

Stellungnahme

der Deutschen Krankenhausgesellschaft

zum

Referentenentwurf

eines

**Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur
Stärkung der Resilienz von Betreibern kritischer Anlagen**

(KRITIS-Dachgesetz – KRITIS-DachG)

Stand: 24.01.2024

Inhaltsverzeichnis

| | |
|---|-----------|
| Allgemeiner Teil | 4 |
| Besonderer Teil | 8 |
| Artikel 1 Dachgesetz zur Stärkung der physischen Resilienz von Betreibern kritischer Anlagen (KRITIS-Dachgesetz – KRITIS-DachG) | 8 |
| § 1 Nationale KRITIS-Resilienz-Strategie | 8 |
| § 3 Zentrale Anlaufstelle; Zuständigkeiten; behördliche Zusammenarbeit | 9 |
| Zu Abs. 1 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) als zentrale Anlaufstelle nach der CER-Richtlinie | 9 |
| Zu Abs. 2 Zuständige Behörden im Sinne der CER-Richtlinie auf Ebene des Bundes | 9 |
| Zu Abs. 3 - 4 Zuständigkeiten des Bundes, sektorenübergreifende Ansprechpartner auf Ebene der Länder..... | 10 |
| Zu Abs. 5 Zuständigkeiten der Bundesländer für die Durchführung des Gesetzes..... | 10 |
| Zu Abs. 6 Zuständigkeit nach dem Hauptsitz des Betreibers kritischer Infrastruktur | 11 |
| Zu Abs. 7 - 8 Informationsaustausch zwischen den beteiligten Aufsichtsbehörden auf Ebene des Bundes; Konsultation der zuständigen Behörden anderer Mitgliedsstaaten der EU | 11 |
| § 4 Anwendungsbereich; kritische Anlagen; Geltungsumfang | 12 |
| Zu Abs. 1 - 2 Festlegung von Schwellenwerten für die Identifikation kritischer Anlagen durch Rechtsverordnung, Ersatzvornahme zur Registrierung | 12 |
| § 6 Registrierung der kritischen Anlage und Ansprechpartner; Geltungszeitpunkt..... | 13 |
| Zu Abs. 1 Registrierung der kritischen Anlage | 13 |
| Zu Abs. 3 Ersatzvornahme der Registrierung | 13 |
| § 8 Nationale Risikoanalysen und Risikobewertungen | 16 |
| Zu Abs. 1 Erstellung von Risikoanalysen und -bewertungen durch die für die Sektoren zuständigen Bundesministerien | 16 |
| Zu Abs. 5 Bereitstellung der Elemente der Risikoanalysen der Bundesministerien durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) an die Betreiber kritischer Anlagen | 17 |
| § 9 Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen | 18 |
| Zu Abs. 1 Erstellung von Risikoanalysen und -bewertungen durch Betreiber kritischer Anlagen | 18 |
| Zu Abs. 2 Festlegung von Vorlagen und Mustern für Risikoanalysen und -bewertungen durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)..... | 19 |
| § 10 Resilienz-Maßnahmen der Betreiber kritischer Anlagen; Resilienzplan | 21 |
| Zu Abs. 1 Umsetzung geeigneter und verhältnismäßiger technischer, sicherheitsbezogener und organisatorischer Maßnahmen zur Gewährleistung der Resilienz durch Betreiber kritischer Anlagen..... | 21 |
| Zu Abs. 3 Aufzählung von Maßnahmen zur Gewährleistung der Resilienz durch Betreiber kritischer Anlagen..... | 22 |
| Zu Abs. 4 Katalog sektorenübergreifender Mindestanforderungen zur Konkretisierung von Absatz 1 | 22 |
| Zu Abs. 6 Vorschlag branchenspezifischer Resilienzstandards zur Gewährleistung der Anforderung nach Absatz 1 | 23 |

| | |
|--|-----------|
| Zu Abs. 9 - 10 Erstellung eines Resilienzplans, Bereitstellung von Vorlagen und Mustern für einen Resilienzplan..... | 24 |
| § 11 Nachweise, behördliche Anordnungen..... | 25 |
| Zu Abs. 1 Nachweis der Erfüllung der Anforderungen nach Absatz 1 | 25 |
| Zu Abs. 5 Überprüfung der Einhaltung der Anforderungen durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) | 25 |
| Zu Abs. 6 Anweisung zur Mängelbeseitigung durch die zuständige Behörde | 26 |
| § 12 Meldewesen für Vorfälle | 27 |
| Zu Abs. 1 - 2 Verpflichtung zur Meldung von Vorfällen, welche die Erbringung der kritischen Dienstleistung erheblich stören oder stören könnten..... | 27 |
| Zu Abs. 3 Erstmeldung innerhalb von 24 Stunden, ausführlicher Bericht spätestens nach einem Monat..... | 28 |
| § 13 Unterstützung der Betreiber kritischer Anlagen | 29 |
| § 14 Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleiter für Betreiber kritischer Anlagen..... | 30 |
| § 16 Ermächtigung zum Erlass von Rechtsverordnungen..... | 31 |
| § 19 Bußgeldvorschriften..... | 32 |
| Zu Abs. 1 Festlegung von Ordnungswidrigkeitstatbeständen | 32 |
| Artikel 2 Änderung des Dachgesetzes zur Stärkung der physischen Resilienz von Betreibern kritischer Anlagen (KRITIS-Dachgesetz – KRITIS-DachG)..... | 33 |
| Artikel 3 Inkrafttreten | 34 |
| Weiterer gesetzlicher Handlungsbedarf | 35 |

Allgemeiner Teil

Mit dem Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz - KRITIS-DachG) sollen einheitliche bundesgesetzliche sektorenübergreifende Mindeststandards für den physischen Schutz kritischer Anlagen normiert werden. Dabei ist vorgesehen, dass diese Regelungen neben die bisherigen Vorgaben für kritische Infrastrukturen, insbesondere aus dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), treten und dabei – soweit möglich und sinnvoll – übereinstimmend geregelt werden sollen. Das Bundesministerium des Innern und für Heimat hatte bereits im Juli 2023 einen ersten Referentenentwurf vorgelegt, für den zum damaligen Zeitpunkt die Ressortabstimmung noch nicht abgeschlossen war. Es wurde jedoch angekündigt, zu einem späteren Zeitpunkt im Rahmen einer erneuten Verbändeanhörung einen zweiten, überarbeiteten Referentenentwurf zur Kommentierung bereitzustellen. Dieser liegt nun vor. Im Folgenden nehmen die Krankenhäuser zu den geplanten Regelungen sowie insbesondere zu den im Vergleich zum ersten Referentenentwurf aus Mitte 2023 genannten Punkten Stellung.

Im Kern der neuen Vorgaben zur Stärkung der Resilienz kritischer Anlagen steht ein Risikomanagement, welches dem All-Gefahren-Ansatz folgend Maßnahmen zur Aufrechterhaltung, Stärkung oder Herstellung der Handlungsfähigkeit identifiziert und dem Risiko einer Beeinträchtigung des Geschäftsbetriebs entgegenwirken soll.

Für den Cyberschutz bestehen heute bereits weitreichende gesetzliche Regelungen, die im vorliegenden Gesetzentwurf auf den Bereich des physischen Schutzes ausgedehnt werden sollen. Erstmals sollen durch das KRITIS-DachG bundeseinheitliche und sektorenübergreifende Vorgaben, Maßnahmen und Mindeststandards für physische Resilienz etabliert werden. Ziel ist es, Risiken zu minimieren, welche die Wirtschaftsstabilität der betreffenden Einrichtungen bedrohen oder beeinträchtigen können. Hierzu zählen im Sinne des Entwurfs unter anderem naturbedingte, klimatische oder vom Menschen verursachte Risiken, wie zum Beispiel Unfälle, Naturkatastrophen, gesundheitliche Notlagen, hybride Bedrohungen oder andere feindliche Bedrohungen einschließlich terroristischer Straftaten.

Ein zentraler Punkt der Überarbeitung wird dabei besonders begrüßt: Für eine bessere Übersichtlichkeit soll es eine gemeinsame Rechtsverordnung zur Bestimmung von Betreibern kritischer Anlagen sowie wichtiger und besonders wichtiger Einrichtungen nach dem KRITIS-DachG und dem BSIG geben. Mit der Rechtsverordnung soll ersichtlich werden, welche Verpflichtungen für Betreiber von kritischen Anlagen sowie wichtigen und besonders wichtigen Einrichtungen im Hinblick auf physische Resilienz-Maßnahmen nach dem KRITIS-DachG und im Hinblick auf den Cyberschutz nach BSIG gelten. Darüber hinaus soll für die Registrierung der Betreiber sowie für die Meldung von Störungen eine gemeinsame technische Lösung angestrebt werden, sodass hier ein möglichst geringer Verwaltungsaufwand für die Wirtschaft entsteht. Die Krankenhäuser hatten sich dafür ausgesprochen, soweit wie möglich Synergie-Effekte zwischen den bisherigen Regelungen im Cyberschutz und den neuen Resilienz-Anforderungen zu nutzen. Mit den geplanten Regelungen werden die Voraussetzungen hierfür geschaffen. Vorgesehen ist nun auch eine Evaluierung der weiteren Angleichungen zwischen den Regelungen dieses Gesetzes und den Regelungen des Cyberschutzes.

Während das KRITIS-DachG die Regelungen und Strukturen im Kontext Cyberschutz weitgehend repliziert, werden nun erstmals Auswirkungen von Abhängigkeiten einzelner Sektoren auf kritische Anlagen in anderen Sektoren (auch grenzüberschreitend) betrachtet. Die Berücksichtigung solcher Interdependenzen war in den bisherigen KRITIS-Vorgaben unter anderem mit Blick auf die kaum zu beherrschende Komplexität sektorenübergreifender Risikobewertungen und Maßnahmenpakete nicht erfolgt.

Schon jetzt zählen Krankenhäuser zu den kritischen Infrastrukturen in Deutschland. Für sie gelten insbesondere im Bereich Cyberschutz schon heute umfangreiche Vorgaben, die in Teilen aufgrund spezialgesetzlicher Regelungen, z. B. im Fünften Buch Sozialgesetzbuch, über die allgemeinen Anforderungen für kritische Infrastrukturen hinausgehen. Trotz schwieriger wirtschaftlicher Rahmenbedingungen bildet die Thematik einen wesentlichen Handlungsschwerpunkt in den Krankenhäusern. Dabei werden schon heute physische Absicherungsmaßnahmen für sensible Organisationsbereiche, wie z. B. das Rechenzentrum, durch einen von der Deutschen Krankenhausgesellschaft vorgelegten branchenspezifischen Sicherheitsstandard (B3S) gefordert und umgesetzt. Auch Anforderungen an ein Sicherheitsmanagement, wie Sicherheitsüberprüfungen bei Neueinstellungen, sind für ausgewählte Organisationsbereiche als Anforderung definiert. Der B3S für die Branche „medizinische Versorgung“ geht in seiner Definition der Schutzziele sogar über die geforderten Schutzziele der Informationssicherheit hinaus, indem branchenspezifische Schutzziele (Patientensicherheit, Behandlungseffektivität) definiert und in den Anforderungen adressiert wurden.

Der mit der Umsetzung dieser Maßnahmen verbundene Aufwand wurde schon 2019 allein für die ca. 150 Krankenhäuser, die mit mehr als 30.000 vollstationären Behandlungsfällen pro Jahr als kritische Infrastruktur im Sinne der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) gelten, mit mehr als einer halben Milliarde Euro erhoben. Eine aktuelle Studie von 2023 beziffert die Mehrkosten, die infolge einer allgemeinen Vorgabe gemäß § 75c SGB V zur Umsetzung von Maßnahmen für Informationssicherheit in allen Krankenhäusern vorgehalten werden müssen, auf ca. 1,5 Milliarden Euro pro Jahr. Unabhängig vom entstehenden Aufwand ist die Digitalisierung des Gesundheitswesens ohne ausreichende Schutzmaßnahmen, insbesondere im Bereich Informationssicherheit, nicht denkbar. Allerdings muss dabei beachtet werden, dass die Preise der Krankenhäuser für Leistungen nach der gesetzlichen Krankenversicherung bundeseinheitlich vorgegeben werden. Steigende Kosten können nicht auf die Preise der Krankenhäuser aufgeschlagen werden. Die Kostensteigerungen in den Krankenhäusern infolge der Inflation sowie die gestiegenen Personalkosten zwingen aktuell viele Krankenhäuser in die Insolvenz. Unter den aktuellen Rahmenbedingungen werden daher viele der im vorliegenden Gesetzentwurf enthaltenen Maßnahmen einer Wirtschaftlichkeitsbetrachtung kaum standhalten können. Zudem wird die teils prekäre Ressourcenknappheit durch den Fachkräftemangel, insbesondere in der IT, weiter verschärft.

Eine valide Aufwandsschätzung war mit Blick auf die bisher fehlende Definition von Schutzzielen oder die ebenfalls nicht vorliegende nationale Risikoanalyse, welche die Grundlage der individuellen branchenspezifischen Betrachtungen bilden soll, im Bereich der Krankenhäuser nicht möglich. Auch der überarbeitete Gesetzentwurf trifft hierzu keine Aussagen für die Wirtschaft im Allgemeinen oder einzelne Sektoren im Besonderen. Allerdings wird nun der für die öffentliche Verwaltung entstehende Aufwand mit ca. 6 Millionen Euro einmalig und ca. 6,4 Millionen Euro jährlich als „erheblich“ eingeschätzt. Wie auch für die Wirtschaft, wird eine reelle Aufwandsschätzung erst möglich sein, wenn durch die zugehörigen Rechtsverordnungen der Anwendungsbereich und die sektorspezifischen Mindestanforderungen konkret bestimmt werden. Allerdings ist bereits jetzt absehbar, dass für die von den Regelungen betroffenen Krankenhäuser der Umsetzungsaufwand noch wesentlich höher ausfallen dürfte, als für die mit der Kontrolle der Umsetzung beauftragten öffentliche Verwaltung.

Gerade KRITIS-Krankenhäuser haben bereits heute umfangreiche Nachweis- und Prüfverfahren in regelmäßigen Abständen, wie Wirtschaftsprüfungen, Nachweise gemäß § 8a Abs. 3 BSIG oder Zertifizierungen durch die Kooperation für Transparenz und Qualität im Gesundheitswesen (KTQ), zu erbringen. Die im Referentenentwurf des KRITIS-DachG vorgesehenen Nachweise würden erhebliche zusätzliche Ressourcen binden. Daher wird die Regelung einer Nachweispflicht nur noch auf Anforderung

ausdrücklich begrüßt, da diese Ressourcen nicht in jedem Krankenhaus ohne Weiteres zur Verfügung stehen.

Dennoch ist es von großer Bedeutung, dass sich auch Krankenhäuser mit den steigenden Risiken infolge naturbedingter, klimatischer oder von Menschen verursachten Veränderungen auseinandersetzen. Die Gesellschaft vertraut auf die medizinische Versorgung gerade bei Unfällen, Naturkatastrophen oder gesundheitlichen Notlagen. Die Einrichtungen, welche die medizinische Versorgung in Deutschland sicherstellen, müssen selbst ausreichend vor entsprechenden Bedrohungen geschützt werden. Die Krankenhäuser unterstützen daher – wie schon bisher – die Bemühungen des Gesetzgebers ausdrücklich, die kritischen Infrastrukturen in Deutschland durch entsprechende Maßnahmen adäquat abzusichern.

Schon den ersten Referentenentwurf von Juli 2023 haben die Krankenhäuser daher im Grundsatz begrüßt. Allerdings hatten sich die Krankenhäuser für eine Reihe von Anpassungen ausgesprochen. Es ist positiv zu bewerten, dass ein Teil der Änderungsvorschläge aufgegriffen wurde. Hierzu zählen insbesondere die Berücksichtigung der zuständigen Behörden auf Ebene der Länder (§ 3 Abs. 5) sowie Maßnahmen zur Bürokratievermeidung bei den Nachweisen nach § 11. Auch die nun nicht mehr als Mindestvorgaben gefassten Maßnahmen des § 10 (zuvor in Anlage 1 enthalten) können helfen, den physischen Schutz öffentlicher Einrichtungen, die 365 Tage im Jahr rund um die Uhr allen Bürgerinnen und Bürgern offenstehen, sachgerecht abzubilden. Hier bedarf es anderer Kriterien, als sie beispielsweise in einem schon heute abgeschotteten Kraftwerksbetrieb mit Perimeterschutz, wo Zutrittskontrollsysteme o. ä. eingesetzt werden, zur Anwendung kommen können.

Die zuständige nationale Behörde für die Resilienz kritischer Anlagen – das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) – hat aktuell noch keine Antwort auf die Fragen, die sich gerade Betreibern öffentlich zugänglicher kritischer Infrastrukturen stellen. Für die Umsetzung des Gesetzentwurfes bedarf es daher intensiver Abstimmungen zwischen dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und den betroffenen Sektoren, um ineffektive oder dem Versorgungsauftrag entgegenwirkende, bürokratische Vorgaben zu vermeiden. Der Abbau von Bürokratie ist ein zentrales Anliegen der Krankenhäuser. Daher begrüßen die Krankenhäuser, dass für die Umsetzung des KRITIS-DachG eine größtmögliche Konsistenz zu den bestehenden Vorgaben aus dem Bereich Cyberschutz hergestellt werden soll. Die Einrichtung einer gemeinsamen digitalen Meldeplattform für Meldepflichten nach dem BSI-Gesetz an das Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie nach dem KRITIS-DachG an das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) kann helfen, Synergien zu nutzen und unnötigen Aufwand zu reduzieren.

Schon in der Stellungnahme zum ersten Referentenentwurf haben die Krankenhäuser sowohl auf bestehende inhaltliche als auch auf organisatorische Abhängigkeiten zum geplanten Gesetzgebungsverfahren zur Umsetzung der NIS2-Richtlinie hingewiesen. Aus den nicht konsistenten Begriffsdefinitionen bei Kernbereichen, z. B. bei den betroffenen Anlagen, Betreibern und Einrichtungen, können weitreichende Unklarheiten folgen, welche die Gesetzgebung und ihre Umsetzung erschweren können. Als Beispiel seien hier die „besonders wichtigen Einrichtungen“ sowie die „wichtigen Einrichtungen“ genannt, die mit den bisherigen Definitionen für kritische Dienstleistungen und Schwellenwerte nicht konsistent sind.

Die Krankenhäuser unterstützen auch weiterhin den Gesetzgebungsprozess aktiv und behalten bei der Erhöhung des physischen Schutzes der Kliniken in Deutschland die branchenspezifischen Besonderheiten des Gesundheitswesens im Blick.

Die bereits geäußerte Kritik an der Vielzahl von Maßnahmen und dem auch nach objektiven Maßstäben unrealistischen Zeitplan für die Umsetzung (zehn Monate vom Zeitpunkt der Registrierung einer kritischen Anlage bis hin zur Umsetzung der Resilienzmaßnahmen) bleibt jedoch erhalten.

Erneut weisen die Krankenhäuser darauf hin, dass es für die Erhöhung der Resilienz der kritischen Infrastrukturen in Deutschland einer engen und vertrauensvollen Zusammenarbeit zwischen den Betreibern kritischer Infrastrukturen und den zuständigen Behörden bedarf. Die mehrfach angebrachten Bedenken, die Risiken für die kritischen Infrastrukturen in Deutschland könnten sich durch das Gesetzesvorhaben noch weiter erhöhen, konnten mit dem zweiten Referentenentwurf noch nicht ausgeräumt werden.

Unverständlich bleibt weiterhin, weshalb die nach Art. 10 der CER-Richtlinie vorgesehenen finanziellen Unterstützungsmöglichkeiten der Mitgliedsstaaten für Betreiber kritischer Anlagen im Entwurf des Gesetzes nicht aufgegriffen wurden. Auch, wenn die geltenden Beihilferegulungen auf EU-Ebene weitreichende Unterstützungen zumindest erschweren, wurde die Tragweite der Richtlinie bereits durch den Richtliniengeber selbst als sehr weitreichend eingeschätzt und entsprechende Unterstützungsmöglichkeiten ausdrücklich in die Richtlinie aufgenommen.

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

Besonderer Teil

Artikel 1

Dachgesetz zur Stärkung der physischen Resilienz von Betreibern kritischer Anlagen

(KRITIS-Dachgesetz – KRITIS-DachG)

§ 1

Nationale KRITIS-Resilienz-Strategie

Beabsichtigte Neuregelung

Der vormalig an dieser Stelle definierte „Zweck des Gesetzes“ wird gestrichen und durch die Festlegung einer Nationalen KRITIS-Resilienz-Strategie ersetzt. Diese soll bis 17.01.2026 von der Bundesregierung verabschiedet werden.

Stellungnahme

Ursprünglich sollte durch das Gesetz die Festlegung von Kriterien zur Identifizierung kritischer Anlagen und entsprechender Verpflichtungen für Betreiber erfolgen. Dies wurde im vorliegenden Absatz durch die Festlegung einer KRITIS-Resilienz-Strategie ersetzt. Die Vereinheitlichung der Vorgaben und Prozesse sollte konsequent weiterverfolgt werden. Im Rahmen der Kommentierung wurde darauf hingewiesen, dass ein mögliches Auseinanderlaufen der Definitionen zwischen Cyberschutz und Resilienz kaum beherrschbare Risiken für die nachfolgende Umsetzung bedeuten würde.

Änderungsvorschlag

Entfällt.

§ 3

Zentrale Anlaufstelle; Zuständigkeiten; behördliche Zusammenarbeit

Zu Abs. 1

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) als zentrale Anlaufstelle nach der CER-Richtlinie

Beabsichtigte Neuregelung

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) soll zentrale Anlaufstelle im Sinne des Artikels 9 Absatz 2 der Richtlinie (EU) 2022/2557 des Europäischen Parlamentes und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen werden.

Stellungnahme

Die Regelung ist sachgerecht und wurde redaktionell geschärft.

Die zuvor enthaltene Regelung, dass das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) Betreiber kritischer Anlagen bei der Umsetzung ihrer nach dem Gesetz zu erfüllenden Maßnahmen unterstützen sollte, wurde nun an dieser Stelle gestrichen und in § 13 überführt.

Änderungsvorschlag

Entfällt.

Zu Abs. 2

Zuständige Behörden im Sinne der CER-Richtlinie auf Ebene des Bundes

Beabsichtigte Neuregelung

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) soll zuständige Behörde auf Bundesebene im Sinne des Artikels 9 Absatz 1 der Richtlinie (EU) 2022/2557 des Europäischen Parlamentes und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen werden.

In Bezug auf öffentliche Telekommunikationsnetze oder öffentlich zugängliche Telekommunikationsdienste soll diese Aufgabe durch die Bundesnetzagentur und für alle anderen Betreiber kritischer Anlagen im Sektor Informationstechnik und Telekommunikation durch das Bundesamt für Sicherheit in der Informationstechnik, in Bezug auf den Sektor Finanz- und Versicherungswesen durch die Bundesanstalt für Finanzdienstleistungsaufsicht sowie die weiteren Aufsichtsbehörden des Bundes nach Absatz 3 und im Hinblick auf Aufgaben der Länder durch die zuständigen Landesbehörden nach Absatz 5 wahrgenommen werden.

Stellungnahme

Die Änderung war mit Blick auf die föderale Zuständigkeit der Bundesländer insbesondere für den Krankenhausbereich gefordert worden und wird begrüßt.

Änderungsvorschlag

Entfällt.

Zu Abs. 3 - 4

Zuständigkeiten des Bundes, sektorenübergreifende Ansprechpartner auf Ebene der Länder

Beabsichtigte Neuregelung

In Absatz 3 werden diejenigen kritischen Dienstleistungen benannt, für die der Bund zuständig ist. Der Sektor Gesundheit zählt nicht hierzu und wird in der Aufzählung entsprechend nicht benannt. Absatz 4 fordert eine Benennung einer Landesbehörde bis 02.01.2025, die für sektorenübergreifende Angelegenheiten auf Ebene der Länder zuständig ist.

Stellungnahme

Die Regelung ist sachgerecht.

Änderungsvorschlag

Entfällt.

Zu Abs. 5

Zuständigkeiten der Bundesländer für die Durchführung des Gesetzes

Beabsichtigte Neuregelung

Die Länder sind aufgefordert, dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) die zuständige Landesbehörde zu benennen, welche die Aufgaben nach diesem Gesetz wahrnimmt. Dies kann auch die nach Absatz 4 benannte Behörde sein.

Stellungnahme

Die Regelung ist sachgerecht und wird ausdrücklich begrüßt. Die Krankenhäuser hatten eine entsprechende Regelung in der Stellungnahme zum ersten Referentenentwurf gefordert. Zuständig für die Krankenhausplanung und Investitionsfinanzierung der Krankenhäuser sind die Bundesländer, die nun das jeweils zuständige Ressort gemäß diesem Gesetz als zuständige Behörde benennen können.

Änderungsvorschlag

Entfällt.

Zu Abs. 6

Zuständigkeit nach dem Hauptsitz des Betreibers kritischer Infrastruktur

Beabsichtigte Neuregelung

Für Betreiber kritischer Anlagen, für die die Länder zuständig sind, soll sich das zuständige Land nach dem Hauptsitz des Betreibers kritischer Anlagen bestimmen.

Stellungnahme

Für den Sektor Gesundheit greift diese Festlegung der Zuständigkeit ggf. in die Regelungskompetenz der einzelnen Länder ein. Es stellt sich dann die Frage nach der Durchsetzungsmöglichkeit „gebietsfremder“ Regelungen. Aus Sicht der Krankenhäuser ist eine einheitliche Regelung für Betreiber, die in mehreren Bundesländern Krankenhäuser unterhalten, u. U. jedoch stark vereinfachend. Vergleichbar sind hier beispielsweise die Regelungen zur Datenschutzaufsicht im Gesundheitsdatennutzungsgesetz (GDNG). In jedem Falle sind die Länder zu der Frage einzubeziehen, um rechtliche Unsicherheiten für die Betreiber zu vermeiden.

Änderungsvorschlag

Entfällt.

Zu Abs. 7 - 8

Informationsaustausch zwischen den beteiligten Aufsichtsbehörden auf Ebene des Bundes; Konsultation der zuständigen Behörden anderer Mitgliedsstaaten der EU

Beabsichtigte Neuregelung

Es wird ein wechselseitiger Informationsaustausch zwischen den beteiligten Aufsichtsbehörden auf Ebene des Bundes und der Länder festgeschrieben. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) konsultiert in regelmäßigen Abständen die zuständigen Behörden anderer Mitgliedstaaten der Europäischen Union.

Stellungnahme

Die Regelung wird ausdrücklich begrüßt. Ein regelmäßiger Informationsaustausch ist eine notwendige Grundlage, um auf sich ändernde Anforderungen reagieren zu können.

Änderungsvorschlag

Entfällt.

§ 4

Anwendungsbereich; kritische Anlagen; Geltungsumfang

Zu Abs. 1 - 2

Festlegung von Schwellenwerten für die Identifikation kritischer Anlagen durch Rechtsverordnung,
Ersatzvornahme zur Registrierung

Beabsichtigte Neuregelung

Die Festlegung, welche Anlagen als kritische Anlagen im Sinne des Gesetzes gelten, soll durch eine Rechtsverordnung festgelegt werden. Dabei soll auf branchenspezifische Schwellenwerte abgestellt und Stichtagsregelungen festgelegt werden, wobei ein Regelschwellenwert von 500.000 zu versorgenden Einwohnerinnen und Einwohnern zugrunde gelegt wird. Weiterhin wird die Möglichkeit der Ersatzvornahme einer Registrierung für verschiedene Kriterien, u. a. die Zahl betroffener Nutzerinnen und Nutzer oder die Abhängigkeit von anderen Sektoren oder Branchen, geschaffen.

Stellungnahme

Die Regelungen entsprechen dem bisherigen Vorgehen der BSI-Kritis-Verordnung. Neu ist die Möglichkeit der Ersatzvornahme zur Registrierung weiterer Einrichtungen für das Bundesministerium des Innern und für Heimat (BMI). Die Kriterien hierfür sind sehr weitreichend gefasst, eine Abstimmung mit der zuständigen Behörde, insbesondere nach § 3 Abs. 5 (zuständige Behörde auf Landesebene) ist nicht vorgesehen.

Nach wie vor ist die vorgesehene Frist zur Umsetzung der Maßnahmen gemäß § 6 Absatz 6 und § 10 Absatz 1 enthaltenen Vorlaufzeiten von zehn Monaten ab dem festgelegten Stichtag (Zeitpunkt der Registrierung als kritische Infrastruktur), auch vor dem Hintergrund noch festzulegender Maßnahmen, unrealistisch.

Änderungsvorschlag

In Absatz 2 sollte das Einvernehmen zwischen Bundesministerium des Innern und für Heimat (BMI) und zuständiger Aufsichtsbehörde nach § 3 Abs. 5 aufgenommen werden. Die Umsetzungsfristen sind auf mindestens 18 Monate zu erhöhen.

§ 6

Registrierung der kritischen Anlage und Ansprechpartner; Geltungszeitpunkt

Zu Abs. 1

Registrierung der kritischen Anlage

Beabsichtigte Neuregelung

Betreiber kritischer Anlagen sind zur Registrierung der Anlagen bei einer von Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeinsam eingerichteten Registrierungsstelle verpflichtet. Die Registrierung muss spätestens drei Monate nach dem Zeitpunkt, der auf die erstmalige oder erneute Einstufung als kritische Anlage nach § 4 folgt, erfolgen.

Stellungnahme

Die Krankenhäuser begrüßen ausdrücklich, dass es eine von Bundesamt für Sicherheit in der Informationstechnik und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe gemeinsam eingerichtete Registrierungsmöglichkeit geben soll. Die bereits heute etablierten Strukturen und Maßnahmen im Bereich Cybersicherheit müssen ressourcenschonend nachgenutzt werden können. Die Anpassung der Frist zur Registrierung von einem Werktag auf drei Monate wird ausdrücklich begrüßt.

Änderungsvorschlag

Entfällt.

Zu Abs. 3

Ersatzvornahme der Registrierung

Beabsichtigte Neuregelung

Es wird die Ersatzvornahme der Registrierung geregelt, wenn der Betreiber kritischer Anlagen seine Pflicht zur Registrierung nicht erfüllt. Die Registrierung soll im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes nach § 3 Absatz 3 oder im Benehmen mit der zuständigen Behörde der Länder nach § 3 Absatz 5 durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe vorgenommen werden können.

Das Bundesamt für Sicherheit in der Informationstechnik und die zuständigen Aufsichtsbehörden des Bundes nach § 3 Absatz 3 oder die zuständigen Behörden der Länder nach § 3 Absatz 5 können dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe Vorschläge für die Registrierung weiterer Betreiber kritischer Anlagen unterbreiten. Dafür übermitteln sie dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe die erforderlichen Informationen zur Identifizierung der Betreiber kritischer Anlagen.

Stellungnahme

Gerade im Bereich der Krankenhausplanung bestehen nach wie vor grundgesetzlich garantierte, föderale Hoheiten und Entscheidungskompetenzen der Bundesländer. Je nach Ausgestaltung der Rechtsverordnung nach § 16 muss darauf geachtet werden, die Kompetenzen der Länder nicht zu übergehen. Für die Identifikation kritischer Infrastrukturen bestehen für die Branche der medizinischen Versorgung Vorgaben, die zwischen dem Bundesministerium für Gesundheit (BMG) sowie dem Bundesministerium des Innern und für Heimat (BMI) abgestimmt wurden. Dabei wurden die Besonderheiten der Landeskrankenhausplanung in Deutschland berücksichtigt.

Es erscheint daher nicht sachgerecht, dass mit den zuständigen Behörden auf Ebene der Länder gemäß § 3 Absatz 5 nur eine Benehmensherstellung erfolgen soll, wenn diese die Aufgaben einer sonst zuständigen Bundesbehörde wahrnehmen. Für Krankenhäuser sind die Bundesländer zuständig, bei einer Ersatzvornahme zur Registrierung ist hier ebenfalls das Einvernehmen herzustellen.

Die föderal geregelten Vorgaben im Bereich der Gesundheitsversorgung im Krankenhaus (speziell planungsrechtliche Vorgaben) sind für die Identifikation der kritischen Infrastruktur schon heute maßgeblich. Ausweislich der Begründung zur Ersten Änderungsverordnung der BSI-Kritis-Verordnung ist der Krankenhausbegriff dabei „[...] im Sinne der Landeskrankenhauspläne zu verstehen, welche die zugelassenen Krankenhäuser, teilweise differenziert nach Betriebsstätten oder Standorten, ausweisen. Dabei sind räumlich getrennte Standorte oder Betriebsstätten eines Krankenhauses als eine Anlage anzusehen, wenn sie aus planungsrechtlicher Sicht, etwa aus organisatorischen, technischen, medizinischen oder sicherheitsbezogenen Aspekten als Einheit betrachtet werden.“ Bei der Festlegung der Rechtsverordnung nach § 16 sollten diese Rahmenbedingungen übernommen werden, um ein Auseinanderlaufen der bisherigen Definitionen im Cyberschutz von den Vorgaben zur Absicherung der Resilienz zu vermeiden.

Die Möglichkeit der Ersatzvornahme dürfte ohnehin nur in Einzelfällen infrage kommen, in denen unterschiedliche Interpretationen in der Frage der zugrunde liegenden Kennzahlen (Schwellenwert) ursächlich für eine anderslautende Einschätzung des Betreibers waren. Daher wird die Möglichkeit der Anhörung des Betreibers begrüßt.

Für die Frage, ob beispielsweise die Fallzahlen mehrerer Krankenhausstandorte desselben Krankenträgers zusammenzufassen sind, sind die Angaben im Feststellungsbescheid des Krankenhauses der zuständigen Landesbehörde (die erwartbar auch als Behörde nach § 3 Absatz 5 benannt wird) maßgeblich. Enthält beispielsweise der Landeskrankenhausplan keine Angaben zur Zusammenfassung mehrerer Betriebsstätten, ist aus dem Umstand, dass ein gemeinsamer Feststellungsbescheid für mehrere Standorte ergangen ist, nicht zwangsläufig abzuleiten, dass diese planungsrechtlich als Einheit zu betrachten sind, da in der Regel der Träger des Krankenhauses auch bei räumlich getrennten Standorten nur einen einzigen Feststellungsbescheid erhält. Vielmehr ist im Einzelfall zu prüfen, ob sich aus dem Feststellungsbescheid Anhaltspunkte ergeben, die eine planungsrechtliche Eigenständigkeit der einzelnen Betriebsstätten rechtfertigen könnten. Hierfür ist zum Beispiel zu berücksichtigen, ob im Feststellungsbescheid mehrere Standorte mit unterschiedlichen Adressen ausgewiesen sind oder ob die Fachabteilungsplanung jeweils unabhängig für die einzelnen Betriebsstätten erfolgt. In diesen Fällen sind diese räumlich getrennten Standorte oder Betriebsstätten nicht als Einheit im Sinne der Identifikation kritischer Infrastrukturen zu betrachten, sodass keine Zusammenfassung der an den einzelnen Standorten ausgewiesenen vollstationären Fallzahlen erfolgt.

Werden dagegen im Feststellungsbescheid die Adressen der unterschiedlichen Standorte nicht gesondert ausgewiesen oder geht aus dem Feststellungsbescheid hervor, dass die Fachabteilungsplanung für mehrere Betriebsstätten übergreifend erfolgt, sind diese als planungsrechtliche Einheit anzusehen.

Änderungsvorschlag

§ 6 Abs. 3 wird wie folgt geändert:

Wenn der Betreiber kritischer Anlagen seine Pflicht zur Registrierung nicht erfüllt, kann das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe nach Anhörung des betroffenen Betreibers kritischer Anlagen die Registrierung im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes nach § 3 Absatz 3 oder im **Bereichen Einvernehmen** mit der zuständigen Behörde der Länder nach § 3 Absatz 5 selbst vornehmen.
[...]

Die Regelungen zur Definition kritischer Anlagen im Bereich der Krankenhäuser bezüglich krankenhauplanerischer Vorgaben, die in der BSI-Kritis-Verordnung mit Blick auf die föderale Zuständigkeit der Bundesländer aufgenommen wurden, sind in die Rechtsverordnung nach § 16 dieses Gesetzes zu übernehmen.

§ 8

Nationale Risikoanalysen und Risikobewertungen

Zu Abs. 1

Erstellung von Risikoanalysen und -bewertungen durch die für die Sektoren zuständigen Bundesministerien

Beabsichtigte Neuregelung

Als Grundlage für alle weitergehenden Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen sollen die für die Sektoren zuständigen Bundesministerien alle vier Jahre oder auf Veranlassung eine sektorspezifische Risikoanalyse und -bewertung durchführen. Dabei sollen naturbedingte, klimatische und vom Menschen verursachte Risiken, welche die Wirtschaftsstabilität der kritischen Anlage bedrohen, berücksichtigt werden. Dies schließt insbesondere Unfälle, Naturkatastrophen, gesundheitliche Notlagen, hybride Bedrohungen und andere feindliche Bedrohungen, einschließlich terroristischer Straftaten, ausdrücklich mit ein.

Weiterhin sollen Risiken berücksichtigt werden, die sich aus dem Ausmaß der Abhängigkeit zu anderen Sektoren, inklusive dem Ausmaß der Abhängigkeit gegenüber anderen Mitglieds- und Drittstaaten, ergeben. Schließlich soll auch betrachtet werden, welche Auswirkungen sich durch eine im betrachteten Sektor auftretende erhebliche Störung in anderen Sektoren ergeben können. Dabei stehen wesentliche Risiken für den Binnenmarkt und die Bevölkerung im Mittelpunkt.

Stellungnahme

Es ist sachgerecht, dass die zuständigen Bundesministerien zunächst ein Lagebild im eigenen Sektor ermitteln und durch entsprechende Risikoanalysen und -bewertungen den Status quo erheben. Da jedoch die Risikoanalyse nach § 8 Grundlage für die nachfolgenden Risikoanalysen der Betreiber kritischer Anlagen selbst sind, sind diese – und auch die umzusetzenden Maßnahmen – maßgeblich von der rechtzeitigen Bereitstellung dieser Risikoanalyse durch die jeweils zuständigen Bundesministerien abhängig. Mit Blick auf die fristgerechte Umsetzung der geforderten Maßnahmen müssen die nationalen Risikoanalysen rechtzeitig vorliegen.

Verzögerungen infolge nicht rechtzeitig bereitgestellter nationaler Risikoanalysen dürfen keine negativen Konsequenzen für die Betreiber kritischer Anlagen entfalten. Zunächst muss für die Definition und später die Umsetzung von Maßnahmen zur Erhöhung der Resilienz nach § 10, die mindestens auf der sektorspezifischen Risikoanalyse basiert, ausreichender Vorlauf eingeplant werden. Zeitliche Verzögerungen, die auf die nationalen Risikoanalysen zurückgehen, müssen im weiteren Verlauf entsprechend berücksichtigt werden.

Änderungsvorschlag

Die zeitlichen Vorgaben für die Erstfassung der nationalen Risikoanalyse müssen ergänzt und Folgeregelungen im Falle von Verzögerungen bei der Bereitstellung durch die zuständigen Bundesministerien aufgenommen werden.

Zu Abs. 5

Bereitstellung der Elemente der Risikoanalysen der Bundesministerien durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) an die Betreiber kritischer Anlagen

Beabsichtigte Neuregelung

Die zu erstellenden nationalen Risikoanalysen und Bewertungen sollen an das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) übermittelt, dort ausgewertet und entsprechende Elemente den Betreibern kritischer Anlagen Verfügung gestellt werden.

Stellungnahme

Sowohl mit Blick auf den zeitlichen Vorlauf als auch die notwendige Transparenz ist es geboten, die Risikoanalysen und Bewertungen der Bundesministerien den im entsprechenden Sektor registrierten Betreibern kritischer Anlagen direkt zur Verfügung zu stellen. Damit werden zeitliche Verzögerungen minimiert. Zudem werden Informationsverluste vermieden, die bei einer durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) gefilterten Weiterleitung entstehen.

Änderungsvorschlag

Der Absatz ist dahingehend zu ergänzen, dass die Risikoanalysen und -bewertungen der Bundesministerien durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) ohne zeitliche Verzögerung und inhaltlich unverändert an die Betreiber kritischer Anlagen weitergegeben werden.

§ 9

Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen

Zu Abs. 1

Erstellung von Risikoanalysen und -bewertungen durch Betreiber kritischer Anlagen

Beabsichtigte Neuregelung

Analog zu und aufbauend auf den nationalen Risikoanalysen und Risikobewertungen nach § 8 sowie anderen Informationsquellen sollen Betreiber kritischer Anlagen erstmals neun Monate nach der Registrierung des Betreibers kritischer Anlagen und darauf folgend spätestens alle vier Jahre Risikoanalysen und Bewertungen durchführen, welche die Wirtschaftsstabilität beeinträchtigende, naturbedingte, klimatische oder vom Menschen verursachten Risiken, insbesondere Unfälle, Naturkatastrophen, gesundheitliche Notlagen sowie hybride oder andere feindliche Bedrohungen einschließlich terroristischer Straftaten, berücksichtigen.

Darüber hinaus sind auch Risiken zu berücksichtigen, die sich aus dem Ausmaß der Abhängigkeit anderer Sektoren von der eigenen kritischen Dienstleistung sowie dem Ausmaß der Abhängigkeit der eigenen kritischen Anlage von kritischen Dienstleistungen Dritter ergeben können. Als zeitlicher Bezugspunkt für die Erstellung der Risikoanalyse und Bewertung wird die Registrierung der kritischen Anlage festgelegt.

Stellungnahme

In Ergänzung zu den unter § 8 dargestellten zeitlichen Abhängigkeiten weisen die Krankenhäuser auf die inhaltliche Abhängigkeit der hier geforderten betreiberspezifischen Risikoanalyse von der nationalen Risikoanalyse einerseits und der inhaltlichen Abhängigkeit der umzusetzenden Maßnahmen von der hier vorgenommenen Risikoanalyse andererseits hin. Bei nicht rechtzeitigem Vorliegen der nationalen Risikobewertung nach § 8 können die Verpflichtungen nach § 9 schlechterdings nicht eingehalten werden.

Die Betrachtung von Interdependenzen zu anderen kritischen Infrastrukturen ist sachgerecht, jedoch birgt die Komplexität dieser Abhängigkeiten mit Blick auf die Vollständigkeit der Risikoanalyse hohe Risiken. Gleiches gilt für die sich aus der Analyse und Bewertung ergebenden Maßnahmen und Verantwortlichkeiten. Derzeit kann noch nicht abgeschätzt werden, welche Folgen sich aus einer Risikobetrachtung eines Krankenhauses hinsichtlich der notwendigen Strom-, Wärme- und Wasserversorgung für den Betreiber der kritischen Infrastruktur ergeben. Die Verantwortlichkeit des Betreibers einer kritischen Infrastruktur erstreckt sich naturgemäß auf die eigene kritische Anlage. Mögliche Risiken, die sich aus etwaigen Abhängigkeiten ergeben, können zwar aufgezeigt werden. Eine direkte Mitigation dieser Risiken wird in diesen Fällen für den Betreiber jedoch meistens ausscheiden. Schon die Anbindung mehrerer Versorger ist mit Blick auf die Leistungskapazitäten z. B. bei der Gas- und Wasserversorgung häufig unrealistisch. Ein Krankenhaus kann einem Wasserversorger auch keine technischen oder organisatorischen Maßnahmen zur Absicherung der dort genutzten Infrastruktur vorschreiben. Die in den jeweiligen Branchen und Sektoren etablierten Sicherheits- und Resilienz-Standards sollten jedoch langfristig auf eine Verzahnung der Maßnahmen ausgerichtet werden.

Es muss zudem eine Regelung getroffen werden, ob sich Betreiber kritischer Anlagen, die schon heute als kritische Infrastruktur im Sinne der BSI-Kritis-Verordnung gelten, erneut registrieren müssen. Falls nicht, ist der Bezugszeitpunkt für die Frist nach Absatz 1 festzulegen, der jedoch frühestens neun Monate nach dem Inkrafttreten des vorliegenden Gesetzes liegen kann.

Änderungsvorschlag

Die zeitlichen und inhaltlichen Abhängigkeiten der Risikoanalysen nach den §§ 8 und 9 sind zu berücksichtigen und aufeinander abzustimmen. Die zeitlichen Vorgaben zur Erstellung der Risikoanalyse sind klarzustellen. Schon eine Mindestumsetzungszeit von 24 Monaten wird für viele Betreiber kritischer Infrastrukturen eine besondere Herausforderung darstellen, kürzere Umsetzungsfristen werden sich mit den angestrebten Zielen nicht vereinbaren lassen.

Im Weiteren sind Lösungsansätze für die komplexen Folgebetrachtungen der Interdependenzen zwischen kritischen Infrastrukturen zu erarbeiten. Dabei sind die Zuständigkeiten und Kompetenzbereiche der jeweiligen kritischen Infrastruktur zu beachten.

Zu Abs. 2

Festlegung von Vorlagen und Mustern für Risikoanalysen und -bewertungen durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)

Beabsichtigte Neuregelung

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) kann inhaltliche und methodische Vorgaben einschließlich Vorlagen und Muster für die Risikoanalysen und Risikobewertungen nach Absatz 1 festlegen. Die Festlegung nach Satz 1 erfolgt durch eine öffentliche Mitteilung auf der Internetseite des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK).

Stellungnahme

Die Krankenhäuser begrüßen, dass im Sinne einheitlicher Vorgaben und zur Unterstützung der verschiedenen Branchen und Sektoren inhaltliche und methodische Vorgaben entwickelt werden können. Dabei besteht jedoch die Gefahr, dass diese Vorgaben dazu genutzt werden, zusätzliche Anforderungen an der Gesetzes- und Verordnungsgebung „vorbei“ festzulegen. Diese aktuell durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) genutzte Praxis, bei der mithilfe von „Orientierungshilfen“ unter Umgehung parlamentarischer Prozesse normative Vorgaben erlassen und teils jahrelang durchgeführte Prozesse ohne Angaben von Gründen und auf intransparente Weise verändert werden, sollte für das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) ausgeschlossen werden.

Die zuvor in Absatz 2 enthaltene Möglichkeit der Nachnutzung gleichwertiger Risikoanalysen und -bewertungen aufgrund anderer rechtlicher Vorschriften wurde dagegen ersatzlos gestrichen. Die Streichung ist unverständlich, da die vorgesehene Regelung die Nutzung möglicher Synergieeffekte zugelassen hätte – eine mit Blick auf die Herausforderungen in der Umsetzung wertvolle Unterstützung würde damit entfallen. Bereits heute werden z. B. im branchenspezifischen Sicherheitsstandard für die medizinische Versorgung gemäß § 8a Abs. 3 BSiG-Maßnahmen für den physischen Schutz der kritischen Infrastruktur vorgesehen. Um nicht verfügbare personelle und finanzielle Ressourcen einerseits zu schonen und andererseits keine bürokratisch aufwändigen Doppelverfahren zu etablieren, strebt die Deutsche Krankenhausgesellschaft eine Abstimmung mit dem Bundesamt für Bevölkerungsschutz und

Katastrophenhilfe (BBK) zu den aktuell bereits vorgesehenen Maßnahmen zur physischen Resilienz an. Dabei ist zu klären, ob diese Maßnahmen ganz oder in Teilen als ausreichend im Sinne der Vorschrift nach § 9 gelten können. Eine zusätzliche Umsetzung an anderer Stelle kann dann entfallen.

Änderungsvorschlag

Zur Schonung der personellen und finanziellen Ressourcen und zur Vermeidung bürokratisch aufwändiger Doppelverfahren sollte die ursprüngliche Regelung des Absatz 2 wieder eingeführt werden.

§ 10

Resilienz-Maßnahmen der Betreiber kritischer Anlagen; Resilienzplan

Zu Abs. 1

Umsetzung geeigneter und verhältnismäßiger technischer, sicherheitsbezogener und organisatorischer Maßnahmen zur Gewährleistung der Resilienz durch Betreiber kritischer Anlagen

Beabsichtigte Neuregelung

Betreiber kritischer Anlagen sind verpflichtet, spätestens zehn Monate nach Registrierung als kritische Anlage geeignete und verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen zur Gewährung ihrer Resilienz zu treffen. Diese Maßnahmen basieren auf den nach den §§ 8 und 9 bereitgestellten Informationen. Dabei soll der Stand der Technik berücksichtigt werden.

Weiterhin wird festgelegt, wann technische, sicherheitsbezogene und organisatorische Maßnahmen verhältnismäßig im Sinne des Gesetzes sind. Dabei wird der Aufwand zur Verhinderung oder Begrenzung eines Ausfalls oder einer Beeinträchtigung der kritischen Dienstleistung zu den Folgen ihres Ausfalls oder ihre Beeinträchtigung ins Verhältnis gesetzt.

Stellungnahme

Bisher sind die konkreten Schutzziele des Gesetzes nicht klar definiert. Eine Bewertung, ob eine Maßnahme für die Zielerreichung „geeignet“ erscheint, ist damit nicht möglich.

Dennoch werden Maßnahmen aufgezählt, die hierfür als „erforderlich“ angesehen werden. Unter Absatz 1 Ziffer 5 wird z. B. ein „angemessenes Sicherheitsmanagement“ hinsichtlich der Mitarbeitenden gefordert. Dabei soll auch das Personal externer Dienstleister einbezogen werden. Hierfür bestehen jedoch sehr enge Grenzen, die über die Vorlage eines polizeilichen Führungszeugnisses nicht hinausgehen können. Schon mit Blick auf datenschutzrechtliche Vorgaben sind personelle Überprüfungen selbst in sensiblen Bereichen in aller Regel nur unter hohen Auflagen möglich, meist jedoch generell unzulässig.

Nachträgliche anlasslose Kontrollen über den gesamten Personalbestand hinweg verbieten sich grundsätzlich. Wenn sich die Verpflichtung dann auch noch auf externe Dienstleister, wie Catering-Anbieter oder Wäschereien beziehen soll, bestehen hierfür - über die bestehenden rechtlichen Bedenken hinaus - schlicht keinerlei Kapazitäten für eine entsprechende Prüfung.

Während der Aufwand zur Umsetzung von konkret geforderten Maßnahmen in der Regel durch entsprechende Markterkundungen, Angebote oder Aufwandsschätzungen ermittelt werden kann, lässt sich der Ausfall oder eine Beeinträchtigung einer kritischen Dienstleistung, wie beispielsweise der stationären medizinischen Versorgung, in aller Regel nicht quantifizieren. Insbesondere die Beeinträchtigung für Leib und Leben sind schon aus ethisch-moralischen Gründen wirtschaftlich nicht zu bewerten. In der Praxis hat sich daher schon die Abschätzung der Verhältnismäßigkeit umzusetzender Maßnahmen im Bereich der Informationssicherheit als herausfordernd dargestellt. Betreiber kritischer Infrastrukturen sind bei der Frage der Verhältnismäßigkeit mit ethisch-moralischen Problemen konfrontiert. Gerade mit Blick auf das Vertrauensverhältnis der Bevölkerung in die medizinische Versorgung in Deutschland einerseits und die wirtschaftlichen Rahmenbedingungen der medizinischen

Versorgung andererseits darf die Entscheidung über die Verhältnismäßigkeit von Maßnahmen durch den Betreiber nicht regelmäßig angezweifelt werden.

Änderungsvorschlag

Es müssen konkrete Schutzziele zur Erhöhung der Resilienz der kritischen Anlagen definiert werden. Wo notwendig, sind diese branchenspezifisch festzulegen. Dies ist insbesondere für den Bereich öffentlich zugänglicher kritischer Anlagen geboten.

Weiterhin muss eine Klarstellung erfolgen, dass sich ein angemessenes Sicherheitsmanagement nur auf besonders sensible Bereiche der kritischen Anlage beziehen darf. Gegebenenfalls bedarf es der Schaffung entsprechender rechtlicher Grundlagen.

Es sollte eine Klarstellung erfolgen, wie mit den in Absatz 1 genannten Maßnahmen im Hinblick auf die Abwägung der Verhältnismäßigkeit umgegangen werden sollte.

Zu Abs. 3

Aufzählung von Maßnahmen zur Gewährleistung der Resilienz durch Betreiber kritischer Anlagen

Beabsichtigte Neuregelung

Es werden Maßnahmen aufgezählt, die der Zielerreichung der Zwecke nach Absatz 1 dienen können.

Stellungnahme

Die in Absatz 3 aufgenommenen Maßnahmen sind als mögliche Maßnahmen aufgezählt, im Gegensatz zum ersten Referentenentwurf werden sie nicht mehr als „Mindestvorgaben“ interpretiert. Dies begrüßen die Krankenhäuser ausdrücklich, da sie sich für Krankenhäuser in Teilen einer Abwägung der Verhältnismäßigkeit entziehen oder in Organisationsbereichen, die für die Öffentlichkeit zugänglich oder auf schnelle medizinische Versorgung ausgerichtet sind, nicht umsetzbar sind. Eine Sicherheitsüberprüfung durch Körperscanner, die an Flughäfen als Sicherheitsmaßnahme standardmäßig zum Einsatz kommen, wäre beim Zugang zu medizinischer Versorgung selbst bei elektiven Krankenhausbehandlungen außerhalb der Notfallversorgung nicht vermittelbar.

Änderungsvorschlag

Entfällt.

Zu Abs. 4

Katalog sektorenübergreifender Mindestanforderungen zur Konkretisierung von Absatz 1

Beabsichtigte Neuregelung

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) erstellt zur Konkretisierung von Absatz 1 im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) einen Katalog von sektorenübergreifenden Mindestanforderungen und veröffentlicht diesen auf der Internetseite des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe. Die zuständigen Aufsichtsbehörden des Bundes nach § 3 Absatz 3 und die zuständigen Behörden der Länder nach § 3

Absatz 5 sind bei der Erarbeitung des Katalogs von sektorenübergreifenden Mindestanforderungen durch Anhörung zu beteiligen. Die betroffenen Betreiber kritischer Anlagen und die betroffenen Wirtschaftsverbände sind anzuhören.

Stellungnahme

Bei der Festlegung von Mindestanforderungen ist darauf zu achten, dass diese nicht den Zwecken der betroffenen kritischen Infrastruktur entgegenstehen. Beispielsweise dürfen Betriebsabläufe, die der Patientensicherheit dienen, insbesondere die schnelle Zugänglichkeit zu Operationsräumen bei Sektio-OPs, die Bildgebung bei Schlaganfallbehandlungen oder die Zuwegung von Hubschrauberlandeplätzen zu Schockräumen, bereits aufgrund anderslautender normativer Vorgaben nicht durch die nach Absatz 3 festgelegten Mindestanforderungen unterlaufen werden.

Zur adäquaten Abbildung branchenspezifischer Anforderungen bedarf es bei der Erarbeitung des Katalogs mindestens der Einvernehmensherstellung mit den zuständigen Aufsichtsbehörden.

Änderungsvorschlag

Absatz 4 Satz 2 wird wie folgt gefasst:

Die Der Katalog von sektorenübergreifenden Mindestanforderungen ist im Einvernehmen mit den zuständigen Aufsichtsbehörden des Bundes nach § 3 Absatz 3 und die den zuständigen Behörden der Länder nach § 3 Absatz 5 sind bei der Erarbeitung des Katalogs von sektorenübergreifenden Mindestanforderungen durch Anhörung zu beteiligen festzulegen.

Zu Abs. 6

Vorschlag branchenspezifischer Resilienzstandards zur Gewährleistung der Anforderung nach Absatz 1

Beabsichtigte Neuregelung

Betreibern kritischer Anlagen sowie ihren Branchenverbänden wird der Vorschlag branchenspezifischer Resilienz-Standards zur Gewährleistung der Anforderungen nach Abs. 1 ermöglicht. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Abs. 1 zu gewährleisten.

Stellungnahme

Die Möglichkeit, branchenspezifische Resilienz-Standards zur Umsetzung gesetzlich geforderter Maßnahmen zu erarbeiten, stellt in Anbetracht der fehlenden Verfügbarkeit international anerkannter Standards, welche ausreichend auf die gesetzgeberischen Besonderheiten in Deutschland eingehen, einen herausfordernden aber grundsätzlich gangbaren Weg dar. Damit könnten die Betreiber jeweils im Einzelfall vom Nachweis der Eignung der vorgesehenen Maßnahmen entlastet werden, indem diese Prüfung stellvertretend durch den Herausgeber mit der zuständigen Stelle auf Bundesebene durchgeführt wird. Die Deutsche Krankenhausgesellschaft wird analog zum bestehenden Branchensicherheitsstandard („B3S“) einen branchenspezifischen Resilienz-Standard erarbeiten, der auch im B3S bereits enthaltene Maßnahmen für den Bereich der physischen Sicherheit aufgreifen wird.

Änderungsvorschlag

Entfällt.

Zu Abs. 9 - 10

Erstellung eines Resilienzplans, Bereitstellung von Vorlagen und Mustern für einen Resilienzplan

Beabsichtigte Neuregelung

Betreiber kritischer Anlagen müssen die Maßnahmen nach Absatz 1 in einem Resilienzplan darstellen.

Stellungnahme

Die Bereitstellung von Vorlagen und Mustern für den Resilienzplan nach Absatz 10 wird ausdrücklich begrüßt. Dies kann mit Blick auf die Regelungen zu entsprechenden Bußgeldvorschriften in § 19 Abs. 1 Ziffer 5 helfen, Unsicherheiten in der Praxis zu vermeiden.

Änderungsvorschlag

Es ist eine Regelung aufzunehmen, wonach auf Basis der Vorlagen nach Absatz 10 und in Abstimmung mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) branchenspezifische Resilienzpläne durch die Branchen selbst erstellt werden können.

§ 11

Nachweise, behördliche Anordnungen

Zu Abs. 1

Nachweis der Erfüllung der Anforderungen nach Absatz 1

Beabsichtigte Neuregelung

Betreiber kritischer Anlagen müssen spätestens zehn Monate nach Registrierung dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) auf Verlangen und auf geeignete Weise die Erfüllung der Anforderungen nach Abs. 1 nachweisen. Der Nachweis kann durch Audits erfolgen. Dabei aufgedeckte Mängel sind dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) zu übermitteln. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) kann die Beseitigung der Mängel verlangen. Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) kann zur Ausgestaltung des Verfahrens der Audit- und Nachweiserbringung Anforderungen an die Art und Weise der Durchführung, an die Geeignetheit der zu erbringenden Nachweise sowie fachliche und organisatorische Anforderungen an die Prüfer und die prüfende Stelle festlegen.

Stellungnahme

Das Vorgehen folgt im Wesentlichen den Vorgaben des § 8a BSIG und ist im Grundsatz nachvollziehbar. Im Gegensatz zum ersten Referentenentwurf sind jedoch zwei wesentliche Änderungen aufgenommen worden, die begrüßt werden. Zum einen erfolgt die Überprüfung nicht mehr regelmäßig alle zwei Jahre, sondern nur auf Verlangen des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK). Zum anderen soll dabei auf die Nachweise des § 39 Absatz 1 BSIG (bisher § 8a BSIG) zurückgegriffen werden. Ausweislich der Begründung zu § 11 sollen diejenigen „Bestandteile des Nachweises der Einhaltung der Maßnahmen nach § 39 Absatz 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit der Informationstechnik von Einrichtungen“ verlangt werden, „die für die Überprüfung der Einhaltung der Maßnahmen nach § 10 Absatz 1 erforderlich sind. Dies dient der Reduzierung der Bürokratie und stellt eine Verbindung dazu her, dass bereits nach § 39 Absatz 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit der Informationstechnik von Einrichtungen Maßnahmen umfasst sind, die auch der physischen Resilienz von Betreibern kritische Anlagen dienen und nach dem KRITIS-DachG verlangt werden.“

Änderungsvorschlag

Entfällt.

Zu Abs. 5

Überprüfung der Einhaltung der Anforderungen durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)

Beabsichtigte Neuregelung

Bestehen erhebliche Zweifel an der Einhaltung der Anforderungen nach Abs. 1, kann das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) diese Einhaltung überprüfen. Dabei kann es sich eines

qualifizierten unabhängigen Dritten bedienen. Für die Überprüfung kann das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) Gebühren und Auslagen bei den Betreibern der kritischen Anlage erheben, wenn das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) aufgrund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Einhaltung der Anforderungen nach Abs. 1 begründen.

Stellungnahme

Die Durchführung von Audits hat sich aus den bisherigen Erfahrungen mit vergleichbaren Regelungen des § 39 Abs. 1 BSIG (bisher § 8a BSIG) als umfangreich und ressourcenintensiv dargestellt. Wurde ein Audit nach Abs. 4 nachgewiesen, muss sich der Betreiber auch auf das Ergebnis des Audits verlassen können. Hat der Betreiber den Nachweis auf andere Weise erbracht, stellt sich die Frage nach der Qualifizierung eines unabhängigen Dritten, auf dessen Urteil sich das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) in diesem Fall verlassen und gegebenenfalls die Behebung festgestellter Mängel oder das Verhängen von Bußgeldern durchsetzen wird. Dies ist bei der Festlegung der fachlichen und organisatorischen Anforderungen an die Prüfer und die prüfende Stelle nach Absatz 4 Satz 1 zu berücksichtigen.

Änderungsvorschlag

Entfällt.

Zu Abs. 6

Anweisung zur Mängelbeseitigung durch die zuständige Behörde

Beabsichtigte Neuregelung

Die zuständige Behörde kann die Behebung aufgetretener Mängel innerhalb einer angemessenen Frist anordnen, wenn diese angeordneten Maßnahmen nicht im Widerspruch zu Anforderungen des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit der Informationstechnik von Einrichtungen stehen.

Stellungnahme

Die Anweisung zur Umsetzung erforderlicher und verhältnismäßiger Maßnahmen durch eine Aufsichtsbehörde ist nachvollziehbar. Im Gegensatz zum ersten Referentenentwurf wird diese Aufgabe sachgerechter Weise nun der zuständigen Behörde zugewiesen. Dem Betreiber muss ausreichend Gelegenheit gegeben werden, die Sachlage zu begründen.

Änderungsvorschlag

Entfällt.

§ 12

Meldewesen für Vorfälle

Zu Abs. 1 - 2

Verpflichtung zur Meldung von Vorfällen, welche die Erbringung der kritischen Dienstleistung erheblich stören oder stören könnten

Beabsichtigte Neuregelung

Betreiber kritischer Anlagen werden verpflichtet, Vorfälle, die die Erbringung ihrer kritischen Dienstleistung erheblich stören oder stören könnten, an eine gemeinsame Meldestelle von Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Dabei sind insbesondere Angaben zur Anzahl und Anteil der von der Störung Betroffenen, bisherige und voraussichtliche Dauer der Störung sowie des betroffenen geographischen Gebietes der Störung unter Berücksichtigung des Umstandes, ob das Gebiet geographisch isoliert ist, zu berücksichtigen.

Absatz 2 legt fest, dass die Meldungen sämtliche verfügbaren Informationen enthalten müssen, um den Vorfall, dessen Ursache und mögliche Folgen nachzuvollziehen.

Stellungnahme

Das Interesse der zuständigen Bundesbehörde und die Regelung entsprechender Informationspflichten sind nachvollziehbar. Dabei ist zu berücksichtigen, dass sich Betreiber während einer solchen Störung häufig in einer Ausnahmesituation befinden, die in aller Regel bereits erhebliche zusätzliche Ressourcen bindet und für die betroffenen Mitarbeitenden zu erheblichen Stresssituationen führt.

Gerade bei erheblichen Störungen der kritischen Dienstleistung steht die Wiederherstellung derselben für die Betreiber in der Regel an erster Stelle. Gleichzeitig greifen häufig unterschiedliche Meldeverpflichtungen gegenüber zuständigen Aufsichtsbehörden, deren Nichteinhaltung auch mit empfindlichen Bußgeldern belegt werden kann. Die Praxis zeigt, dass sich – unter Berücksichtigung der jeweiligen Informationserfordernisse der zuständigen öffentlichen Stellen – der bürokratische Meldeaufwand in der akuten Phase der Störung auf ein Minimum reduzieren sollte.

Es sollten daher nur die unbedingt notwendigen Informationen abgefragt werden, um nicht für die Beseitigung der Störung notwendige personelle Ressourcen anderweitig zu binden.

Dem Ansatz „ein Vorfall - eine Meldung“ folgend, wird die Meldung an eine gemeinsame Meldestelle von Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) begrüßt und mit der Erwartung verbunden, dass keine Doppelmeldungen zu ein und derselben Ursache notwendig sind.

Änderungsvorschlag

Um die Fehleranfälligkeit, insbesondere in Stresssituationen für die zuständigen Beschäftigten weitgehend zu minimieren, sollten standardisierte digital und analog verfügbare Meldeformulare bereitgestellt werden, welche die zum jeweiligen Zeitpunkt notwendigen Informationen eindeutig benennen und dabei nur unbedingt notwendige Inhalte der Meldung definieren.

Zu Abs. 3

Erstmeldung innerhalb von 24 Stunden, ausführlicher Bericht spätestens nach einem Monat

Beabsichtigte Neuregelung

Eine Erstmeldung soll dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) bereits innerhalb von 24 Stunden nach Kenntnisnahme des Vorfalls übermittelt werden. Ein ausführlicher Bericht ist spätestens nach einem Monat zu übermitteln.

Stellungnahme

Eine Mitteilung innerhalb von 24 Stunden nach Kenntnisnahme wird in vielen Fällen allenfalls eine rudimentäre Beantwortung der in der Erstmeldung abgefragten Informationen zulassen. Hierbei ist zwischen einer schnellen Meldung und einem möglichst gesicherten Meldeinhalt abzuwägen.

Während das Bundesamt für Sicherheit in der Informationstechnik (BSI) bei der Weiterleitung von Informationen zu Sicherheitsvorfällen dem Grundsatz „Gründlichkeit vor Schnelligkeit“ folgt und dies mit dem Anspruch begründet, als zuständige Behörde nur gesicherte Informationen nach außen geben zu wollen, dürfen im Nachgang als unvollständig oder fehlerhaft erkannte Erstmeldungen den meldenden Einrichtungen nicht nachteilig angelastet werden, wenn von ihnen eine Meldung in möglichst kurzer Frist verlangt wird. § 8b BSIG verlangt die unverzügliche Meldung einer Störung, und damit ohne schuldhaftes Verzögern durch den Betreiber.

Änderungsvorschlag

Es sollte geprüft werden, ob gerade auch im Hinblick auf die gemeinsame Meldestelle die Angleichung der (Frist-)Vorgaben zur Meldung einer Störung oder Beeinträchtigung an die im BSIG enthaltene Formulierung anzugleichen ist.

§ 13

Unterstützung der Betreiber kritischer Anlagen

Beabsichtigte Neuregelung

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) stellt Vorlagen, Muster und Leitlinien zur Umsetzung der Verpflichtungen nach diesem Gesetz zur Verfügung und kann auch Beratungen, Schulungen und Übungen anbieten. Das Bundesministerium des Innern und für Heimat (BMI) kann bei der Europäischen Kommission einen Antrag auf Organisation einer Beratungsmission zur Bewertung der Maßnahmen stellen, die ein Betreiber kritischer Anlagen ergriffen hat, um seine Verpflichtungen der §§ 9 bis 12 zu erfüllen.

Stellungnahme

Die nun definierten Unterstützungsleistungen des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK) wurden seitens der Krankenhäuser in der Kommentierung des ersten Referentenentwurfs vorgeschlagen und deshalb ausdrücklich begrüßt.

Änderungsvorschlag

Entfällt.

§ 14

Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleiter für Betreiber kritischer Anlagen

Beabsichtigte Neuregelung

Geschäftsleiterinnen und -leiter von Betreibern kritischer Anlagen sind zur Billigung der nach § 10 ergriffenen Maßnahmen verpflichtet. Der Verzicht auf Ersatzansprüche gegenüber Geschäftsleiterinnen und -leitern aufgrund von Pflichtverletzungen ist unwirksam. Geschäftsleiterinnen und -leiter müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken und deren Auswirkungen auf die von dem Betreiber der kritischen Anlage eingebrachten Dienstleistungen zu erwerben, und auf Nachfrage entsprechende Nachweise an die zuständige Behörde übermitteln.

Stellungnahme

Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken gehören grundsätzlich zum Repertoire von Führungskräften. Es erscheint jedoch fraglich, ob die hier notwendigen, teils sehr fachspezifischen Kenntnisse auf Ebene der Geschäftsleiterinnen und -leiter notwendig und sachgerecht sind. Auch in anderen Bereichen, wie z. B. dem Risikomanagement in medizinischen IT-Netzwerken oder beim Risikomanagement im Zusammenhang mit Medizinprodukten, erfolgt heute eine Delegation an speziell geschultes Personal. Die vorgesehene Regelung ist daher zu eng gefasst und nicht sachgerecht.

Die Fokussierung auf die „Geschäftsleitung“ stellt zudem 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.

Änderungsvorschlag

Es sollte die Möglichkeit der Delegation der Aufgaben zur Erkennung und Bewertung von fachspezifischen Risiken und Risikomanagementpraktiken aufgenommen werden.

§ 16

Ermächtigung zum Erlass von Rechtsverordnungen

Beabsichtigte Neuregelung

Das Bundesministerium des Innern und für Heimat (BMI) soll durch Rechtsverordnung ohne Zustimmung des Bundesrates ermächtigt werden, kritische Anlagen im Sinne des Gesetzes, Einrichtungsarten besonders wichtiger Einrichtungen und Einrichtungsarten wichtiger Einrichtungen festzulegen. Grundlage hierfür bildet der Versorgungsgrad, der anhand branchenspezifischer Schwellenwerte sektorspezifisch zu bestimmen ist. Die Rechtsverordnung kann auch Stichtage festlegen sowie Teile der Bundesverwaltung als kritische Infrastruktur bestimmen.

Zudem wird eine Verordnungsermächtigung u. a. für das Bundesministerium für Gesundheit (BMG) geschaffen, im Einvernehmen mit dem Bundesministerium des Innern und für Heimat (BMI) die Mindestvorgaben für Maßnahmen nach § 10 im Wege einer Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, festzulegen.

Stellungnahme

Der Gesetzesentwurf greift hier das im BSI-Gesetz etablierte Vorgehensmodell der BSI-Kritis-Verordnung auf. Die Regelung ist dahingehend sachgerecht. Allerdings sollte bei der vorgesehenen branchenspezifischen Festlegung von Schwellenwerten auf die im BSI Gesetz bzw. der BSI-Kritis-Verordnung enthaltenen Vorgaben zurückgegriffen werden. Eine auseinanderlaufende Definition kritischer Infrastrukturen mit Blick auf den Cyberschutz einerseits und den physischen Schutz kritischer Infrastrukturen andererseits muss unbedingt vermieden werden. Zur Klärung dieser Frage bietet es sich an, die im Rahmen der BSI-Kritis-Verordnung durchgeführten Abstimmungen im Rahmen der sogenannten „Kernteam-Beratungen“ zu wiederholen.

Die gegenüber dem ersten Referentenentwurf aufgenommene Möglichkeit der Verordnungsermächtigung für das Bundesministerium für Gesundheit (BMG) im Sektor Gesundheit erscheint sachgerecht.

Änderungsvorschlag

Entfällt.

§ 19

Bußgeldvorschriften

Zu Abs. 1

Festlegung von Ordnungswidrigkeitstatbeständen

Beabsichtigte Neuregelung

In den Ziffern 1 - 11 werden Tatbestände genannt, die bei vorsätzlichem Handeln eine Ordnungswidrigkeit darstellen. Hierzu zählen insbesondere eine nicht oder nicht rechtzeitig erfolgte Registrierung, das Fehlen einer Kontaktstelle, die nicht erfolgte oder nicht rechtzeitige Durchführung von Risikoanalysen und -bewertungen nach § 9 Abs. 1, die Nichtvorlage eines Resilienzplans und weiterer Dokumente sowie fehlende Unterstützung bei behördlichen Anordnungen nach § 11.

Stellungnahme

Die Definition von Bußgeldvorschriften im Rahmen des Gesetzes folgt üblichen gesetzgeberischen Mustern. Dabei werden jedoch keine Konsequenzen für fehlende, aber notwendige Beistellungen durch öffentliche Stellen, insbesondere die zuständige Aufsichtsbehörde, berücksichtigt. Die Krankenhäuser sprechen sich dafür aus, bis auf Weiteres auf die Konkretisierung von Bußgeldvorschriften zu verzichten, bis Erfahrungen mit der Umsetzung der erforderlichen und verhältnismäßigen Maßnahmen gesammelt werden konnten und branchenspezifische Besonderheiten ausreichend berücksichtigt werden. Vor der Verhängung von Bußgeldern sollte stets die Unterstützung der betroffenen Einrichtungen stehen, beispielsweise indem fachliche Beratungs- und Schulungsangebote zur Verfügung gestellt werden.

Auch die Höhe der Bußgelder ist im aktuellen Bearbeitungsstand des Referentenentwurfs noch unbestimmt. Der Grundsatz der Verhältnismäßigkeit wird an dieser Stelle jedoch besonders betont und ausdrücklich begrüßt.

Änderungsvorschlag

Auf die näheren Festlegungen, insbesondere die Höhe der Bußgelder, ist zunächst zu verzichten. Alternativ müssen die Festlegungen den zu erwartenden Zuwachs an Erfahrung mit den neuen Anforderungen berücksichtigen.

Artikel 2

Änderung des Dachgesetzes zur Stärkung der physischen Resilienz von Betreibern kritischer Anlagen (KRITIS-Dachgesetz – KRITIS-DachG)

Beabsichtigte Neuregelung

Die Landesregierungen werden ermächtigt, im Benehmen mit dem Bundesministerium des Innern und für Heimat (BMI) durch Rechtsverordnung sektorspezifische Mindestvorgaben für Resilienzmaßnahmen nach § 10 Absatz 1 festzulegen, solange und soweit kein entsprechender branchenspezifischer Resilienzstandard gemäß § 10 Absatz 6 Satz 2 durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe als geeignet anerkannt wurde.

Stellungnahme

Die Festlegung von Mindestvorgaben auf Ebene der Länder kann geeignet sein, bei Fehlen entsprechender branchenspezifischer Resilienzstandards, entsprechende Vorgaben zu erlassen. Die Deutsche Krankenhausgesellschaft wird sich nach aktueller Planung und im Sinne einheitlicher Lösungen für eine schnelle Bereitstellung eines entsprechenden Resilienzstandards für Krankenhäuser einsetzen.

Änderungsvorschlag

Entfällt.

Artikel 3

Inkrafttreten

Beabsichtigte Neuregelung

Es wird das Inkrafttreten der gesetzlichen Regelungen festgelegt. Artikel 1 tritt am 18.10.2024 in Kraft. Die §§ 6, 7, 9 bis 12, 13 Abs. 2, §§ 4, 17 und 19 des Artikel 1 treten am 17.07.2026 in Kraft. § 19 Absatz 1 Nr. 5 bis 12 des Artikel 1 treten am Werktag auf den folgenden Tag in Kraft, nachdem das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) die jeweiligen branchenspezifische Resilienz-Standards nach § 10 Absatz 6 als geeignet zur Erfüllung der Verpflichtungen nach § 10 Absatz 1 festgestellt hat, frühestens jedoch am 17. 07.2026 Artikel 2 tritt am 01.01.2029 in Kraft.

Stellungnahme

Krankenhäuser, die sich mit der durch Bundesgesundheitsminister Lauterbach angekündigten Krankenhausreform aktuell in der größten Umbruchphase seit Einführung des DRG-Systems Anfang der 2000er Jahre befinden, stellen die zusätzlichen technischen und organisatorischen Anforderungen an die physische Resilienz vor enorm große Herausforderungen. Während der durch das Krankenhaus-Zukunftsgesetz ausgelastete Markt der Hersteller und Beratungsunternehmen auf absehbare Zeit keine Unterstützung leisten können wird, stehen viele Krankenhäuser in Deutschland aufgrund der allgemeinen Inflation, extrem gestiegener Energiekosten, hoher Tarifaabschlüsse und der fehlenden Planbarkeit des Leistungsgeschehens in den kommenden Jahren vor noch nie dagewesenen strukturellen und wirtschaftlichen Herausforderungen.

Dabei wirkt die durch die heute noch völlig offene Ausgestaltung der Krankenhausreform in mehrfacher Hinsicht schädlich, da schon die Infragestellung der Daseinsberechtigung für eine große Zahl an Krankenhaus-Standorten die Möglichkeit erschwert, auf notwendige Investitionsmittel zuzugreifen bzw. diese zu beantragen und bewilligt zu bekommen, welche für die Umsetzung der hier geforderten Maßnahmen notwendig wären.

Während der Cyberschutz für Krankenhäuser inhaltlich inzwischen klar definiert und eine Umsetzungsperspektive durch einen wiederholt als geeignet im Sinne des § 8a BSI-Gesetz festgestellten branchenspezifischen Sicherheitsstandard besitzt, fehlen diese Grundlagen bisher für den Bereich der physischen Resilienz in weiten Teilen noch. Gerade für öffentlich zugängliche Anlagen kritischer Infrastrukturen sind die Schutzziele derzeit auch durch die zuständige Bundesbehörde noch nicht klar definiert.

Zudem werden inhaltliche Abhängigkeiten für die Umsetzung von Maßnahmen definiert, die eine rechtzeitige Umsetzung der Maßnahmen erschweren.

Der vorgesehene Zeitplan ist damit vor allem für Krankenhäuser äußerst ambitioniert.

Änderungsvorschlag

Es sollte geprüft werden, ob im Einklang mit den Vorgaben des EU-Rechtes eine noch weiter gestufte Realisierung der Anforderungen infrage kommen kann, um Staat und Wirtschaft eine realistische Umsetzungsperspektive für die sinnvollen grundsätzlichen Ziele des Gesetzes zu bieten.

Weiterer gesetzlicher Handlungsbedarf

Grundsätzlich sollte geprüft werden, inwieweit bei den entsprechenden Festlegungen normativer Vorgaben auf die Umsetzung durch international anerkannte Normen und Standards zurückgegriffen werden kann. In vielen Bereichen agieren international tätige Unternehmen, die sich aufgrund überbordender gesetzlicher Anforderungen aus dem Binnenmarkt Deutschland bereits zurückgezogen haben.