld hat das betroffene Leitungsorgan vielmehr aus seinem Privatvermögen zu zahlen, ohne die Möglichkeit einer steuerlichen Geltendmachung.

Daneben gibt es im Recht der Ordnungswidrigkeiten die Möglichkeit – wovon in der Praxis auch vielfach Gebrauch gemacht wird – nach § 30 OWiG eine Verbandsgeldbuße zu verhängen, sofern das Leitungsorgan eine Pflicht verletzt hat, die den Verband trifft. Dies ist bei der neu geschaffenen Verpflichtung aus § 75c Absatz 1 S. 1 SGB V ohne weiteres der Fall; danach sind nämlich „Krankenhäuser verpflichtet“, die genannten Vorkehrungen zu treffen.

Die Bußgelder für diese Verbandsgeldbuße sind nach § 30 Absatz 2 OWiG hoch, sie können bis zu 10 Mio. € betragen; auch für das Krankenhaus bzw. den Krankenhausträger gibt es keine Möglichkeit einer Versicherung, die eine Geldbuße übernehmen würde.

Selbstverständlich bergen Störungen in der Informationssicherheit, erst recht mit anschließenden straf- oder bußgeldrechtlichen Ermittlungen, immer die Gefahr eines hohen Reputationsschadens – vor allem, wenn es sich um ein medienwirksames Ereignis wie etwa eine Cyberattacke mit nachweisbaren und schweren Auswirkungen auf die Patientensicherheit handelt. Ebenso muss sich der daraus unter Umständen resultierende Rückgang von Patientenzahlen und damit auch Erlösen nicht zwangsläufig auf die akute Phase einer Krise beschränken.

Mögliche Auswirkung auf Krankenhausvergütung

Zu bedenken ist schlussendlich, dass mit dem SGB V ein sozialrechtlich verbindlicher Standard definiert wird. Die Erfüllung der neuen Verpflichtung aus § 75c SGB V kann deshalb unter Umständen vom 1. Januar 2022 an eine Rolle bei der Krankenhausvergütung spielen.

Fazit

Die gemäß SGB V – und auch nach dem BSIG – 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 die Forderungen des § 75 SGB V nicht rechtzeitig oder nicht vollständig erfüllt, so drohen möglicherweise Bußgelder nach dem OWIG.

Resultieren aus Informationssicherheitszwischenfällen Reputationsschäden, Erlösausfälle oder gar Patientenschäden, so bewegen sich die möglichen haftungsrechtlichen Folgen möglicherweise 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, zu prüfen, ob die von ihnen geplanten oder bereits ergriffenen Maßnahmen ausreichen, um die Anforderungen zur Informationssicherheit zu erfüllen.

Kommt es durch erhebliche Störungen oder gar Ausfälle der stationären medizinischen Versorgung, die durch eine Unterschreitung des im Gesetz geforderten Mindestniveaus an Informationssicherheit bedingt sind, zu Patientenschäden[37], 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.

In allen Fällen sind zudem negative Auswirkungen auf die Kosten für die Haftpflicht- beziehungsweise IT-/Cyber-Versicherung eines Krankenhauses sehr wahrscheinlich.

Anmerkungen

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

3) 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

4) 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 Absatz 10 BSIG)

5) 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.

6) Ein Krankenhaus wird in Anhang 5 Teil 1 Absatz 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.

7) Quelle: https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2020/12/it-sig-2-kabinett.html;jsessionid=3757A9B3631663FD7CBC6F0D482855F0.2_cid364 (Zugriff: 1. März 2021)

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

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

10) 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 vertragszahnärztlichen Versorgung" eingefügt wurde.

11) Bundestag-Drucksache 19/20708 vom 1. Juli 2020, Seite 167

12) Authentizität der Informationen ist sichergestellt, wenn sie von der angegebenen Quelle erstellt wurden.

13) DIN EN ISO/IEC 27000. Informationstechnik – Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Überblick und Terminologie (ISO/IEC 27000:2016); Deutsche Fassung EN ISO/IEC 27000:2017. Oktober 2017. (hier: Abschnitt 2, Nr. 2.33)

14) 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. Juni 2017.

15) Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus. Gesamtdokument. Deutsche Krankenhausgesellschaft. Version 1.1, 22.10.2019. (hier: Abschnitt 3.5)

16) Bundestag-Drucksache 19/20708 vom 1. Juli 2020, Seite 167

17) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Amtsblatt der Europäischen Union L 119/1 vom 04.05.2016

18) Auch wenn die DS-GVO für kirchliche Träger nicht anwendbar ist, so ist zu beachten, dass sowohl die evangelische als auch die katholische Kirche entsprechende Regelungen erlassen haben, um den Einklang mit der DS-GVO herzustellen. In: Hauser, Andrea; Haag, Ina. Datenschutz im Krankenhaus. 6., aktualisierte Auflage. Kohlhammer Verlag. Kindle-Version. (hier: Kapitel III, Abschnitte 2.2 und 7)

19) 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. (hier: Bemessungskriterium vollstationäre Fallzahl/Jahr in Anhang 5 Teil 3 Nr. 1.1 Spalte C)

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

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

22) Siehe dazu orientierend: Dillschneider J, Gross B (2020). Das Krankenhauszukunftsgesetz. Förderung für Digitalisierung und Cybersicherheit. das Krankenhaus. 2020; 112. (11): 976-981 / Gross B, Asma J (2021). Wie der Krankenhauszukunftsfonds das Klinikmanagement fordert und verändern wird. Sechs zentrale Handlungsfelder. das Krankenhaus. 2021; 113. (2): 94-96

23) Quelle: www.teletrust.de (Zugriff: 2. März 2021)

24) Quelle: www.bsi.bund.de (Zugriff: 2. März 2021)

25) 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.

26) https://www.kma-online.de/aktuelles/klinik-news/detail/900000-euro-gesamtschaden-durch-cyberattackea-31629 (Zugriff: 11. März 2021)

27) Versicherungsvertragsgesetz vom 23. November 2007 (BGBl. I S. 2631), das zuletzt durch Artikel 2 des Gesetzes vom 10. Juli 2020 (BGBl. I Seite 1653) geändert worden ist

28) 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 Seite 3256) geändert worden ist

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

30) Aus § 116 AktG ergibt sich – mit dem Verweis auf den genannten § 93 AktG – sogar eine gesetzlich normierte Sorgfaltspflicht und Verantwortlichkeit für die Aufsichtsratsmitglieder.

31) D&O-Versicherung steht für „Directors-and-Officers-Versicherung", sie wird auch Organ- bzw. Manager-Haftpflichtversicherung genannt: Eine Vermögensschadenhaftpflichversicherung, die Unternehmen für ihre Organe und leitende Angestellte abschließt, wobei die Prämienzahlungen hierfür dienstvertragliche regelmäßig der Arbeitgeber übernimmt.

32) Ob die unterlassene Bußgeldandrohung im Falle der Verletzung der neu geschaffenen gesetzlichen Verpflichtung ein gesetzgeberisches Versehen war, kann nicht abschließend beurteilt werden. Für ein solches Versehen spricht die in § 75c SGB V enthaltene fast wortgleich übernommene Verpflichtung der Nicht-KRITIS-Krankenhäuser zur Schaffung entsprechender Vorkehrungen. Für ein gesetzgeberisches Versehen spricht auch die Gesetzesbegründung zu § 75c SGB V, wonach nämlich die fortschreitende Digitalisierung in der medizinischen Versorgung zugleich auch das Bedrohungspotenzial für zunehmend zielgerichtete, technologisch ausgereiftere und komplexere Angriffe wachsen lässt. Sofern aber die Gesundheitsversorgung und damit auch Leib und Leben von Patienten gesetzgeberisches Leitmotiv war, ist die Verpflichtung zur Umsetzung auch für die „kleineren", Nicht-KRITIS-Krankenhäuser keineswegs weniger bedeutsam.

33) Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I Seite 3322, das zuletzt durch Artikel 47 des Gesetzes vom 21. Dezember 2020 (BGBl. I Seite 3096) geändert worden ist

34) Bundesdatenschutzgesetz Artikel 1 des Gesetzes vom 30. Juni 2017 (BGBl. I Seite 2097), in Kraft getreten am 25.05.2018, geändert durch Gesetz vom 20. November 2019 (BGBl. I Seite 1626)

35) Datenschutz-Grundverordnung: Verordnung Nr. 2016/679 des Europäischen Parlaments und Rates vom 27. April 2016

36) Gegen den Mobilfunkkonzern 1&1 etwa wurde ein Bußgeld i.H.v. 9,6 Mio. € verhängt, die Deutsche Wohnen Berlin soll gar 14,5 Mio. € bezahlen. Auch kleine und mittlere Unternehmen sind davon mittlerweile betroffen. Im DS-GVO-Portal kann online eine Bußgeld-Datenbank abgerufen werden, woraus sich die Höhe und der Anlass der jeweiligen Bußgelder in den europäischen Staaten ergeben.

37) 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 Absatz 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)

Anschrift der Verfasser

Prof. Dr. med. Andreas Becker, Öffentlich bestellter und vereidigter Sachverständiger für Qualitäts-, Informationssicherheits- und Risikomanagement in Krankenhäusern, Nonnenweg 120a, 51503 Rösrath, www.becker-sachverstaendiger.de/Edgar Gärtner, Rechtsanwalt, Fachanwalt für Strafrecht, Compliance Officer (Univ.), Zertifizierter Verteidiger für Wirtschafts- und Steuerstrafrecht, Viktoriastraße 28, 68165 Mannheim, www.gaertner-slania.de ■