DEUTSCHE KRANKENHAUS GESELLSCHAFT

Bundesverband der Krankenhausträger in der Bundesrepublik Deutschland

Stellungnahme

der Deutschen Krankenhausgesellschaft

zum

Referentenentwurf

eines

Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen

(KRITIS-Dachgesetz – KRITIS-DachG)

Stand: 24.08.2023

Inhaltsverzeichnis

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.

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 dienen 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. Erstmalig 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 Wirtschafts-stabilität der betreffenden Einrichtungen bedrohen oder beeinträchtigen können. Hierzu zählen nach dem Entwurf 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.

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, zum Beispiel 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 zum Beispiel 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 aus diesem Jahr 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 € 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.

Gerade KRITIS-Krankenhäuser haben bereits heute umfangreiche Nachweis- und Prüfverfahren in regelmäßigen Abständen, wie Wirtschaftsprüfungen, Nachweise gemäß § 8a Absatz 3 BSIG oder Zertifizierungen durch die Kooperation für Transparenz und Qualität im Gesundheitswesen (KTQ), zu erbringen. Die im Referentenentwurf des KRITIS-DachG vorgesehenen Nachweise dürften erhebliche zusätzliche Ressourcen binden. Diese Ressourcen stehen nicht in jedem Krankenhaus ohne Weiteres zur Verfügung.

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 Deutsche Krankenhausgesellschaft unterstützt daher – wie schon bisher – die Bemühungen des Gesetzgebers, die kritischen Infrastrukturen in Deutschland durch entsprechende Maßnahmen adäquat abzusichern, ausdrücklich.

Der vorliegende Gesetzentwurf wird daher im Grundsatz begrüßt. Im Detail ergeben sich jedoch eine Reihe von ungeklärten Fragen, die im Verlauf des Gesetzgebungsverfahrens aufgegriffen werden sollten. Beispielsweise ist mit Blick auf die bisher fehlende Definition von Schutzzielen oder die bisher nicht vorliegende nationale Risikoanalyse, welche die Grundlage der individuellen branchenspezifischen Betrachtungen bilden soll, keine valide Aufwandsschätzung für den Gesetzentwurf möglich. Der physische Schutz öffentlicher Einrichtungen, die 365 Tage im Jahr rund um die Uhr allen Bürgerinnen und Bürgern offenstehen, folgt anderen Kriterien, als sie beispielsweise in einem schon heute abgeschotteten Kraftwerksbetrieb mit Perimeterschutz, wo Zutrittskontrollsysteme o. ä. 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 BBK und den betroffenen Sektoren, um ineffektive, oder dem Versorgungsauftrag entgegenwirkende und bürokratische Vorgaben zu vermeiden. Der Abbau von Bürokratie ist ein zentrales Anliegen der Krankenhäuser. Daher wird begrüßt, dass für die Umsetzung des KRITIS-DachG eine größtmögliche Konsistenz zu den bestehenden Vorgaben aus dem Bereich Cyberschutz hergestellt werden soll.

Gleichzeitig bestehen sowohl inhaltliche als auch organisatorische Abhängigkeiten zum geplanten Gesetzgebungsverfahren zur Umsetzung der NIS2-Richtlinie. Das bisher noch nicht offiziell vorliegende Gesetz zur Umsetzung von EU NIS2 und die Stärkung der Cybersicherheit (NIS2UmsuCG) legt offenbar bereits begriffliche Definitionen fest, die bestenfalls in Ergänzung, im Zweifel aber auch im Widerspruch zu bisherigen Definitionen aus der KRITIS-Gesetzgebung stehen. Als Beispiel seien hier die „besonders wichtigen Einrichtungen“ sowie die „wichtigen Einrichtungen“ genannt, die mit den bisherigen Definitionen für britische Dienstleistungen und Schwellenwerte nicht konsistent sind.

Die Deutsche Krankenhausgesellschaft wird sich daher auch über die aktuelle Stellungnahme hinaus engagieren, den Gesetzgebungsprozess aktiv zu unterstützen und mit Blick auf die Erhöhung des physischen Schutzes der Krankenhäuser die branchenspezifischen Besonderheiten des Gesundheitswesens in Deutschland im Blick zu behalten.

Es ist jedoch schon heute absehbar, dass aufgrund der Vielzahl bisher noch nicht geregelter Vorgaben und Rahmenbedingungen die vorgesehenen Umsetzungsfristen nicht realistisch sein können. Die vorgesehene Frist von zehn Monaten vom Zeitpunkt der Registrierung einer kritischen Anlage bis hin zur Umsetzung der Resilienz-maßnahmen gerechnet, stellen – insbesondere in Verbindung mit den vorgesehenen Bußgeldvorschriften – eine Bedrohung der Versorgungssicherheit auf Grund der Absenkung der Wirtschaftsstabilität der betreffenden Einrichtungen dar. Gleichzeitig besteht Verständnis dafür, dass die Erhöhung der Resilienz der kritischen Infrastrukturen in Deutschland so früh wie möglich erreicht werden muss. Es bedarf daher einer engen und vertrauensvollen Zusammenarbeit zwischen den Betreibern kritischer Infrastrukturen und den zuständigen Behörden, um gemeinsam das definierte Ziel des Gesetzentwurfes zu erreichen. Keinesfalls dürfen die Risiken für die kritischen Infrastrukturen in Deutschland durch das Gesetzesvorhaben noch weiter erhöht werden.

Unverständlich bleibt jedoch, 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 Beihilferegelungen 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.

Zum vorliegenden Referentenentwurf wurde die Ressortabstimmung noch nicht abgeschlossen. Zum Zeitpunkt der Einreichung dieser Kommentierung wird sich der aktuelle Bearbeitungsstand des Gesetzentwurfs daher notwendigerweise bereits vom aktuellen Entwurfsstand unterscheiden. Dabei wird durchaus begrüßt, dass eine Verbändeanhörung vor Abschluss der Ressortabstimmung die Möglichkeit eröffnet, auch grundsätzliche Hinweise zur Überarbeitung vor einer „finalen Entwurfsfassung“ einzubringen, während dies bei einem Gesetzentwurf nach Ressortabstimmung in der Regel mit deutlich größeren Hürden verbunden ist. Es sollte jedoch geprüft werden, ob nach Abschluss der Ressortabstimmung eine weitere Verbändeanhörung – gegebenenfalls auch mit verkürzter Rückmeldefrist – ermöglicht werden kann, um zu den bisher noch unbekannten Regelungsinhalten Stellung nehmen zu können.

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

Besonderer Teil

§ 1

Zweck des Gesetzes

Beabsichtigte Neuregelung

Dem Zweck des Gesetzes nach sollen Kriterien zur Identifizierung kritischer Anlagen und Verpflichtungen für Betreiber kritischer Anlagen zur Gewährleistung der ungehinderten Erbringung ihrer Dienstleistungen definiert werden.

Stellungnahme

Eine solche Definition muss sich an den bisherigen Definitionen für kritische Infrastrukturen in Deutschland orientieren. Ein Auseinanderlaufen der Definition würde kaum beherrschbare Risiken für die nachfolgende Umsetzung bedeuten. Schon jetzt übersteigt die Komplexität der Risiko-Betrachtungen zum Schutz kritischer Infrastrukturen die Möglichkeiten mancher Branchen und Sektoren. Es ist zwingend erforderlich, auf das Wissen, die Erfahrungen und Strukturen aus der bisherigen Absicherung kritischer Infrastrukturen insbesondere im Kontext Cyberschutz zurückzugreifen. Dies beginnt mit der Definition der kritischen Infrastrukturen.

Änderungsvorschlag

Entfällt.

§ 2

Begriffsbestimmungen

Zu Ziffer 11 und 12
Definition „besonders wichtiger“ und „wichtiger“ Einrichtungen

Beabsichtigte Neuregelung

Es ist beabsichtigt, die Begriffsbestimmungen aus der Umsetzung der NIS-2 Richtlinie in den vorliegenden Gesetzentwurf zu überführen. Dabei werden unter Ziffer 11 „besonders wichtige Einrichtungen“ und unter Ziffer 12 „wichtige Einrichtungen“ festgelegt und auf die Definition von Großunternehmen (mehr als 250 Mitarbeitende oder mehr als 50 Millionen € Umsatz pro Jahr) bzw. mittleren Unternehmen (zwischen 50 und 249 Mitarbeitende oder mehr als 10 Millionen € Umsatz im Jahr) zurückgegriffen.

Stellungnahme

In der bisherigen KRITIS-Gesetzgebung spielt der Versorgungsgrad eine maßgebliche Rolle bei der Identifikation kritischer Infrastrukturen. Sollten sich aus den genannten Definitionen relevante Änderungen ergeben, welche von der bisherigen Definition kritischer Infrastrukturen nach BSI-KritisV abweichen bzw. diese maßgeblich ergänzen, darf dies nicht zu nicht-umsetzbaren Anforderungen für Einrichtungen führen, die bisher keinen vergleichbaren Anforderungen unterworfen waren.

Änderungsvorschlag

Entfällt.

§ 3

Nationale zuständige Behörde für die Resilienz kritischer Anlagen

Zu Abs. 1
Unterstützung der Betreiber kritischer Anlagen durch das BBK

Beabsichtigte Neuregelung

Das BBK soll Betreiber kritischer Anlagen bei der Umsetzung ihrer nach dem Gesetz zu erfüllenden Maßnahmen unterstützen.

Stellungnahme

Eine vergleichbare Regelung für das Bundesamt für Sicherheit in der Informationstechnik (BSI) besteht bereits heute, allerdings wird diese Unterstützung inzwischen hauptsächlich in Form der Aufsichtsfunktion durch das BSI wahrgenommen. Steigender bürokratischer Aufwand durch eine immer engere zeitliche Abfolge bei der Abfrage von Informationen sowie Androhungen von Bußgeldern, wenn Mängel nicht innerhalb enger zeitlicher Fristen beseitigt werden, haben den früher als kooperativ empfundenen Austausch zwischen Betreibern und dem BSI nachhaltig gestört.

Für die vorgesehene Regelung sollte daher von Beginn an wieder auf den kooperativen Austausch gesetzt werden. Hierzu zählt insbesondere auch eine vertrauensvolle Zusammenarbeit als Grundlage. Konkrete Unterstützungsmöglichkeiten sollten zumindest an Beispielen dargestellt werden.

Änderungsvorschlag

Es sollte klargestellt werden, in welcher Form die Unterstützung des BBK erfolgen kann. Hierzu kommt eine beispielhafte Aufzählung infrage.

§ 4

Kritische Anlagen

Zu Absatz 1
Festlegung von Schwellenwerten für die Identifikation kritischer Anlagen durch Rechtsverordnung

Beabsichtigte Neuregelung

Die Festlegung, welche Anlagen als kritische Anlage im Sinne des Gesetzes gelten, soll durch eine Rechtsverordnung festgelegt werden. Dabei soll auf branchenspezifische Schwellenwerte abgestellt und Stichtagsregelungen festgelegt werden.

Stellungnahme

Die Regelungen entsprechen dem bisherigen Vorgehen der BSI-KritisV. Es muss jedoch darauf geachtet werden, dass ein ausreichender zeitlicher Vorlauf bei der Umsetzung gesetzlich vorgeschriebener Maßnahmen gegeben wird. Die aktuell in den §§ 11 und 12 enthaltenen Vorlauffristen von 10 Monaten ab dem hier festgelegten Stichtag sind, auch vor dem Hintergrund noch festzulegender Maßnahmen, unrealistisch.

Änderungsvorschlag

Entfällt.

§ 5

Verhältnis zu weiteren spezialgesetzlichen Regelungen

Zu Abs. 1
Verhältnis der Mindestvorgaben nach diesem Gesetz zu anderen Anforderungen

Beabsichtigte Neuregelung

Andere, über die Mindestvorgaben nach diesem Gesetz hinausgehende Anforderungen an die Betreiber kritischer Anlagen sollen hiervon unberührt bleiben.

Stellungnahme

Die Regelung ist grundsätzlich sachgerecht. Im Weiteren ist jedoch darauf zu achten, dass sich Mindestvorgaben nach diesem Gesetz und Anforderungen aus anderen spezialgesetzlichen Regelungen nicht entgegenstehen. Dies gilt insbesondere, da die Schutzziele zur Erhöhung der Resilienz noch nicht festgelegt sind und gerade im öffentlichen Bereich der Zugang zu Infrastrukturen des Gemeinwesens, wie zum Beispiel Krankenhäusern oder dem öffentlichen Personennahverkehr, nicht behindert werden dürfen. Aus diesem Grund sind entsprechende gesetzliche Anforderungen auf ihre Widerspruchsfreiheit hin zu prüfen.

Änderungsvorschlag

Entfällt.

Zu Abs. 2
Festlegung Resilienz steigender Maßnahmen sowie Vorgaben für Störungs-Monitoring

Beabsichtigte Neuregelung

Die Regelung stellt klar, dass Bund und Länder im Rahmen ihrer jeweiligen Zuständigkeiten resilienzsteigernde Maßnahmen sowie Vorgaben für ein Störungs-monitoring festlegen können.

Stellungnahme

Es ist fraglich, inwieweit es einer solchen Vorgabe bedarf, die explizit auf andernorts geregelte Zuständigkeiten und damit Kompetenzen von Bund und Ländern abstellt. Allerdings ist bereits der bloße Hinweis auf redundante Maßnahmefestlegungen und bürokratische Doppelerhebungen (hier: Störungsmonitoring vs. Meldewesen für Störungen nach § 12) kritisch.

Änderungsvorschlag

Bürokratische Doppelerhebungen und redundante Festlegung von Maßnahmen sind zu vermeiden.

§ 6

Anforderungen an Betreiber Kritischer Infrastrukturen

Zu Abs. 1
Freiwillige Umsetzung von Resilienzmaßnahmen

Beabsichtigte Neuregelung

Die obligatorischen Resilienzmaßnahmen für Betreiber kritischer Infrastrukturen, welche die jeweiligen Schwellenwerte der Rechtsverordnung überschreiten, sollen auch von Betreibern umgesetzt werden können, welche die festgelegten Schwellenwerte nicht erreichen.

Stellungnahme

Es bedarf keiner expliziten Erlaubnis zur Umsetzung von Maßnahmen zur Steigerung der Resilienz.

Änderungsvorschlag

§ 6 Absatz 1 KRITIS-DachG ist ersatzlos zu streichen.

Zu Abs. 2
Berücksichtigung branchenspezifischer Resilienzstandards

Beabsichtigte Neuregelung

Werden branchenspezifische Resilienzstandards nach § 11 Abs. 5 entwickelt, sollen Betreiber kritischer Infrastrukturen diese berücksichtigen können.

Stellungnahme

Es erscheint sachgerecht, die Anwendung branchenspezifischer Resilienzstandards nicht verpflichtend vorzuschreiben. Diese sollen als Angebot an die jeweilige Branche dienen. Im Ergebnis dürfen diese jedoch nicht dazu führen, dass bereits in der Anwendung befindliche Maßnahmen, die sich von den im jeweiligen Resilienzstandard enthaltenen Maßnahmen unterscheiden, jedoch ebenfalls das gewünschte Ziel erreichen, abgeändert und an den Resilienzstandard angepasst werden müssen. Diese Freiwilligkeit muss dringend beibehalten werden, um Betreibern kritischer Infrastrukturen ausreichende Flexibilität in der Umsetzung adäquater Maßnahmen zu gewähren.

Änderungsvorschlag

Entfällt.

§ 8

Registrierung der kritischen Anlage

Zu Abs. 1
Registrierung kritischer Anlagen bei einer gemeinsam von BBK und BSI eingerichteten Registrierungsmöglichkeit

Beabsichtigte Neuregelung

Betreiber kritischer Anlagen sind zur Registrierung der Anlagen bei einer von BBK und BSI gemeinsam eingerichteten Registrierungsstelle verpflichtet. Die Registrierung muss spätestens bis zum 1. Werktag, der auf die erstmalige oder erneute Einstufung als kritische Anlage nach § 4 folgt, erfolgen.

Stellungnahme

Die Krankenhäuser begrüßen ausdrücklich, dass es eine von BSI und BBK gemeinsam eingerichtete Registrierungsmöglichkeit geben soll. Die bereits heute etablierten Strukturen und Maßnahmen im Bereich Cybersicherheit müssen ressourcenschonend nachgenutzt werden können. Die Frist zur Registrierung von einem Werktag erscheint jedoch deutlich zu kurz. Zwar darf es in diesen Fällen nicht zu einem schuldhaften Verzögern der Registrierung kommen, mit Blick auf die komplexen organisatorischen Abläufe in vielen kritischen Infrastrukturen ist die Frist von einem Werktag jedoch zu kurz ausgestaltet.

Änderungsvorschlag

Die Frist zur Registrierung sollte von einem auf 10 Werktage verlängert werden.

Zu Abs. 2
Registrierung einer kritischen Anlage durch das BBK

Beabsichtigte Neuregelung

Kommt der Betreiber seiner Pflicht zur Registrierung nicht nach, soll das BBK im Einvernehmen mit den sonst zuständigen Aufsichtsbehörden des Bundes diese im Wege einer Zwangsregistrierung auch selbst vornehmen können.

Stellungnahme

Gerade im Bereich der Krankenhausplanung bestehen nach wie vor grundgesetzlich garantierte, föderale Hoheiten und Entscheidungskompetenzen der Bundesländer. Je nach Ausgestaltung der Rechtsverordnung nach § 15 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 sowie dem Bundesministerium des Innern und für Heimat abgestimmt wurden. Dabei wurden die Besonderheiten der Landeskrankenhausplanung in Deutschland berücksichtigt.

Änderungsvorschlag

Bei einer Zwangsregistrierung durch das BBK ist mindestens das Einvernehmen auch mit den zuständigen Aufsichtsbehörden auf Ebene der Bundesländer herzustellen. Die Regelungen zur Definition kritischer Anlagen im Bereich der Krankenhäuser (Stichwort: krankenhausplanerische Vorgaben), die in der BSI-KritisV mit Blick auf die föderale Zuständigkeit der Bundesländer aufgenommen wurde, ist in die Rechtsverordnung nach § 15 dieses Gesetzes zu übernehmen.

Zu Abs. 5
Erstellung einer Liste der Betreiber kritischer Anlagen durch das BBK

Beabsichtigte Neuregelung

Das BBK soll eine Liste der Betreiber kritischer Anlagen erstellen und diese spätestens alle vier Jahre aktualisieren.

Stellungnahme

Bisher gilt bereits die Information darüber, ob eine Anlage eine kritische Anlage im Sinne der BSI-KritisV ist, als schützenswertes und nicht-öffentlich zugängliches Gut. Inwieweit die sich registrierenden Betreiber kritischer Anlagen durch das BBK intern erfasst werden, muss nicht gesetzlich geregelt werden, es sei denn, damit wären weitergehende Aufgaben (zum Beispiel eine Veröffentlichung o. ä.) verbunden.

Änderungsvorschlag

§ 8 Absatz 5 KRITIS-DachG ist ersatzlos zu streichen.

Alternativ ist eine Klarstellung zum Zweck des Absatzes aufzunehmen.

§ 9

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 des Ausmaßes 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 erscheint 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 § 9 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 spätestens zum 1. Oktober 2024 vorliegen. Dies erfolgt nur unter der Maßgabe, dass sich die aktuell vom Bundesministerium des Innern und für Heimat vertretene Rechtsauffassung, dass zu diesem Zeitpunkt mit der Erarbeitung der branchenspezifischen Risikoanalysen durch die Betreiber kritischer Anlagen begonnen werden kann, auch weiterhin als mit dem EU-Recht vereinbar vertreten lässt.

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 § 11, 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. 2
Bereitstellung der Elemente der Risikoanalysen der Bundesministerien durch das BBK an die Betreiber kritischer Anlagen

Beabsichtigte Neuregelung

Die zu erstellenden nationalen Risikoanalysen und Bewertungen sollen an das BBK übermittelt, dort ausgewertet und entsprechende Elemente den Betreibern kritischer Anlagen zur Verfügung gestellt werden.

Stellungnahme

Sowohl mit Blick auf den zeitlichen Vorlauf als auch die notwendige Transparenz erscheint 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 BBK gefilterten Weiterleitung notwendigerweise entstehen.

Änderungsvorschlag

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

§ 10

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 § 9 sowie anderen Informationsquellen sollen Betreiber kritischer Anlagen erstmals neun Monate nach der Registrierung als kritische Anlage und im weiteren 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 Bedrohungen 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 § 9 dargestellten zeitlichen Abhängigkeiten wird 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 hingewiesen. Aufgrund der gegenwärtigen Formulierung bleibt jedoch unklar, ob die Erstellung der Risikoanalyse und -bewertung spätestens neun Monate nach der erstmaligen Registrierung als kritische Anlage nach § 8 abgeschlossen oder begonnen werden muss. Dies ist klarzustellen. Sollte mit dem Zeitpunkt der Abschluss der Risikoanalyse gemeint sein, steht dies im Konflikt mit der Vorrausetzung einer nationalen Risikoanalyse.

Die Betrachtung von Interdependenzen zu anderen kritischen Infrastrukturen ist sachgerecht, jedoch birgt die Komplexität dieser Abhängigkeiten hohe Risiken mit Blick auf die Vollständigkeit der Risikoanalyse. 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 Leitungskapazitäten zum Beispiel 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.

Änderungsvorschlag

Die zeitlichen und inhaltlichen Abhängigkeiten der Risikoanalysen nach den §§ 9 und 10 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

Erfüllung der nach § 10 festgelegten Anforderungen aufgrund von Verpflichtungen aus anderen öffentlich-rechtlichen Vorschriften

Beabsichtigte Neuregelung

Wurden bereits gleichwertige Risikoanalysen und -bewertungen aus anderen Anlässen vorgenommen, erfüllt der Betreiber die nach § 10 festgelegten Anforderungen. Das BBK kann im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes bestehende Risikoanalysen und Bewertungen als vollständig oder teilweise den Verpflichtungen nach dieser Vorschrift entsprechend erklären. Dazu sind diese dem BBK vorzulegen.

Stellungnahme

Die Regelung erscheint sachgerecht. Bereits heute werden zum Beispiel 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 BBK zu den aktuell bereits vorgesehenen Maßnahmen zur physischen Resilienz an. Dabei ist das Ziel, zu klären, ob diese Maßnahmen ganz oder in Teilen als ausreichend im Sinne

der Vorschrift nach § 10 gelten können. Eine zusätzliche Umsetzung an anderer Stelle muss dann entfallen.

Änderungsvorschlag

Entfällt.

§ 11

Resilienzmaßnahmen der Betreiber kritischer Anlagen

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, geeignete und verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen zur Gewährung ihrer Resilienz zu treffen. Diese Maßnahmen basieren auf den nach den §§ 9 und 10 bereitgestellten Informationen. Dabei soll der Stand der Technik berücksichtigt werden.

Stellungnahme

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

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.

Zu Abs. 2
Verhältnismäßigkeit technischer, sicherheitsbezogener und organisatorischer Maßnahmen

Beabsichtigte Neuregelung

Es 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

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 kaum wirtschaftlich 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.

Die in Anhang 1 aufgenommenen „insbesondere zu berücksichtigenden Maßnahmen“ werden als „Mindestvorgaben“ interpretiert, die infolge einer Abwägung nach Abs. 2 gegebenenfalls gar nicht zugänglich sind. Für Krankenhäuser sind die unter Anhang 1 lit. b) genannten Maßnahmen „Detektionsgeräte“ und „Zugangskontrollen“ für die der Öffentlichkeit zugänglichen oder auf schnelle medizinische Versorgung ausgerichteten Organisationsbereiche nicht darstellbar. Betriebsabläufe, die der Patientensicherheit dienen, insbesondere die schnelle Zugänglichkeit zu Operationsräumen bei Sektio-OPs; der Bildgebung bei Schlaganfallbehandlungen oder der Zuwegung von Hubschrauber-landeplätzen zu Schockräumen entziehen sich schon teils anderslautender normativer Vorgaben den angedachten Maßnahmen.

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

Es sollte eine Klarstellung erfolgen, wie mit den in Anhang 1 genannten Maßnahmen im Hinblick auf die Abwägung nach Abs. 2 umgegangen werden sollte.

Zu Abs. 3
Aufzählung von Maßnahmen, die als Resilienzmaßnahmen umzusetzen sind

Beabsichtigte Neuregelung

Es werden Maßnahmen aufgezählt, die als Resilienzmaßnahmen verstanden werden.

Stellungnahme

Unter Ziffer 5 wird auch 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 kaum 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 schlicht keinerlei Kapazitäten für eine entsprechende Prüfung.

Änderungsvorschlag

Es 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.

Zu Abs. 4
Aufzählung von Maßnahmen, die bei der Abwägung nach Abs. 2 insbesondere berücksichtigt werden können

Beabsichtigte Neuregelung

Es werden „insbesondere zu berücksichtigende Maßnahmen nach § 11 Abs. 1“ aufgezählt.

Stellungnahme

Siehe Stellungnahme zur Abs. 2.

Änderungsvorschlag

Siehe Änderungsvorschlag zu Abs. 2.

Zu Abs. 5
Vorschlag branchenspezifischer Resilienzstandards zur Gewährleistung der Anforderung nach Abs. 1

Beabsichtigte Neuregelung

Betreibern kritischer Anlagen sowie ihren Branchenverbänden wird der Vorschlag branchenspezifischer Resilienzstandards zur Gewährleistung der Anforderungen nach Abs. 1 ermöglicht. Das BBK stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Abs. 1 zu gewährleisten.

Stellungnahme

Die Möglichkeit, branchenspezifische Resilienzstandards 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 spricht sich dafür aus, die bisher im bestehenden Branchensicherheitsstandard („B3S“) bereits enthaltenen Maßnahmen für den Bereich der physischen Sicherheit zu erweitern und in einem gemeinsamen Standard abzubilden.

Änderungsvorschlag

Es sollte die Möglichkeit geschaffen werden, analog zu einer gemeinsamen Registrierungsmöglichkeit, einer gemeinsamen Meldestelle etc. auch eine Verzahnung des bisherigen Branchensicherheitsstandards nach § 8a Abs. 3 BSIG mit den hier vorgesehenen Regelungen zu ermöglichen.

Darüber hinaus sollte bei der Erarbeitung gesetzlicher Anforderungen in Deutschland die Verfügbarkeit international anerkannter Standards zur Umsetzung der Anforderungen grundsätzlich stärker berücksichtigt werden.

Zu Abs. 6
Erstellung eines Resilienzplans

Beabsichtigte Neuregelung

Betreiber kritischer Anlagen müssen die Maßnahmen nach Abs. 1 in einem Resilienzplan darstellen. Der Resilienzplan ist dem BBK im Weiteren alle zwei Jahre nachzuweisen.

Stellungnahme

Es ist unklar, welche Vorgaben für die Erstellung eines Resilienzplans heranzuziehen sind. Weder Art noch Umfang werden spezifiziert. Diese fehlenden Vorgaben dürften in der Praxis, insbesondere mit Blick auf die Regelungen zu entsprechenden Bußgeldvorschriften in § 19 Abs. 1 Ziffer 4 1. Halbsatz, zu großen Unsicherheiten führen.

Änderungsvorschlag

Das BBK sollte in Abstimmung mit den einzelnen Sektoren und Branchen Vorgaben für Form und Inhalt des Resilienzplans erarbeiten und veröffentlichen.

Zu Abs. 8

Nachweis der Erfüllung der Anforderungen nach Abs. 1

Beabsichtigte Neuregelung

Betreiber kritischer Anlagen müssen, spätestens zu einem bei der Registrierung festgelegten Zeitpunkt und anschließend alle zwei Jahre, dem BBK auf geeignete Weise die Erfüllung der Anforderungen nach Abs. 1 nachweisen. Der Nachweis kann durch Audits erfolgen. Dabei aufgedeckte Mängel sind dem BBK zu übermitteln. Das BBK kann die Beseitigung der Mängel verlangen. Das 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. Es ist jedoch scharf zu kritisieren, wenn durch das im Bereich Informationssicherheit zuständige BSI als „Orientierungshilfen“ veröffentlichte normative Vorgaben der Umgehung parlamentarischer Mechanismen dienen. Diese, teils als willkürlich empfundenen Regelungen nehmen zu und können nicht einer echten Branchenbeteiligung gleichgesetzt sein, zumal die im „Kommentierungsverfahren“ vorgebrachten Inhalte in aller Regel aber nicht oder nur rudimentär berücksichtigt werden.

Dieses Vorgehen durch das BSI sollte durch das zuständige Ministerium einerseits hinterfragt und für das BBK von Beginn an ausgeschlossen werden. Die als „Orientierungshilfen“ gekennzeichneten Vorgaben führen in der Praxis zu enormer Verunsicherung. Dies gilt insbesondere für das Verhältnis zwischen den prüfenden Stellen und geprüften Betreibern. Außerdem schaden diese Vorgaben durch die inhärente Intransparenz und rechtliche Unsicherheiten bei der Bewertung normativer Vorgaben dem gesetzlich verfolgten Ziel.

Änderungsvorschlag

Soweit sich die öffentliche Mitteilung nach § 11 Abs. 8 Satz 8 auch auf Satz 7 und nicht nur auf Satz 1 bezieht, sollten die o. g. Hinweise zwingend berücksichtigt werden. Die zweckentfremdende, sich ausweitende Nutzung von „Orientierungshilfen“ zum Ersatz gesetzgeberischen Handelns muss eingestellt werden.

Zu Abs. 9
Überprüfung der Einhaltung der Anforderungen durch das BBK

Beabsichtigte Neuregelung

Bestehen erhebliche Zweifel an der Einhaltung der Anforderungen nach Abs. 1, kann das BBK die Einhaltung der Anforderung überprüfen. Dabei kann es sich eines qualifizierten unabhängigen Dritten bedienen. Für die Überprüfung kann das BBK Gebühren und Auslagen bei den Betreibern der kritischen Anlage erheben, wenn das 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 den vergleichbaren Regelungen des § 8a BSIG als in aller Regel umfangreich und ressourcenintensiv dargestellt. Wurde ein Audit nach Abs. 8 nachgewiesen, muss sich der Betreiber dann auch auf das Ergebnis des Audits verlassen können. In diesem Fall scheidet eine Überprüfung durch das BBK grundsätzlich aus. Hat der Betreiber den Nachweis auf andere Weise erbracht, stellt sich die Frage nach der Qualifizierung eines unabhängigen Dritten, auf dessen Urteil sich das BBK in diesem Fall verlassen und gegebenenfalls die Behebung festgestellter Mängel oder das Verhängen von Bußgeldern durchsetzen wird. Unabhängig davon, ob es entsprechende Vorgaben für die Qualifizierung, insbesondere die Branchenkompetenz der das Audit durchführenden prüfenden Stelle geben wird, müssen dieselben Vorgaben auch für die Auswahl qualifizierter unabhängiger Dritter nach § 9 Abs. 9 Satz 2 gelten.

Änderungsvorschlag

Es sollten entsprechende Vorgaben für die prüfenden Stellen erlassen werden. In diesem Fall müssen diese Vorgaben dann auch durch das BBK bei der Auswahl qualifizierter unabhängiger Dritter gemäß Satz 2 berücksichtigt werden.

Zu Abs. 10
Anweisung zur Umsetzung erforderlicher und verhältnismäßiger Maßnahmen durch das BBK

Beabsichtigte Neuregelung

Im Anschluss an behördliche Aufsichtsmaßnahmen nach § 11 Abs. 9 soll das BBK Betreiber kritischer Anlagen anweisen können, erforderliche und verhältnismäßige Maßnahmen zu ergreifen, um festgestellte Verstöße innerhalb einer angemessenen Frist zu beheben.

Stellungnahme

Die Anweisung zur Umsetzung erforderlicher und verhältnismäßiger Maßnahmen durch eine Aufsichtsbehörde ist nachvollziehbar. Folgt jedoch die behördliche Überprüfung nach Abs. 9 einer abweichenden Einschätzung zur Verhältnismäßigkeit umzusetzender Maßnahmen (siehe Kommentierung zu Abs. 2), wird sich dieser Dissens auch bei der Einschätzung, welche Maßnahmen verhältnismäßig seien, fortsetzen. Dem Betreiber muss ausreichend Gelegenheit gegeben werden, die getroffene Entscheidung zu begründen.

Zudem verkennt die vorgesehene gesetzliche Regelung, die nach Abs. 10 lediglich das Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes vorsieht, die Zuständigkeit der Länder im Bereich der Gesundheitsversorgung. Diese sind daher – zumindest für den Bereich der Gesundheitsversorgung – zwingend mit einzubeziehen.

Änderungsvorschlag

Dem Betreiber ist die Gelegenheit zur Begründung zu geben, weshalb Maßnahmen, die nach Meinung des BBK erforderlich und verhältnismäßig seien, bisher nicht umgesetzt wurden. Das Einvernehmen mit den zuständigen Aufsichtsbehörden der Bundesländer ist zu ergänzen.

Zu Abs. 13
Umsetzung der Verpflichtungen nach den Absätzen 1 bis 10 innerhalb von 10 Monaten nach Registrierung als kritische Anlage

Beabsichtigte Neuregelung

Die Verpflichtungen nach den Absätzen 1 bis 10 treffen die Betreiber frühestens nach Ablauf von 10 Monaten nach Registrierung als kritische Anlage.

Stellungnahme

Auch, wenn Betreiber die Vorgaben nach den Absätzen 1 bis 10 „frühestens nach 10 Monaten nach Registrierung als kritische Anlage“ berücksichtigen müssen, sind die aktuell vorgesehenen zeitlichen Abläufe mit den inhaltlichen Vorgaben nicht vereinbar.

Änderungsvorschlag

Siehe Änderungsvorschlag zu § 10 Abs. 1.

§ 12

Meldewesen für Störungen

Zu Abs. 1
Verpflichtung zur Meldung von Vorfällen die Erbringung der kritischen Dienstleistung erheblich stören könnten

Beabsichtigte Neuregelung

Betreiber kritischer Anlagen werden verpflichtet, Vorfälle, die die Erbringung ihrer kritischen Dienstleistung erheblich stören könnten, an eine gemeinsame Meldestelle von BBK und BSI zu melden. Dabei sind insbesondere Angaben zur Anzahl und Anteil der von der Störung betroffenen Nutzer, 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.

Stellungnahme

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

Änderungsvorschlag

Entfällt.

Zu Abs. 2
Inhalt der Meldungen

Beabsichtigte Neuregelung

Es wird festgelegt, dass die Meldungen sämtliche verfügbaren Informationen enthalten müssen, um den Vorfall, dessen Ursache und mögliche Folgen nachzuvollziehen.

Stellungnahme

Das Informationsinteresse der zuständigen Bundesbehörde ist 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 Stress-situationen führt. Es sollten daher nur die unbedingt notwendigen Informationen abgefragt werden, um nicht für die Beseitigung der Störung notwendige personelle Ressourcen anderweitig zu binden.

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 – vorbehaltlich der operativen Unmöglichkeit – dem 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 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 Meldung einer Störung „unverzüglich“ – 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

Einsatz kritischer Komponenten; Verordnungsermächtigung

Beabsichtigte Neuregelung

Nicht definiert.

Stellungnahme

Aufgrund der im Referentenentwurf noch nicht aufgenommenen Regelungen zum Einsatz kritischer Komponenten kann eine Stellungnahme derzeit noch nicht erfolgen. Wie im Allgemeinen Teil bereits vorgeschlagen, sollte den Verbänden nach Abschluss der Ressortabstimmung die Möglichkeit zur Stellungnahme zu den bisher noch nicht bekannten Regelungstatbeständen gegeben werden.

Änderungsvorschlag

Entfällt.

§ 15

Ermächtigung zum Erlass von Rechtsverordnungen

Beabsichtigte Neuregelung

Das Bundesministerium des Innern und für Heimat 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.

Stellungnahme

Der Gesetzesentwurf greift hier das im BSI-Gesetz etablierte Vorgehensmodell der BSI-KritisV auf. Die Regelung ist dahingehend sachgerecht. Allerdings sollte bei der vorgesehenen branchenspezifischen Festlegung von Schwellenwerten auf die im BSI Gesetz bzw. der BSI-KritisV 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-KritisV durchgeführten Abstimmungen im Rahmen der sogenannten „Kernteam-Beratungen“ zu wiederholen.

Änderungsvorschlag

Entfällt.

§ 19

Bußgeldvorschriften

Zu Abs. 1
Festlegung von Ordnungswidrigkeitstatbeständen

Beabsichtigte Neuregelung

In den Ziffern 1-5 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 § 10 Abs. 1, die Nichtvorlage eines Resilienzplans und weiterer Dokumente sowie fehlende Unterstützung des BBK bei Aufsichtsmaßnahmen nach § 11 Abs. 9 infolge erheblicher Zweifel an der Einhaltung der Anforderungen nach § 11 Abs. 1.

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 – hier das BBK, 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 in 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.

§ 20

Inkrafttreten

Beabsichtigte Neuregelung

Es wird das Inkrafttreten der gesetzlichen Regelungen festgelegt. Die §§ 6 bis 8, 10 bis 12 und § 16 sollen am 1. Januar 2026 in Kraft treten. § 19 soll am 1. Januar 2027 in Kraft treten. Die übrigen Festlegungen des Gesetzes sollen am Tag nach Verkündung in Kraft treten.

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 völlig überforderte 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 Tarifabschlüsse und der fehlenden Planbarkeit des Leistungsgeschehens in den kommenden Jahren vor nie da gewesenen strukturellen und wirtschaftlichen Herausforderungen.

Dabei wirkt 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 durch einen wiederholt als geeignet im Sinne des § 8a BSI-Gesetz festgestellten branchenspezifischen Sicherheitsstandard eine Umsetzungsperspektive besitzt, fehlen diese Grundlagen für den Bereich der physischen Resilienz bisher 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-Rechts eine noch stärker gestufte Realisierung der Anforderungen infrage kommen kann, um Staat und

Wirtschaft eine realistische Umsetzungsperspektive für die zweifellos 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. Als jüngstes Beispiel sei hier die Ankündigung des Anbieters SAP genannt, der sich aus dem Krankenhausbereich vollständig zurückziehen wird.