DEUTSCHE KRANKENHAUS GESELLSCHAFT

Bundesverband der Krankenhausträger in der Bundesrepublik Deutschland

Stellungnahme

der Deutschen Krankenhausgesellschaft

zum

Referentenentwurf des Bundesministeriums des Inneren, für Bau und Heimat

eines

Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0)

vom 10. Dezember 2020

Inhaltsverzeichnis

Allgemeiner Teil

Das Bundesministerium des Innern, für Bau und Heimat (BMI) hat am 03.12.2020 den noch nicht innerhalb der Ressorts abgestimmten Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0) auf seiner Webseite veröffentlicht. Zunächst hat das BMI nicht die übliche Möglichkeit zur Anhörung der Verbände eingeräumt und stattdessen lediglich um eine allgemeine Rückmeldung zum Gesetzentwurf bis zum 09.12.2020 (zunächst 06.12.2020) gebeten. Kurzfristig wurde der umfangreiche Referentenentwurf Verbänden mit einer eintägigen Stellungnahmefrist übersandt.

Es ist richtig, angesichts der wachsenden Digitalisierung auch im Gesundheitswesen die gesetzlichen Rahmenbedingungen zum Schutz vor Cyberangriffen weiterzuentwickeln und dabei den notwendigen Diskurs mit allen hieran Beteiligten zu suchen, auch um Akzeptanz für die geplanten und teils weitreichenden Änderungen zu sichern. Dabei wurde der kooperative und vertrauensvolle Ansatz der vergangenen Jahre, bei dem Behörden und Privatwirtschaft, Interessenvertretungen und beteiligte Ministerien gemeinsam und auf Augenhöhe die Weiterentwicklung von IT-Sicherheit diskutiert haben, als Beispiel für gesamtgesellschaftliches Handeln gegenüber einer wachsenden Bedrohung durch weltweit zunehmende Cyberangriffe wahrgenommen.

Dieser Ansatz wird mit der Novellierung des IT-Sicherheitsgesetzes in Teilen infrage gestellt. Weder wurde die im IT-SiG von 2015 vorgesehene Evaluierung der dort festgelegten Maßnahmen umgesetzt, noch scheint der aktuelle „Stellungnahmeprozess“ angesichts der Vielzahl kontroverser Regelungstatbestände geeignet, notwendige Abwägungen der Verhältnismäßigkeit einzelner Maßnahmen sicherstellen zu können. Darüber hinaus werden mit einzelnen Regelungen bewusst nationale Regelungen ohne europäisches Pendant verfolgt. Dies könnte Wettbewerbsnachteile für den Standort Deutschland nach sich ziehen oder, im ungünstigsten Fall, zu einer nachträglich notwendig werdenden Harmonisierung mit der auf europäischer Ebene maßgeblichen Netzwerk- und Informationssicherheits-Richtlinie (NIS-RL) führen.

Inhaltlich erweitert der Gesetzentwurf den bestehenden Ordnungsrahmen teilweise erheblich. Neben der Aufnahme neuer KRITIS-Sektoren und der Ausweitung der Befugnisse des Bundesamtes für Sicherheit in der Informationstechnik (BSI), z. B. für aktive Detektion von Sicherheitslücken („Portscans“), steht insbesondere die Ausweitung der Pflichten für Betreiber Kritischer Infrastrukturen – hier die Verpflichtung zur Detektion von Schadprogrammen - im Fokus des Gesetzgebers.

Auch eine massive Erhöhung möglicher Bußgelder sieht der Gesetzentwurf vor, um „Wertungswidersprüche bei Verstößen gegen die DSGVO und die NIS-Richtlinie zu beheben“.

Die Deutsche Krankenhausgesellschaft setzt sich seit vielen Jahren aktiv für die Verbesserung der Informationssicherheit in den deutschen Krankenhäusern ein. Neben dem Engagement im Rahmen des „Umsetzungsplans Kritische Infrastrukturen

(UP KRITIS)“ steht vor allem die Veröffentlichung und Weiterentwicklung des sog. „Branchenspezifischen Sicherheitsstandards (B3S)“ im Mittelpunkt der Aktivitäten.

Informationssicherheit als ein Grundpfeiler für Digitalisierung im Gesundheitswesen bildet gemeinsam mit dem Datenschutz das Fundament für eine sichere und vertrauensvolle Nutzung digitaler Dienste im medizinischen Umfeld, insbesondere in den Krankenhäusern. Informationssicherheit ist letztlich immer auch Patientensicherheit. Diesem Umstand tragen Änderungen im SGB V Rechnung, nach denen künftig alle Krankenhäuser in Deutschland Maßnahmen zum Schutz ihrer informationstechnischen Systeme vorhalten müssen.

Die Position der Krankenhäuser zu einzelnen Regelungen sind dem Besonderen Teil zu entnehmen.

Besonderer Teil

Artikel 1

Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)

Zu Artikel 1 Nummer. 1 Buchstabe f (§ 2 Absätze 13 und 14 BSIG – neu)
Definition kritischer Komponenten sowie Unternehmen im besonderen öffentlichen Interesse

Beabsichtigte Neuregelung

Es werden sogenannte „kritische Komponenten“ im Sinne des Gesetzes definiert. Diese sollen für Betreiber nach § 8d Absatz 2 Nummer 1 (Betreiber öffentlicher Telekommunikationsnetze oder -dienste) durch den Katalog von Sicherheitsanforderungen nach § 109 Absatz 6 des Telekommunikationsgesetzes näher bestimmt werden. Alle übrigen kritischen Komponenten werden gesetzlich festgelegt.

Weiterhin werden sogenannte „Unternehmen im öffentlichen Interesse“ definiert, die zwar keine kritischen Infrastrukturen darstellen, jedoch ebenfalls per Rechtsverordnung (BSI-KritisV) definiert werden. Maßgeblich hierfür sei, dass diese Unternehmen nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind.

Stellungnahme

Mit der Definition sog. „kritischer Komponenten“ werden IT-Produkte, die in kritischen Infrastrukturen eingesetzt werden und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, besonderen Anforderungen unterstellt, weil Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit dieser IT-Produkte zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit kritischer Infrastrukturen oder zu Gefährdungen für die öffentliche Sicherheit führen können.

Für den Bereich der Anbieter von Telekommunikationsnetzen oder -diensten werden die Festlegungen zu kritischen Komponenten durch den Katalog von Sicherheitsanforderungen nach § 109 Abs. 6 Telekommunikationsgesetz (TKG) näher bestimmt. Für die weiteren KRITIS-Sektoren sollen die kritischen Komponenten jeweils gesetzlich festgelegt werden.

Die erwartete Einstufung, z. B. des Krankenhaus-Informationssystems als sog. „kritische Komponente“, hätte umfangreiche Auswirkungen, insbesondere auf die Hersteller entsprechender Produkte, die sich in einem ohnehin stark begrenzten Marktgeschehen

europäisch wie international als Standortnachteil für Deutschland erweisen könnten. Für das Konzept der kritischen Komponente besteht weder auf europäischer noch auf internationaler Ebene ein Pendant, weswegen überdies eine nachträgliche (negative) Harmonisierung mit der NIS-Richtlinie nicht ausgeschlossen wäre. Die Klarstellung, dass eine Festlegung hierzu für die übrigen Sektoren gesondert gesetzlich festgelegt werden muss, wird daher ausdrücklich begrüßt.

Bei der Festlegung von „Unternehmen im besonderen öffentlichen Interesse“ wird derzeit nicht davon ausgegangen, dass hierunter Krankenhäuser gefasst werden, die nicht ohnehin bereits als kritische Infrastruktur gelten. Überdies sind mit den Festlegungen in § 75c SGB V spezialgesetzliche Regelungen zur Umsetzung von Maßnahmen zur Verbesserung der IT-Sicherheit in Kraft getreten, die für alle nach § 108 SGB V für die Behandlung gesetzlich Versicherter zugelassenen Krankenhäuser Anwendung finden.

Änderungsvorschlag

Entfällt.

Zu Artikel 1 Nummer 12 Buchstabe b (§ 8a Absätze 1a und 1b BSIG – neu)
Verpflichtung zur Vorhaltung von Systemen zur Angriffserkennung sowie Protokollierung entsprechender Information

Beabsichtigte Neuregelung

Mit § 8a Absätze 1a und 1b werden ausweislich der amtlichen Begründung die Betreiber kritischer Infrastrukturen verpflichtet, Systeme zur Angriffserkennung einzurichten.

Stellungnahme

Als Systeme zur Angriffserkennung (Intrusion Detection Systeme – IDS) werden teils komplexe Systeme zur Erkennung von Angriffen und damit zum Schutz vor Missbrauch bezeichnet, deren Ziel aus Sicht des BSI darin besteht, *„aus allen im Überwachungsbereich stattfindenden Ereignissen diejenigen herauszufiltern, die auf Angriffe, Missbrauchsversuche oder Sicherheitsverletzungen hindeuten, um diese anschließend vertieft zu untersuchen. Ereignisse sollen dabei zeitnah erkannt und gemeldet werden. Intrusion-Detection ist als Prozess zu verstehen und bedarf einer geeigneten organisatorischen Einbindung sowie der technischen Unterstützung durch geeignete Werkzeuge.“*[1]

[1] BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen, abgerufen am 06.12.2020 unter https://www.bsi.bund.de/DE/Publikationen/Studien/IDS02/gr1_htm.html

Zur Detektion von Angriffen kommen dabei gemäß BSI folgende Methoden zur Anwendung:

- Erkennung von Angriffsmustern
- Anomalieerkennung
    - durch Protokollanalyse
    - auf Basis statistischer Daten
    - auf Basis von Künstlicher Intelligenz
    - auf Basis von Honeypots
- Korrelation von Ereignisdaten

Die genannten Methoden machen deutlich, dass es sich hierbei um wesentlich höhere Anforderungen handelt, als gemeinhin mit einer „Firewall“ verbunden werden. Neben entsprechender (Echtzeit-)Analyse des Netzwerkverkehrs, von Protokolldaten oder (intelligenter) Verknüpfung verschiedener Ereignisdaten kommt selbst die Einrichtung sogenannter Honeypots – also vermeintliche Echtsysteme, die potenziellen Angreifern ein lohnendes Ziel versprechen, um diese anzulocken und eine Angriffserkennung in einer kontrollierten Umgebung zu erleichtern – zum Einsatz.

Die Verpflichtung zur Einrichtung entsprechender Systeme besteht ab dem 01.01.2022. Somit bleibt voraussichtlich maximal ein Jahr zur Vorbereitung, um diese teils erheblich komplexen Anforderungen umzusetzen, die nicht allein im Bereich der Investitionen, sondern insbesondere bei „Betrieb“, „Personal“ und „Organisation“ ambitioniert sind. Neben der Einführung von geeigneter Hard- und Software ist auch der Aufbau entsprechender Monitoring-, Detektions-, Analyse-, Alarmierungs- und Reaktionsprozesse notwendig. Diese Aufgaben werden üblicherweise durch sog. Security Operation Center (SOC) wahrgenommen. Hierbei handelt es sich faktisch um den Aufbau von hochspezialisierten Teams, die 24/7 tätig sind. Für den Bereich des Gesundheitswesens – hier insbesondere die Krankenhäuser – besteht aktuell aufgrund der Covid-19-Pandemie sowie der massiven Digitalisierungsbestrebungen im Kontext der Telematikinfrastruktur, die seitens des BSI gesondert begleitet wird, ein erheblicher Handlungsdruck, der zu einer Überforderung der Krankenhäuser, die als kritische Infrastrukturen gelten, in diesem Bereich führen könnte. IDS sind bisher kein Gegenstand des branchenspezifischen Sicherheitsstandards. Auch wenn dies für die anstehende Überarbeitung berücksichtigt wird, halten zum gegenwärtigen Zeitpunkt selbst diejenigen Krankenhäuser, die entsprechende Maßnahmen zur Verbesserung der IT-Sicherheit umsetzen, ein IDS in der Regel nicht vor. Zudem bleibt die konkrete Ausgestaltung offen. Hier muss die Regelung auf IT-technische Minimalanforderungen begrenzt sein.

Mit der Verpflichtung zur Protokollierung von Ereignisdaten über einen Zeitraum von vier Jahren wird Betreibern Kritischer Infrastrukturen ein unverhältnismäßiger Aufwand für die Unterstützung der Strafverfolgungsbehörden auferlegt. Eine datenschutzkonforme Speicherung würde jedoch unterstellen, dass aus diesen Informationen personenbezogene Daten herausgelöst werden könnten. Dies ist Stand heute nicht verhältnismäßig.

Änderungsvorschlag

Es ist eine realistische Übergangsfrist von mindestens zwei Jahren für die grundsätzliche Einführung von Systemen zur Angriffserkennung notwendig. Wenn es Branchen gibt, in denen entsprechende Systeme schon heute zum Stand der Technik zählen, könnte alternativ auch der Umsetzungszeitpunkt des Einsatzes von IDS in der Verordnung nach § 10 Abs. 5 BSIG branchenspezifisch geregelt werden und dabei die in der Gesetzesbegründung bereits angesprochenen unterschiedlichen Voraussetzungen in den einzelnen Branchen und Sektoren berücksichtigt werden.

Die Vorhaltung von Protokollierungsdaten sollte im Normalfall auf 3 Monate beschränkt sein. In potenziellen Detektionsfällen sollten diese Daten über einen Zeitraum von maximal 1 Jahr aufbewahrt werden müssen.

Zu Artikel 1 Nummer 22 (§ 14 BSIG – neu)

Bußgeldvorschriften

Beabsichtigte Neuregelung

Aufgrund von Fragen der Zuständigkeit bei der Festlegung eines Strafmaßes im Falle einer Zuwiderhandlung gegen die im Gesetzentwurf enthaltenen Vorgaben werden Verstöße als Ordnungswidrigkeit geahndet, die jedoch mit Blick auf die Höhe des Strafmaßes (bis zu 20 Mio. EUR bei vorsätzlichem, bis zu 10 Mio. EUR bei fahrlässigem Handeln) dem europäischen Bußgeldrahmen der DSGVO entsprechen.

Stellungnahme

Die Angleichung des Strafmaßes an den europäischen Bußgeldrahmen zur DSGVO war erwartet worden und das vorgeschlagene abgestufte Sanktionsmaß wird dabei als grundsätzlich sachgerecht angesehen. Allerdings erscheint die Erhöhung um das bis zu 200-fache des jetzigen Sanktionsmaßes (von derzeit 100.000 EUR auf bis zu 20 Mio. EUR) unverhältnismäßig und ist zu streichen. Der Erfüllungsaufwand für die Wirtschaft sollte gemäß der kürzlich durchgeführten Erhebung des Statistischen Bundesamts in den Sektoren der Kritischen Infrastrukturen beziffert werden.

Änderungsvorschlag

§ 14 Absatz 2 BSIG – neu wird wie folgt geändert:

(2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 1 Buchstabe a, Nummern 2, 9, 13, 14, 16, 17 und 18 mit einer Geldbuße bis zu 2 Millionen Euro geahndet werden. ~~**, auf § 30 Absatz 2 Satz 3 des Gesetzes über Ordnungswidrigkeiten wird verwiesen.**~~ Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 1 Buchstabe b und Nummern 3, 5, 8, 10, 11, 12 und 15 mit einer Geldbuße bis zu 1 Million Euro geahndet werden. In den übrigen Fällen kann die Ordnungswidrigkeit mit einer Geldbuße bis zu 100.000 Euro geahndet werden.

Artikel 7

Evaluierung

Zu Artikel 7 IT-SiG 2.0
Evaluierung

Beabsichtigte Neuregelung

Die bisherigen Regelungen zur Evaluierung von Artikel 1 Nr. 2, 7 und 8 des IT-Sicherheitsgesetzes vom 17.7.2015 werden ersetzt durch eine im wesentlichen äquivalente Regelung, die eine Evaluierung des § 2 Absatz 10 sowie der §§ 8a, 8b, 8d, 8e und 10 des BSIG zum 31.12.2022 vorsieht.

Stellungnahme

Die ursprünglich mit Artikel 10 des IT-Sicherheitsgesetzes vom 17. Juli 2015 festgelegte Evaluierung der Definition kritischer Infrastrukturen (Artikel 1 Nr. 2 IT-SiG), der Anforderungen an Betreiber kritischer Infrastrukturen nach den §§ 8a - 8d BSIG (Artikel 1 Nr. 7 IT-SiG) sowie der Rechtsverordnung nach § 10 BSIG (Artikel 1 Nr. 8 IT-SiG) unter Einbeziehung eines wissenschaftlichen Sachverständigen ist bisher nicht erfolgt. Dies hätte vier Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 BSIG (3.5.2016) erfolgen müssen. Die Verschiebung der Evaluation mit Verweis auf Änderungen der rechtlichen Grundlagen (Änderung der BSI-KritisV v. 30.06.2017) ist nicht nachvollziehbar. Mit diesem Argument könnte die Evaluierung auch zukünftig verschoben werden. Das Ergebnis der geforderten Evaluierung ist aber für die Betreiber der Kritischen Infrastrukturen von großem Interesse hinsichtlich der Wirksamkeit der Anforderungen des IT-SiG.

Mit der Neuregelung wird die Evaluierung zeitlich um bis zu weitere zwei Jahre verschoben. Es soll zudem keine Evaluierung des Anwendungsbereichs der §§ 8a und 8b erfolgen.

Die Evaluierung war gesetzlicher Auftrag, dem unabhängig von der laufenden Überarbeitung hätte Rechnung getragen werden müssen. Die erneute Verschiebung der wissenschaftlich begleiteten Evaluation ist nicht sachgerecht.

Änderungsvorschlag

Artikel 7 Absatz 1 IT-SiG 2.0 wird wie folgt geändert:

(1) Die §§ 2 Absatz 10, 8a, 8b, 8d und 8e sowie 10 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (Artikel 1) sind zum 31. Dezember **2021** ~~2022~~ unter Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem deutschen Bundestag bestellt wird, zu evaluieren.

Weiterer gesetzlicher Handlungsbedarf

Für den Gesundheitsbereich sind inzwischen eine Reihe von spezialgesetzlichen Regelungen zur Verbesserung der IT-Sicherheit u. a. im fünften Buch Sozialgesetzbuch, aufgenommen worden (vgl. § 75c SGB V).

Im Zuge der Digitalisierung der Krankenhäuser hat das Bundesministerium für Gesundheit (BMG) eine Förderung, z. B. für Vorhaben zur Verbesserung der IT-Sicherheit in Krankenhäusern, über den so genannten Krankenhaus-Zukunftsfonds vorgesehen, dabei jedoch Krankenhäuser als Betreiber Kritischer Infrastrukturen explizit von dieser Fördermöglichkeit ausgenommen. Zur Begründung wird ausgeführt, dass diese nach dem so genannten Krankenhaus-Strukturfonds förderfähig wären und eine Doppelförderung ausgeschlossen werden müsse.

Mit dem Krankenhaus-Zukunftsfonds hat der Gesetzgeber einen Webfehler des Krankenhaus-Strukturfonds bereinigt, infolge dessen sich dieser Fonds als völlig dysfunktional in Bezug auf Maßnahmen für KRITIS-Betreiber herausgestellt hatte. Die bisher erforderliche Einvernehmensherstellung mit den gesetzlichen Krankenkassen wurde auf eine Benehmensherstellung reduziert. Bundesweit haben nach aktuellem Stand lediglich vier Krankenhäuser Fördermittel aus dem Krankenhaus-Strukturfonds erhalten, da in den meisten Fällen beantragte Mittel seitens der Krankenkassen mit deren Veto-Recht verhindert wurden.

In der aktuellen Covid-19-Pandemie wird der gesamtgesellschaftliche Wert der Krankenhäuser für die Gesundheitsversorgung deutlich. Ausgerechnet die Kliniken, die bereits gesetzlich dazu verpflichtet sind, hohe Anforderungen an die IT-Sicherheit ihrer informationstechnischen Systeme umzusetzen, werden jedoch seitens des BMG explizit von einer dringend benötigten Förderung dieser Maßnahmen ausgeschlossen. Dies widerspricht den Zielen der Vorsorgegesetzgebung und bestraft am Ende diejenigen Kliniken finanziell, die gemäß den Vorgaben der BSI-KritisV gesamtgesellschaftlich relevant sind. Es sollte ressortübergreifend sichergestellt werden, dass im Zuge von Gesetzgebungsverfahren keine solchen Fehlentwicklungen entstehen, die dem Ziel, die IT-Sicherheit zu verbessern und Cyberangriffe zu vermeiden, aktiv entgegenstehen. Noch befinden sich einige Gesetzgebungsverfahren aus dem BMG im parlamentarischen Prozess, sodass hier Fehlentwicklungen entgegengewirkt werden sollte.