VERBAND KOMMUNALER UNTERNEHMEN e.V.

STELLUNGNAHME

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

Referentenentwurf des Bundesministeriums des Innern und für Heimat vom 21.12.2023

Berlin, 24.01.2024

Der Verband kommunaler Unternehmen e. V. (VKU) vertritt über 1.550 Stadtwerke und kommunalwirtschaftliche Unternehmen in den Bereichen Energie, Wasser/Abwasser, Abfallwirtschaft sowie Telekommunikation. Mit über 300.000 Beschäftigten wurden 2021 Umsatzerlöse von 141 Milliarden Euro erwirtschaftet und mehr als 17 Milliarden Euro investiert. Im Endkundensegment haben die VKU-Mitgliedsunternehmen signifikante Marktanteile in zentralen Ver- und Entsorgungsbereichen: Strom 66 Prozent, Gas 60 Prozent, Wärme 88 Prozent, Trinkwasser 89 Prozent, Abwasser 45 Prozent. Die kommunale Abfallwirtschaft entsorgt jeden Tag 31.500 Tonnen Abfall und hat seit 1990 rund 78 Prozent ihrer CO2-Emissionen eingespart – damit ist sie der Hidden Champion des Klimaschutzes. Immer mehr Mitgliedsunternehmen engagieren sich im Breitbandausbau: 206 Unternehmen investieren pro Jahr über 822 Millionen Euro. Künftig wollen 80 Prozent der kommunalen Unternehmen den Mobilfunkunternehmen Anschlüsse für Antennen an ihr Glasfasernetz anbieten.
Zahlen Daten Fakten 2023
Wir halten Deutschland am Laufen – denn nichts geschieht, wenn es nicht vor Ort passiert: Unser Beitrag für heute und morgen: #Daseinsvorsorge. Unsere Positionen: www.vku.de

Verband kommunaler Unternehmen e.V. · Invalidenstraße 91 · 10115 Berlin
Fon +49 30 58580-0 · Fax +49 30 58580-100 · info@vku.de · www.vku.de

Der VKU bedankt sich für die Möglichkeit, zu dem Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen in Form des Referentenentwurfs des Bundesministeriums des Innern, für Bau und Heimat Stellung nehmen zu können.

Bedeutung des Vorhabens für kommunale Unternehmen

Der Verband kommunaler Unternehmen (VKU) vertritt rund 1.500 kommunalwirtschaftliche Unternehmen in den Bereichen Energie, Wasser/Abwasser, Abfallwirtschaft sowie Telekommunikation. Bei einer Vielzahl dieser Unternehmen handelt es sich um Betreiber von kritischen Anlagen. In Zusammenschau mit dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz ist wahrscheinlich jedes unserer Mitgliedsunternehmen von der Regulierung betroffen.

Positionen des VKU in Kürze

Der **VKU begrüßt ausdrücklich den Entwurf eines Kritis-Dachgesetzes** (KRITIS-DachG), um den physischen Schutz der kritischen Anlagen in Deutschland zu erhöhen. Auch der VKU sieht hier im Vergleich zur Cybersichersicherheitsregulierung in vielen Sektoren einen dringend notwendigen Bedarf und ist sich der Verantwortung seiner Mitglieder für die gesamtgesellschaftliche Stabilität Deutschlands bewusst. Auch erkennt der VKU an, dass der aktuelle Entwurf des Gesetzes viele Kritikpunkte des Vorentwurfs beseitigt hat.

Gleichwohl besteht weiterhin ein **deutlicher Verbesserungsbedarf:**

- Zunächst stellt sich **grundsätzlich die Frage nach der Verantwortungsteilung zwischen Staat und Gesellschaft**. Aus dem Gesetzesentwurf ergibt sich nicht, wo die Verantwortung des Staates für die Sicherheit der Bevölkerung endet und wo die Verantwortung der Betreiber der kritischen Anlagen beginnt. Dies muss dringend im Dialog mit den Betreibern klargestellt werden (siehe hierzu unter Nr. 8a.). Eng hiermit verbunden ist die Frage, wie die Betreiber die ihnen verbleibenden Pflichten **refinanzieren** können (siehe hierzu unter Nr. 8b).
- Die Betreiber können ihre **Pflichten in zeitlicher Hinsicht** nicht erfüllen. Insbesondere haben die Betreiber im Moment nur einen Monat Zeit, um nach ihrer Risikoanalyse und Risikobewertung die entsprechenden Resilienzmaßnahmen zu treffen. Dies ist offensichtlich **unmöglich** (Nr. 8c, 10a).
- Die **geteilte Zuständigkeit** beim Vollzug **zwischen Bund und Ländern wird abgelehnt**. Die Unternehmen würden mit einer unübersehbaren Anzahl von Aufsichtsbehörden und Anforderungen konfrontiert und müssten einen enormen bürokratischen Aufwand leisten, um dem gerecht zu werden (Nr. 4). Perspektivisch sollte die **Gesetzgebungskompetenz** zur Regulierung der kritischen Infrastrukturen vollständig auf die Bundesebene verlagert werden (Nr. 5c).
- Es muss ein **Vorrang der branchenspezifischen Sicherheitsstandards** festgelegt werden. Nur wenn solche nicht zeitnah von den Branchen entwickelt werden, sollte der

Bund die Möglichkeit haben, **Resilienzvorgaben** vorzuschreiben (Nr. 8d). Auch verpflichtende Muster und Vorlagen für die Risikoanalyse und Risikobewertung durch die Betreiber werden abgelehnt (Nr. 9). Gleiches gilt für verpflichtende Muster für Resilienzpläne (Nr. 10f).

- Der **Betreiber einer kritischen Anlage** muss im Grundsatz **einheitlich** im NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz und im KRITIS-DachG **definiert** werden (Nr. 14a). Soweit Betreiber von kritischen Anlagen im Einzelfall festgelegt werden, müssen diesen **längere Umsetzungsfristen** eingeräumt werden (Nr. 5b).
- Die **Wirtschaft** muss bei der Erstellung der **nationalen Risikoanalyse und Risikobewertung eng eingebunden** werden. Die Ergebnisse müssen den Betreibern zeitnah mitteilt werden (Nr. 7).
- Das Gesetz muss klar benennen, dass mit diesem Gesetz auch eine **grundsätzliche Entscheidung über eine Ressourcenverteilung festgelegt wird**. Da den Betreibern eine Vielzahl von Pflichten auferlegt werden, die der gesamtgesellschaftlichen Stabilität dienen, müssen die **Betreiber** im Gegenzug auch **besondere Rechte** erlangen. Dies muss sich manifestieren, indem der **Schutz der kritischen Anlagen als überragendes öffentliches Interesse anerkannt** wird. Diese Wertung muss dann in jeder Abwägungsentscheidung auf gesetzlicher Ebene und auf Ebene der Verwaltung berücksichtigt werden (Nr. 1a). Dies wird sich insbesondere zu einer **Beschränkung der Transparenzpflichten** führen müssen, denen die Betreiber der kritischen Anlagen bisher unterliegen (siehe hierzu unter Nr. 1b).
- Das **KRITIS-DachG** und das **NIS2UmsuCG** müssen zukünftig **zusammen behandelt werden** und insbesondere gemeinsam in das Parlament eingebracht werden. Beide Gesetze sind untrennbar miteinander verwoben, so dass das eine Gesetz ohne das andere Gesetz nicht abschließend bewertet werden kann. Bereits jetzt zeigt sich, dass eine Vielzahl von Inkonsistenzen bestehen, da **Begriffe doppelt** und **uneinheitlich definiert** werden (Nr. 3) und **Pflichten widersprüchlich** festgelegt werden.

Stellungnahme

1. Grundsatzentscheidungen in Bezug auf kritische Anlagen
Bei den folgenden Ausführungen handelt es sich um Fragen, die Grundsatzentscheidungen in Bezug auf die Stellung der Betreiber von kritischen Anlagen betreffen. Sie lassen sich nicht einzelnen Normen zuordnen und werden deshalb „vor die Klammer" gezogen.

a. Ressourcenverteilung und Bevorzugung von kritischen Anlagen
Laut der Gesetzesbegründung (S. 3) enthält das Gesetz keine Entscheidungen über die Ressourcenverteilungen. Es soll nicht regeln, dass Anlagen und Einrichtungen in bestimmten Situationen auf Grund anderer Normen eine Bevorzugung erfahren, nur, weil sie nach diesem Gesetz als kritische Anlagen identifiziert wurden. Dem kann nicht gefolgt werden.

Den Betreibern von kritischen Anlagen werden über das KRITIS-DachG (und das NIS2UmsuCG[1]) besondere Pflichten aufgrund gesamtgesellschaftlicher Erwägungen auferlegt. Wie bereits aus der Nationalen Sicherheitsstrategie erkennbar wird, hat die Resilienz der kritischen Anlagen (dort noch als kritische Infrastrukturen bezeichnet) eine besondere Bedeutung für die Resilienz der gesamten Gesellschaft. **Diese Pflichten aus gesamtgesellschaftlichen Erwägungen müssen aber auf der anderen Seite zu besonderen Rechten führen.** Bereits in der Vergangenheit wurde dies so auch gehandhabt. So wurden Mitarbeitern von kritischen Anlagen der Zugang zu Gebieten gewährt, obwohl aufgrund der Corona Pandemie eigentlich eine Ausgangssperre galt.

Es muss folglich festgeschrieben werden, dass die Identifizierung als kritische Anlage besonders in gesetzgeberische und verwaltungsrechtliche Abwägungsentscheidungen einzubeziehen ist und dies ggf. auch zu einer Bevorzugung in anderen Bereich führen muss. Orientiert werden sollte sich an einer ähnlichen Formulierung in § 2 Erneuerbare-Energien-Gesetz (2023), § 11c EnWG und § 14d Abs. 10 EnWG.

Formulierungsvorschlag:

§ 1a Besondere Bedeutung der kritischen Anlagen

Der Schutz der kritischen Anlagen liegt im überragenden öffentlichen Interesse und dient der öffentlichen Sicherheit.

Diese Lösung hätte den Vorteil, dass keine Anpassungen in einer Vielzahl von Gesetzen vorgenommen werden müssen, sondern im Rahmen von behördlichen Ermessensentscheidungen diese Interessen automatisch mit einem hohen Gewicht berücksichtigt werden. Ein Beispiel ist

[1] Diskussionspapier des BMI- Wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland, Fassung vom 03.07.2023.

z.B. der Denkmalschutz, der anderenfalls Baumaßnahmen zur Erhöhung der Sicherheit verhindern könnte.

b. Verhältnismäßige Transparenz- und Auskunftspflichten
Insbesondere im Bereich der Transparenz- und Auskunftspflichten müssen Betreiber von kritischen Anlagen aufgrund einer grundsätzlichen Wertentscheidung zukünftig deutlich bessergestellt werden.

Eine wesentliche Gefahr für kritische Anlagen geht von zu großer Sichtbarkeit der eigenen Infrastruktur aus. Diese Gefahr wächst durch vielfältige Transparenz- und Auskunftspflichten. Diesen wichtigen Aspekt sollte das KRITIS-DachG adressieren. Die Anschläge auf die Infrastruktur der Deutschen Bahn sollten hier ein deutlicher Weckruf sein.

Eine Ausweitung der Datenveröffentlichungspflichten für Betreiber kritischer Anlagen durch gesetzliche Regelungen sollte vermieden bzw. auf ein notwendiges Minimum begrenzt werden. Das Argument der Transparenz darf dabei kein alleiniges Kriterium zur Begründung der Notwendigkeit darstellen. Bereits bestehende gesetzliche Verpflichtungen sind zwingend darauf zu überprüfen und ggf. anzupassen.

Die gesetzlichen Vorgaben des Telekommunikationsgesetzes (insbesondere § 79 TKG) verlangen von Betreibern öffentlicher Versorgungsnetze, dass sie der zentralen Informationsstelle des Bundes – dem Infrastrukturatlas bei der Bundesnetzagentur – bestimmte netzbezogene Daten zur Verfügung stellen. Diese grundsätzliche Datenlieferungspflicht ist sehr umfassend. Über den Infrastrukturatlas können die Daten von Dritten eingesehen werden. **Der Gesetzgeber sollte prüfen, ob die grundsätzliche Datenlieferungspflicht und die anschließende Einsichtnahmemöglichkeit durch Dritte noch benötigt werden oder ggf. aufgehoben werden können**. Soweit die gesetzlichen Vorgaben auf europäisches Recht (z.B. zukünftig auf den Gigabit Infrastructure Act) zurückzuführen sind, wäre die europäische Ebene einzubeziehen.

Formulierungsvorschlag:

§ 79 TKG - Informationen über Infrastruktur

(2) [S. 1 - 3]: **<u>Einrichtungen, die durch Gesetz oder aufgrund eines Gesetzes als kritische Anlage bestimmt worden, unterliegen nicht den Pflichten dieses Absatzes.</u>** (Satz 4 neu)

Soweit an den gesetzlichen Vorgaben im TKG festgehalten werden sollte, sollte der Gesetzgeber weiter prüfen, ob das Datenlieferungsverfahren im Interesse der Informationssicherheit angepasst werden kann. Aktuell müssen zunächst sämtliche mitteilungspflichtigen Netzbetreiberdaten übermittelt werden, obwohl im Rahmen bestimmter Ausnahmeregelungen die betroffenen Daten nach einer dahingehenden Prüfung nicht im Infrastrukturatlas zur Verfügung gestellt werden. In einem solchen Fall sollten die Verteilnetzbetreiber die betreffenden

Daten aber auch nicht an die Bundesnetzagentur liefern müssen.

Bereits öffentlich verfügbare Daten zu kritischen Anlagen, die von externen Akteuren systematisch aus pflichtgemäß veröffentlichten Daten und weiteren Quellen zusammengetragen und online gestellt werden, stellen ein erhebliches Risiko dar. Elemente der Infrastruktur sind so für jedermann im Internet leicht zugänglich; vulnerable Punkte werden mit wenig Fachkenntnis leicht identifizierbar. Zum Beispiel sammeln Open Source Plattformen solche Informationen mit Schwarmintelligenz und vervollständigen so schrittweise ein strukturiertes Abbild kritischer Anlagen. **Im Rahmen des KRITIS-DachG sollte eine Möglichkeit geschaffen werden, gegen solche Veröffentlichungen von Daten zu kritischen Anlagen durch Dritte vorzugehen. D.h., der Eigner der kritischen Anlage sollte ein Recht auf Löschung der Daten haben. Auch sollten die Betreiber von kritischen Anlagen ein Auskunftsrecht gegenüber Dritten (z.B. Open Source Plattformen) haben, woher die veröffentlichten Daten stammen**.

c. Anpassungen des Vergaberechts

Die Vorgaben zum Aufbau von Schutzmechanismen für kritische Anlagen dürfen zudem nicht durch Vorgaben des Vergaberechts beeinträchtigt werden.

Vergabeverfahren erfordern einerseits Transparenz im Hinblick auf den Beschaffungsgegenstand. Andererseits können sich Beschaffungsverfahren gerade im Fall von Nachprüfungsverfahren deutlich in die Länge ziehen. Beide Aspekte sind im Hinblick auf die zügige Umsetzung und die gebotene Geheimhaltung hinsichtlich der zu beschaffenden Schutzinstrumente äußerst kontraproduktiv. Teilweise wird es kaum möglich sein, die nach dem KRITIS-DachG erforderlichen Maßnahmen zeitgerecht umzusetzen, wenn das reguläre Vergabeverfahren eingehalten werden muss (siehe zur bereits jetzt kaum möglichen zeitlichen Reinfolge der Pflichten die Kommentierung unter Nr. 8c).

Wir schlagen daher vor, die vergaberechtliche Ausnahmevorschrift in § 107 Abs. 2 des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) für Aufträge, die im Zusammenhang stehen mit wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland, auf Aufträge im Zusammenhang mit dem Schutz von kritischen Anlagen zu erweitern.

Der Gesetzgeber hat bereits mit dem „Gesetz zur beschleunigten Beschaffung im Bereich der Verteidigung und Sicherheit und zur Optimierung der Vergabestatistik“ im Jahr 2019 anerkannt, dass Fragen der Sicherheit und die Abwehr entsprechender terroristischer Gefahren zu den wesentlichen sicherheitspolitischen Herausforderungen gehören und daher das Vergaberecht, konkret § 107 Abs. 2 GWB, angepasst.

Die Fragen der Sicherheit betreffen aber nicht nur die militärischen und zivilen Sicherheitsbehörden, sondern, wie jetzt der aktuelle Gesetzentwurf zeigt, auch die Betreiber kritischer Anlagen. Dies gilt insbesondere für kommunale Unternehmen, die zukünftig auf Grund von Überlegungen zur nationalen Sicherheit wahrscheinlich einen deutlich höheren Sicherheitsstandard

erreichen müssen. Auch für diese Unternehmen besteht die Notwendigkeit, kurzfristig und effektiv auf sicherheitsrelevante Entwicklungen im Bereich der Sicherheit ihrer kritischen Anlagen reagieren zu können bzw. zu müssen. Insbesondere erfolgreiche Angriffe auf die Stromnetze sind durch den dadurch verursachten Ausfall der Energie- oder Wasserversorgung zweifellos geeignet, schwerwiegende Störungen der öffentlichen Sicherheit und Ordnung zu verursachen, die einer Krise im Sinne des Art. 1 Nr. 10 der Richtlinie 2009/81/EG über die Koordinierung der Verfahren zur Vergabe bestimmter Bau-, Liefer- und Dienstleistungsaufträge in den Bereichen Verteidigung und Sicherheit gleichstehen.

Vor diesem Hintergrund ist es daher aus unserer Sicht dringend geboten, die Ausnahmevorschrift für sicherheitsrelevante Vergaben in § 107 Abs. 2 GWB noch einmal anzupassen und S. 3 folgendermaßen zu fassen:

Formulierungsvorschlag:

§ 107 GWB - Allgemeine Ausnahmen

(2) *[S. 1, 2, …] „Ferner können im Fall des Satzes 1 Nummer 1 wesentliche Sicherheitsinteressen im Sinne des Artikels 346 Absatz 1 Buchstabe a des Vertrags über die Arbeitsweise der Europäischen Union insbesondere berührt sein, wenn der öffentliche Auftrag oder die Konzession*
1. sicherheitsindustrielle Schlüsseltechnologien betreffen oder
2. Leistungen betreffen, die
a) für den Grenzschutz, die Bekämpfung des Terrorismus oder der organisierten Kriminalität oder für verdeckte Tätigkeiten der Polizei oder der Sicherheitskräfte bestimmt sind,
b) Verschlüsselung betreffen ***oder***
c) für die Betreiber kritischer Anlagen zum Zwecke der Erfüllung der Anforderungen nach dem KRITIS-DachG bestimmt sind.

Und soweit ein besonders hohes Maß an Vertraulichkeit erforderlich ist.“

Angesichts der oft kurzfristig entstehenden sicherheitsrelevanten Herausforderungen und der Erforderlichkeit schneller, effektiver und robuster Reaktionen zur Gefahrenabwehr ist es aus unserer Sicht sowohl sachgerecht als auch notwendig, den Betreibern kritischer Anlagen diese vergaberechtliche Ausnahmeregel grundsätzlich zu eröffnen.

Wir gehen davon aus, dass es sich um eine eng auszulegende Ausnahmeregelung handelt und in jedem Einzelfall das besonders hohe Maß an Vertraulichkeit darzulegen ist.

Eine ähnliche Regelung müsste im Rahmen des NIS2UmsuCG in Bezug auf die Cybersicherheitspflichten der Betreiber der kritischen Anlagen, der Betreiber der besonders wichtigen Einrichtungen und der Betreiber der wichtigen Einrichtungen gefunden werden.

2. § 1 KRITIS-DachG – Nationale KRITIS-Resilienzstrategie

Zumindest ungewöhnlich ist, dass in § 1 nicht der Anwendungs- und Geltungsbereich des Gesetzes beschrieben wird,[2] sondern die Ankündigung der Erarbeitung einer Strategie zur Verbesserung der Resilienz kritischer Infrastrukturen. **Aus Gründen der Lesbarkeit und Systematik sollte diese Norm am Ende des Gesetzes verankert werden.** Im Idealfall sollte zudem eine Strategie erarbeitet sein, bevor ein Gesetz erarbeitet wird.

3. § 2 KRITIS-DachG-RefE – Begriffsbestimmungen

a. Allgemeines
Zunächst sollten die Begriffsbestimmungen alphabetisch geordnet werden. Dies vereinfacht die Lesbarkeit des Gesetzes deutlich.

Zudem werden im Folgenden Begriffe definiert, die ebenfalls im neuen BSIG[3] oder in der bisherigen BSI-Kritisverordnung (BSI-KritisV) definiert werden. Dies betrifft beispielsweise den Begriff „Betreiber kritischer Anlagen“, der ebenfalls in § 28 Abs. 5 BSIG definiert wird. Auf der anderen Seite wird der Begriff der Anlage bisher in § 1 Abs. 1 Nr. 1 BSI-KritisV definiert. **Es wird gefordert die maßgeblichen Definitionen nur einmal und eindeutig zu definieren. Zudem sollte, wenn eine Definition einheitlich im Kritis-DachG vorgenommen wird, in der Gesetzesbegründung darauf hingewiesen werden, woher der Begriff ursprünglich stammt.** So kann auf die bisherigen Gesetzgebungs- und Verordnungsmaterialien zur Auslegung der Begriffe deutlich einfacher zurückgegriffen werden.

Im Übrigen ist folgendes anzumerken:

b. Nr. 1 - Betreiber kritischer Anlagen
In Bezug auf den Betreiber einer kritischen Anlage liegt eine Doppelung vor. Der Begriff würde nunmehr in § 2 Nr. 1 Kritis-DachG, § 28 Abs. 5 BSIG und § 1 Abs. 1 Nr. 2 BSI-KritisV definiert. **Es wird eine einheitliche Definition an nur einer Stelle gefordert.**

Der bisher in der Kritis-Verordnung definierte Begriff des Betreibers hat in der Vergangenheit zu Abgrenzungsproblemen geführt. Insbesondere stellt sich die Frage, wer Betreiber einer Anlage innerhalb eines Konzerns ist. Häufig ist es so, dass aus rechtlichen und wirtschaftlichen Gründen die Konzernmutter bestimmenden Einfluss auf eine Anlage hatte, allerdings die Anlage tatsächlich von einem Tochterunternehmen betrieben wird.

Auch in Dienstleistungskonstellationen stellen sich ähnliche Fragestellungen. Häufig sind Betreiber von Rechenzentren selbst unter den maßgeblichen Schwellenwerten, betreiben aber

[2] Vgl. Handbuch der Rechtsförmigkeit, Rn. 362
[3] Diskussionspapier des BMI- Wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland, Fassung vom 03.07.2023.

die maßgebliche IT-Landschaft für den Betreiber einer kritischen Anlage. Insbesondere im Bereich der Smart Meter gibt es solche Konstellationen. Eine andere mögliche Konstellation ist der Fall, dass ein Betreiber einer kritischen Anlage Teile eines Serverraums bei einem Rechenzentrum mietet, das selbst die maßgeblichen Kritis-Schwellenwerte nicht überschreitet.

Weitere Fallgestaltungen stellen sich beim gesamten Komplex der Betriebsführung durch Dritte.[4] Auch bei einer Überwachung von mehreren Anlagen durch eine gemeinsame Leitstelle können Unklarheiten auftreten, wenn beispielsweise die Leitstelle isoliert gesehen die maßgeblichen Schwellenwerte nicht erreicht, aber die insgesamt überwachten Anlagen in Summe die Schwellenwerte erreichen.

Aufgrund der weitreichenden Konsequenzen der Betreibereigenschaft wird gefordert, nähere Ausführungen in der Gesetzesbegründung zu liefern, an welchen Kriterien sich genauer orientiert werden soll. Es muss klar sein, ob die rechtlichen, wirtschaftlichen oder tatsächlichen Umstände im Zweifel ausschlaggebend sind zur Bestimmung der Betreibereigenschaft. Hierfür muss zuvor in den Dialog mit den Betreibern eingetreten werden, um die Vielzahl der Gestaltungsmöglichkeiten sinnvoll klären zu können.

c. Nr. 2 – Anlage

Der Begriff der Anlage wird bisher in § 1 Abs. 1 Nr. 1 BSI-KritisV definiert und unterscheidet sich von der hier gewählten Definition. **Es wird eine einheitliche Definition an nur einer Stelle gefordert. Sollte aufgrund der unterschiedlichen Zielrichtung des NIS-2-Umsetzungsgesetzes und dem Kritis-DachG eine unterschiedliche Definition gewählt werden, so sollte auch ein unterschiedlicher Begriff genutzt werden.**

d. Nr. 3 – Kritische Anlage

Der Begriff der Kritischen Anlage wird im KRITIS-DachG in § 2 Nr. 3 i.V.m. § 4 definiert, während der gleiche Begriff im NIS2UmsuCG in § 2 Nr. 19 i.V.m. § 28 Abs. 3 BSIG definiert wird. **Es wird eine einheitliche Definition an nur einer Stelle gefordert. Im Übrigen wird auf die Ausführungen zu § 4 verwiesen.**

e. Nr. 4 – Kritische Dienstleistungen

Im Moment ist der Begriff der kritischen Dienstleistung in § 1 Abs. 1 Nr. 3 Kritis-Verordnung definiert. Es stellt sich zunächst das grundsätzliche Problem, dass es wiederum zu einer doppelten Definition des gleichen Begriffs kommen würde, wenn nicht gleichzeitig mit dem KRITIS-Dachgesetz auch die BSI-KritisV angepasst wird. Zudem unterscheiden sich die Definitionen. So grenzt die Definition in § 2 Nr. 4 KRITIS-DachG im Gegensatz zur Begriffsdefinition in der BSI-KritisV den Begriff nicht ein auf bestimmte Sektoren. Dies ist unlogisch, weil es nur um Dienstleistungen innerhalb der definierten Kritis-Sektoren gehen kann. **Es wird eine einheitliche Definition gefordert.**

Bisher wird der Begriff der kritischen Infrastruktur auf gesetzlicher Ebene in § 2 Abs. 10 BSIG

[4] Siehe hierzu näher: https://www.vku.de/themen/recht/artikel/betriebsfuehrung-durch-dritte/.

definiert. Zukünftig soll dieser Begriff im Begriff der kritischen Anlagen aufgehen. Allerdings verwenden verschiedenste gesetzliche Regelungen den Begriff der kritischen Infrastruktur im bisher verstandenen Sinne. Beispielhaft genannt seien §§ 17, 18 Zivilschutz- und Katastrophenhilfegesetz, § 55a Außenwirtschaftsverordnung, § 79 Abs. 3 TKG. Eine Anpassung dieser Begrifflichkeiten wird hier nicht vorgenommen, sondern soll anscheinend über das NIS 2-Umsetzungsgesetz erfolgen. Hier sind allerdings bereits nach kursorischer Durchsicht nicht alle Gesetze angepasst worden. **Es wird gefordert, dass der Bund alle Gesetze auf die neuen Begrifflichkeiten anpasst, soweit dies in seiner Gesetzgebungskompetenz steht.**

Ähnliches gilt auf Ebene der Landesgesetzgebung. So nimmt beispielhaft § 5a Niedersächsisches Katastrophenschutzgesetz Bezug auf die bisherige Begriffsdefinition der kritischen Infrastruktur und verknüpft Verpflichtungen hiermit. Auch auf kommunaler Ebene gibt es Regelungen, die auf den bisherigen Begriff der kritischen Infrastruktur referenzieren. **Auf den bestehenden Anpassungsbedarf sollte der Bund die Länder deutlich hinweisen, damit ein konsistenter Rechtsrahmen entsteht.**

f. Nr. 9 – Vorfall

Der Begriff ist des Vorfalls wird aus der CER-Richtlinie übernommen und ist äußerst weit bzw. unbestimmt. Hier braucht es für die Praxis ergänzende FAQs oder ähnliches. Anderenfalls ist insbesondere unklar, wann durch die Unternehmen Meldungen abgesetzt werden müssen.

Im Bereich der IT-Sicherheit hat das BSI beispielsweise FAQs zum IT-Sicherheitsvorfall veröffentlicht.[5] Diesem Beispiel sollte auch für den physischen Bereich gefolgt werden.

4. § 3 KRITIS-DachG – Zentrale Anlaufstelle; Zuständigkeiten; behördliche Zusammenarbeit

a. § 3 Abs. 2 KRITIS-DachG

In § 3 Abs. 2 KRITIS-DachG werden insbesondere die Aufsichtsbehörden des Bundes in Bezug auf das KRITIS-DachG festgelegt. Im Grundsatz soll das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) zuständig sein. Für bestimmte Sektoren werden abweichend von diesem Grundsatz wiederum Sektorbehörden als zuständig bestimmt.

Auffällig ist, dass der Sektor Energie anscheinend unter die Aufsicht des BBK fallen soll. Zumindest wird dieser Sektor in § 3 Abs. 2 S. 2 KRITIS-DachG nicht ausdrücklich von der grundsätzlichen Zuständigkeit des BBK ausgenommen. Dies ist nicht sinnvoll. Ähnlich wie im Sektor der Informationstechnik und Telekommunikation besteht im Energiesektor eine grundsätzliche Zuständigkeit der Bundesnetzagentur (BNetzA). Diese Zuständigkeit betrifft insbesondere den Bereich der IT-Sicherheit, weshalb in diesem Bereich die BNetzA und nicht das Bundesamt für Sicherheit in der Informationstechnik (BSI) zuständig ist (siehe bisher § 11 EnWG). Diese Zusammenarbeit hat sich bewährt, denn in der BNetzA besteht ein tiefes Verständnis der Aspekte der Sicherheit für den Sektor Energie, der auch für die Aufsicht im Bereich des KRITIS-DachG genutzt werden sollte. **Es wird deshalb gefordert, dass als zuständige Aufsichtsbehörde für den Sektor**

[5] https://www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/KRITIS-FAQ/FAQ-zur-Meldepflicht/faq-zur-meldepflicht_node.html

Energie die BNetzA bestimmt wird.

Formulierungsvorschlag:

§ 3 Zentrale Anlaufstelle; Zuständigkeiten; behördliche Zusammenarbeit

(2) Zuständige Behörde im Sinne des Artikels 9 Absatz 1 der Richtlinie (EU) 2022/2557 ist im Hinblick auf Aufgaben des Bundes das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. Abweichend von Satz 1 ist zuständige Behörde **in Bezug auf die Betreiber im Sektor Energie die Bundesnetzagentur,** in Bezug auf öffentliche Telekommunikationsnetze oder öffentlich zugängliche Telekommunikationsdienste die Bundesnetzagentur und für alle anderen Betreiber kritischer Anlagen im Sektor Informationstechnik und Telekommunikation das Bundesamt für Sicherheit in der Informationstechnik, in Bezug auf den Sektor Finanz- und Versicherungswesen die Bundesanstalt für Finanzdienstleistungsaufsicht sowie die weiteren Aufsichtsbehörden des Bundes nach Absatz 3 und im Hinblick auf Aufgaben der Länder die zuständigen Landesbehörden nach Absatz 5.

Unklar bleibt zudem, wer „die weiteren Aufsichtsbehörden des Bundes nach Absatz 3" sind. Dies muss klargestellt werden. Sollte davon ausgegangen werden, dass über diesen Verweis der Sektor Energie der BNetzA unterstellt wird, so ist dies nicht ausreichend. Vielmehr muss dies explizit in den Wortlaut der Norm aufgenommen werden.

b. § 3 Abs. 3 KRITIS-DachG

In § 3 Abs. 3 KRITIS-DachG wird explizit aufgeführt, für welche kritische Dienstleistungen der Bund für den Vollzug des KRITIS-DachG zuständig ist. Im Umkehrschluss bedeutet dies, dass für sämtliche hier nicht aufgeführten kritischen Dienstleistungen die Zuständigkeit des Vollzugs des KRITIS-DachG bei den Ländern liegt (so auch die Gesetzesbegründung). Diese Regelung ist neu und problematisch. **Es wird gefordert, dass der Vollzug des KRITIS-DachG auf Bundesebene angesiedelt wird.** Anderenfalls wird der Informationsfluss zwischen den Behörden nicht sichergestellt werden können und insbesondere Querverbundsunternehmen werden mit übermäßiger Bürokratie belastet.

aa. fehlender Informationsfluss zwischen den Behörden

Zum einen werden die Vorfälle weiterhin an die gemeinsame Meldestelle von BBK und BSI gemeldet (§ 12 KRITIS-DachG), was auch zu begrüßen ist. Wie hier die Länder für die Aufsicht an die entsprechenden Informationen kommen ist im Gesetz nicht weiter beschrieben. Es besteht trotz der allgemeinen Regelung in § 3 Abs. 7 KRITIS-DachG die große Gefahr, dass Informationen verlorengehen oder nicht rechtzeitig an der zuständigen Stelle ankommen. Bei der Vielzahl der involvierten Behörden auf Bundesebene und Landesebene kommt es zwangsläufig zu Reibungsverlusten beim Informationsaustausch.

Zudem werden sich aus etwaigen Vollzugsmaßnahmen der Länder wichtige Informationen hinsichtlich des bundeseinheitlichen Lagebilds ergeben. Auch hier besteht die Gefahr, dass die Informationen aus dem Vollzug des Gesetzes nicht hinreichend für die Erstellung des bundeseinheitlichen Lagebilds genutzt werden können.

Auch die Registrierung soll einheitlich bei der Registriermöglichkeit von BSI und BBK vorgenommen werden (§ 6 KRITIS-DachG), was ebenfalls zu begrüßen ist. Unklar bleibt auch hier, wie die Länder die entsprechenden Informationen bekommen.

bb. Ausufernde Bürokratie bei Querverbundsunternehmen

Besondere Probleme treten bei sogenannten Querverbundsunternehmen auf, also Unternehmen, die in mehreren Sektoren tätig sind. So ist es z.B. nicht ungewöhnlich, dass ein Stadtwerk sowohl Telekommunikationsnetze betreibt, als auch die Trinkwasserversorgung übernimmt und zudem in der Stromversorgung tätig ist. Es werden also Tätigkeiten erbracht, die teilweise durch die Bundesbehörden und teilweise durch die Landesbehörden überwacht werden. Dies ist mehr als misslich, da so ein einheitlicher Vollzug nur sehr schwierig sichergestellt werden kann und insbesondere die Unternehmen sich mit einer Vielzahl von Behörden sowohl auf der Bundes- als auch der Landesebene (vgl. § 3 Abs. 4, 5 KRITIS-DachG) abstimmen müssen. Sollte ein Unternehmen zudem in mehreren Bundesländern tätig sein, wird absehbar ein nochmals erhöhter bürokratischer Aufwand auf die Unternehmen zukommen. Wenn man bedenkt, dass auch die einzelnen Bundesländer noch zusätzlich ihre eigenen Kritis-Gesetze erlassen können (wie bereits heute im IT-Sicherheitsbereich teilweise praktiziert, siehe dazu die Kommentierung unter Nr. 5c), so entsteht ein Regulierungs- und Bürokratiedschungel, der kaum mehr zu durchblicken ist. Zielrichtung der Bundesregierung ist es jedoch Bürokratie abzubauen, wie der Entwurf des Bürokratieentlastungsgesetzes deutlich zeigt. Die Kritis-Regulierung in ihrer jetzigen Form bewirkt allerdings genau das Gegenteil. Zudem würden in den Ländern Parallelstrukturen aufgebaut werden müssen, was nicht ein ineffizienter Einsatz der knappen Personalressourcen bedeuten würde. Ferner wird der Aufbau von einheitlichen Managementsystemen innerhalb der Unternehmen fast unmöglich gemacht, sodass auch hierdurch vermehrte bürokratische Aufwände entstehen und die tatsächliche Sicherheit der Unternehmen leidet.

Entsprechend gelten diese Ausführungen für solche Betreiber, die gleichzeitig die Betriebsführung für Dritte übernehmen. Auf die Dienstleistungen der technischen Betriebsführer sind hunderte kleine und meist kommunale Stadtwerke in Deutschland angewiesen. Durch das gleichzeitige Ansetzen verschiedener landesrechtlicher Regelungen droht, dass aufgrund des anfallenden Mehraufwandes die technischen Betriebsführer ihre Dienstleistung diesen kommunalen Stadtwerken nicht mehr wirtschaftlich anbieten können.

c. § 3 Abs. 6 KRITIS-DachG

§ 3 Abs. 6 KRITIS-DachG zielt auf die Betreiber von kritischen Anlagen ab, die in mehreren Bundesländern tätig sind und eine kritische Dienstleistung erbringen, dessen Vollzug die Länder überwachen. In einem solchen Fall soll einheitlich das Land für den Vollzug zuständig sein, in dem sich der Hauptsitz des Unternehmens befindet.

Es stellt sich hier die Frage, wie der behördliche Vollzug bundeslandübergreifend sichergestellt wird. Wird beispielsweise eine Berliner Landesbehörde den Vollzug des KRITIS-DachG in Bayern überwachen, wenn der Hauptsitz des Unternehmens in Berlin ist aber die kritische Anlage potentiell Gefahren für das Land Bayern bedeutet? Auf welcher Rechtsgrundlage werden die Berliner Landesbehörden in Bayern tätig? Und was passiert, wenn Bayern ein eigenes KRITIS-Gesetz erlässt und diese Betreiber somit auch seinen Landesbehörden unterstellt?

Auch aus diesen Gründen wird gefordert, dass der Vollzug des KRITIS-DachG auf Bundesebene vorgenommen wird.

5. § 4 KRITIS-DachG - Anwendungsbereich; kritische Anlagen; Geltungsumfang

a. § 4 Abs. 1 KRITIS-DachG

§ 4 Abs. 1 KRITIS-DachG bildet im Prinzip die bisherige Logik aus dem IT-Sicherheitsrecht ab. Es ist dabei zu begrüßen, dass der Regelschwellenwert von 500.000 zu versorgenden Einwohnern bereits im Gesetz festgelegt wurde. Somit kann im Einzelfall zwar hiervon durch die noch erlassenden KritisV abgewichen werden, allerdings ist somit auch klar, dass die bisherige Logik aus der BSI-KritisV fortgeschrieben wird.

Die Definition in § 2 Abs. Nr. 3; § 4 KRITIS-DachG unterscheidet sich jedoch in der Formulierung von der parallelen Definition in § 2 Abs. 1 Nr. 18; § 28 Abs. 6 BSIG. **Es wird gefordert eine einheitliche Formulierung zu finden, die den Regelschwellenwert von 500.000 zu versorgenden Einwohnern bereits im Gesetz festschreibt.**

b. § 4 Abs. 2 KRITIS-DachG

§ 4 Abs. 2 KRITIS-DachG bricht mit der bisherigen Logik zur Bestimmung der Betreiber der kritischen Anlagen. Bisher wurden diese ausschließlich über die (BSI-)KritisV bestimmt. Zudem geschah dies nicht unterjährig, sondern ganz überwiegend einheitlich zum 1. April eines jeden Jahres. Über § 4 Abs. 2 KRITIS-DachG wird es dem Bundesinnenministerium ermöglicht, jederzeit (also auch unterjährig) ein Unternehmen als Betreiber einer kritischen Anlage zu bestimmen.

Problematisch ist dies insofern, als dass die so bestimmten Unternehmen ggf. keine Erfahrung mit der Umsetzung von (IT-)Sicherheitsanforderungen im Rahmen von Managementsystemen wie einem ISMS oder BCMS haben. Denn während im Grundsatz die bisherigen Betreiber von kritischen Infrastrukturen bereits Erfahrungen im Bereich der IT-Sicherheitsvorschriften sammeln konnten, ist dies für die im Einzelfall bestimmten Betreiber nicht der Fall. Kombiniert mit den sehr ambitionierten Fristen zur Umsetzung der Pflichten für die Betreiber nach § 4 Abs. 1 KRITIS-DachG (siehe hierzu die Kommentierung unter Nr. 8c), kann dies die Betreiber nach § 4 Abs. 2 KRITIS-DachG schnell überfordern.

Es wird deshalb gefordert, dass die Betreiber nach § 4 Abs. 2 KRITIS-DachG möglichst früh in diese Einzelfallentscheidung einbezogen werden. Im Gesetz sollte deshalb die vorherige und frühzeitige Anhörung des Unternehmens vor einer solchen Entscheidung festgeschrieben werden. Die allgemeinen Regeln (vgl. § 28 VwVfG) sehen dies zwar im Grundsatz auch vor, jedoch könnte hiervon im Einzelfall abgesehen werden.

Formulierungsvorschlag:

§ 4 Anwendungsbereich; kritische Anlagen; Geltungsumfang

(2) […] Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe teilt dem Betreiber der betreffenden kritischen Anlage mit, dass er den Verpflichtungen dieses Gesetzes unterliegt und fordert ihn zur Registrierung nach § 6 Absatz 1 auf. **Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe hört den Betreiber einer kritischen Anlage in jedem Falle frühzeitig vor der Entscheidung an und gibt ihm Gelegenheit, sich zu den für die Entscheidung erheblichen Tatsachen zu äußern.**

Zudem müssen diese Unternehmen bei der Umsetzung dieser Maßnahmen eng unterstützt und zusätzliche Umsetzungsfristen vorgesehen werden. Nach der Mitteilung der Betreibereigenschaft dürfen diese Unternehmen nicht alleine gelassen werden und ihnen muss zusätzlich Zeit gegeben werden, um die für sie vollkommen neue Pflichten umzusetzen.

Unklar sind weiterhin die Auswirkungen dieser Einzelfallentscheidung auf das NIS-2-Umsetzungsgesetz. In den dortigen Regelungen ist eine solche Einzelfallentscheidung zur Bestimmung von kritischen Anlagen nicht vorgesehen. **Es wird gefordert insoweit zwischen dem KRITIS-DachG und dem NIS-2-Umsetzungsgesetz Kohärenz herzustellen.**

c. § 4 Abs. 7 KRITIS-DachG

Gemäß § 4 Abs. 7 KRITIS-DachG bleiben andere bestehende Regelungen, die die Resilienz von Betreibern kritischer Anlagen zum Ziel haben, von diesem Gesetz unberührt. Hinzuweisen ist, dass dies auch die IT-Sicherheitskataloge nach dem EnWG betrifft, in denen die BNetzA im Energiebereich verbindliche und tiefgehende Anforderungen für die Betreiber festlegt (siehe § 11 Abs. 1a, 1b EnWG). **Wichtig ist, dass auch in Bezug zu den IT-Sicherheitskatalogen eine enge Abstimmung mit der BNetzA stattfindet, damit die IT-Sicherheitskataloge und das KRITIS-DachG einander nicht widersprechen.**

Keine Aussage trifft § 4 Abs. 7 KRITIS-DachG zum Verhältnis des KRITIS-DachG zu möglichen auf Länderebene noch zu erlassenden Gesetzen zur Stärkung der Resilienz von Betreibern von kritischen Anlagen. Dies ist folgerichtig, da aus Gründen der Gesetzgebungskompetenz der Bund die Ländergesetzgebung nicht vollends ausschließen kann. Dies führt aber in der Praxis zu ganz erheblichen Problemen.

Ein konkretes Beispiel hierfür war die unterschiedliche Ausstellungspraxis von KRITIS-Bescheinigungen durch die Landkreisämter bzw. Ministerien in den unterschiedlichen Bundesändern. Nur mit diesen Bescheinigungen war es für die Mitarbeiter von kritischen Infrastrukturen während der Corona-Pandemie möglich, trotz Ausgangssperre an den Arbeitsplatz zu kommen. In vielen Fällen war auch unklar, wer diese KRITIS-Bescheinigungen ausstellt. Zukünftig könnten diese Bescheinigungen z.B. bei einem Blackout und den darauf möglicherweise folgenden Straßensperren notwendig werden.

Im Bereich der IT-Sicherheitsgesetzgebung sind auf Ebene der Bundesländer teilweise bereits eigene IT-Sicherheitsgesetze erlassen worden (siehe z.B. das Hessisches IT-Sicherheitsgesetz oder die Regeln zur IT-Sicherheit im Bayerischen Digitalgesetz). Ähnliches ist wohl auch für den Bereich der physischen Sicherheit zu erwarten. Es besteht die Gefahr, dass die Regelungen zur physischen Sicherheit in jedem Bundesland zusätzlich zum BSIG mit zusätzlichen Pflichten und eigenen Aufsichtsbehörden reguliert werden. Im Ergebnis müssten deutschlandweit tätige Unternehmen 17 verschiedene gesetzliche Regelungen beachten und sich mit einer Vielzahl an verschiedenen Aufsichtsbehörden abstimmen (siehe zu dem ähnlich gelagerten Problem beim Vollzug des KRITIS-DachG die Ausführungen zu Nr. 4). Es würde somit zu einer ähnlichen Situation wie im Datenschutz kommen, wo auch jedes Bundesland seine eigenen Regelungen und Aufsichtsbehörden hat.

Vor diesem Hintergrund wird gefordert, dass sich der Bund mit den Ländern auf einheitliche Regelungen einigt, wie gesetzliche Vorgaben auf der Landesebene und Landkreisebene ausgestaltet werden. Es sollte ein Mustergesetz erarbeitet werden, an dem sich die Länder eng orientieren. Perspektivisch sollte überdacht werden, ob nicht der Bund die alleinige Gesetzgebungskompetenz zur Regulierung der durch das KRITIS-DachG (und das NIS2UmsuCG) erfassten Unternehmen bekommt. Eine Zentralisierung der Vorgaben erscheint dringend geboten.

d. § 4 Abs. 8 KRITIS-DachG

Positiv zu bemerken ist, dass nach § 4 Abs. 8 KRITIS-DachG ein Betreiber einer kritischen Anlage die Anforderungen aus §§ 9 – 11 KRITIS-DachG auch dann erfüllen kann, wenn er aufgrund von Verpflichtungen aus anderen öffentlich-rechtlichen Vorschriften für einen anderen Anlass bereits gleichwertige, Risikoanalysen und -bewertungen vorgenommen hat (bzw. Maßnahmen umgesetzt oder Dokumente erstellt hat). Dies soll sicherlich die Risikoanalyse und Risikobewertung im Rahmen der Pflichten nach dem IT-Sicherheitsrecht betreffen (z.B. Risikoanalysen und Risikobewertungen innerhalb eines ISMS). **Es sollte jedoch explizit in der Gesetzesbegründung festgestellt werden, dass hiermit insbesondere die Risikoanalyse und Risikobewertung innerhalb eines ISMS gemeint ist.**

Unklar ist die Aussage von § 4 Abs. 8 S. 2 KRITIS-DachG zur Äquivalenzprüfung. Es stellt sich die Frage, ob diese Äquivalenzprüfung zwangsläufig vorgenommen und positiv beschieden werden muss, bevor bestehende Risikoanalysen und Risikobewertungen berücksichtigt werden können bei der Erfüllung der Pflichten nach §§ 9 – 11 KRITIS-DachG. Sollte dies der Fall sein, so wäre

dies keine sinnvolle Regelung. Grob geschätzt werden einige tausend Unternehmen bereits auf Grund ihrer Verpflichtungen als Betreiber einer kritischen Infrastruktur eine Risikoanalyse und Risikobewertung vorgenommen haben. Diese zukünftig als Betreiber von kritischen Anlagen bezeichneten Betreiber werden überwiegend ihre Risikoanalyse und Risikobewertung aus dem Bereich der IT-Sicherheit in den Bereich des KRITIS-DachG einbringen wollen. Es ist nicht ersichtlich, wie und in welcher Zeit die zuständigen Aufsichtsbehörden hierüber entscheiden könnten. Es ist zu vermuten, dass dies die zuständigen Behörden personell überfordert würde. **Es wird deshalb gefordert klarzustellen, dass die Äquivalenzprüfung nicht zwangsläufig vorgenommen werden muss, um die vorgenommene Risikobetrachtung aus dem IT-Sicherheitsbereich auch im Bereich des KRITIS-DachG zu verwenden. Vielmehr sollte die Äquivalenzprüfung als zusätzliche Möglichkeit festgelegt werden, um Rechtssicherheit über diese Frage erlangen zu können. Hierfür müssen aber klare Fristen für die Behörde gesetzt werden, bis wann mit einer Entscheidung über die Äquivalenz zu rechnen ist.**

Unklar ist zudem das Verhältnis von § 4 Abs. 8 KRITIS-DachG zu den Nachweisvorschriften nach § 11 KRITIS-DachG. Nach § 11 Abs. 1 KRITIS-DachG können behördenintern die Nachweise nach § 39 BSIG angefordert werden, um die Erfüllung der Pflichten nach § 10 KRITIS-DachG zu überprüfen. Muss hierfür nun eine vorherige Äquivalenzprüfung erfolgt sein? Schließt eine vorherige erfolgreiche Äquivalenzprüfung weitere Nachweispflichten nach § 11 KRITIS-DachG aus? **Es wird gefordert, das Verhältnis der Äquivalenzprüfung in § 4 Abs. 8 KRITIS-DachG zu § 11 KRITIS-DachG klarer herauszuarbeiten.**

Formulierungsvorschlag

§ 4 Anwendungsbereich; kritische Anlagen; Geltungsumfang

(8) [S. 1, 2…] **Die Vorlage der bestehenden Risikoanalyse und Risikobewertung sowie Dokumente und Maßnahmen zur Stärkung der Resilienz durch den Betreiber der kritischen Anlage nach S. 2 ist freiwillig und lässt die Anrechnungsmöglichkeit gemäß § 11 unberührt. Werden die Unterlagen nach S. 2 vorgelegt, so unterrichtet die zuständige Behörde den Betreiber über das Ergebnis innerhalb von zwei Monaten nach Eingang der Unterlagen. Erfolgt bis zu diesem Zeitpunkt keine Unterrichtung des Betreibers, so gilt die Äquivalenzprüfung als positiv beschieden.**

6. § 6 Registrierung der kritischen Anlage und Ansprechpartner; Geltungszeitpunkt

Positiv zu bemerken ist zunächst, dass die Registrierung an einer einheitlich zwischen BBK und BSI betriebenen Registrierungsstelle vorgenommen werden kann. Hierdurch werden Doppelmeldungen vermieden und ein weniger an Bürokratie erzielt. Dies gilt auch im Falle einer sonstigen Vollzugszuständigkeit von Landesbehörden. Wichtig ist, dass etwaige Landesbehörden ebenfalls auf diese Informationen zugreifen können, damit in jeder Behörde ein einheitlicher Kenntnisstand besteht.

Allerdings springen auch hier wieder Doppelregulierungen für Betreiber von kritischen Anlagen in Bezug auf das NIS2UmsuCG ins Auge. Die Pflicht zur Registrierung und Benennung der Kontaktstelle, sowie die Möglichkeit der zuständigen Behörde die Registrierung selbst vorzunehmen, sind zum einen in § 6 KRITIS-DachG, als auch in § 33 BSIG geregelt. Hierbei überschneiden sich die Regeln, ohne dass das Verhältnis zueinander klar ist. So haben z.B. sowohl das BBK als auch das BSI die Möglichkeit, einen Betreiber einer kritischen Anlage zwangsweise zu registrieren (vgl. § 6 Abs. 2 - 4 KRITIS-DachG und § 33 Abs. 4 BSIG). Ferner werden z.B. auch unterschiedliche Anforderungen an die Registrierung selbst aufgestellt (vgl. die Anforderungen aus § 31 Abs. 1 BSIG iVm. der Möglichkeit der ergänzenden Ausgestaltung in Abs. 6 auf der einen Seite und die Anforderungen aus § 8 Abs. 1 KRITIS-DachG iVm. der Möglichkeit der ergänzenden Ausgestaltung in Abs. 7 KRITIS-DachG). Auch findet sich die Passage der einheitlichen Kontaktstelle nur in § 6 Abs. 1 KRITIS-DachG und nicht in § 33 BSIG.

Es wird gefordert, dass die Registrierungspflichten für Betreiber von kritischen Anlagen aus dem KRITIS-DachG und dem BSIG eindeutig und übergreifend in einer Norm geregelt werden. Sollten die Pflichten in zwei verschiedenen Normen geregelt werden, so müssen sie aufeinander abgestimmt sein und dürfen sich nicht widersprechen.

Nach § 6 Abs. 1 KRITIS-DachG ist ein Betreiber einer kritischen Anlage verpflichtet, sich spätestens drei Monate nachdem er erstmals oder erneut als Betreiber einer kritischen Anlage gilt, zu registrieren. Ein Betreiber gilt dann als Betreiber einer kritischen Anlage, wenn sich dies aus der KritisV (inklusive der dort vorgesehenen Übergangsfristen) für ihn ergibt oder er im Einzelfall bestimmt wird (vgl. § 4 KRITIS-DachG). Geht man nun davon aus, dass die KritisV bereits Mitte 2025 verabschiedet wird, so würden die Betreiber nach Ablauf der Übergangsfristen aus der KritisV Ende 2025 als Betreiber von kritischen Anlagen gelten. Es ist jetzt unklar, ob die dreimonatige Frist schon zu diesem Zeitpunkt anfängt zu laufen. Dies würde dazu führen, dass mit in Kraft treten des § 6 KRITIS-DachG zum 17.07.2026 (siehe Art. 3 Abs. 2 KRITIS-DachG) gleichzeitig die Registrierung vorliegen müsste. Die drei monatige Übergangsfrist wäre also vor dem in Kraft treten des § 6 KRITIS-DachG bereits abgelaufen. Für eine solche Sichtweise spricht wohl Art. 6 Abs. 1 CER-Richtlinie, da danach die Mitgliedsstaaten bis zum 17.07.2026 die kritischen Einrichtungen (bzw. in Deutschland die kritischen Anlagen) ermittelt haben müssen. Diese Sichtweise wird in der Stellungnahme dem Zeitstrahl zu Grunde gelegt.

Eine andere Interpretation wäre, dass erst mit in Kraft treten des § 6 KRITIS-DachG am 17.07.2026 die dreimonatige Frist zur Registrierung anfangen würde zu Laufen. Somit hätten die Betreiber einen weiteren Übergangszeitraum bis zum 17.10.2026.

Es wird gefordert eindeutig festzulegen, ab wann spätestens die (Erst-)Registrierung durch die Betreiber vorgenommen sein muss. Hierbei muss ein ausreichender Zeitraum zwischen in Kraft setzen der KritisV und der Pflicht zur Registrierung bestehen. Zudem müssen wohl spezielle Regelungen getroffen werden für den Fall, dass eine Einzelfallentscheidung zu einer Betreibereigenschaft führt (vgl. § 4 Abs. 2 KRITIS-DachG).

Der Begriff des Betreibers der kritischen Infrastruktur soll in den Begriff des Betreibers der kritischen Anlage überführt werden. Zudem sollen die Begriffe der kritischen Anlagen im NIS2UmsuCG und im KRITIS-Dachgesetz wohl deckungsgleich erfolgen. In Bezug auf die kritischen Anlagen wären die Adressaten des NIS 2-Umsetzungsgesetzes und des KRITIS-DachG somit ebenfalls deckungsgleich. **Da sich die Betreiber der kritischen Anlagen (und zukünftig die Betreiber der kritischen Anlagen) bereits nach aktuellen BSIG registriert haben, so sollte diese Registrierung übertragen werden in das Register nach dem KRITIS-DachG.** Eine eigenständige Registrierung der Betreiber der kritischen Anlagen wäre nicht notwendig. Es sollte lediglich eine Mitteilung des BBK an die Betreiber der kritischen Anlage über die erfolgte Übertragung der Betreibereigenschaft in das gemeinsame Register erfolgen. So werden Doppelaufwände für die Unternehmen vermieden, zu denen es unweigerlich bei einer erneuten Registrierung kommen würden.

7. § 8 KRITIS-DachG - Nationale Risikoanalysen und Risikobewertungen

In § 8 KRITIS-DachG wird die nationale Risikoanalyse und Risikobewertung beschrieben. Dies soll durch die jeweils zuständigen Bundes- oder Landesministerien geschehen. Eine Beteiligung der Wirtschaftsvertreter/Betreiber der kritischen Anlagen ist allerdings nicht vorgeschrieben. Dies ist unverständlich. **Im KRITIS-DachG muss festgelegt werden, dass die nationale Risikoanalyse und Risikobewertung unter Beteiligung der Wirtschaftsvertreter stattfindet.** So kann die behördliche Sicht mit den Praxiserfahrungen gespiegelt und um spezielle Kenntnisse aus den einzelnen Sektoren und Branchen ergänzt werden. Art. 4 Abs. 1 CER-Richtlinie legt eine solche Beteiligung den Mitgliedsstaaten ausdrücklich nahe.

Formulierungsvorschlag

§ 8 Nationale Risikoanalysen und Risikobewertungen

(1) Die für die jeweiligen kritischen Dienstleistungen nach § 3 Absatz 3 und 5 zuständigen Bundesministerien und Landesministerien führen **nach Anhörung von Vertretern der betroffenen Betreiber und Einrichtungen und der betroffenen Wirtschaftsverbände** alle vier Jahre oder auf Veranlassung und erstmalig bis 17. Januar 2026 für die auf der Grundlage der Rechtsverordnung nach § 16 Absatz 1 bestimmten kritischen Dienstleistungen nationale Risikoanalysen und Risikobewertungen durch, die mindestens Folgendes berücksichtigen: […]

Weiterhin ist festzulegen, wer unter welchen Voraussetzungen Veranlassung dazu geben kann, eine Risikoanalyse und Risikobewertung vor Ablauf der vier Jahre anzuordnen. Innerhalb von vier Jahren sind viele Änderungen der Realität denkbar, die eine Anpassung zwingend erforderlich machen können. So gab es vor vier Jahren keine Pandemie und keinen russischen

Angriffskrieg. Es muss klar sein, dass unter solchen Voraussetzungen die nationale Risikoanalyse und Risikobewertung zeitnah angepasst werden. Hierauf sind die Betreiber der kritischen Anlagen in ihrer eigenen Risikoanalyse und Risikobewertung angewiesen.

Nach § 8 Abs. 5 KRITIS-DachG stellt das BBK den Betreibern der kritischen Anlagen die für sie wesentlichen Elemente der nationalen Risikoanalysen und Risikobewertungen zur Verfügung. Es wird jedoch nicht festgeschrieben, bis wann dies geschieht. Da die Betreiber der kritischen Anlagen jedoch für ihre eigene Risikoanalyse und Risikobewertung auf die nationale Risikoanalyse und Risikobewertung angewiesen sind, muss dies klargestellt werden. Je später die Übermittlung erfolgt, desto weniger Zeit haben die Betreiber, um ihre Pflichten zu erfüllen. **Es wird deshalb gefordert, dass den Betreibern innerhalb von einem Monat nach Abschluss der nationalen Risikoanalyse und Risikobewertung die für sie wesentlichen Elemente zur Verfügung gestellt werden. Zudem muss geklärt werden, wie Betreiber an diese Informationen kommen, wenn sie z.B. erst im Laufe des Jahres 2027 (ggf. durch Einzelfallentscheidung nach § 4 Abs. 2 KRITIS-DachG) Betreiber einer kritischen Anlage werden.**

Formulierungsvorschlag

§ 8 Nationale Risikoanalysen und Risikobewertungen

(5) [S.1] **Innerhalb eines Monats nach Vorliegen der nationalen Risikoanalyse und Risikobewertung werden den Betreibern der kritischen Anlagen die für sie wesentlichen Elemente zur Verfügung gestellt.**

8. Übergreifendes zu den Pflichten aus §§ 9 – 12 KRTIS-DachG

Die §§ 9 – 12 KRITIS-DachG legen die Hauptpflichten der Betreiber der kritischen Anlagen fest. Hierbei ist auf folgende Aspekte hinzuweisen, die sich nicht konkret an einer einzelnen Norm festmachen lassen, sondern im Gesamtzusammenhang gesehen werden müssen.

a. Abgrenzung staatliche Schutzpflichten und Pflichten der Unternehmen

Das KRITIS-DachG legt fest, dass die Unternehmen in ihrer Risikoanalyse und Risikobewertung nach § 9 Abs. 1 Nr. 1 i.V.m. § 8 Abs. 1 Nr. 1c KRITIS-DachG insbesondere hybride Bedrohungen und andere feindliche Bedrohungen, einschließlich terroristischer Straftaten Rechnung tragen müssen. Auf Grund dieser Risikoanalyse und Risikobewertung müssen die Betreiber der kritischen Anlagen gemäß § 10 Abs. 1 KRITIS-DachG geeignete und verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen zur Gewährleistung ihrer Resilienz (bzw. ihrer kritischen Dienstleistung) treffen. Diese der CER-Richtlinie nachgebildete Normen berühren in letzter Konsequenz das Grundverständnis der Aufgabenverteilung zwischen Staat und Gesellschaft bzw. Privatwirtschaft. Es stellt sich die grundsätzliche Frage, welche Schutzpflichten der Staat gegenüber seinen Bürgern hat und welche dieser Pflichten faktisch auf die

Betreiber der kritischen Anlagen verlagert werden können. In der rechtswissenschaftlichen Literatur wird dies unter dem Begriff der „Verantwortungsteilung zwischen Staat und Gesellschaft“ diskutiert. Dabei ist als Ausgangspunkt anerkannt, dass die Gewährleistung innerer und äußerer Sicherheit dem Staat und seinen Organen obliegt.[6]

Die folgenden Beispiele dürften das Spannungsverhältnis deutlich machen und zeigen zwei Extreme des Kontinuums auf. An einem Ende des Kontinuums müssen kritische Anlagen davor geschützt werden, dass diese nicht durch Teenager im jugendlichen Übermut beschädigt oder zerstört werden. Diese Pflicht liegt unzweifelhaft bei den Betreibern der kritischen Anlagen und wird z.B. durch das Aufstellen von Zäunen und eine entsprechende Überwachung sichergestellt. Auf der anderen Seite des Kontinuums steht der Schutz von kritischen Anlagen vor Anschlägen durch von feindseligen Staaten finanzierte Terrorzellen, die im Besitz eines Panzers sind. Es dürfte auf der Hand liegen, dass die Abwehr solcher Gefahren nicht in der Verantwortung der Betreiber der kritischen Anlagen liegt. Vielmehr greift hier die staatliche Schutzpflicht, entsprechende Abwehrmaßnahmen vorzunehmen.

Es wird gefordert, gesetzlich eindeutig auszuschließen, dass die Betreiber der kritischen Anlagen für die Abwehr von hochprofessionellen, staatlich gesteuerten Angriffen zuständig sind. Zudem wird gefordert, mit den Betreibern der kritischen Anlagen eine grundsätzliche Diskussion zu führen, welche Risiken genau nur durch den Staat übernommen werden können und welche Risiken durch die Betreiber der kritischen Anlagen übernommen werden sollen. Es muss für die Betreiber klar sein, ob sie bestimmte in der Risikoanalyse und Risikobewertung identifizierte und bewertete Risiken auf Grund ihres Risikoappetits akzeptieren können und so in letzter Konsequenz keine Maßnahmen zu deren Behandlung treffen. Insbesondere zur Risikoakzeptanz fehlen bisher jegliche Ausführungen im Gesetz. Dies dürfte schwerlich die Anforderung an „eine klare und eindeutige gesetzgeberische Aussage“ erfüllen, die nach dem Bundesverwaltungsgericht[7] notwendig ist, um staatliche Schutzpflichten auf privatwirtschaftlich strukturierte Unternehmen zu übertragen zu können.

Eng hiermit verwandt ist die Pflicht in § 9 Abs. 1 Nr. 2 KRITIS-DachG, die Abhängigkeiten anderer Sektoren von der Erbringung der eigenen kritischen Dienstleistung zu betrachten. Insbesondere im Bereich der Energieversorgung bestehen Abhängigkeiten zu sämtlichen Sektoren, da jeder Sektor auf die Stromversorgung ganz unmittelbar angewiesen ist. Faktisch würden die Risiken ins Unendliche reichen können (z.B. europaweiter Stromausfall auf Grund von Kaskadeneffekten). Im IT-Sicherheitsgesetz wurden diese Effekte bisher mit gutem Grund ausgeblendet, da sonst keine wirtschaftliche Betrachtung der Risiken und der zu ergreifenden Maßnahmen möglich sind. Es stellt sich somit wiederum die Frage nach der Möglichkeit der Risikoakzeptanz durch die Unternehmen. **Auch hierüber muss eine grundsätzliche Diskussion mit den Betreibern der kritischen Anlagen geführt werden.**

[6] Huerkamp, RdE 2016, 280.
[7] BVerwG, Urteil vom 4. Oktober 1985 – 4 C 76/82 –, Rn. 22, juris; Huerkamp, RdE 2016, 280, 281.

b. Refinanzierung

Unabhängig von der Frage, welche Pflichten weiterhin vom Staat zu erfüllen sind und welche Pflichten durch die Betreiber zu erfüllen sind, steht bereits jetzt fest, dass die Erfüllung der Pflichten für die Betreiber sehr kostspielig werden kann. Genaue Aussagen können noch nicht getroffen werden, weil die Adressaten des Gesetzes und die konkret von den Unternehmen zu behandelnden Risiken noch ungeklärt sind. Klar ist jedoch, dass sämtliche ergriffenen Maßnahmen durch die Unternehmen refinanziert werden müssen. Die Refinanzierungsmöglichkeiten unterscheiden sich zwischen den verschiedenen Sektoren, weshalb diese im Folgenden getrennt voneinander betrachtet werden. Zudem können innerhalb der Sektoren teilweise regulierte und unregulierte Bereiche unterschieden werden. Während im unregulierten Bereich die Preise der Unternehmen grundsätzlich frei durch die Unternehmen festgelegt werden und sich die Preise nach Angebot und Nachfrage richten, sind im regulierten Bereich die Unternehmen in ihrer Preissetzung nicht frei. Vielmehr müssen sie sich nach den Vorgaben der Regulierungsbehörden richten.

aa. Energiewirtschaft

Insbesondere beim Netzbetrieb innerhalb der Energiewirtschaft handelt es sich um einen **regulierten Bereich**. Refinanziert werden die Netze über die sogenannten Netzentgelte für den Zugang zu den Energienetzen. Die zulässige Höhe der Netzentgelte wird über die sogenannte Anreizregulierung ermittelt. Die Anreizregulierung erfolgt dabei in 4 Schritten[8]:

In einem ersten Schritt wird das Ausgangsniveau durch die Kostenprüfung[9] nach Vorgaben der Netzentgeltverordnungen ermittelt. Grundlage der Kostenprüfung sind die handelsrechtlichen Jahresabschlüsse bzw. die für den Netzbereich relevanten Tätigkeitsabschlüsse des letzten abgeschlossenen Geschäftsjahres.

Die im Ausgangsniveau enthaltenen Kosten werden in einem zweiten Schritt in Kostenkategorien aufgeteilt (vgl. § 11 Anreizregulierungsverordnung):

- dauerhaft nicht beeinflussbare Kosten und
- grundsätzlich beeinflussbare Kosten

[8] Siehe näher zu den Netzentgelten und der Anreizregulierung: https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Netzentgelte/Anreizregulierung/start.html; https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Netzentgelte/Anreizregulierung/WesentlicheElemente/start.html;
[9] Siehe näher zur Kostenprüfung: https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Netzentgelte/Anreizregulierung/WesentlicheElemente/Netzkosten/Netzkostenermittlung_node.html

Die dauerhaft nicht beeinflussbaren Kosten sind zwar Bestandteil der Erlösobergrenze, gehen aber nicht in den Effizienzvergleich ein. Da somit keine Ineffizienzen abzubauen sind, gehen diese Kosten vollständig in die Erlösobergrenzen ein. Darüber hinaus erlauben Änderungen an den dauerhaft nicht beeinflussbaren Kosten die jährliche Anpassung der Erlösobergrenzen innerhalb einer Regulierungsperiode, wodurch eine unmittelbare Refinanzierung ermöglicht wird.

Aufgrund des kürzlich ergangenen EUGH-Urteils[10] zur Unabhängigkeit der Regulierungsbehörden obliegt es der Bundesnetzagentur, bestimmte Kosten als nicht dauerhaft/nicht beeinflussbar anzuerkennen, beziehungsweise eine etwaige Anerkennung durch Anpassung der Anreizregulierungsverordnung zu ermöglichen. **Da es sich bei den durch die Anforderungen des KRITIS-Dachgesetzes um gesetzlich mandatierte Investitionen handelt, fordert der VKU die Einordnung der dadurch entstehenden Kosten als dauerhaft nicht beeinflussbar**. Dies erscheint insbesondere vor dem Hintergrund sinnvoll, dass sicherheitsrelevante Investitionen keinem besonderen Effizienzdruck unterliegen sollten, da dadurch ggf. die Sicherheit der ergriffenen Maßnahmen gefährdet wird. Darüber hinaus stehen diese vorgesehenen, verpflichtenden Investitionen auch im Kontext weiterer unerlässlicher, teilweise ebenfalls gesetzlich vorgeschriebener Investitionen seitens der Netzbetreiber im Rahmen der Energiewende, bspw. in den Smart Meter Rollout, die Wärmewende oder den vorausschauenden Netzausbau. Alle zusätzlichen Kosten für die Netzbetreiber, die nicht vollständig und zeitnah refinanziert werden können, bremsen andere Investitionen potenziell aus.

Da das KRITIS-Dachgesetz der BNetzA keine Vorgaben bezüglich der Kostenanerkennung machen kann, fordert der VKU eine Festlegungsermächtigung im Gesetz zu verankern, die die Möglichkeit der Anerkennung als dauerhaft nicht beeinflussbare Kosten explizit einräumt. Hierbei kann sich an die Formulierung des § 118 Abs. 46e EnWG angelehnt werden.

Formulierungsvorschlag

§ 19a – Anerkennung von dauerhaft nicht beeinflussbaren Kosten

Die Bundesnetzagentur kann durch Festlegung nach § 29 Absatz 1 EnWG Regelungen für die Anerkennung der den Betreibern von kritischen Anlagen im Bereich der Stromverteilung entstehenden Kosten nach dem KRITIS-DachG treffen, die von einer Rechtsverordnung nach § 21a EnWG in Verbindung mit § 24 EnWG oder von einer Rechtsverordnung nach § 24 EnWG abweichen oder diese ergänzen. Sie kann dabei insbesondere entscheiden, dass Kosten oder Kostenanteile als dauerhaft nicht beeinflussbar angesehen werden.

Aber auch im **unregulierten Bereich** ist es wichtig, die Refinanzierungsmöglichkeiten zu bedenken. Sind die Kosten für die Umsetzung der Maßnahmen nach dem KRITIS-DachG besonders teuer, so wird sich dies in den Preisen an die Kunden wiederspiegeln. Dies gilt insbesondere im

[10] EuGH, Urteil vom 02.09.2021, Rs. C-718/18.

Bereich der Stromerzeugung. Werden zu hohe Anforderungen an die Betreiber festgelegt, so werden diese die Kosten in ihre Preise einbeziehen und an die Verbraucher und Industriekunden weitergeben. In der Folge würde der Strompreis noch weiter steigen. **Da der hohe Strompreis bereits jetzt ein volkswirtschaftliches Problem darstellt, sollte hier mit Augenmaß vorgegangen werden.** Verschärft wird das Problem dadurch, dass die Unternehmen hohe Investitionskosten über Fremdkapital vorfinanzieren müssten. Da es auch eine Zinswende gegeben hat, würden sich die Kapitalkosten zusätzlich im Strompreis wiederfinden.

bb. Wasser- und Abwasserwirtschaft

Die Abwassergebühren werden nach den Kommunalabgabengesetzen der Länder erhoben. Die Gebühren dürfen dabei im Grundsatz höchstens so bemessen werden, dass die nach betriebswirtschaftlichen Grundsätzen insgesamt ansatzfähigen Kosten der Einrichtung gedeckt werden (vgl. z.B. § 14 Kommunalabgabengesetz Baden-Württemberg). Hierbei besteht zwischen den verschiedenen Bundesländern häufig eine Diskrepanz, welche Kosten für die Erhöhung der Sicherheit als notwendige Kosten anzuerkennen sind und dementsprechend in die Gebührenkalkulation einbezogen werden können. Dies ist insbesondere deshalb problematisch, da im Bereich der Sicherheit die Motivation dahingehend gesetzt werden sollte, nicht nur das absolute Minimum an Maßnahmen umzusetzen, sondern ggf. auch freiwillig ein höheres Sicherheitsniveau zu erreichen. Insbesondere müssen hierbei auch etwaige Kapitalkosten zur Finanzierung der Sicherheitsmaßnahmen ansatzfähig sein. **Es wird gefordert, dass der Bund auf die Länder zugeht und eine einheitliche Lösung abstimmt.** Dies dient der gesamtgesellschaftlichen Sicherheit der Bundesrepublik Deutschland.

cc. Abfallwirtschaft

Für die Abfallwirtschaft gilt das zur Abwasserwirtschaft zuvor Ausgeführte.

c. Zeitliche Vorgaben für die Pflichterfüllung der Betreiber

Das KRITIS-DachG folgt einer bestimmten zeitlichen Logik der Pflichtenabfolge. Ausführlich wird diese im Zeitstrahl in **Anlage 1** dieser Stellungnahme dargestellt. Grob lässt sich die Pflichtenfolge wie folgt beschreiben:

- Nationale KRITIS-Strategie und nationale Risikoanalyse und Risikobewertung (17.01.2026)
- Mitteilung der wesentlichen Elemente der nationalen Risikoanalyse und Risikobewertung an die Betreiber (offen wann)
- Pflichten der Betreiber nach KRITIS-DachG treten in Kraft (17.07.2026)
- Registrierung als kritische Anlage spätestens drei Monate nach Vorliegen kritischer Anlage (voraussichtlich ebenfalls am 17.07.2026, da die neue KritisV wohl mehr als drei Monate vor diesem Datum beschlossen wird)
- Risikoanalyse und Risikobewertung durch Betreiber; 9 Monate nach Registrierung (17.04.2027)
- Resilienzmaßnahmen und Resilienzplan; Nachweise; Meldewesen; 10 Monate nach Registrierung (17.05.2027)

Zunächst wird es Probleme geben, wenn die nationale Risikoanalyse und Risikobewertung nicht rechtzeitig vorliegt oder die wesentlichen Elemente den Betreibern nicht schnellst möglichst mitgeteilt werden. Die Betreiber sind für ihre eigene Risikoanalyse und Risikobewertung auf die Kenntnis der nationalen Risikoanalyse und Risikobewertung angewiesen. Die Frist der Betreiber ist allerdings nicht daran gekoppelt ob/wann sie den Inhalt der nationalen Risikoanalyse und Risikobewertung kennen, sondern nur an ihre Registrierung als Betreiber einer kritischen Anlage. Sollte nunmehr die nationale Risikoanalyse und Risikobewertung nicht zum 17.01.2026 vorliegen oder den Betreibern mitgeteilt werden, so würde der hierfür zur Verfügung stehende Zeitraum verkürzt werden. **Aus diesem Grund eine entsprechende zeitliche Abhängigkeit von nationaler Risikoanalyse und Risikobewertung mit der Risikoanalyse und Risikobewertung der Betreiber gefordert** (siehe näher die Kommentierung unter Nr. 9 und 10).

Es ist nicht klar, ab wann die Pflicht zur Registrierung besteht. In dem Zeitstrahl der Stellungnahme wird vom 17.07.2026 ausgegangen. Man kann dies aber auch anders sehen und den spatest möglichen Zeitpunkt der Registrierung als den 17.10.2027 verstehen (siehe näher die Kommentierung unter Nr. 6).

Ferner ist die im Moment vorgesehen Pflichtenreinfolge von Risikoanalyse und Risikobewertung durch die Betreiber und dem Treffen von Resilienzmaßnahmen unmöglich, falls das Treffen der Resilienzmaßnahmen umfassend verstanden wird. Die Betreiber treffen Resilienzmaßnahmen, nachdem sie ihre eigene Risikoanalyse und Risikobewertung vorgenommen haben. In der vorgesehenen zeitlichen Abfolge haben die Betreiber nach ihrer eigenen Risikoanalyse und Risikobewertung einen Monat Zeit, um die Resiliezmaßnahmen „zu treffen“. Falls Resilienzmaßnahmen nur dann getroffen wurden, wenn sie vollständig umgesetzt wurden, so ist dies unmöglich für die Betreiber (siehe näher die Kommentierung unter Nr. 10a).

Insgesamt wird gefordert, die zeitliche Reinfolge der Pflichten in enger Abstimmung mit den Betreibern festzulegen. Anderenfalls werden Pflichten so festgelegt, dass sie zeitlich für die Betreiber unmöglich zu erfüllen sind. **Ergänzend wird auf die Stellungnahme des UP-Kritis hingewiesen.** Dort wird der Zeitstrahl ebenfalls ausführlich dargestellt und ein alternativer Zeitstrahl vorgeschlagen.

d. Konkretisierung durch behördlich festgelegte Resilienzmaßnahmen

Das KRITIS-DachG sieht zum einen vor, dass die Bundesbehörden sektorübergreifende Resilienzmaßnahmen sowie sektorspezifische Resilienzmaßnahmen über Kataloge bzw. Verordnung erlassen können (§ 10 Abs. 4, 5 KRITIS-DachG). Auch Landesbehörden können im Rahmen ihrer Zuständigkeit sektorspezifische Resilienzmaßnahmen festlegen. Die Ermächtigung der Länder steht allerdings unter der Voraussetzung, dass bis zum 01.01.2029 keine entsprechenden branchenspezifischen Sicherheitsstandards anerkannt wurden (Art. 2 Nr. 1; Art. 3 Abs. 4 KRITIS-DachG).

Es wird gefordert, dass auch im Rahmen der Bundeszuständigkeit zunächst von einer behördlichen Festlegung von Resilienzmaßnahmen abgesehen wird und branchenspezifischen Sicherheitsstandards ein Vorrang eingeräumt wird. Hierfür kann zum einen die zeitliche Abfolge der Pflichten, als auch die Erfahrungen aus der IT-Sicherheitsgesetzgebung ins Feld geführt werden.

Im Hinblick auf die zeitliche Abfolge wird davon ausgegangen, dass die entsprechenden behördlichen Resilienzvorgaben nur dann hilfreich sind, wenn sie den Betreibern sehr frühzeitig bekannt sind. Denn nur so können diese rechtzeitig von den Betreibern in ihrer Umsetzung eingeplant werden. Allerdings wird dies wohl nicht der Fall sein. Es wird davon ausgegangen, dass diese behördlichen Resilienzvorgaben erst nach Vorliegen der nationalen KRITIS-Strategie und der nationalen Risikoanalyse und Risikobewertung zum 17.01.2026 erarbeitet werden können. Für die Erarbeitung dieser Resilienzvorgaben muss wiederum Zeit eingerechnet werden. Gleichzeitig werden die Betreiber der kritischen Anlagen mit Vorliegen der nationalen Risikoanalyse und Risikobewertung mit der Erarbeitung ihrer eigenen Risikoanalyse und Risikobewertung beginnen, die zum 17.04.2027 vorliegen muss. Auch die Resilienzmaßnahmen werden wohl bereits durch die Betreiber geplant werden, die zum 17.05.2027 getroffen sein müssen. Wenn nun zu einem späten Zeitpunkt (z.B. Anfang 2027) die behördlichen Resilienzvorgaben veröffentlicht werden, so müssten die Betreiber ihre eigenen Risikoanalyse und Risikobewertung bzw. ihre zu treffenden Resilienzmaßnahmen anpassen. Hierfür wird im Zweifel die Zeit dann aber nicht mehr ausreichen.

Die Einführung des IT-Sicherheitsgesetzes hat zudem nachweislich gezeigt, dass die Wirtschaft mit ihren Branchenverbänden auch ohne derartige Vorgaben von behördlicher Seite geeignete Maßnahmen und Prozesse (branchenspezifischen Sicherheitsstandards) etablieren konnte. Im europäischen Vergleich wurde in Deutschland so ein sehr hohes Sicherheitsniveau erreicht. Es ist zusätzlich davon auszugehen, dass die zukünftig betroffenen Unternehmen auch schon heute, u.a. aufgrund von bereits existierenden rechtlichen Rahmenbedingungen (insbesondere aus der IT-Sicherheitsgesetzgebung) auch im eigenen Interesse und nach Risikoabwägungen, ein geeignetes Maß an physischen Maßnahmen etabliert haben.

Eine Ausnahme für die vorherige Forderung kann für die Bereiche anerkannt werden, die bisher über IT-Sicherheitskataloge erfasst wurden (siehe die entsprechenden IT-Sicherheitskataloge im Sektor Energie und Telekommunikation). Dort hat sich die behördliche Festlegung von Resilienzvorgaben bereits etabliert und diese Kataloge können entsprechend weiterentwickelt werden unter enger Beteiligung der Betreiber der kritischen Anlagen. Hierfür sollte im noch zu erlassenden EnWG eine spezielle Ermächtigungsgrundlage für die BNetzA geschaffen werden, die vergleichbar mit der bisherigen Ermächtigungsgrundlage in § 11 Abs. 1a, 1b EnWG ist.

Weitergehende Ausführungen zu dieser Thematik finden sich in der Kommentierung unter Nr. 10d und Nr. 16.

9. § 9 KRITIS-DachG - Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen
Nach § 9 Abs. 1 KRITIS-DachG müssen Betreiber von kritischen Anlagen regelmäßig Risikoanalysen und Risikobewertungen durchführen. Dies soll auf Grundlage der durchgeführten staatlichen Risikoanalysen und Risikobewertungen nach § 9 KRITIS-DachG und anderer vertrauenswürdiger Informationsquellen erstmals neun Monate nach der Registrierung als kritische Anlage nach § 6 KRITIS-DachG (siehe § 6 Abs. 6 KRITIS-DachG) und dann spätestens alle vier Jahre erfolgen.

Die Frist zur Umsetzung der betrieblichen Risikoanalyse und –bewertung darf erst anfangen zu laufen, wenn seinerseits die staatliche Risikoanalyse und –bewertung vorliegt und die wesentlichen Elemente zur Verfügung gestellt wurden. Anderenfalls könnte die Frist für die Umsetzung der betrieblichen Risikoanalyse und -bewertung einseitig durch den Staat verkürzt werden (siehe bereits die Kommentierung zu den übergreifenden Pflichten unter Nr. 8c).

Formulierungsvorschlag

§ 9 Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen

(1) [S. 1 …] **Liegt im Zeitpunkt der Registrierung als kritische Anlage den Betreibern die für sie wesentlichen Elemente der nationale Risikoanalyse und Risikobewertung nicht vor, so beginnt die Frist nach S. 1 erst zu laufen, nachdem das BBK dem Betreiber der kritischen Anlage die wesentlichen Elemente der Risikoanalyse und Risikobewertung nach § 8 Abs. 5 zur Verfügung gestellt hat.** (S. 2 neu)

Nach § 9 Abs. 2 KRITIS-DachG kann das BBK inhaltliche und methodische Vorgaben einschließlich Vorlagen und Muster für die Risikoanalysen und Risikobewertungen festlegen. Solange dies nur als Hilfestellung zu verstehen ist, wird dies begrüßt. **Keinesfalls darf dies allerdings so verstanden werden, dass zwangsläufig und ausschließlich diese Vorlagen und Muster von den Unternehmen genutzt werden müssen.** Vielmehr nutzt jedes Unternehmen bereits seine eigenen bewährten Vorlagen und Muster zur Risikoanalyse und Risikobewertung. Dies muss zwingend beibehalten werden.

Formulierungsvorschlag

§ 9 Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen

(2) [S. 1,2 …] **Die Nutzung dieser Vorlagen und Muster ist für die Betreiber der kritischen Anlagen freiwillig.**

10. § 10 KRITIS-DachG - Resilienzmaßnahmen der Betreiber kritischer Anlagen; Resilienzplan

a. § 10 Abs. 1 KRITIS-DachG

Bei § 10 Abs. 1 KRITIS-DachG handelt es sich um eine Parallelvorschrift zu § 30 Abs. 1 BSIG. Es fallen jedoch auch Unterschiede in der Formulierung auf, die nicht ohne weiteres verständlich sind. Insbesondere sollen „geeignete und verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen" getroffen werden, während nach § 30 Abs. 1 S. 1 BSIG „geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen" getroffen werden sollen. Es erschließt sich nicht, warum in einem Fall von „sicherheitsbezogenen" und in einem anderen Fall von „wirksamen" Maßnahmen gesprochen wird. Unterschiedliche Wortlaute legen unterschiedliche Abwägungsmechanismen nahe, ohne dass dies näher erläutert wird. **Es wird gefordert, dass die Vorschriften aus § 10 Abs. 1 KRTIS-DachG und aus § 30 Abs. 1 BSIG möglichst weitgehend aufeinander abgestimmt werden und parallel laufen.**

Nach § 10 Abs. 1, 2 KRITIS-DachG müssen sich die Maßnahmen unter anderem auf die staatliche Risikoanalyse nach § 8 KRITIS-DachG stützen. Für die Frist wird an die Registrierung der Betreiber von kritischen Anlagen angeknüpft. Probleme treten jedoch auf, wenn die staatliche Risikoanalyse nicht rechtzeitig vorliegen sollte. **Die Frist zur Umsetzung der Resilienzmaßnahmen darf erst anfangen zu laufen, wenn seinerseits die staatliche Risikoanalyse und –bewertung vorliegt und die wesentlichen Elemente zur Verfügung gestellt wurden.** Anderenfalls könnte die Frist für die Umsetzung der Resilienzmaßnahmen einseitig durch den Staat verkürzt werden (siehe bereits die Kommentierung zu den übergreifenden Pflichten unter Nr. 8c).

Weiterhin ist die Frist zum Treffen der Resilienzmaßnahmen extrem kurz. Die Resilienzmaßnahmen sollen bereits 10 Monate nach der Registrierung als Betreiber einer kritischen Anlage getroffen sein. Die betriebliche Risikoanalyse und Risikobewertung muss 9 Monate nach der Registrierung vorliegen. Resilienzmaßnahmen können erst dann umgesetzt werden, wenn die betriebliche Risikoanalyse und Risikobewertung vorgenommen wurden. Dies bedeutet, dass für die Betreiber nach der betrieblichen Risikoanalyse und Risikobewertung nur ein Monat Zeit besteht, um die Resilienzmaßnahmen zu treffen.
Es dürfte auf der Hand liegen, dass innerhalb von einem Monat nicht alle durch die Risikoanalyse und Risikobewertung identifizierten Resilienzmaßnahmen vollständig umgesetzt werden können. Für die vollständige Umsetzung von größeren baulichen Resilienzmaßnahmen können mit Planung, Finanzierung, Vergabeverfahren, Baugenehmigung und Ausführung schnell mehrere Jahre vergehen. **Es wird deshalb gefordert mit dem KRITIS-DachG klar zu definieren, was mit „treffen" von Resilienzmaßnahmen gemeint ist. Eine vollständige Umsetzung der Maßnahmen kann hiermit nicht gemeint sein, denn dies ist den Betreibern unmöglich.**

Positiv zu bemerken ist, dass laut Gesetzesbegründung bei der Abwägung im Rahmen der Verhältnismäßigkeit auch wirtschaftliche Aspekte berücksichtigt werden können. Dieser Hinweis ist wichtig, damit nicht nur eine sicherheitsspezifische Abwägung, sondern auch eine wirtschaftliche Abwägung stattfinden kann. **Es wird gefordert, dass der Aspekt der Abwägung un-**

ter Berücksichtigung der wirtschaftlichen Auswirkungen auch in den Wortlaut der Norm aufgenommen wird. Es muss klar sein, dass die sicherheitspolitischen Maßnahmen immer unter Berücksichtigung der wirtschaftlichen Gegebenheiten getroffen werden müssen. Die Höhe der Kosten muss in einem gesunden Verhältnis zu der dadurch erreichten Senkung des Risikos stehen. Eine Berücksichtigung dieses Aspekts ist z.B. in § 30 Abs. 1 BSIG geschehen („Umsetzungskosten").

Formulierungsvorschlag

§ 10 Resilienzmaßnahmen der Betreiber kritischer Anlagen; Resilienzplan

(1) [S. 1 …] **Liegt im Zeitpunkt der Registrierung als kritische Anlage den Betreibern die für sie wesentlichen Elemente der nationale Risikoanalyse und Risikobewertung nicht vor, so beginnt die Frist nach S. 1 erst zu laufen, nachdem das BBK dem Betreiber der kritischen Anlage die wesentlichen Elemente der Risikoanalyse und Risikobewertung nach § 8 Abs. 5 zur Verfügung gestellt hat.** Die Maßnahmen sind verhältnismäßig, wenn der Aufwand zur Verhinderung oder Begrenzung eines Vorfalls zum Risiko eines Vorfalls angemessen erscheint. **Bei der Bewertung, ob Maßnahmen dem bestehenden Risiko angemessen sind, können auch die wirtschaftlichen Auswirkungen für den Betreiber der kritischen Anlage berücksichtigt werden.**

b. § 10 Abs. 2 KRITIS-DachG

Nach § 10 Abs. 2 soll bei der Umsetzung der Resilienzmaßnahmen der Stand der Technik eingehalten werden. Was der Stand der Technik ist, wird in der Gesetzesbegründung weiter ausgeführt.

Für den Begriff des Stands der Technik existiert jedoch eine übergreifende Definition im Handbuch der Rechtsförmlichkeit (Stand: September 2008, Rn. 256). Dort wird dieser Begriff wie folgt definiert:

> *„Stand der Technik ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, der nach herrschender Auffassung führender Fachleute das Erreichen des gesetzlich vorgegebenen Zieles gesichert erscheinen lässt. Verfahren, Einrichtungen und Betriebsweisen oder vergleichbare Verfahren, Einrichtungen und Betriebsweisen müssen sich in der Praxis bewährt haben oder sollten – wenn dies noch nicht der Fall ist – möglichst im Betrieb mit Erfolg erprobt worden sein."*

Die Gesetzesbegründung liefert eine andere Definition und gibt keinen Hinweis auf die bereits bestehende Definition. **Es wird gefordert, dass die Definition entsprechend dem Handbuch der Rechtsförmlichkeit festgelegt wird und ein Verweis auf diese Definition in der Gesetzesbegründung erfolgt.**

Ferner darf nicht der Versuch unternommen werden, den Stand der Technik durch eine Behörde abschließend zu definieren. Entsprechende Ermächtigungsnormen wurden im Rahmen

des Gesetzgebungsprozesses im IT-Sicherheitsgesetz 2.0 aus guten Gründen verworfen. Es darf auch keine Definition „durch die Hintertür“ erfolgen, indem eine Behörde einen Leitfaden oder ähnliches hierzu herausbringt. Dies ist z.B. faktisch durch die „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“[11] geschehen. Obgleich die Orientierungshilfe nicht formell verbindlich ist, wird sie doch von den Auditoren im Zweifel als Grundlage der Prüfung genommen.

Nicht ganz klar ist, was die weiteren Ausführungen in der Gesetzesbegründung zum Stand der Technik bedeuten sollen. So heißt es:

> *„Die Verpflichtung zur Berücksichtigung des Stands der Technik schließt die Möglichkeit zum Ergreifen solcher Maßnahmen nicht aus, die einen ebenso effektiven Schutz wie die anerkannten Vorkehrungen nach dem Stand der Technik bieten“.*

Falls Maßnahmen einen ebenso effektiven Schutz wie die anerkannten Vorkehrungen nach dem Stand der Technik bieten, handelt es sich um Maßnahmen nach dem Stand der Technik. Entscheidender ist die Frage, ob der Wort „soll“ in § 10 Abs. 2 bedeuten soll, dass nicht in jedem Fall der Stand der Technik eingehalten werden muss. **Es muss klargestellt werden, ob immer der Stand der Technik eingehalten werden muss oder es hiervon Ausnahmen gibt**.

c. § 10 Abs. 3 KRITIS-DachG

§ 10 Abs. 3 KRITIS-DachG enthält eine beispielhafte Auflistung von Maßnahmen, die die Betreiber kritischer Anlagen bei der Abwägung, welche Maßnahmen zur Erreichung der Ziele nach Absatz 1 geeignet und verhältnismäßig sind, berücksichtigen können. § 10 Abs. 3 Nr. 5b KRITIS-DachG enthält laut Gesetzesbegründung eine Klarstellung, dass das von den Betreibern kritischer Anlagen zu berücksichtigende Sicherheitsmanagement im Hinblick auf Zuverlässigkeitsüberprüfungen hinsichtlich der Mitarbeitenden unbeschadet der Vorschriften des Sicherheitsüberprüfungsgesetzes (SÜG) in Verbindung mit der Sicherheitsüberprüfungsfeststellungsverordnung (SÜFV) sowie unbeschadet weiterer Fachgesetze erfolgt. Probleme gibt es allerdings bereits jetzt in Bezug auf die staatliche Sicherheitsüberprüfung (bzw. Zuverlässigkeitsprüfung) von Mitarbeitern.

Bereits jetzt hat der Bund die Pflicht, bestimmte Personen auch im nichtöffentlichen Bereich (also in der Privatwirtschaft) einer Sicherheitsüberprüfung zu unterziehen. Dies gilt beispielsweise für Teile von Übertragungsnetzbetreibern oder Verteilnetzbetreibern, da sie eine lebenswichtige Einrichtung darstellen können (vgl. § 1 Abs. Abs. 4, 5; 2 Abs. 1 Sicherheitsüberprüfungsgesetz; § 16 Sicherheitsüberprüfungsfeststellungsverordnung). Allerdings besteht auch außerhalb des in § 16 Sicherheitsüberprüfungsfeststellungsverordnung genannten Leitstellenbetriebs teilweise ein Bedürfnis (potentielle) Mitarbeiter einer Sicherheitsüberprüfung unterziehen zu lassen. **Es wird gefordert, dass der Staat einen Anspruch für die Betreiber der kritischen Anlagen schafft, auf Antrag auch (potentielle) Mitarbeiter in sonstigen sicherheitsrelevanten Bereichen einer Sicherheitsüberprüfung zu unterziehen.** Bisher wird dieses Thema nur

[11] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.pdf?__blob=publicationFile&v=14.

durch Überprüfung der Terrorliste/Sanktionsliste bei Bestandspersonal und durch Vorlage des polizeilichen Führungszeugnisses bei Einstellung abgedeckt. Dies entspricht nicht mehr den Anforderungen an die veränderte Sicherheitslage nach Beginn des russischen Angriffskriegs gegen die Ukraine.

Besondere Probleme bestehen, falls die Anforderungen an die Bedeutung der Einrichtung nach § 16 Sicherheitsüberprüfungsfeststellungsverordnung nicht erreicht werden. In einem solchen Fall erklärt sich der Bund für nicht zuständig für die Sicherheitsüberprüfung und die Länder können diese teilweise nicht anbieten. Es kann allerdings auch unterhalb der Anforderungen des § 16 Sicherheitsüberprüfungsfeststellungsverordnung ein Bedürfnis für eine Sicherheitsüberprüfung von Personen im sicherheitsrelevanten Bereich geben. **Es wird gefordert, dass der Bund sich mit den Ländern abstimmt und gemeinsam genügend Kapazitäten aufbaut, um auch in solchen Fällen eine Sicherheitsüberprüfung anbieten zu können.**

d. § 10 Abs. 4, 5, 6 KRITIS-DachG

Das Kritis-DachG sieht in § 10 Abs. 4, 5 KRITIS-DachG vor, dass die Bundesbehörden sektorübergreifende Resilienzmaßnahmen sowie sektorspezifische Resilienzmaßnahmen über Kataloge bzw. Verordnung erlassen können. Diese Regelung ist zwar im Grundsatz sinnvoll, sollte jedoch zunächst hinter die noch zu erarbeitenden branchenspezifischen Sicherheitsstandards zurücktreten.

Die Erarbeitung von branchenspezifischen Sicherheitsstandards wird in § 10 Abs. 6 KRITIS-DachG geregelt. Dieses Vorgehen ist im IT-Sicherheitsbereich lange erprobt und hat sich bewährt. Die auf dieser Grundlage verabschiedeten B3S bieten der Branche wertvolle Möglichkeiten den Anforderungen pragmatisch gerecht zu werden (vgl. auch die parallele Umsetzung in § 30 Abs. 9 BSIG).

Es wird gefordert, dass den branchenspezifischen Sicherheitsstandards ein noch größeres Gewicht eingeräumt wird. Insbesondere sollten den Betreibern bis zum 01.01.2029 Zeit gegeben werden, entsprechende Branchenstandards zu erarbeiten. Erst wenn bis zu diesem Zeitpunkt keine Standards vorliegen, sollte der Bund die Möglichkeit haben, entsprechende Standards nach Abs. 4, 5 KRITSI-DachG zu erlassen. § 10 Abs. 4, 5 KRITIS-DachG sollten deshalb an dieser Stelle gestrichen werden und in Art. 2 verschoben werden. Dies würde zu einem Gleichlauf mit der entsprechenden Ermächtigung der Länder in diesem Bereich führen (siehe auch näher die Kommentierung unter Nr. 8d und Nr. 16).

e. § 10 Abs. 9 KRITIS-DachG

In Bezug auf § 10 Abs. 9 KRITIS-DachG stellt sich die Frage, was genau in dem Resilienzplan festgehalten werden soll, denn der Begriff des Resilienzplans wird nicht weiter definiert. Geht es um die Planung der noch zukünftig durchzuführenden Maßnahmen oder geht es um die auf Grundlage einer Planung bereits realisierten Maßnahmen zum Schutz der Resilienz oder um beides? **Es wird gefordert, dass bereits aus dem Gesetzeswortlaut (bzw. der Gesetzesbegründung) klar hervorgeht, was der grundsätzliche Inhalt dieses Resilienzplans sein soll**. **Zudem**

muss klargestellt werden, ab wann dieser Resilienzplan vorliegen muss. Es wird vermutet, dass dies ebenfalls 10 Monate nach der Registrierung der Fall ist (vgl. § 6 Abs. 6 KRITIS-DachG). Da aber § 10 Abs. 1 KRITIS-DachG ebenfalls diese Frist festlegt, sich aber nur auf § 10 Abs. 1 KRITIS-DachG selbst bezieht, bestehen Unsicherheiten.

f. § 10 Abs. 10 KRITIS-DachG

Nach § 10 Abs. 10 KRITIS-DachG kann das BBK den Betreibern kritischer Anlagen Vorlagen und Muster für einen Resilienzplan zur Verfügung stellen. Dies ist im Grundsatz zu begrüßen, allerdings darf dies nicht mit einer Pflicht einhergehen, exakt diese Vorlagen und Muster auch zu nutzen. Es kann gute Gründe für Unternehmen geben, eine andere Form der Darstellung zu wählen. **Es wird gefordert festzulegen, dass diese Vorlagen und Muster nicht verbindlich für die Betreiber sind.**

Formulierungsvorschlag

§ 9 Resilienzmaßnahmen der Betreiber kritischer Anlagen; Resilienzplan

(10) [S. 1,2 …] **Die Nutzung dieser Vorlagen und Muster ist für die Betreiber der kritischen Anlagen freiwillig.**

11 § 11 KRITIS-DachG - Nachweise; behördliche Anordnungen

a. Vorbemerkung

§ 11 KRITIS-DachG regelt die Nachweiserbringung über die Einhaltung der Maßnahmen nach § 10 Abs. 1 KRITIS-DachG. Positiv ist zunächst zu bemerken, dass keine generelle ex ante-Nachweispflicht mehr vorgesehen ist, sondern nur im Einzelfall vom Betreiber ein Nachweis angefordert werden soll. Positiv ist weiterhin, dass die Behörden zunächst auf bereits beim BSI vorliegenden Unterlagen zurückgreifen müssen, bevor sich an die Betreiber für weitere Nachweise gewendet wird (vgl. § 11 Abs. 1, 2 KRITIS-DachG).

b. § 11 Abs. 1 KRTISI-DachG

Der behördeninterne Austausch ist kompliziert geregelt und umfasst ein Zusammenspiel von mindestens drei Behörden. Die anfragende Behörde kann das BSI nicht direkt anfragen, sondern muss immer über das BBK die Anfrage stellen. Zudem darf nur auf die Unterlagen des BSI Rückgriff genommen werden, nicht aber auf die Nachweise, die ggf. in anderen Behörden vorliegen. Im Falle der Energiewirtschaft werden die Nachweise allerdings bei der BNetzA vorliegen (vgl. die IT-Sicherheitskataloge), auf die z.B. etwaige Landesbehörden bei der aktuellen Gesetzesfassung keinen Zugriff hätten. **Es wird gefordert, dass auch die Unterlagen der speziellen Sektorbehörden des Bundes (z.B. BNetzA) angefordert werden müssen, bevor sich nach § 11 Abs. 2 KRITIS-DachG an die Betreiber gewendet werden kann.**

c. § 11 Abs. 2 KRITIS-DachG

Im Einzelfall können die zuständigen Behörden Unterlagen nachfordern, falls die behördenintern nach § 11 Abs. 1 KRIITIS-DachG angeforderten Unterlagen nicht ausreichen sollten. **Zunächst wird gefordert, dass diese Nachforderung von den Behörden in einheitlicher Form erfolgt.** Es muss unbedingt vermieden werden, dass Betreiber mit Nachforderungen von verschiedenen Behörden konfrontiert werden, die sich inhaltlich und formal unterscheiden. Anderenfalls drohen massive bürokratische Mehraufwände, wenn die Unternehmen für jede Anfrage einen kompletten neuen Prozess aufsetzen müssen und ggf. ganz unterschiedliche Unterlagen ausfüllen müssen.

Weiterhin muss das Verhältnis von § 11 Abs. 2 KRITIS-DachG zur Äquivalenzprüfung in § 4 Abs. 8 KRITIS-DachG geklärt sein. **Es muss klargestellt werden, dass eine durchgeführte Äquivalenzprüfung keine Voraussetzung dafür ist, die entsprechenden weiteren Informationen und Nachweise nach § 11 Abs. 2 KRTIS-DachG einzureichen** (siehe bereits die Kommentierung unter Nr. 5d).

12. § 12 KRITIS-DachG - Meldewesen für Vorfälle

a. § 12 Abs. 1 KRITIS-DachG

Nach § 12 Abs. 1 KRITIS-DachG müssen Betreiber kritischer Anlagen Vorfälle, die die Erbringung ihrer kritischen Dienstleistungen erheblich stören könnten, unverzüglich melden. Es stellt sich die Frage, warum die erhebliche Störung zusätzlich adressiert wird. Nach § 2 Nr. 10 KRTIS-DachG ist ein Vorfall ein Ereignis, das die Erbringung einer kritischen Dienstleistung erheblich beeinträchtigt oder beeinträchtigen könnte. **Es zeigt sich somit, dass es sich hierbei wahrscheinlich um eine Doppelung handelt, die gestrichen werden kann.**

Positiv zu bemerken ist, dass es nach § 12 Abs. 1 KRITIS-DachG eine gemeinsame Meldestelle von BSI und BBK geben soll. Dies gilt auch dann, wenn eine Landesbehörde für den Vollzug dieses Gesetzes zuständig sein sollte. Dies erfüllt zumindest teilweise eine zentrale Forderung: Ein Vorfall – eine Meldung! **Es sollte aber darüber nachgedacht werden, ob nicht auch andere Meldepflichten hiermit erfüllt werden können, außerhalb von solchen gegenüber BSI und BBK (z.B. gegenüber der BNetzA).** Dies Gesetzesbegründung schließt gerade dies aus. **Zudem ist darauf zu achten, dass auch die zuständigen Landesbehörden einen Zugang zu diesen Meldungen bekommen.**

b. § 12 Abs. 7 KRITIS-DachG

Nach § 12 Abs. 7 KRITIS-DachG kann das BBK dem von dem Vorfall betroffenem Betreiber kritischer Anlagen sachdienliche Folgeinformationen übermitteln. Dies ist nicht ausreichend und bleibt hinter der Vorfassung des Gesetzesentwurf zurück. **Es wird gefordert, dass dem betroffenen Betreiber sachdienliche Folgeinformation auch tatsächlich mitgeteilt werden.** Der Behörde darf hinsichtlich des „ob“ kein Ermessen eingeräumt werden. **Zudem muss sichergestellt werden, dass sämtliche Betreiber von kritischen Anlagen über die sie betreffenden physikalische Störungen/Bedrohungen/Risiken zeitnah informiert werden.** Dies ist auch im BSIG

so geregelt (siehe § 5 Abs. 3 Nr. 4; 40 Abs. 2 Nr. 4 BSIG) und hilft den Betreibern, sich gegen vorsätzliche Handlungen zu schützen bzw. diese bei ihren Risikobetrachtungen zu berücksichtigen.

Formulierungsvorschlag

§ 12 Meldewesen für Vorfälle

(7) **Das BBK übermittelt dem betreffenden Betreiber der kritischen Anlage im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes und der Länder sachdienliche Folgeinformationen. Das BBK soll die gemeldeten Informationen nutzen, um alle Betreiber der kritischen Anlagen über die sie betreffenden Informationen zu unterrichten.**

Ferner wird angeregt, dass ein Notfallteam aufgebaut wird, mit dem die Betreiber bei Notfällen unterstützt werden können. Im Bereich der Cybersicherheit kann das BSI ein entsprechendes Computer-Notfallteam (CSIRT) zur Verfügung stellen (vgl. § 5 Abs. 3 Nr. 5 BSIG).

13. § 14 KRITIS-DachG - Billigungs -, Überwachungs -, und Schulungspflicht für Geschäftsleiter für Betreiber kritischer Anlagen

a. § 14 Abs. 1 KRITIS-DachG

§ 14 KRITIS-DachG entspricht fast vollständig dem § 38 BSIG und regelt die Pflichten des Geschäftsleiters, sowie dessen Haftung bei Pflichtverstößen.

Bereits heute besteht weitgehend Einigkeit, dass die allgemeinen Sorgfaltspflichten von Leitungsorganen und die gesellschaftsrechtlich gebotene Etablierung von Maßnahmen zum angemessenen Risikomanagement (vgl. § 91 Abs. 2, § 92 Abs. 1 AktG; § 43 GmbHG) auch die Pflicht zu angemessenen Maßnahmen für die IT-Sicherheit umfasst. Es handelt sich hierbei um eine Aufgabe der Unternehmensleitung.[12] Entsprechendes dürfte für die Einhaltung der Vorgaben der physischen Sicherheit gelten. Insoweit statuiert § 14 KRITIS-DachG lediglich den bisherigen Status Quo, der sich aus den allgemeinen gesellschaftsrechtlichen Regeln ableiten lässt. **Es wird gefordert in der Gesetzesbegründung klarzustellen, dass mit dem § 14 Abs. 1 KRITIS-DachG keine Ausdehnung der Haftung des Geschäftsleiters statuiert werden soll, der über die allgemeinen gesellschaftsrechtlichen Regelungen hinausgeht.**

Zudem muss der Begriff des Geschäftsleiters definiert werden. Bisher sieht das Kritis-DachG (anders als § 2 Abs. 1 Nr. 11 BSIG) keine Definition des Geschäftsleiters vor. Dieser Begriff sollte im IT-Sicherheitsrecht und im KRITIS-DachG einheitlich definiert werden.

Anders als § 93 Abs. 4 S. 3 AktG enthält das GmbHG keine generelle Einschränkung für den

[12] Krieger/Schneider, Handbuch Managerhaftung, 4. Auflage 2023, Rz. 45.10.

Verzicht auf oder den Vergleich über Schadensersatzansprüche der Gesellschaft gegen ihren Geschäftsführer. Ein Verzicht oder ein Vergleich sind deshalb grundsätzlich zulässig. Die Entscheidung darüber obliegt gemäß § 46 Nr. 8 GmbHG den Gesellschaftern.[13] Durch § 14 Abs. 1 S. 2/3 KRITIS-DachG wird zumindest für die GmbH der Verzicht und der Vergleich im Grundsatz ausgeschlossen. Warum nur für den Bereich von Verstößen gegen das KRITIS-DachG vom Grundsatz eines möglichen Verzichts oder Vergleichs bei einer GmbH abgewichen wird, erschließt sich nicht. **Sollte eine solche Modifizierung des GmbHG gewollt sein, so muss dies in der Gesetzesbegründung begründet werden.**

b. § 14 Abs. 2 KRITIS-DachG

Gemäß § 14 Abs. 2 KRITIS-DachG muss die Geschäftsleitung regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken im Bereich der Sicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

Es sollte klargestellt werden, ob es sich hierbei um eine spezielle und tiefergehende Schulung speziell für die Geschäftsleiter handelt oder auch die Teilnahme an allgemeinen Sicherheitsschulungen für die Belegschaft ausreichend ist.

Zudem wird lediglich auf „erbrachte Dienstleistungen“ Bezug genommen. **Es kann aber nur um die „erbrachten kritischen Dienstleistungen“ gehen. Dies sollte im Wortlaut korrigiert werden.**

14. § 16 KRITIS-DachG - Ermächtigung zum Erlass von Rechtsverordnungen

a. § 16 Abs. 1 KRITIS-DachG

Zunächst handelt es sich auch hier wiederum teilweise um eine Doppelregulierung zu § 57 BSIG, die aber wiederum Abweichungen im Detail beinhaltet, die nicht weiter ausgeführt werden.

Zudem sollte die bisherige Kritis-Verordnung und die nach dem KRITIS-DachG zu erlassende KritisV einheitlich in einer gemeinsamen Verordnung geregelt werden. Dies sollte auch unmissverständlich im Gesetzeswortlaut festgeschrieben werden. Insbesondere darf es keine abweichenden Definitionen der kritischen Anlagen im NIS2UmsuCG und im KRITIS-DachG geben. Dies gilt zumindest für die generelle Bestimmung der kritischen Anlagen über Verordnungen.

b. § 16 Abs. 2 KRITIS-DachG

§ 16 Abs. 2 KRITIS-DachG regelt die sektorspezifische Konkretisierung von Resilienzmaßnahmen nach § 10 Abs. 5 KRITIS-DachG und schafft die dafür notwendige Ermächtigungsgrundlage**. Da zunächst keine Resilienzmaßnahmen von Bundesbehörden näher beschrieben werden sollten, sollte § 16 Abs. 2 KRITIS-DachG in Art. 2 KRITIS-DachG verschoben werden.** Zur Begründung wird auf die Kommentierung unter Nr. 10d verwiesen.

[13] Fleischer, in: Münchener Kommentar GmbH, 4. Auflage 2023, § 43, Rn. 350.

15. § 19 - Bußgeldvorschriften

Unklar ist das Verhältnis dieser Bußgelder gegenüber anderen Bußgeldern, insbesondere gegenüber den Bußgeldern aus dem NIS2UmsuCG. **Es wird gefordert, dass Bußgelder nach dem KRITIS-DachG nicht verhängt werden dürfen, soweit für den gleichen Verstoß bereits Bußgelder auf Grund von anderen Normen (z.B. dem NIS2UmsuCG) verhängt wurden**. Eine doppelte Bußgeldverhängung ist nicht verhältnismäßig. Eine vergleichbare Norm für das Verhältnis von BSIG zur Datenschutzgrundverordnung findet sich in § 60 Abs. 9 BSIG.

Entsprechendes gilt für den Fall, dass unterschiedliche Bundes- und Landesbehörden zuständig für den Vollzug des KRITIS-DachG sind und voneinander unabhängig Bußgelder für den gleichen Verstoß verhängen möchten. Dies könnte insbesondere bei Mehrspartenunternehmen der Fall sein.

Formulierungsvorschlag

§ 19 Bußgeldvorschriften

(4) Verhängen andere Aufsichtsbehörden eine Geldbuße, so darf ein weiteres Bußgeld für einen Verstoß nach diesem Gesetz, der sich aus demselben Verhalten ergibt wie jener Verstoß, nicht verhängt werden.

Die Bußgeldhöhe wurde bisher noch nicht festgelegt (§ 19 Abs. 3 KRITIS-DachG). Da sich die CER-Richtlinie und das KRITIS-DachG erkennbar an der Umsetzung der NIS 1-Richtlinie orientiert, sollte sich auch an der damaligen Bußgeldhöhe orientiert werden. Diese betrug höchstens 100.000 Euro. **Es wird gefordert, dass der Bußgeldrahmen den Betrag von 100.000 Euro nicht übersteigt.** Sowohl die Unternehmen, als auch die Behörden müssen noch Erfahrung mit diesem Gesetz und den sich hieraus ergebenden Pflichten sammeln. Es liegt daher nahe, in einem ersten Schritt den Bußgeldrahmen nicht zu hoch anzusetzen.

16. Art. 2 - Änderung des Dachgesetzes zur Stärkung der physischen Resilienz von Betreibern kritischer Anlagen

Die bisherigen § 10 Abs. 4, 5 und § 16 Abs. 2 KRITIS-DachG sollten aus dem KRITIS-DachG gestrichen und in Art. 2 KRITIS-DachG verschoben werden. Das Kritis-DachG sieht in § 10 Abs. 4, 5; § 16 Abs. 2 KRITIS-DachG vor, dass die Bundesbehörden sektorübergreifende Resilienzmaßnahmen sowie sektorspezifische Resilienzmaßnahmen über Kataloge bzw. Verordnung erlassen können. Diese Möglichkeit sollte erst bestehen, wenn keine branchenspezifischen Sicherheitsstandards zum 01.01.2029 erarbeitet wurden. Zur Begründung wird auf die Kommentierung unter Nr. 10d und Nr. 16b verwiesen.

VERBAND KOMMUNALER UNTERNEHMEN e.V.

VKU-Ansprechpartner:

Wolf Buchholz
Fachgebietsleiter Kritische Infrastruktur und Cybersicherheit
Abteilung Recht, Finanzen und Steuern

Telefon: +49 30 58580-317
E-Mail: buchholz@vku.de