DEUTSCHE KRANKENHAUS GESELLSCHAFT

DKG

Stellungnahme

zum Gesetzentwurf der Bundesregierung

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

Mit dem Regierungsentwurf eines Gesetzes für die Umsetzung der NIS-2-Richtlinie und Stärkung der Cybersicherheit (NIS2UmsuCG) hat die Bundesregierung die in den bisher bekannt gewordenen Referentenentwürfen vorgesehenen gesetzlichen Vorgaben weiter konsolidiert. Die Krankenhäuser unterstützen die weitere Umsetzung der europäischen Regelungen zur Verbesserung der Informationssicherheit gemäß der NIS-2-Richtlinie. Auch aufgrund verschiedener Cyberangriffe und -vorfälle ist es ein zentrales Anliegen der Krankenhäuser, informationstechnische Systeme sicher auszugestalten.

Die Krankenhäuser begrüßen die Verzahnung mit der parallel erfolgenden Resilienzgesetzgebung des BMI, bei der mit dem KRITS-Dachgesetz (KRITIS-DachG) zeitnah ebenfalls das parlamentarische Verfahren eröffnet wird, ausdrücklich. So können insbesondere bei der Registrierung und dem Meldewesen Synergieeffekte genutzt und bestehende Strukturen effizient genutzt werden. Nach wie vor kritisieren die Krankenhäuser allerdings den hohen Meldeaufwand (Erst- und Hauptmeldung, Zwischen-, Folge- und Abschlussmeldung). Dieser soll zwar nur bei „erheblichen Sicherheitsvorfällen“ greifen. Aufgrund der Verbindung mit der Definition eines erheblichen Sicherheitsvorfalls, wonach schon potenzielle Gesundheitsgefährdungen ausreichen, sind die Aufwände für die Krankenhäuser jedoch erheblich. Im Gesundheitssektor sind potentielle Gesundheitsgefährdungen immer vorstellbar. Es sind daher pragmatische Festlegungen notwendig, um eine unsachgemäße und für alle Beteiligten überfordernde Meldeflut zu verhindern.

Die im Grundgesetz föderal verankerte Krankenhausplanung, die eine zuständige Aufsichtsbehörde auf Bundesebene ausschließt, wird im Gesetzentwurf nur unzureichend berücksichtigt. Insbesondere bei behördlichen Aufsichtsmaßnahmen wird das sonst selbstverständliche Einvernehmen mit den Aufsichtsbehörden umgangen und lediglich eine Benehmensherstellung mit den „sonst zuständigen Aufsichtsbehörden“ – hier die für Gesundheit zuständigen Ministerien der Länder – vorgesehen. Krankenhäuser drohen damit zwischen den Anforderungen des BSI einerseits und für (fehlende) Investitionen zuständigen Bundesländern zerrieben zu werden. Hier ist dringend eine Einvernehmensherstellung vorzusehen.

Darüber hinaus bewerten die Krankenhäuser die Vorgaben in Bezug auf die Kontrolle der Lieferkette für die Kliniken als nicht durchsetzbar. Der „Marktmacht“ weltweit agierender Großkonzerne haben auch alle deutschen Krankenhäuser kaum etwas entgegenzusetzen. Die Einflussmöglichkeiten eines einzelnen Krankenhauses sind verschwindend gering.

Auch wenn die Krankenhäuser seit Jahren Vorgaben für mehr Informationssicherheit umsetzen und dies auch bereichsspezifisch im Fünften Buch Sozialgesetzbuch geregelt ist, stellen die nach dem NIS2UmsuCG vorgesehenen Maßnahmen in ihrer Qualität und Quantität – insbesondere die Anforderungen des § 30 Abs. 2 Nr. 1 - 10 BSIG – noch einmal eine neue und zusätzliche Anforderung an die Umsetzung in den Krankenhäusern. Dies erfordert einen zeitlichen Vorlauf, der im Gesetz nicht ausdrücklich enthalten ist. Aus der mit dem Entwurf auf fünf Jahre nach Inkrafttreten verlängerten Frist für die Abforderung von Nachweisen nach § 61 Abs. 3 Satz 5 BSIG schließen die Krankenhäuser, dass der Gesetzgeber diese Umsetzungsdauer anerkennt. Allerdings dürften nach dem Gesetz nicht nur zugelassene Krankenhäuser nach § 108 SGB V, sondern auch Rehakliniken nach § 111 SGB V als

wichtige oder besonders wichtige Einrichtung gelten. Diese sind in die Regelung des § 61 Abs. 3 Satz 5 aufzunehmen. Eine nachvollziehbare Begründung für die Ausnahme dieser Einrichtungen besteht nicht.

Krankenhäuser in Deutschland übernehmen Verantwortung für das Wohl der Patientinnen und Patienten und sind sich dessen bewusst. Dies gilt auch für den Cyberschutz. Dennoch spielt der damit unzweifelhaft verbundene hohe Ressourceneinsatz noch immer eine untergeordnete Rolle. Insbesondere in der Krankenhausfinanzierung werden Aufwände für Digitalisierung bisher vollständig ausgeblendet, da durch die Digitalisierung vermeintliche Einsparpotenziale entstehen. Krankenhäuser haben derzeit keinerlei Refinanzierungsmöglichkeiten der aus Digitalisierungsmaßnahmen entstehenden laufenden Kosten. Auch die im Rahmen des Krankenhaus-Zukunftsgesetzes vorgesehenen Mittel für die Verbesserung der Informationssicherheit sind den im KHZG vorgesehenen Förderschwerpunkten – und damit neuen Themen – vorbehalten und können nicht zur Absicherung der bestehenden Systeme eingesetzt werden.

Die erhobenen Kosten für die Umsetzung von Informationssicherheit im Krankenhaus (Studie goldmedia, 2023) belaufen sich allein bei den initialen Mehrkosten auf 1,5 Milliarden Euro. Der laufende Betrieb, der mit ca. 760 Millionen Euro jährlich erhoben wurde, ist dabei noch nicht berücksichtigt. Im Gegensatz zu anderen vom Gesetz betroffenen Sektoren und Branchen haben Krankenhäuser keine Möglichkeit, diese steigenden Kosten an anderer Stelle auszugleichen. Diese systematische Unterfinanzierung bedroht mittlerweile nicht nur die Existenz der Krankenhäuser, sie droht sich auch noch weiter negativ auf die Cybersicherheit auszuwirken. Der Gesetzgeber muss hier reagieren und endlich anerkennen, dass die Absicherung digitaler Systeme und Prozesse Fachkräfte mit besonderem Know-How, spezialisierte Software („Systeme zur Angriffserkennung“) und weitreichende Anpassungen bestehender IT-Systeme erfordert.

In der aktuellen bedrohlichen finanziellen Situation, in der viele Krankenhäuser aufgrund fehlender Finanzierungsausgleiche für inflationsbedingte Mehrkosten und Tarifsteigerungen vor der Insolvenz stehen, darf sich auch das für IT-Sicherheit zuständige Bundesministerium des Innern und für Heimat (BMI) nicht mehr allein auf die Zuständigkeit anderer Ressorts zurückziehen. Die Krankenhäuser benötigen aufgrund ihrer gesellschaftlichen Bedeutung dringend die finanzielle Unterstützung des BMI für die Umsetzung von Cybersicherheit und Resilienz. Für eine wirkungsvolle Informationssicherheit sind zusätzliche Mittel bereitzustellen.

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 NIS-2-Richtlinie in die Nomenklatur des BSIG überführt.

Stellungnahme zu ausgewählten Regelungen

Zu § 2 Abs. 1 Nr. 4 „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. Auch sollte ein Abgleich mit den aus dem Digitalgesetz (DigiG) resultierenden Vorgaben des § 393 SGB V zu Anforderungen an Cloud-Computing-Diensten erfolgen, die am 1.7.2024 in Kraft getreten sind.

Zu § 2 Abs. 1 Nr. 11 „erheblicher Sicherheitsvorfall“

Noch immer wird jeder Vorfall, der auch nur theoretisch zu einem Schaden hätte führen können, meldepflichtig. Die Krankenhäuser fordern, dass sich ein erheblicher Sicherheitsvorfall in der Definition auf tatsächlich eingetretene Vorfälle mit erheblichem materiellem oder immateriellem Schaden beschränken sollte. Für potenzielle Sicherheitsvorfälle ist ggf. die Definition des „Beinahe-Vorfalls“ (§ 2 Abs. 1 Nr. 1) geeignet zu ergänzen.

Zu § 2 Abs. 1 Nr. 35 „Rechenzentrumsdienst“

Nach der vorgesehenen 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.

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 § 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

Die Regelung im Gesetzentwurf 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. Gemäß der mit dem Gesetzentwurf vorgesehenen Regelung in § 30 Abs. 1 BSI-Gesetz sind hingegen 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.

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 Absatz 6 dürfen besonders wichtige Einrichtungen und wichtige Einrichtungen 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 oder eine 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 BSI-Gesetz für Betreiber kritischer Infrastrukturen enthaltene Regelung zur Erstellung branchenspezifischer Sicherheitsstandards wird in Absatz 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 Abs. 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

§ 30 Abs. 2 BSI-Gesetz 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. In einem Forschungsprojekt gemeinsam mit der TH Brandenburg wurde unter fachlicher Leitung von Prof. Michael Pilgermann der im Krankenhaus anwendbare Stand der Technik für Systeme zur Angriffserkennung evaluiert. Die Ergebnisse werden aktuell in den branchenspezifischen Sicherheitsstandard der DKG überführt.

Zu § 32 Meldepflichten

Die Meldungen nach dem NIS2UmsuCG und dem KRITIS-DachG sind zu vereinheitlichen. 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.

Die Definition eines erheblichen Sicherheitsvorfalls gemäß § 2 Abs. 1 Nr. 10 stellt Krankenhäuser bei der Abgrenzung meldepflichtiger Sicherheitsvorfälle vor Herausforderungen. Die Definition schließt ausdrücklich auch potentielle Ereignisse ein, wenn hierdurch u. a. natürliche Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt werden können, was im Gesundheitswesen regelmäßig der Fall sein kann. 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 zusätzlich noch einen erheblichen Mehraufwand 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. Letzteres 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, darf nicht erfolgen, ohne mit der dafür zuständigen und verantwortlichen Aufsichtsbehörde das Einvernehmen herzustellen.

Änderungsbedarf

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

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

Es bedarf 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 sogenannte „Kritische Komponente“ gemäß § 2 Abs. 1 Nr. 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 § 58 Ermächtigung zum Erlass von Rechtsverordnungen

Die Streichung der Anhörung der betroffenen Wirtschaftsverbände bewerten die Krankenhäuser kritisch. Sie steht dem auch aktuell gelebten und als fruchtbar für die Zielerreichung empfundenen kooperativen Ansatz entgegen und sollte daher zurückgenommen werden.

Zu Teil 7 Sanktionsvorschriften und Aufsicht

Stellungnahme zu ausgewählten Regelungen

Zu § 61 Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtiger Einrichtungen

§ 61 Abs. 3 BSI-Gesetz 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.

In Satz 5 wird die Frist zur Nachweiserbringung für zugelassene Krankenhäuser nach § 108 SGB V auf fünf Jahre nach Inkrafttreten des Gesetzes verlängert. Diese Vorgabe sollte auf Vorsorge- oder Rehabilitationseinrichtungen nach § 111 SGB V („Rehakliniken“) ausgeweitet werden. Diese befinden sich häufig in gleicher Trägerschaft, wie nach § 108 SGB V zugelassene Krankenhäuser, und werden häufig auch von der gleichen IT-Abteilung betreut. Es wäre nicht sachgerecht, hier eine künstliche Trennung vorzusehen und gerade den Rehakliniken die Fristverlängerung nicht einzuräumen.

Gemäß Absatz 9 Nummer 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

In § 61 Abs. 3 Satz 5 BSI-Gesetz sind nach § 111 SGB V zugelassene Vorsorge- und Rehabilitationseinrichtungen zu ergänzen.

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 zu geben.

Es muss bei den Aufsichtsmaßnahmen nach Absatz 9 auch geregelt werden, wer den Betrieb im Sinne des Gesellschaftsrechts 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 Aufsichts- und Durchsetzungsmechanismen entwickelt werden.

In Absatz 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