DEUTSCHE KRANKENHAUS GESELLSCHAFT

Stellungnahme

zum Referentenentwurf

des Bundesministeriums des Innern

für ein

Gesetz 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 Referentenentwurf zum Gesetz für die Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2UmsuCG) übernimmt das BMI im Wesentlichen die Regelungen aus dem Regierungsentwurf der Vorgängerregierung vom 22.7.2024. Die Vorgängerregierung hatte die Regelungen mit der parallel erfolgenden Resilienzgesetzgebung des BMI (Kritis-DachG) verzahnt. Dies wird aus Sicht der Krankenhäuser weiter ausdrücklich begrüßt. Insbesondere bei der Registrierung und dem Meldewesen entstehen dadurch Synergien, die eine effiziente Nutzung bestehender Strukturen ermöglichen. Gleichwohl erzeugt das Gesetz hohen bürokratischen Aufwand. Die Krankenhäuser kritisieren die umfangreichen Meldepflichten – von der Erst- und Hauptmeldung über Zwischen- und Folgemeldungen bis hin zur Abschlussmeldung. Zwar ist die Meldepflicht auf „erhebliche Sicherheitsvorfälle“ beschränkt, da bereits potenzielle Gesundheitsgefährdungen darunterfallen, entsteht jedoch ein breites Anwendungsspektrum – ein Szenario, das im Gesundheitswesen nahezu immer vorstellbar ist. Um eine unkontrollierbare und überfordernde Meldeflut zu vermeiden, braucht es daher pragmatische und klar abgegrenzte Vorgaben.

Die Regelungen zum Risikomanagement beinhalten Maßnahmen, die im Krankenhausbereich nicht ohne Weiteres gewährleistet werden können. Die zuständigen Aufsichtsbehörden sind daher einzubeziehen um branchenspezifische und praxistaugliche Lösungen zu entwickeln, die den realen Rahmenbedingungen im deutschen Gesundheitswesen gerecht werden.

Der notwendige erhebliche Ressourceneinsatz für verantwortungsvollen Cyberschutz bleibt in der politischen Diskussion um „Einsparpotenziale durch Digitalisierung“ und der Krankenhausfinanzierung weitgehend unbeachtet. Die im Krankenhauszukunftsgesetz (KHZG) bereitgestellten Mittel sind an projektgebundene Förderschwerpunkte geknüpft und lassen sich nicht für die Absicherung und den Betrieb bestehender Systeme einsetzen. Krankenhäuser haben keinerlei Refinanzierungsmöglichkeiten der entstehenden laufenden Kosten für Cybersicherheit. Die im Rahmen des Krankenhaus-Zukunftsgesetzes (KHZG) vorgesehenen Mittel für die Verbesserung der Informationssicherheit sind an die vorgesehenen Förderschwerpunkte geknüpft und können nicht zur Absicherung der bestehenden Systeme eingesetzt werden. In der aktuellen Situation, in der mehr die Hälfte der Krankenhäuser negative Jahresabschlüsse schreibt (Rating Report 2025), benötigen die Krankenhäuser die Unterstützung des BMI für die verlässliche Umsetzung von Cybersicherheit- und Resilienzmaßnahmen. Die Kosten für die Umsetzung von Informationssicherheit im Krankenhaus belaufen sich allein bei den initialen Mehrkosten auf 1,5 Mrd € (goldmedia 2023). Der laufende Betrieb (ca. 760 Mio. € p.a.) ist dabei noch nicht berücksichtigt. Im Gegensatz zu anderen vom Gesetz betroffenen Sektoren und Branchen haben Krankenhäuser, Reha- und Vorsorgeeinrichtungen keine Möglichkeit, diese steigenden Kosten an anderer Stelle vollständig auszugleichen. Es steht zu befürchten, dass sich diese systematische Unterfinanzierung negativ auf die Versorgung der Patientinnen und Patienten auswirkt. Der Gesetzgeber muss reagieren und die rechtlichen Grundlagen für die Finanzierung der Absicherung digitaler Systeme und Prozesse, das besondere Know-How, die spezialisierte Software und die weitreichenden Anpassungen bestehender IT-Landschaften schaffen.

Allgemeine Bewertung

Meldepflichten

Der vorige Gesetzentwurf sah vor, die Meldeverfahren nach dem NIS2UmsuCG und dem KRITIS-DachG zu vereinheitlichen. Dieses Vorhaben begrüßen die Krankenhäuser ausdrücklich. 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. NIS2UmsuCG und KRITIS-DachG sollten ein einheitliches Meldeverfahren vorsehen.

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 ist. In Verbindung mit einer unverzüglichen, spätestens innerhalb von 24 Stunden nach Kenntniserlangung an das BSI zu übermittelnden Erstmeldung, droht den Beteiligten eine erhebliche Flut von Meldungen. Stellt die Übermittlung hierfür genutzter Meldebögen einen erheblichen Zusatzaufwand dar, ist absehbar, dass die ohnehin knappen Personalressourcen durch 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 ist vorzusehen, um die Validierung des erfolgreichen Meldeprozesses abzusichern. Es bedarf klarer 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.

Im Rahmen der Informationsübermittlungspflichten während einer erheblichen Störung können nach § 40 auch personenbezogene Daten übermittelt werden. Diese Regelungen sind in Gesundheitseinrichtungen sowohl mit Blick auf personenbezogene Daten nach Art. 9 DSGVO als auch den Beschlagnahmeschutz und die ärztliche Schweigepflicht für die meldende Einrichtung von besonderer Bedeutung. Es sollte eine klarstellende Regelung aufgenommen werden, dass unter bestimmten Voraussetzungen auch besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO, beispielsweise bei Störungen in Gesundheitseinrichtungen, übermittelt werden dürfen, wenn dies für die Bewertung des erheblichen Sicherheitsvorfalles zwingend erforderlich ist.

Risikomanagement

Die Regelungen in § 30 zum Risikomanagement fordern Maßnahmen (nach Nr. 4 Sicherheit der Lieferkette, nach Nr. 10 Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung), die im Krankenhausbereich nicht ohne Weiteres gewährleistet werden können. Es sind branchenspezifische Lösungen notwendig, die unter den nationalen Rahmenbedingungen realisierbar sind. Für die Durchsetzung der Vorgaben in Bezug auf die Kontrolle der Lieferkette für Krankenhäuser bedarf es der „Marktmacht“ weltweit agierender Großkonzerne. Die Einflussmöglichkeiten eines einzelnen Krankenhauses sind gering. Selbst Betreiber kritischer Anlagen haben keinen Rechtsanspruch auf die

Durchführung entsprechender Lieferanten-Audits. Damit kann die Durchführung entsprechender Kontrollen nur auf einzelvertraglicher Basis durchgeführt werden. Um hier Fortschritte zu erzielen, ist den Betreibern kritischer Anlagen mindestens ein entsprechender Anspruch auf Auditierung kritischer Lieferanten zuzubilligen.

§ 30 Abs. 3 verweist auf Anforderungen für Einrichtungsarten, die mit den Begriffsdefinitionen für Krankenhäuser nur schwer abgrenzbar sind. 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 Nr. 4 Begriffsbestimmungen verwiesen.

Nach § 30 Abs. 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, 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.

Systeme zur Angriffserkennung

§ 31 Abs. 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. Andernorts gängige Präventionsmaßnahmen „nach dem Stand der Technik“ sind im Krankenhaus unter Umständen aus Gründen des Schutzes von Patientinnen und Patienten nicht anwendbar, so dass 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. Bei der Definition der Anforderungen an Betreiber kritischer Anlagen und deren Systeme, die zur Angriffserkennung eingesetzt werden müssen, sind branchenspezifische Rahmenbedingungen zu berücksichtigen.

Branchenspezifischer Sicherheitsstandard

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, ist auf eine eindeutige Verwendung der Begrifflichkeiten zu achten. Außerdem ist klar zu regeln, für welchen Zeitrahmen die Eignungsfeststellung ausgesprochen wird.

Kritische Komponente

Sollte ein für die kritische Dienstleistung notwendiges Informationssystem (z. B. das Krankenhausinformationssystem) als „Kritische Komponente“ im Sinne des § 41 BSIG 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 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, so dass dieser nicht kurzfristig angeordnet werden kann.

Aufsichts- und Durchsetzungsmaßnahmen

Auch wenn alle Krankenhäuser in Deutschland seit Jahren Vorgaben für mehr Informationssicherheit umsetzen und dies 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 andere und zusätzliche Anforderung an die Umsetzung in den Krankenhäusern. Dies erfordert einen zeitlichen Vorlauf, der im Gesetz nicht vorgesehen ist. Aus der mit dem Referentenentwurf auf fünf Jahre nach Inkrafttreten verlängerten Frist für die Anforderung von Nachweisen nach § 61 Abs. 3 Satz 5 BSIG schließt die DKG, dass der Gesetzgeber dies anerkennt. Allerdings gelten nach dem Gesetz nicht nur zugelassene Krankenhäuser nach § 108 SGB V, sondern auch Rehakliniken nach § 111 SGB V als wichtige oder besonders wichtige Einrichtung. Diese müssen deshalb aus Sicht der DKG in die Regelung des § 61 Abs. 3 Satz 5 aufgenommen werden, eine sachlogische Begründung für die Ausnahme dieser Einrichtungen besteht nach Kenntnis der DKG nicht.

Aufsichtsbehörden

Die im Grundgesetz föderal verankerte Krankenhausplanung, die eine zuständige Aufsichtsbehörde auf Bundesebene ausschließt, wird im Gesetzentwurf 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 die Einvernehmensherstellung vorzusehen.

Anlage – Übersicht der Änderungsvorschläge der DKG zum Referentenentwurf des Bundesministeriums des Innern für ein Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG)

Nr.	Bezug	Regelungstext/Inhalt	Art der Anmerkung	Anmerkung	Konkreter Änderungsvorschlag
1	§ 2 Abs. 1 Nr. 4	„Cloud-Computing-Dienst“ ein digitaler Dienst, der auf Abruf die Verwaltung eines skalierbaren und elastischen Pools gemeinsam nutzbarer Rechenressourcen sowie den umfassenden Fernzugang zu diesem Pool ermöglicht, auch wenn die Rechenressourcen auf mehrere Standorte verteilt sind;	Allgemein	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 ab dem 1.7.2024 in Kraft treten.	
2	§ 2 Abs. 1 Nr. 11	„erheblicher Sicherheitsvorfall“ ein Sicherheitsvorfall, der a) schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder	Inhaltlich	Noch immer wird jeder Vorfall, der auch nur theoretisch zu einem Schaden hätte führen können, meldepflichtig. Die Krankenhäuser halten die Forderung aufrecht, dass sich ein erheblicher Sicherheitsvorfall in der Definition auf tatsächlich eingetretene Vorfälle mit	„erheblicher Sicherheitsvorfall“ ein Sicherheitsvorfall, der a) schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat ~~oder verursachen kann~~ oder

Nr.	Bezug	Regelungstext/Inhalt	Art der Anmerkung	Anmerkung	Konkreter Änderungsvorschlag
		b) andere natürliche oder juristische Personen durch erhebliche materielle oder im-materielle Schäden beeinträchtigt hat oder beeinträchtigen kann, sofern durch die Rechtsverordnung nach § 56 Absatz 5 keine konkretisierende Begriffsbestimmung erfolgt;		erheblichem materiellen oder immateriellen Schaden beschränken sollte. Für potenzielle Sicherheitsvorfälle ist ggf. die Definition des „Beinahe-Vorfalls“ (§ 2 Abs. 1 Nr. 1) geeignet zu ergänzen.	b) andere natürliche oder juristische Personen durch erhebliche materielle oder im-materielle Schäden beeinträchtigt hat ~~**oder beeinträchtigen kann**~~, sofern durch die Rechtsverordnung nach § 56 Absatz 5 keine konkretisierende Begriffsbestimmung erfolgt;
3	§ 2 Abs. 1 Nr. 35	„Rechenzentrumsdienst“ ein Dienst, der Strukturen umfasst, die dem vorrangigen Zweck der zentralen Unterbringung, der Zusammenschaltung und dem Betrieb von IT- oder Netzwerkausrüstungen dienen, und die Datenverarbeitungsdienste erbringen, mitsamt allen benötigten Anlagen und Infrastrukturen, insbesondere für die Stromverteilung und die Umgebungskontrolle;	Allgemein	Nach der hier vorgenommenen Definition eines Rechenzentrumsdienstes würde sich für die meisten Krankenhäuser der Betrieb eines Rechenzentrums mit entsprechenden Regulationsfolgen ergeben. Der Eigenbetrieb von IT- und Netzwerkausrüstung ist von den regulatorischen Anforderungen auszunehmen, die sich bei der zur Verfügungstellung für Dritte ergeben.	
4	§ 30 Abs. 1	Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen, die nach Absatz 2 konkretisiert werden, zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von	Inhaltlich	Die Regelung im Regierungsentwurf 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 § 30 Abs. 1 des Regierungsentwurfes hingegen sind besonders wichtige Einrichtungen und wichtige Einrichtungen verpflichtet, Maßnahmen zu ergreifen, um Störungen zu vermeiden. Dies stellt im Gegensatz zur europarechtlichen Vorgabe eine	Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, **geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen zu ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu**

Nr.	Bezug	Regelungstext/Inhalt	Art der Anmerkung	Anmerkung	Konkreter Änderungsvorschlag
		Sicherheitsvorfällen möglichst gering zu halten.		Verschärfung dar, die in der amtlichen Begründung nicht nachvollziehbar begründet ist.	**beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.**
5	§ 30 Abs. 5	Sofern die Durchführungsrechtsakte der Europäischen Kommission nach Artikel 21 Absatz 5 der NIS-2-Richtlinie keine abschließenden Bestimmungen über die technischen und methodischen Anforderungen sowie erforderlichenfalls über die sektoralen Anforderungen an die in Absatz 2 genannten Maßnahmen in Bezug auf besonders wichtige Einrichtungen und wichtige Einrichtungen enthalten, können diese Bestimmungen vom Bundesministerium des Innern im Benehmen mit den jeweils betroffenen Ressorts durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, unter Berücksichtigung der möglichen Folgen unzureichender Maßnahmen sowie der Bedeutung bestimmter Einrichtungen präzisiert und erweitert werden.	Inhaltlich	Abs. 5 sieht vor, dass die Bestimmungen in Bezug auf die in Abs. 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.	Sofern die Durchführungsrechtsakte der Europäischen Kommission nach Artikel 21 Absatz 5 der NIS-2-Richtlinie keine abschließenden Bestimmungen über die technischen und methodischen Anforderungen sowie erforderlichenfalls über die sektoralen Anforderungen an die in Absatz 2 genannten Maßnahmen in Bezug auf besonders wichtige Einrichtungen und wichtige Einrichtungen enthalten, können diese Bestimmungen vom Bundesministerium des Innern im ~~**Benehmen**~~ **Einvernehmen** mit den jeweils betroffenen Ressorts durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, unter Berücksichtigung der möglichen Folgen unzureichender Maßnahmen sowie der Bedeutung bestimmter Einrichtungen präzisiert und erweitert werden.
6	§ 39 Abs. 1 Satz 4	Es kann bei Sicherheitsmängeln die Vorlage eines geeigneten Mängelbeseitigungsplanes und im Einvernehmen mit der zuständigen	Inhaltlich	Das Bundesamt kann – wie bisher – die Beseitigung von Sicherheitsmängeln verlangen. Gerade in Bezug auf Mängel, die nur durch investive Maßnahmen zu	Es kann bei Sicherheitsmängeln die Vorlage eines geeigneten Mängelbeseitigungsplanes und im Einvernehmen mit der zuständigen

Nr.	Bezug	Regelungstext/Inhalt	Art der Anmerkung	Anmerkung	Konkreter Änderungsvorschlag
		Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen.		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 ausdrücklich untersagt, und wäre 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.	Aufsichtsbehörde des Bundes oder im ~~**Benehmen**~~ **Einvernehmen** mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen.
7	§ 61 Abs. 3 Satz 5	Abweichend von Satz 1 kann das Bundesamt gegenüber zugelassenen Krankenhäusern nach § 108 des Fünften Buches Sozialgesetzbuch frühestens fünf Jahre nach Inkrafttreten dieses Gesetzes die Vorlage von Nachweisen über die Erfüllung einzelner oder aller der in Absatz 1 genannten Verpflichtungen anordnen, soweit nicht durch Rechtsverordnung nach § 56 Absatz 6 ein früherer Zeitpunkt bestimmt wird.	Inhaltlich	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 ist 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, eine	Abweichend von Satz 1 kann das Bundesamt gegenüber zugelassenen Krankenhäusern nach § 108 **und Vorsorge- oder Rehabilitationseinrichtungen nach § 111** des Fünften Buches Sozialgesetzbuch frühestens fünf Jahre nach Inkrafttreten dieses Gesetzes die Vorlage von Nachweisen über die Erfüllung einzelner oder aller der in Absatz 1 genannten Verpflichtungen anordnen, soweit nicht durch Rechtsverordnung nach § 56 Absatz 6 ein früherer Zeitpunkt bestimmt wird.

Nr.	Bezug	Regelungstext/Inhalt	Art der Anmerkung	Anmerkung	Konkreter Änderungsvorschlag
				künstliche Trennung vorzusehen und den Rehakliniken die Fristverlängerung nicht einzuräumen.	
8	§ 61 Abs. 6 Satz 1	Das Bundesamt kann gegenüber besonders wichtigen Einrichtungen im Benehmen mit der zuständigen Aufsichtsbehörde zur Verhütung oder Behebung eines Sicherheitsvorfalls oder eines Mangels erforderliche Maßnahmen nach § 30 Absatz 1 Satz 1 sowie die Vorlage eines geeigneten Mängelbeseitigungsplanes und eines geeigneten Nachweises über die erfolgte Mängelbeseitigung anordnen.	Inhaltlich	Bei der Anordnung von Maßnahmen nach Abs. 6 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.	Das Bundesamt kann gegenüber besonders wichtigen Einrichtungen im ~~**Benehmen**~~ **Einvernehmen** mit der zuständigen Aufsichtsbehörde zur Verhütung oder Behebung eines Sicherheitsvorfalls oder eines Mangels erforderliche Maßnahmen nach § 30 Absatz 1 Satz 1 so-wie die Vorlage eines geeigneten Mängelbeseitigungsplanes und eines geeigneten Nach-weises über die erfolgte Mängelbeseitigung anordnen. **Der besonders wichtigen Einrichtung ist vor der Anordnung die Gelegenheit zur Stellungnahme zu geben**.
9	§ 61 Abs. 7 Satz 1	Das Bundesamt kann gegenüber besonders wichtigen Einrichtungen im Benehmen mit der zuständigen Aufsichtsbehörde Anordnungen zur Umsetzung der in Absatz 1 genannten Verpflichtungen erlassen.		Beim Erlass von Maßnahmen nach Abs. 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.	Das Bundesamt kann gegenüber besonders wichtigen Einrichtungen im ~~**Benehmen**~~ **Einvernehmen** mit der zuständigen Aufsichtsbehörde Anordnungen zur Umsetzung der in Absatz 1 genannten Verpflichtungen erlassen. **Der besonders wichtigen Einrichtung ist vor dem Erlass die Gelegenheit zur Stellungnahme zu geben**.
10	§ 61 Abs. 9 Satz 2 Nr. 2	unzuverlässigen Geschäftsleitungen die Ausübung der Tätigkeit, zu der sie berufen sind (§ 2 Nummer 13), vorübergehend untersagen	Inhaltlich	Es muss bei den Aufsichtsmaßnahmen nach Abs. 9 auch geregelt werden, wer den Betrieb im Sinne des Gesellschaftsrechts leiten oder führen soll	unzuverlässigen Geschäftsleitungen **unter Beachtung gesellschaftsrechtlicher Vorschriften** die Ausübung der Tätigkeit,

Nr.	Bezug	Regelungstext/Inhalt	Art der Anmerkung	Anmerkung	Konkreter Änderungsvorschlag
				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.	zu der sie berufen sind (§ 2 Nummer 13), vorübergehend untersagen.
11	§ 61 Abs. 10 Satz 1	Soweit das Bundesamt Maßnahmen gegenüber besonders wichtigen Einrichtungen durchführt, informiert es die zuständige Aufsichtsbehörde des Bundes darüber.	Inhaltlich	In Abs. 10 müssen zudem die sonst zuständigen Aufsichtsbehörden ergänzt werden.	Soweit das Bundesamt Maßnahmen gegenüber besonders wichtigen Einrichtungen durchführt, informiert es die zuständige Aufsichtsbehörde des Bundes **oder die sonst zuständige Aufsichtsbehörde** darüber.

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