DEUTSCHE KRANKENHAUS GESELLSCHAFT

Bundesverband der Krankenhausträger in der Bundesrepublik Deutschland

Stellungnahme

der Deutschen Krankenhausgesellschaft

zum

Diskussionspapier des Bundesministeriums des Innern und für Heimat

zu

Wirtschaftsbezogenen Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland

Stand: 20.10.2023

Inhaltsverzeichnis

Allgemeiner Teil

Mit dem „Diskussionspapier zu wirtschaftsbezogenen Regelungen zur Umsetzung der NIS-2 Richtlinie Deutschland“ wird die geplante Umsetzung der Richtlinie in Deutschland skizziert, auch wenn noch kein finaler, mit allen Ressorts abgestimmter Gesetzentwurf vorliegt. Die Vorgehensweise wird mit Blick auf die Vermeidung weiterer Verzögerungen ausdrücklich begrüßt.

Es hatte sich bereits abgezeichnet, dass die bisher in Deutschland umgesetzten Regelungen für die Verbesserung der Informationssicherheit kritischer Infrastrukturen insbesondere mit Blick auf den Anwendungsbereich nicht im Einklang mit den seitens der EU vorgesehenen Vorgaben sein würden. Dies wird insbesondere in den neuen Kategorien „besonders wichtiger“ und „wichtiger“ Einrichtungen deutlich, für die im Diskussionspapier umfangreiche Regelungen – häufig in Analogie zu bestehenden Regelungen für Betreiber kritischer Anlagen – aufgenommen worden.

Mit den enthaltenen Festlegungen zur Identifikation betroffener Einrichtungen fallen alle Krankenhäuser in Deutschland mindestens in die Kategorie „wichtige Einrichtung“. Für die Kliniken gelten bereits heute spezialgesetzliche Regelungen zur Verbesserung der Informationssicherheit, die zum Zeitpunkt der Stellungnahme in aktuellen Gesetzentwürfen des Bundesministeriums für Gesundheit überarbeitet und weiter ergänzt werden. Es erscheint daher geboten, die bestehenden Ausnahmeregelungen für das Gesundheitswesen im Anwendungsbereich des geplanten Gesetzentwurfes auf die durch das Bundesministerium für Gesundheit geplanten Regelungen (insbesondere § 391 Fünftes Buch Sozialgesetzbuch) auszuweiten. Parallele, sich gegebenenfalls widersprechende gesetzliche Anforderungen sind zwingend zu vermeiden.

Mit Blick auf die äußerst begrenzten Ressourcen im Gesundheitswesen, insbesondere im Krankenhausbereich, müssen bürokratische Anforderungen an Registrierungs- und Meldepflichten ebenfalls vermieden werden, was nicht zwangsläufig im Konflikt mit einer notwendigen Meldung von Sicherheitsvorfällen gemäß der Intention der Richtlinie stehen muss. Hier bedarf es spezieller branchenspezifischer Lösungen für das Gesundheitswesen, die nicht ohne weiteres auf andere Branchen übertragbar sind oder von diesen übernommen werden können.

Darüber hinaus ist die Krankenhausplanung und -investitionsfinanzierung in Deutschland föderal geregelt. 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.

Die Umsetzung neuer oder verschärfter Anforderungen an die Informationssicherheit in Krankenhäusern wird zu Mehrkosten führen, die aufgrund des dualen Finanzierungs-systems im Gegensatz zu anderen Branchen nicht weitergegeben werden können. Es gibt derzeit keine Refinanzierung von Betriebskosten für Digitalisierungsprojekte im Allgemeinen oder Informationssicherheit im Besonderen. Während Krankenhäuser sich ihrer Verantwortung für die Patientinnen und Patienten nicht nur aus medizinischer Sicht sondern auch mit Blick auf die Sicherheit ihrer Behandlungsinformationen wohl bewusst sind und seit Jahren intensiv an der Verbesserung der Informationssicherheit arbeiten,

gibt es auf der anderen Seite keinerlei belastbare Zusagen, wie die daraus resultierenden Kosten refinanziert werden sollen. 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 Anforderungen zunehmend zerrieben und damit die Versorgungssicherheit in Deutschland gefährdet.

Die Deutsche Krankenhausgesellschaft wird sich ungeachtet dessen weiter aktiv in die Anstrengungen zur Verbesserung der Informationssicherheit in den Krankenhäusern einbringen, beispielsweise indem sie ihren branchenspezifischen Sicherheitsstandard auch an die zu erwartenden neuen gesetzlichen Anforderungen anpasst.

Im Folgenden wird auf wesentliche Einzelregelungen eingegangen und ggf. erkannter Anpassungsbedarf dargestellt.

Besonderer Teil

Artikel 1

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

Zu Teil 1 Allgemeine Vorschriften

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

Stellungnahme

§ 2 Abs. 1 (2) Cloud-Computing-Dienst

Stellungnahme

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.

§ 2 Abs. 1 (9) erheblicher Sicherheitsvorfall

Stellungnahme

In Verbindung mit § 2 Absatz 2 kommt einer präzisen Definition eines erheblichen Sicherheitsvorfalls eine maßgebliche Bedeutung zu. Diese im Rahmen einer nicht-zustimmungspflichtigen Rechtsverordnung zu bestimmen, birgt in Verbindung mit der hypothetischen 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.

§ 2 Abs. 1 (10) Forschungseinrichtungen

Stellungnahme

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.

§ 2 Abs. 1 (11) Geschäftsleiter

Stellungnahme

Die Fokussierung auf die „Geschäftsleitung“ stellt auf eine einzelne, natürliche Person ab. Dies kommt bei großen Unternehmen in der Praxis so gut wie nicht vor, da die Verantwortung hier regelmäßig über verschiedene Vorstände abgebildet wird.

§ 2 Abs. 1 (30) Rechenzentrumsdienst

Stellungnahme

Nach der hier genannten Definition eines Rechenzentrumsdienstes würde sich für die meisten Krankenhäuser der Betrieb eines Rechenzentrums mit entsprechenden Regulationsfolgen ergeben.

§ 2 Abs. 1 (34) Sicherheit in der Informationstechnik

Stellungnahme

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 bloße Sicherheitsvorkehrungen, sondern die Steigerung von Produktqualität erreicht werden sollte.

Zu Teil 2 Das Bundesamt

Zu Kapitel 1 Aufgaben und Befugnisse des Bundesamtes

Beabsichtigte Neuregelung

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

§ 6 Informationsaustausch

Stellungnahme

Bisher bleibt das Bundesamt 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 wird daher grundsätzlich begrüßt, jedoch sollte bei der Definition der Teilnahmebedingungen eine sinnvolle Auswahl erfolgen. Eine Trennung von Betreibern und Herstellern sollte zukünftig vermieden werden. Ohne Hersteller/ Lieferanten/Prüfende Stellen können die Vorgaben insbesondere für die besonders wichtigen Einrichtungen nicht erbracht werden.

§ 11 Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen

Stellungnahme

Die Mitwirkung des Herstellers bei einem Sicherheitsvorfall wird begrüßt. Die Durchsetzung dieser Vorgaben muss jedoch effektiv möglich sein.

Zu Teil 3 Sicherheit der Informationstechnik von Einrichtungen

Zu Kapitel 1 Anwendungsbereich

Beabsichtigte Neuregelung

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.

§ 28 Besonders wichtige Einrichtungen und wichtige Einrichtungen

Stellungnahme

Die Definition der besonders wichtigen Einrichtungen mit mindestens 250 Mitarbeiter-innen und Mitarbeitern oder einem Jahresumsatz von 50 Mio. EUR, 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 Mio. EUR, 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 (bisher § 75c SGB V, nach dem Regierungsentwurf zum Digitalgesetz des BMG künftig § 391 SGB V), die eine Ausnahmeregelung gemäß § 28 Abs. 4 rechtfertigen dürften. Das in § 30 Abs. 2 geforderte Sicherheitsniveau wird dabei nicht unterschritten. Unabhängig von der hier dargestellten Ausnahmeregelung wird im Folgenden auf die betreffenden Vorgaben der §§ 30 und 31 eingegangen.

§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

Stellungnahme

Die Vorgaben des Absatzes 1 sind 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 Rahmen-bedingungen realisierbar sind. Die Erweiterung der Ausnahmeregelung in § 28 Abs. 4 Nr. 3 würde 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. Sinnvoll und hilfreich wäre es daher, wenn mindestens den Betreibern kritischer Anlagen ein entsprechender Anspruch auf Auditierung kritischer Lieferanten zugebilligt werden könnte.

Absatz 3 verweist auf Anforderungen für Einrichtungsarten, die sich mit den Begriffsdefinitionen für Krankenhäuser nur schwer angrenzen 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 sollte durch das Einvernehmen mit den zuständigen Ressorts ersetzt werden.

Die bisher in § 8a BSIG für Betreiber kritischer Infrastrukturen enthaltene Regelung zur Erstellung branchenspezifischer Sicherheitsstandards wird in Abs. 9 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 Katastrophen-hilfe 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. Es wird ausdrücklich begrüßt, 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 Ausnahmeregelung des § 28 Abs. 4 Nr. 3 sollte neben den bereits aufgeführten § 306 Absatz 1 Satz 3, § 311 Absatz 6 und § 325 des Fünften Buches Sozialgesetzbuch um § 391 Fünftes Buch Sozialgesetzbuch erweitert werden.

Darüber hinaus sind die Begriffsbestimmungen unter § 2 entsprechend zu schärfen und die Regelung des Absatz 5 auf eine Einvernehmensherstellung anstelle des Benehmens mit den zuständigen Ressorts hin zu ändern. Im Zusammenhang mit

branchenspezifischen Sicherheitsstandards sollten die verwendeten Begriffe, wie „Prüfgrundlage“ oder „Sicherheitsstandard“, klar gefasst werden, um bereits aufgetretene Missverständnisse künftig zu vermeiden. Zudem sollte der Zeitrahmen der Eignungsfeststellung festgelegt werden.

§ 31 Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen

Stellungnahme

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 geeignete Beseitigungsmaßnahmen, wenn Störungen eingetreten sind. In der aktuellen Formulierung bleibt jedoch unklar, ob sich die Anforderung auf die Betreiber oder die eingesetzten Systeme beziehen.

An dieser Stelle wird im Übrigen 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.

Änderungsbedarf

Es sollte klargestellt werden, ob sich die Anforderung des Satzes 3 auf die Betreiber nach Satz 1 oder die Systeme nach Satz 2 beziehen.

§ 32 Meldepflichten

Stellungnahme

Mit Blick auf die Definition eines erheblichen Sicherheitsvorfalls unter § 2 Absatz 1 Nr. 9, die ausdrücklich auch potentielle Ereignisse einschließt, wenn hierdurch u. a. natürliche Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt werden können, dürfte die Abgrenzung meldepflichtiger Sicherheitsvorfälle die Krankenhäuser vor Herausforderungen stellen. 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 zu befürchten, dass die ohnehin sehr knappen Personalressourcen mit Bürokratie gebunden werden und dann nicht für die Bewältigung des Sicherheitsvorfalls zur Verfügung stehen.

Änderungsbedarf

Es bedarf einerseits sinnvoller Vorgaben, welche Kriterien eine unverzügliche Meldung auslösen. Darüber hinaus sollten die Erst- und Folgemeldungen in einfach und schnell an das BSI absetzbar sein.

§ 39 Nachweispflichten für Betreiber kritischer Anlagen

Stellungnahme

Das Bundesamt kann – wie bisher – die Beseitigung von Sicherheitsmängeln verlangen. Allerdings muss mit Blick auf die grundgesetzlich geregelte Zuständigkeit der Bundesländer für die Krankenhausplanung und -investitionsfinanzierung in Analogie zur Regelung § 64 Absatz 3 das Einvernehmen auch mit den sonstigen zuständigen Aufsichtsbehörden hergestellt werden.

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

Bisher werden die prüfenden Stellen im Verfahren nicht berücksichtigt. Es erscheint jedoch sinnvoll, diesen die Gelegenheit zur Stellungnahme zu geben.

§ 40 Zentrale Melde- und Anlaufstelle

Stellungnahme

In Analogie zum Bereich der kritischen Anlagen soll das Bundesamt 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 hier dringend einer Klarstellung in Bezug auf die Anwendung der Vorschrift für Gesundheitseinrichtungen.

Zu Teil 7 Sanktionsvorschriften und Aufsicht

§ 64 Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtiger Einrichtungen

Stellungnahme

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

Absatz 3 impliziert, 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 sollte der besonders wichtigen Einrichtung die Gelegenheit zur Stellungnahme gegeben werden.

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.

Änderungsbedarf

Beim Erlass von Maßnahmen entsprechend der Absätze 6 und 7 ist mindestens das Einvernehmen mit den zuständigen Aufsichtsbehörden des Bundes oder sonstigen Aufsichtsbehörden einzuholen. Darüber hinaus sollte der besonders wichtigen Einrichtung die Gelegenheit zur Stellungnahme der Bezug auf die Anordnung der Maßnahmen gegeben werden. In Absatz 11 müssen zudem die sonst zuständigen Aufsichtsbehörden ergänzt werden.