DEUTSCHE KRANKENHAUS GESELLSCHAFT

Stellungnahme

zum Referentenentwurf

des Bundesministeriums des Innern und für Heimat

eines

Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

(NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)

FAIR

Diskutieren, entscheiden, handeln.

Zusammenfassung

Nachdem bereits im Herbst 2023 das Bundesministerium des Innern und für Heimat betroffenen Verbänden ein Diskussionspapier zur ersten Bewertung zur Verfügung gestellt hatte, begrüßen die Krankenhäuser den nun zur Kommentierung bereitgestellten überarbeiteten Referentenentwurf für die weitere Umsetzung der europäischen Regelungen zur Verbesserung der Informationssicherheit gemäß der NIS-2-Richtlinie. Die Verabschiedung des Gesetzes in der seitens der EU-Vorgaben vorgegebenen Zeit wird aller Voraussicht nach jedoch nicht mehr möglich sein.

Mit den enthaltenen Festlegungen zur Identifikation betroffener Einrichtungen fallen alle Krankenhäuser in Deutschland mindestens in die Kategorie „wichtige Einrichtung“. Auch wenn die bereits geforderten Ausnahmeregelungen für das Gesundheitswesen (es bestehen bereits heute spezialgesetzliche Regelungen zur Verbesserung der Informationssicherheit, vgl. § 391 SGB V) nicht umgesetzt wurde, darf es grundsätzlich nicht zu einer Doppelregulierung kommen, die im Zweifel bei wesentlichen Regelungen zu widersprüchlichen Auslegungen führen könnte.

Erkennbar ist, dass die Regelungen des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes und des KRITIS-Dachgesetzes aufeinander abgestimmt werden sollen. Dies ist mit Blick auf die Begriffsbestimmungen und Meldepflichten ausdrücklich zu begrüßen. Auch der Forderung nach Orientierung an europäischen Vorgaben trägt der Entwurf an einigen Stellen Rechnung: Nationale Vorgaben und Genehmigungsprozesse müssen sich an den europäischen Regelungen orientieren. Dies ist in Bezug auf den Nachweiszyklus bereits gelungen. Nationale Alleingänge, z. B. bei der Neuregelung der Prüfung von Konformitätsbewertungsprogrammen, müssen vermieden werden.

Sorge bereitet den Krankenhäusern die vorgesehenen Regelungen zur Zulässigkeit des Einsatzes kritischer Komponenten oder der Verantwortung für die Sicherheit der Lieferkette durch den Betreiber. Dass ein Krankenhaus Einblicke in interne Vertragsbeziehungen zwischen einzelnen Beteiligten in komplexen Lieferketten erhält, ist nicht realistisch.

Nach wie vor weisen die Krankenhäuser darauf hin, dass die Krankenhausplanung und -investitionsfinanzierung in Deutschland föderal geregelt ist. Bei Entscheidungen, die Krankenhäuser betreffen (unter anderem Aufsichtsmaßnahmen des Bundesamtes für Sicherheit in der Informationstechnik), ist daher in jedem Fall immer das Einvernehmen mit den zuständigen Aufsichtsbehörden der Bundesländer herzustellen. Noch immer ist z. B. in Bezug auf die Anordnung der Mängelbeseitigung entweder das Einvernehmen mit der zuständigen Behörde auf Bundesebene (die es im Krankenhausbereich nicht gibt) oder das Benehmen mit der sonst zuständigen Aufsichtsbehörde (in der Regel Landesgesundheits- oder Sozialministerien) herzustellen. Dies hebelt die föderale Zuständigkeit der Bundesländer gerade mit Blick auf Investitionsentscheidungen zur Mängelbeseitigung de facto aus und dürfte auch verfassungsrechtlich fragwürdig sein.

Ausdrücklich begrüßen die Krankenhäuser die Berücksichtigung der föderalen Zuständigkeiten in Bezug auf die Registrierungspflicht. Bei der Zwangsregistrierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist nun das Einvernehmen mit den zuständigen Aufsichtsbehörden

herzustellen. Die aktuell enthaltene Formulierung grenzt die Einvernehmensregelung auch nicht auf die Aufsichtsbehörden des Bundes ein, was aufgrund der föderal organisierten Krankenhausplanung der Länder nicht sachgerecht wäre. Dass die zuständigen Aufsichtsbehörden bei Anordnungen gegenüber besonders wichtigen Einrichtungen gemäß § 65 Abs. 6 und 7 nun zumindest ins Benehmen zu setzen sind, ist ein Schritt in die richtige Richtung. Auch hier wäre jedoch die Einvernehmensherstellung angezeigt, um der grundgesetzlich verbrieften Zuständigkeitsaufteilung Rechnung zu tragen.

Die Umsetzung neuer oder verschärfter Anforderungen an die Informationssicherheit in Krankenhäusern wird zu Mehrkosten führen, die aufgrund der Bedingungen des dualen Finanzierungssystems im Gegensatz zu anderen Branchen nicht weitergegeben werden können. Die Schätzung für den Erfüllungsaufwand der Wirtschaft fällt im Referentenentwurf mit 2,3 Milliarden Euro viel zu gering aus. Laut einer aktuellen Studie zur Umsetzung von Informationssicherheit im Krankenhaus (goldmedia, 2023) belaufen sich allein die initialen Mehrkosten für Kliniken auf 1,5 Milliarden Euro. Der laufende Betrieb, der mit ca. 760 Millionen Euro jährlich erhoben wurde, ist dabei noch nicht berücksichtigt. Angesichts der enorm steigenden Zahl betroffener Einrichtungen ist diese Summe viel zu niedrig angesetzt.

Eine Refinanzierung von Betriebskosten für Digitalisierungsprojekte im Allgemeinen oder des bezifferten Erfüllungsaufwandes für Informationssicherheit im Besonderen besteht heute nicht. Auch die mit dem Krankenhausversorgungsverbesserungsgesetz (KHVVG) geplante Änderung der Krankenhausfinanzierung (Vorhaltekosten) sieht derzeit keine Berücksichtigung von Kosten für Digitalisierung oder Informationssicherheit vor. Dennoch sind sich Krankenhäuser ihrer Verantwortung für die Patientinnen und Patienten nicht nur aus medizinischer Sicht, sondern auch mit Blick auf die Sicherheit ihrer Behandlungsinformationen bewusst. Sie arbeiten seit Jahren intensiv an der Verbesserung der Informationssicherheit. Der Verweis auf die Zuständigkeit der Bundesländer für die Investitionsfinanzierung der deutschen Krankenhäuser ist einerseits richtig und nachvollziehbar, die Kritik der Bundesländer am fehlenden Mitspracherecht bei Vorgaben des Bundes allerdings ebenso erwartbar. Krankenhäuser werden zwischen diesen Positionen zunehmend zerrieben und die Versorgungssicherheit in Deutschland damit gefährdet.

Der Referentenentwurf sieht für „wichtige Einrichtungen“ nicht die erforderlichen Umsetzungs- und Anpassungsfristen zur Umsetzung der Anforderungen, zum Beispiel an einen Risikomanagementprozess, vor. Diese Fristen sind entsprechend zu ergänzen.

Die Krankenhäuser und die Deutsche Krankenhausgesellschaft werden sich ungeachtet dessen weiter aktiv in die Bemühungen zur Verbesserung der Informationssicherheit einbringen, beispielsweise indem sie ihren branchenspezifischen Sicherheitsstandard auch an die zu erwartenden neuen gesetzlichen Anforderungen anpassen.

Allgemeine Bewertung

Artikel 1
Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit der Informationstechnik von Einrichtungen (BSI-Gesetz – BSIG)

Teil 1 Allgemeine Vorschriften

Es werden Begriffsbestimmungen der NIS2-Richtlinie in die Nomenklatur des BSIG überführt.

Stellungnahme zu ausgewählten Regelungen

Zu § 2 Abs. 1 Nr. 3 „Cloud-Computing-Dienst“

Die Abgrenzung der Definitionen von Cloud-Diensten ist zu unspezifisch. Es wird nicht nach den inzwischen etablierten Varianten Privat-Cloud, Public-Cloud oder Hybrid-Cloud-Anwendungen differenziert. Mit Blick auf die Sicherheit und rechtliche Zulässigkeit entsprechender Dienste („Patientenportal“) ergeben sich hier jedoch substanzielle Unterschiede. Die Begriffsbestimmung aus Art. 6 Nr. 30 NIS-2-Richtlinie sollte daher zur Klarstellung in den nationalen Regelungen noch weiter ausdifferenziert werden.

Zu § 2 Abs. 1 Nr. 10 „erheblicher Sicherheitsvorfall“

Einer präzisen Definition eines erheblichen Sicherheitsvorfalls kommt eine maßgebliche Bedeutung zu. Diese im Rahmen einer nicht-zustimmungspflichtigen Rechtsverordnung zu bestimmen, birgt in Verbindung mit der möglichen Voraussetzung, dass ein Schaden hätte eintreten können, die Gefahr, dass jede potenzielle Schwachstelle bereits zu einem „erheblichen Sicherheitsvorfall“ mit entsprechenden Folgen führen dürfte. Ein erheblicher Sicherheitsvorfall sollte sich in der Definition auf tatsächlich eingetretene Vorfälle mit erheblichem materiellem oder immateriellem Schaden beschränken. Für potenzielle Sicherheitsvorfälle ist ggf. die Definition des „Beinahe-Vorfalls“ (§ 2 Abs. 1 Nr. 1) geeignet zu ergänzen.

Zu § 2 Abs. 1 Nr. 11 „Forschungseinrichtungen“

Universitätsklinika sind zur Forschung für kommerzielle Zwecke angehalten, gleichzeitig Krankenhausbetreiber und Bildungseinrichtung. Die Definition ist daher mit Blick auf den differenzierten Auftrag der Universitätsklinika zu unspezifisch.

Zu § 2 Abs. 1 Nr. 34 „Rechenzentrumsdienst“

Nach der hier genannten Definition eines Rechenzentrumsdienstes würde sich für die meisten Krankenhäuser der Betrieb eines Rechenzentrums mit entsprechenden Regulationsfolgen ergeben. Der Eigenbetrieb von IT- und Netzwerkausrüstung sollte nicht von den regulatorischen Anforderungen umfasst werden, die sich bei der zur Verfügungstellung für Dritte ergeben.

Zu § 2 Abs. 1 Nr. 38 „Sicherheit in der Informationstechnik“

Die Definition von Sicherheit in der Informationstechnik blendet Security by Design durch die Hersteller entsprechender Systeme aus. Diese sollte aufgegriffen werden, da im Ergebnis der Verordnung nicht nur die Beschreibung von Sicherheitsvorkehrungen, sondern die Steigerung von Produktqualität erreicht werden sollte.

Zu Teil 2 Das Bundesamt

Kapitel 1 Aufgaben und Befugnisse des Bundesamtes

Dem Bundesamt für Sicherheit in der Informationstechnik (BSI) werden umfangreiche zusätzliche Aufgaben, Verantwortlichkeiten und Befugnisse zugesprochen.

Stellungnahme zu ausgewählten Regelungen

Zu § 6 Informationsaustausch

Bisher bleibt das BSI in Bezug auf den Informationsaustausch hinter den Erwartungen der Betreiber kritischer Infrastrukturen zurück. Zwar bestehen bereits heute umfangreiche Informationspflichten für Betreiber und theoretisch auch Informationsrechte gegenüber dem BSI. Gerade in Bezug auf konkrete Angriffe besteht bislang jedoch ein erheblicher Informationsnachlauf gegenüber der Presse und anderen öffentlich verfügbaren Quellen.

Die Neuregelung in Abs. 2 begrüßen daher die Krankenhäuser grundsätzlich. Jedoch sollte bei der Definition der Teilnahmebedingungen eine sinnvolle Auswahl erfolgen. Eine Trennung von Betreibern und Herstellern ist zukünftig zu vermeiden. Ohne die Aufteilung in Hersteller/Lieferanten/prüfende Stellen können die Vorgaben insbesondere für die besonders wichtigen Einrichtungen nicht erbracht werden. Ein Ermessensspielraum für das BSI („kann“) bei der Einbindung von Teilnehmerinnen oder Teilnehmern erschließt sich nicht. Hersteller, Lieferanten, prüfende Stellen und Dienstleister müssen am Informationsaustausch teilnehmen.

Zu Teil 3 Sicherheit der Informationstechnik von Einrichtungen

Zu Kapitel 1 Anwendungsbereich

Es werden Vorgaben für die Definition besonders wichtiger und wichtiger Einrichtungen festgelegt sowie deren Verantwortung in Bezug auf Risikomanagement, Melde-, Registrierungs-, Nachweis- und Unterrichtungspflichten normiert.

Stellungnahme zu ausgewählten Regelungen

Zu § 28 Besonders wichtige Einrichtungen und wichtige Einrichtungen

Die Definition der besonders wichtigen Einrichtungen mit mindestens 250 Mitarbeiterinnen und Mitarbeitern oder einem Jahresumsatz von 50 Millionen Euro, für die im Wesentlichen die Vorgaben gelten sollen, die bereits heute für Betreiber kritischer Infrastrukturen gelten, wird die Anzahl der von den Regelungen umfassten Krankenhäuser massiv erhöhen. Die Vorgaben des § 30ff. erstrecken sich bis auf wenige Ausnahmen auch auf „wichtige Einrichtungen“ mit mindestens 50 Mitarbeiterinnen und Mitarbeitern und einem Jahresumsatz von 10 Millionen Euro, was alle übrigen Krankenhäuser in Deutschland betreffen dürfte.

Für Krankenhäuser bestehen gemäß BSI-KritisV und dem Fünften Buch Sozialgesetz (SGB V) schon heute spezialgesetzliche Anforderungen (§ 391 SGB V), die eine Ausnahmeregelung gemäß § 28 Abs. 4 rechtfertigen. Das in § 30 Abs. 2 geforderte Sicherheitsniveau wird dabei nicht unterschritten. Diese Forderung der Krankenhäuser wurde im Rahmen des letzten Kommentierungsverfahrens abgelehnt. Unabhängig von der hier dargestellten Ausnahmeregelung wird im Folgenden auf die betreffenden Vorgaben der §§ 30 und 31 eingegangen.

Zu § 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

Die Regelung im Referentenentwurf weicht von den europarechtlichen Vorgaben ab. Nach Art 21 Abs. 1 NIS-2-Richtlinie müssen wesentliche und wichtige Einrichtungen Maßnahmen ergreifen, um die Risiken zu beherrschen. Nach § 30 Abs. 1 des Referentenentwurfes hingegen sind besonders wichtige Einrichtungen und wichtige Einrichtungen verpflichtet, Maßnahmen zu ergreifen, um Störungen zu vermeiden. Dies stellt im Gegensatz zur europarechtlichen Vorgabe eine Verschärfung dar, die in der amtlichen Begründung nicht nachvollziehbar begründet wird.

Zudem sind die Vorgaben des Absatzes 1 allgemein und unbestimmt. Diese können nach Absatz 9 im Rahmen eines branchenspezifischen Sicherheitsstandards ausgestaltet und für geeignet festgestellt werden. Allerdings werden in Absatz 2 konkrete Maßnahmen gefordert (nach Nr. 4 Sicherheit der Lieferkette, nach Nr. 10 Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung), die im Krankenhausbereich nicht ohne Weiteres gewährleistet werden können. Hier müssen branchenspezifische Lösungen erarbeitet werden, welche unter den in Deutschland gegebenen Rahmenbedingungen realisierbar sind. Die Erweiterung der Ausnahmeregelung in § 28 Abs. 5 Nr. 2 kann diese Möglichkeit schaffen, in Abstimmung mit dem Bundesministerium für Gesundheit vergleichbare Regelungen im Gesundheitswesen festzulegen.

In Bezug auf die unter Nummer 4 geforderte Sicherheit der Lieferkette muss festgestellt werden, dass selbst Betreiber kritischer Anlagen heute keinen Rechtsanspruch auf die Durchführung entsprechender Lieferanten-Audits haben. Damit kann die Durchführung entsprechender Kontrollen nur auf einzelvertraglicher Basis durchgeführt werden. Mindestens ist den Betreibern kritischer Anlagen ein entsprechender Anspruch auf Auditierung kritischer Lieferanten zuzubilligen. Es bleibt unklar, ob es sich bei den Einrichtungen in der Formulierung „sicherheitsbezogene Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern“ um Einrichtungen der Betreiber handelt. Falls nicht, entziehen sich diese vertraglichen Beziehungen der Kenntnis des Betreibers.

Absatz 3 verweist auf Anforderungen für Einrichtungsarten, die sich mit den Begriffsdefinitionen für Krankenhäuser nur schwer abgrenzen lassen. Es bleibt unklar, ob ein Krankenhaus Anbieter von Cloud-Computing-Dienstleistungen ist, wenn es ein private-cloud-basiertes Patientenportal betreibt. Auch ist nicht ausreichend definiert, ob Kliniken unter die Regelungen des Absatzes 3 fallen, wenn sie ein Rechenzentrum betreiben, mit dem die IT-Dienstleistungen des Krankenhauses abgebildet werden. An dieser Stelle wird auf die Kommentierung zu Artikel 1 Teil 1 § 2 Begriffsbestimmungen verwiesen.

Absatz 5 sieht vor, dass die Bestimmungen in Bezug auf die in Absatz 2 genannten Maßnahmen durch das BMI im Benehmen mit den jeweils betroffenen Ressorts präzisiert und erweitert werden können. Eine Benehmensherstellung erscheint bei einer so weitreichenden Vorgabemöglichkeit mit Blick auf die im BMI ggf. nicht vorhandene Branchenkompetenz verfehlt. Diese ist durch das Einvernehmen mit den zuständigen Ressorts zu ersetzen.

Nach Abs. 6 dürfen besonders wichtige Einrichtungen und wichtige Einrichtung durch Rechtsverordnung nach § 58 Abs. 3 bestimmte IKT-Produkte, IKT-Dienste und IKT-Prozesse nur verwenden, wenn diese über eine Cybersicherheitszertifizierung gemäß europäischer Schemata nach Artikel 49 der Verordnung (EU) 2019/881 verfügen. Bei diesen Festlegungen muss berücksichtigt werden, dass ein Austausch, Wechsel, Außerbetriebnahme von Produkten oder Diensten ggf. nicht sofort möglich ist, ohne die medizinische Versorgung der Patientinnen und Patienten zu gefährden. Es sind Übergangsfristen zu regeln und ggf. Ausnahmevorschriften zu schaffen, die dem übergeordneten Zweck der kritischen Dienstleistung Rechnung tragen.

Die bisher in § 8a BSIG für Betreiber kritischer Infrastrukturen enthaltene Regelung zur Erstellung branchenspezifischer Sicherheitsstandards wird in Abs. 8 auch für besonders wichtige Einrichtungen vorgesehen. Diese können auch durch Branchenverbände der besonders wichtigen Einrichtungen vorgeschlagen werden. Die Eignungsfeststellung erfolgt im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe sowie im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes und kann durch das BSI auch auf die Eignungsprüfung nach § 39 Abs. 1 (Nachweispflichten für Betreiber kritischer Anlagen) ausgeweitet werden. Die Krankenhäuser begrüßen ausdrücklich, dass weiterhin die Besonderheiten der einzelnen Branchen mit Blick auf die konkrete Umsetzung von Informationssicherheitsvorgaben in branchenspezifischen Sicherheitsstandards abgebildet werden können. Bei der konkreten Ausgestaltung, insbesondere auch der Vorgaben des BSI hinsichtlich der zu verwendenden Prüfgrundlage, sollte unbedingt auf eine eindeutige Verwendung der Begrifflichkeiten geachtet werden. Auch ist aktuell unklar, für welchen Zeitrahmen die Eignungsfeststellung ausgesprochen wird.

Änderungsbedarf

Die Begriffsbestimmungen unter § 2 ist zu präzisieren und die Regelung des Absatz 5 auf eine Einvernehmensherstellung anstelle des Benehmens mit den zuständigen Ressorts hin zu ändern. Im Zusammenhang mit branchenspezifischen Sicherheitsstandards sind die verwendeten Begriffe, wie „Prüfgrundlage“ oder „Sicherheitsstandard“, eindeutig zu definieren, um bereits aufgetretene Missverständnisse künftig zu vermeiden. Zudem ist der Zeitrahmen der Eignungsfeststellung festzulegen.

Zu § 31 Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen

Absatz 2 definiert Anforderungen an Betreiber kritischer Anlagen und deren Systeme, die zur Angriffserkennung eingesetzt werden müssen. Satz 3 fordert die fortwährende Identifikation von Bedrohungen mit dem Ziel ihrer Vermeidung und des Ergreifens geeigneter Beseitigungsmaßnahmen, wenn Störungen eingetreten sind. An dieser Stelle wird deutlich, dass andernorts gängige Präventionsmaßnahmen „nach dem Stand der Technik“ im Krankenhaus unter Umständen nicht anwendbar sein können und es branchenspezifischer Lösungen bedarf. Wird in einem Netzwerk ein

potenzieller Cyberangriff identifiziert, wird häufig die Isolation der betroffenen Komponenten im Netzwerk bis hin zu ihrer Abschaltung angewandt. Ein solches Vorgehen während eines operativen Eingriffs, beispielsweise an einem Linksherzkathetermessplatz (LHK), könnte zum Ausfall der intraoperativen Bildgebung führen und eine erhebliche Gefährdung der Patientensicherheit nach sich ziehen. Gegenwärtig wird in einem Forschungsprojekt gemeinsam mit der TH Brandenburg unter fachlicher Leitung von Prof. Michael Pilgermann der im Krankenhaus anwendbare Stand der Technik für Systeme zur Angriffserkennung evaluiert. Die Ergebnisse werden anschließend in den branchenspezifischen Sicherheitsstandard der DKG überführt.

Zu § 32 Meldepflichten

Die Meldungen nach dem NIS2UmsuCG und dem KRITIS-DachG sollten vereinheitlicht werden. Der Meldende sollte nicht entscheiden müssen, nach welchen Regelungen die Meldung erfolgen muss. Die Einordnung kann in Grenzfällen durch das BSI und das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) erfolgen.

Mit Blick auf die Definition eines erheblichen Sicherheitsvorfalls gemäß § 2 Abs. 1 Nr. 10, die ausdrücklich auch potentielle Ereignisse einschließt, wenn hierdurch u. a. natürliche Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt werden können, stellt die Abgrenzung meldepflichtiger Sicherheitsvorfälle Krankenhäuser vor Herausforderungen. In Verbindung mit einer unverzüglichen, spätestens innerhalb von 24 Stunden nach Kenntniserlangung an das BSI zu übermittelnden Erstmeldung droht den Beteiligten hier eine erhebliche Flut von Meldungen. Stellt die Übermittlung hierfür genutzter Meldebögen dann noch einen erheblichen Zusatzaufwand dar, ist absehbar, dass die ohnehin sehr knappen Personalressourcen mit Bürokratie gebunden werden und dann nicht für die Bewältigung des Sicherheitsvorfalls zur Verfügung stehen. Zudem muss auch das BSI mit der Hilfe eines vollautomatisierten Meldeprozesses in der Lage sein, die absehbar erhebliche Anzahl von Meldungen zu bearbeiten. Eine qualifizierte Rückmeldung an den Meldenden sollte dabei in jedem Fall mitgedacht werden, um die Validierung des erfolgreichen Meldeprozesses abzusichern.

Änderungsbedarf

Es bedarf grundlegend sinnvoller Vorgaben, welche Kriterien eine unverzügliche Meldung auslösen. Darüber hinaus müssen die Erst- und Folgemeldungen einfach, unbürokratisch und schnell an das BSI absetzbar sein. Das Bundesamt benötigt geeignete Technologien und Prozesse, um die hohe Zahl erwarteter Meldungen zu bewältigen.

Zu § 39 Nachweispflichten für Betreiber kritischer Anlagen

Das Bundesamt kann – wie bisher – die Beseitigung von Sicherheitsmängeln verlangen. Gerade in Bezug auf Mängel, die nur durch investive Maßnahmen zu beheben sind (z. B. bauliche Maßnahmen), fehlt Krankenhäusern aus rechtlichen Gründen die Möglichkeit, diese Entscheidung zu treffen bzw. entsprechende Mittel aus der Krankenhausfinanzierung über Fallpauschalen zu verwenden. Letztes ist den Kliniken sogar ausdrücklich untersagt, wäre darüber hinaus aber auch nicht systemkonform, da die Fallpauschalen investive Mittel nicht berücksichtigen. Über Krankenhausinvestitionen entscheiden die Bundesländer. Eine bußgeldbewehrte Auflage zur Mängelbeseitigung zu erlassen, ohne mit der im Zweifel dafür zuständigen Aufsichtsbehörde das Einvernehmen herzustellen, ist Krankenhäusern gegenüber unzumutbar.

Absatz 2 sieht die Möglichkeit vor, dass das BSI zur Ausgestaltung des Verfahrens der Prüfungen und Erbringung der Nachweise nach Absatz 1 sowie weiterer damit in Verbindung stehender Themen fachliche und organisatorische Anforderungen an die prüfenden Stellen festlegen kann.

Änderungsbedarf

Mit Blick auf die grundgesetzlich geregelte Zuständigkeit der Bundesländer für die Krankenhausplanung und -investitionsfinanzierung ist parallel zu § 33 Abs. 3 bzw. § 65 Absatz 3 ebenfalls das Einvernehmen auch mit den sonst zuständigen Aufsichtsbehörden herzustellen.

Auch im überarbeiteten Referentenentwurf werden die prüfenden Stellen im Verfahren nicht berücksichtigt. Die Krankenhäuser sprechen sich erneut dafür aus, diesen die Gelegenheit zur Stellungnahme zu geben.

Zu § 40 Zentrale Melde- und Anlaufstelle

In Analogie zum Bereich der kritischen Anlagen soll das BSI auch für besonders wichtige Einrichtungen die zentrale Meldestelle in Angelegenheiten der Sicherheit in der Informationstechnik werden. Hierzu zählen nach Absatz 4 auch Übermittlungspflichten von Informationen während einer erheblichen Störung, einschließlich personenbezogener Daten. Diese Regelungen sind in Gesundheitseinrichtungen sowohl mit Blick auf besonders personenbezogene Daten nach Art. 9 DSGVO als auch den Beschlagnahmeschutz und die ärztliche Schweigepflicht für die meldende Einrichtung gegebenenfalls strafrechtlich relevant.

Änderungsbedarf

Wie bereits im Diskussionsentwurf detailliert beschrieben, bedarf es einer Klarstellung in Bezug auf die Anwendung der Vorschrift für Gesundheitseinrichtungen mit Blick auf die besonderen Kategorien personenbezogener Daten nach Art 9 DSGVO.

Zu § 41 Untersagung des Einsatzes kritischer Komponenten

Derzeit ist offen, ob und ggf. welche Systeme im Krankenhausbereich als sog. „Kritische Komponente“ gemäß § 2 Absatz 1 Nummer 22 bestimmt werden.

Änderungsbedarf

Sollte ein für die kritische Dienstleistung notwendiges Informationssystem (z. B. das Krankenhausinformationssystem) als „Kritische Komponente“ bestimmt werden, können sich die Regelungen zur Anzeige des erstmaligen Einsatzes sowie der Freigabe durch das BMI nur auf Neuinstallationen nach Inkrafttreten des Gesetzes beziehen. Für bestehende Installationen muss ein Bestandsschutz gelten.

Bei der Entscheidung, den Einsatz einer kritischen Komponente zu untersagen, müssen die Gesamtauswirkungen auf die kritische Dienstleistung berücksichtigt werden. Dem Wechsel eines Krankenhausinformationssystems auf ein anderes System gehen heute in der Regel mehrjährige Vorbereitungen voraus, die nicht kurzfristig angeordnet werden können.

Zu Teil 7 Sanktionsvorschriften und Aufsicht

Stellungnahme zu ausgewählten Regelungen

Zu § 65 Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtiger Einrichtungen

Absatz 1 erlaubt dem BSI die Verpflichtung einzelner, besonders wichtiger Einrichtungen zu Audits, Prüfungen oder Zertifizierungen von unabhängigen Stellen. Es ist klarzustellen, dass mit dieser Verpflichtung keine konkrete Auswahl der prüfenden Stelle durch das Bundesamt erfolgt.

Absatz 3 stellt klar, dass der Einschätzung der prüfenden Stelle hinsichtlich aufgedeckter Sicherheitsmängel in jedem Fall gefolgt und die Beseitigung der Mängel gefordert werden kann. Aus den Erfahrungen der letzten Prüfzyklen ist jedoch inzwischen klar, dass die Einschätzung eines Mangels hinsichtlich der Relevanz für die zu erbringende Dienstleistung häufig differenzierter betrachtet werden muss, als es den am Markt verfügbaren prüfenden Stellen aufgrund begrenzter Ressourcen mit der nötigen Branchenkompetenz oftmals möglich ist. Daher ist den besonders wichtigen Einrichtungen die Gelegenheit zur Stellungnahme einzuräumen.

Noch deutlicher wird die Notwendigkeit entsprechender Branchenkompetenz mit Blick auf die in den Absätzen 6 und 7 enthaltenen Befugnisse zum Erlass von Anweisungen zur Verhütung oder Behebung eines Sicherheitsvorfalls oder anderen Verpflichtungen nach diesem Gesetz.

Gemäß Absatz 9 Nr. 2 kann die zuständige Aufsichtsbehörde natürlichen Personen die Ausübung von Leitungsaufgaben auf Geschäftsführungs- oder Vorstandsebene oder Ebene des rechtlichen Vertreters untersagen. Hier ist sicherzustellen, dass gesellschaftsrechtliche Regelungen eingehalten werden und angemessene Regelungen für die Geschäftsführerhaftung gefunden werden, wenn die medizinische Versorgung im Krankenhaus aufgrund des Eingriffs der Aufsichtsbehörde nicht mehr gewährleistet werden kann.

Änderungsbedarf

Beim Erlass von Maßnahmen entsprechend der Absätze 6 und 7 ist das Einvernehmen mit den zuständigen Aufsichtsbehörden des Bundes oder sonstigen Aufsichtsbehörden einzuholen. Darüber hinaus ist der besonders wichtigen Einrichtung die Gelegenheit zur Stellungnahme mit Bezug auf die Anordnung der Maßnahmen gegeben werden.

Es muss bei den Aufsichtsmaßnahmen nach Abs. 9 auch geregelt werden, wer den Betrieb im Sinne des Gesellschaftsrecht leiten oder führen soll und z. B. für Schäden haftet, die im Zusammenhang mit diesem Eingriff durch die Aufsichtsbehörde oder das BSI entstehen. Anderenfalls müssten andere Aufsicht- und Durchsetzungsmechanismen entwickelt werden.

In Abs. 10 müssen zudem die sonst zuständigen Aufsichtsbehörden ergänzt werden.

Deutsche Krankenhausgesellschaft (DKG)

Bundesverband der Krankenhausträger
in der Bundesrepublik Deutschland

Wegelystraße 3
10623 Berlin

Tel. (030) 3 98 01-0
Fax (030) 3 98 01-3000
E-Mail dkgmail@dkgev.de

FAIR

DEUTSCHE KRANKENHAUS GESELLSCHAFT DKG