VERBAND KOMMUNALER UNTERNEHMEN e.V.

# STELLUNGNAHME

## zum Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen

## Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat vom 27.07.2023

Berlin, 24.08.2023

*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



DIE KOMMUNALEN UNTERNEHMEN

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 das Ziel des Gesetzgebers an, die Betreiber der kritischen Anlagen nicht über Gebühr zu belasten. Dies zeigt sich z.B. im geringeren Anwendungsbereich im Vergleich zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG), da ausschließlich die Betreiber der kritischen Anlagen adressiert werden und nicht die Betreiber der (besonders) wichtigen Einrichtungen. Auch die Anerkenntnismöglichkeiten von Dokumenten und Maßnahmen aus dem Bereich der Cybersicherheit sind positiv zu bewerten. Ferner wird die Maßgabe „Ein Vorfall – eine Meldung“ zumindest teilweise umgesetzt.

Allerdings ist auch noch **deutlicher Verbesserungs- und Klarstellungsbedarf** zu erkennen:

- 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. 11.a.)). Eng hiermit verbunden ist die Frage, wie die Betreiber die ihnen verbleibenden Pflichten **refinanzieren** können (siehe hierzu unter Nr. 11.b).
- 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 (siehe hierzu unter Nr. 1.b). Dies wird sich insbesondere zu einer **Beschränkung der Transparenzpflichten** führen müssen, denen die Betreiber der kritischen Anlagen bisher unterliegen. (siehe hierzu unter Nr. 1.c). Auch muss dies zu Anpassungen im Vergaberecht führen (siehe hierzu unter Nr. 1.d).

- 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 (siehe hierzu unter Nr. 2) und **Pflichten widersprüchlich** festgelegt werden (siehe hierzu unter Nr. 5). Auch muss eine bessere **Abstimmung** der Begriffe mit den **internationalen ISO-Normen** erfolgen (siehe hierzu insbesondere unter Nr. 2.e).
- Ganz maßgebliche Teile des Gesetzes können erst bewertet werden, wenn die entsprechende **Kritis-Verordnung** verabschiedet wird. Dies betrifft insbesondere den genauen personellen Anwendungsbereich des Gesetzes, da in der Kritis-Verordnung die maßgeblichen Schwellenwerte zur Bestimmung der Betreiber der kritischen Anlagen festgelegt werden. Hierfür muss das **Gesetz mehr Leitplanken** bereitstellen, damit die wesentlichen Entscheidungen auch auf Ebene des Gesetzgebers getroffen werden (siehe hierzu insbesondere unter Nr. 2.b).
- Dringend muss **frühzeitig** eine **Abstimmung mit den Ländern** gesucht werden, damit es nicht zu einer Vervielfältigung der Pflichten für die Betreiber auf der Landes- oder kommunalen Ebene kommt. Auch bei dem Austausch zwischen den Bundesbehörden und den Landesbehörden besteht Verbesserungspotential. **Perspektivisch** sollte die Gesetzgebungskompetenz zur Regulierung der kritischen Infrastrukturen vollständig auf die Bundesebene verlagert werden (siehe hierzu unter Nr. 4).
- Das **Schutzgut des Gesetzes** muss deutlicher herausgearbeitet werden. Es muss deutlicher werden, dass es um die **Sicherstellung** von **kritischen Dienstleistungen** geht. Die insofern verwendeten Begriffe der „wirtschaftlichen Tätigkeit“ oder der „Wirtschaftsstabilität“ sind nicht weiterführend und sollten gestrichen werden (siehe hierzu insbesondere unter Nr. 2.b und Nr. 2.c)
- Wenn das **BBK** die im Gesetz beschriebenen Aufgaben sinnvoll wahrnehmen soll, so müssen der Behörde auch die entsprechenden **Ressourcen bereitgestellt werden**. Im Moment bestehen ernsthafte Zweifel, ob das BBK diesen Aufgaben mit den vorhandenen Mitarbeitern gerecht werden kann (siehe hierzu insbesondere unter Nr. 11.g).

## Stellungnahme

### 1. § 1 KRITIS-DachG-RefE – Zweck des Gesetzes

**a. Physische Sicherheit als Zweck des KRITIS-DachG**
Die Gesetzesbegründung stellt zutreffend darauf ab, dass das KRITIS-DachG in Abgrenzung zur IT-Sicherheit den physischen Schutz von kritischen Anlagen in den Blick nimmt. Diese Abgrenzung findet sich in dieser Deutlichkeit jedoch nicht im Wortlaut des § 1 KRITIS-DachG wieder. **Um dem Rechtsanwender die Arbeit mit dem KRITIS-DachG zu erleichtern, sollte diese Zielrichtung bereits in § 1 KRITIS-DachG deutlich festgeschrieben werden.**

**Formulierungsvorschlag:**

**§ 1 Zweck des Gesetzes**

Dieses Gesetz legt Kriterien zur Identifizierung kritischer Anlagen und Verpflichtungen für Betreiber kritischer Anlagen fest zur Gewährleistung der ungehinderten Erbringung von Dienstleistungen, die für die Aufrechterhaltung wichtiger wirtschaftlicher Tätigkeiten und Funktionen unerlässlich sind. **Nach dem All-Gefahrenansatz wird mit dem Gesetz der Schutz der kritischen Anlagen adressiert, soweit er nicht ausschließlich die Informationssicherheit betrifft. […]**

**b. Ressourcenverteilung und Bevorzugung von kritischen Anlagen**
Laut der Gesetzesbegründung 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 auf Grund 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 auf Grund der Corona Pandemie eigentlich eine Ausgangssperre galt. Auch das KRITIS-DachG trägt an anderer Stelle die grundsätzliche Bevorzugung mit von Betreibern von kritischen Anlagen mit. So

[1] Bearbeitungsstand: 03.07.2023

sollen laut Gesetzesbegründung zu § 5 Abs. 2 KRITIS-DachG z.B. die Kinder von Mitarbeitern von kritischen Anlagen bei der Betreuung in Kindergärten bevorzugt berücksichtigt werden.

**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.**

**c. Verhältnismäßige Transparenz- und Auskunftspflichten**

Insbesondere im Bereich der Transparenz- und Auskunftspflichten müssen Betreiber von kritischen Infrastrukturen (bzw. zukünftig kritischen Anlagen) auf Grund 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 allerdings 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]: **Einrichtungen, die durch Gesetz oder aufgrund eines Gesetzes als kritische Anlage bestimmt worden, unterliegen nicht den Pflichten dieses Absatzes.** (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**.

**d. 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.

**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,* ***~~oder~~***
*b) Verschlüsselung betreffen* ***oder***
***c) für die Betreiber kritischer anlagen gemäß § 2 Nr. 3 KRITIS-DachG 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. § 2 KRITIS-DachG-RefE - Begriffsbestimmungen**
**Zunächst sollten die Begriffsbestimmungen alphabetisch geordnet werden**. Dies vereinfacht die Lesbarkeit des Gesetzes deutlich. Im Übrigen ist folgendes anzumerken:

**a. Nr. 2 Kritische Infrastrukturen**
Laut Gesetzesbegründung wird die Definition der kritischen Infrastruktur der Nationalen Strategie zum Schutz Kritischer Infrastrukturen" (KRITIS-Strategie) übernommen. Allerdings sind die Definitionen nicht deckungsgleich. Vielmehr wurde der Satzteil „…erhebliche Störungen der wirtschaftlichen Tätigkeit“ neu eingefügt ohne dies näher zu erläutern.

So bleibt offen, ob hiermit eine Änderung in der Sache erfolgen soll und wessen wirtschaftliche Tätigkeit gestört werden soll. Es könnte z.B. die wirtschaftliche Tätigkeit des Betreibers, die wirtschaftliche Tätigkeit der Kunden oder auch die gesamtwirtschaftliche Tätigkeit Deutschlands gemeint sein. **Es wird gefordert, diese Ergänzung der wirtschaftlichen Tätigkeit zu streichen.**

**Formulierungsvorschlag:**

**§ 2 Begriffsbestimmungen**

[…]

2. „Kritische Infrastrukturen" Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen ~~**der wirtschaftlichen Tätigkeit,**~~ der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

Bisher wird der Begriff der kritischen Infrastruktur auf gesetzlicher Ebene nur in § 2 Abs. 10 BSIG definiert. Zukünftig soll dieser Begriff im Begriff der kritischen Anlagen aufgehen und der Begriff der kritischen Infrastrukturen weiter gefasst werden. 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 Gesetzes 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 im 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.**

**b. Nr. 3 – Kritische Anlagen**

Am Beispiel der Begriffsbestimmung der Kritischen Anlage zeigt sich exemplarisch ein grundsätzliches Problem des Referentenentwurfs – es kommt zu einer Vielzahl von Doppelungen bzw. widersprüchlichen Regelungen im Zusammenspiel mit der NIS 2-Umsetzungsgesetz-RefE. Diese müssen aufgelöst werden. **Es darf für die gleichen Begriffe im KRITIS-DachG und im NIS 2-Umsetzungsgesetz jeweils nur eine Definition geben.**

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[2] definiert wird. Neben der Doppelung der Begriffe zeigen sich auch Unterschiede im Inhalt. Während die Definition in § 2 Nr. 3 KRITIS-DachG auf die Gefährdungen für eine wirtschaftliche Tätigkeit abstellt, wird in § 2 Nr. 19 BSIG auf die Gefährdungen für die öffentliche Sicherheit abgestellt. Zudem wird in § 4 KRITIS-DachG auch der Sektor der öffentlichen Verwaltung genannt, während dies in § 28 Abs. 3 BSIG-RefE nicht der Fall ist. Ferner erschließt sich nicht, welche Teil der öffentlichen Verwaltung damit gemeint ist.

Überdies wird lediglich in der Gesetzesbegründung zu § 4 KRITIS-DachG Bezug genommen auf den Schwellenwert von 500.000 versorgten Personen, wie dies bereits in der aktuell geltenden BSI-KritisV der Fall ist. Zudem „soll" dieser Schwellenwert lediglich zugrunde gelegt werden. Dies ist nicht ausreichend. **Es wird gefordert, dass der Schwellenwert von 500.000 versorgten Personen bereits im Gesetzestext verbindlich festgeschrieben wird. Zudem muss hinreichend deutlich werden, dass im Einzelfall auch andere Schwellenwerte weiter gelten** (siehe z.B. die Schwellenwerte zu den TK-Dienstleistungen in Anhang 4, Teil 3 Nr. 1.1 und Nr. 1.2 oder bei schwarzstartfähigen Stromerzeugungsanlagen in Anhang 1, Teil 3 Nr. 1.1.1). Anderenfalls hat der Verordnungsgeber eine extrem große Macht den Geltungsbereich des KRITIS-DachG zu bestimmen. Es stellt sich die Frage, ob dies dem Wesentlichkeitsgebot gerecht wird, nachdem die wesentlichen Entscheidungen immer in einem formellen Gesetz bestimmt werden müssen.

**Formulierungsvorschlag**

**§ 4 Kritische Anlagen**

**(1)** [S. 1 …] **Der Schwellenwert wird auf Grundlage des Kriteriums der potentiell betroffenen Bevölkerung berechnet. Dabei wird grundsätzlich eine potentiell betroffene Bevölkerung von 500.000 Personen zu Grunde gelegt.** (Satz 2 neu)

Zum Begriff der „wirtschaftlichen Tätigkeit" wird auf die Ausführungen zu § 2 Nr. 2 KRITIS-DachG verwiesen.

[2] Soweit nicht explizit anders bezeichnet wird mit dem Begriff „BSIG" auf das entsprechende Gesetz in der Fassung des NIS2UmsuCG mit Bearbeitungsstand vom 03.07.2023 Bezug genommen.

**Formulierungsvorschlag**

**§ 2 Begriffsbestimmungen**

[…]

**3.** „kritische Anlage“ eine Anlage, die eine hohe Bedeutung für das Funktionieren des Gemeinwesens hat, da durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für ~~**wirtschaftliche Tätigkeiten,**~~ die öffentliche Sicherheit oder Ordnung eintreten würden; welche Anlagen im Einzelnen kritische Anlagen sind, bestimmt sich nach § 4.

Die Ausführungen zum Zusammenspiel mit der Kritis-Verordnung finden sich in den Anmerkungen zu § 15 KRITIS-DachG.

**c. 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 Kritis-Verordnung angepasst wird. Zudem unterscheiden sich die Definition. So grenzt die Definition in § 2 Nr. 4 KRITIS-DachG im Gegensatz zur Begriffsdefinition in der KritisVerordnung den Begriff nicht ein auf bestimmte Sektoren. Dies ist unlogisch, weil es nur um Dienstleistungen innerhalb der definierten Kritis-Sektoren gehen kann. Zudem erweitert die Definition im Kritis-DachG die Gefährdungen auch auf die wirtschaftliche Tätigkeit. Auch dies erscheint unlogisch, weil sich die kritischen Dienstleistungen nur auf die Bereiche beziehen kann, die zur Versorgung der Bevölkerung (inklusive der dort festgelegten Schwellenwerte; siehe im Übrigen die Ausführungen zu § 2 Nr. 2 KRITIS-DachG) unmittelbar notwendig sind. **Es wird gefordert, diesen Begriff einheitlich zu definieren und nur an einer Stelle.**

**Formulierungsvorschlag**

**§ 2 Begriffsbestimmungen**

[…]

4. kritische Dienstleistung“ eine Dienstleistung zur Versorgung der Allgemeinheit **in den Sektoren nach § 4 Abs. 1**, deren Ausfall oder Beeinträchtigung ~~**zu einer Gefährdung von wirtschaftlichen Tätigkeiten,**~~ zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde.

**d. Nr. 5 - Betreiber kritischer Anlagen**

Auch in Bezug auf den Betreiber einer kritischen Anlage liegt eine Doppelung vor. Der Begriff würde nunmehr in § 2 Nr. 5 Kritis-DachG, § 28 Abs. 2 NIS 2-Umsetzungsgesetz und § 1 Abs. 1 Nr. 2 Kritis-Verordnung definiert. **Auch hier 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 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.[3] 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.

**Auf Grund 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.**

**e. Nr. 8, 9 – Risikoanalyse, Risikobewertung und Resilienzplan**

<u>aa. Risikobeurteilung als Oberbegriff zu Risikoanalyse und Risikobewertung</u>

**Die Begriffsverwendung von Risikoanalyse und Risikobewertung sollte überdacht werden.** Art. 2 Nr. 7 CER-Richtlinie[4] benutzt in der deutschen Fassung den Begriff der Risikobewertung und in der englischen Fassung den Begriff des „risk assessment“. Der Begriff

[3] Siehe hierzu näher: https://www.vku.de/themen/recht/artikel/betriebsfuehrung-durch-dritte/.
[4] Richtlinie (EU) 2022/2557.

des „risk assessment“ kommt erkennbar aus der gleichlautenden Verwendung in internationalen Normen zum Risikomanagement. Insbesondere kann hier auf die Norm ISO/IEC 31000:2009 verwiesen werden. Dieser Begriff wird üblicherweise im Deutschen mit dem Begriff der Risikobeurteilung und nicht mit dem Begriff der Risikobewertung übersetzt. Der Begriff der Risikobewertung ist dagegen in den internationalen Normen Teil der Risikobeurteilung. Die Risikobeurteilung besteht danach aus den folgenden Schritten[5]:

- Risikoidentifikation (risk identification)
- Risikoanalyse (risk analysis)
- Risikobewertung (risk evaluation)

Die zuvor beschriebenen Schritte der Risikobeurteilung finden sich so in der englischsprachigen Definition des Begriffs „risk assessment“ in Art. 2 Nr. 7 CER-Richtlinie wieder. Es scheint sich somit um einen Übersetzungsfehler in der CER-Richtlinie zu handeln. Der Begriff „risk asssessment“ hätte wohl mit Risikobeurteilung und nicht mit Risikobewertung übersetzt werden müssen.

**Es wird gefordert, statt der Begriffe Risikoanalyse und Risikobewertung einheitlich den Begriff der Risikobeurteilung zu verwenden. Entnommen werden kann die Begriffsdefinition aus der Art. 7 CER-Richtlinie. Zudem sollte ein Verweis in der Gesetzesbegründung auf die internationalen Normen erfolgen.**

**Formulierungsvorschlag**

**§ 2 Begriffsbestimmungen**

[…]

**Nr. 7a „Risikobeurteilung“ der gesamte Prozess zur Bestimmung der Art und des Ausmaßes eines Risikos, bei dem potenzielle entsprechende Bedrohungen, Schwachstellen und Gefahren, die zu einem Sicherheitsvorfall führen könnten, ermittelt und analysiert und die durch den Sicherheitsvorfall verursachten potenziellen Verluste oder Störungen bei der Erbringung eines wesentlichen Dienstes bewertet werden;**

~~**8. „Risikoanalysen“ das systematische Verfahren zur Bestimmung des Risikos;**~~

~~**9. „Risikobewertungen“ der Prozess des Vergleichs und der Priorisierung von Risiken in Bezug auf deren Wirkung auf die kritische Dienstleistung und das Treffen von Entscheidungen hinsichtlich der**~~

[5] Siehe beispielsweise die Wiedergabe dieser Reinfolge im BSI-Standard 200-3, S. 6, 53.

Im deutschen Sprachgebrauch wird teilweise eine andere Terminologie verwendet. Insbesondere im BSI-Standard 200-3 wird ausgeführt:

> „Im deutschen Sprachgebrauch hat sich allerdings der Begriff „Risikoanalyse“ für den kompletten Prozess der Risikobeurteilung und Risikobehandlung etabliert. Daher wird im IT-Grundschutz und auch in diesem Dokument weiter der Begriff „Risikoanalyse“ für den umfassenden Prozess benutzt.“

Die Ausführungen in der Gesetzesbegründung zur Verwendung des deutschen Begriffs „Risikoanalyse“ erschließen sich somit nicht ohne weiteres. Insbesondere wird keine Quelle zu diesem Verständnis angegeben. **Es wird gefordert, die Gesetzesbegründung wie zuvor beschrieben anzupassen.**

bb. Risikobehandlungsplan als alternativer Begriff zum Begriff des Resilienzplans

Im Rahmen des Risikomanagements erfolgt nach der Risikobewertung die Risikobehandlung (risk treatment). Wichtiger Teil dieser Risikobehandlung ist das Aufstellen eines Risikobehandlungsplans (risk treatment plan). In diesem Handlungsplan werden die Entscheidungen darüber, wie die identifizierten Risiken behandelt werden, dokumentiert. Faktisch wird das Gesamtkonzept der Risikobehandlung festgeschrieben. Es wird vermutet, dass eben dies mit dem in § 11 Abs. 6 KRITIS-DachG genutzten Begriff des Resilienzplans gemeint ist. **Um auch hier die internationalen Normen abzubilden, sollte statt des Begriffs des Resilienzplans der Begriff des Risikobehandlungsplans verwendet werden und entsprechend den internationalen Normen definiert werden.**

**Formulierungsvorschlag**

**§ 2 Begriffsbestimmungen**

[…]

**<u>Nr. 7b „Risikobehandlungsplan“ Beschreibung des Gesamtkonzepts der Risikobehandlung nach Vornahme der Risikobeurteilung.</u>**

Nähere Ausführungen zum Resilienzplan erfolgen in der Kommentierung von § 11 Abs. 6 KRITIS-DachG.

**f. Nr. 10 – Vorfall**

**Es sollte darüber nachgedacht werden, den Begriff des Vorfalls anders zu benennen.** Hintergrund ist, dass der Begriff des „Sicherheitsvorfalls“ in § 1 Abs. 1 Nr. 37 BSIG in der Praxis häufig als Vorfall bezeichnet wird. Dies kann zu Missverständnissen in der täglichen

Arbeit in den Unternehmen führen.

**g. Nr. 11 und Nr. 12 – (Besonders) wichtige Einrichtungen**
Auch diese Definitionen sind eine Doppelung zu § 28 Abs. 6, 7 BSIG und werden innerhalb des KRITIS-DachG nur in der Verordnungsermächtigung in § 15 KRITIS-DachG verwendet. **Auch hier wird eine einheitliche Definition an nur einer Stelle gefordert.** Zudem werden innerhalb der Definition die Begriffe „Großunternehmen“ und „mittleres Unternehmen“ genutzt, ohne diese Begriffe weiter zu definieren. Es kann nur vermutet werden, dass es sich um die Begriffe handelt, wie sie in § 2 Abs. 1 Nr. 12 BSIG definiert werden. Aus sich selbst heraus verständlich sind diese Begriffe jedoch nicht. **Sollte die Definition im KRITIS-DachG bestehen bleiben, so muss eine entsprechende Klarstellung erfolgen.**

**3. § 4 KRITIS-DachG – Kritische Anlagen**
Zunächst wird auf die Anmerkungen zu § 2 Nr. 3 KRITIS-DachG verwiesen.

Ergänzend lässt sich feststellen, dass Aussagen getroffen werden zum zeitlichen Anwendungsbereich, also ab wann eine Anlage bei Überschreiten der Schwellenwerte als kritische Anlage gilt (§ 4 Abs. 1 KRITIS-DachG). Gleiches gilt für den umgekehrten Fall, also ab wann die Anlage nicht mehr als kritische Anlage gilt (§ 4 Abs. 2 KRITIS-DachG). Diese Regelungen finden sich bisher ausschließlich in der Kritis-Verordnung und können sich je nach Sektor und konkreter Anlage unterscheiden (siehe z.B. für den Sektor Energie Anhang 1, Teil 1 Nr. 3, 4 Kritis-Verordnung). In der parallelen Regelung in § 28 Abs. 3 BSIG wird auf den zeitlichen Anwendungsbereich dagegen kein Bezug genommen. **Auch hier wird eine einheitliche Definition an nur einer Stelle gefordert. Allerdings sollte der zeitliche Anwendungsbereich deutlicher als bisher aus dem Gesetz oder der Kritis-Verordnung ersichtlich sein.** In der Praxis ist häufig zu beobachten, dass die entsprechende Stelle in der Kritis-Verordnung nicht bekannt ist. **Hierbei muss jedoch die bisherige Regel aus der Kritis-Verordnung beibehalten werden, dass jeweils immer auf die Werte des Vorjahres abgestellt wird, um die Eigenschaft als kritische Anlage zu bestimmen. Zudem müssen auch die bisher gewährten 3 Monate Übergangsfrist weiterhin gelten** (siehe z.B. für den Sektor Energie Anhang 1, Teil 1 Nr. 3, 4 Kritis-Verordnung).

**4. § 5 KRITIS-DachG - Verhältnis zu weiteren spezialgesetzlichen Regelungen**
Gemäß § 5 Abs. 1 KRITIS-DachG bleiben andere über die Mindestvorgaben nach diesem Gesetz hinausgehende Anforderungen an die Betreiber kritischer Anlagen 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.**

In § 5 Abs. 2 KRITIS-DachG wird explizit der Hinweis gegeben, dass insbesondere die Län-

der auf Grund einer unterschiedlichen Betrachtungsebene oder zu einem anderen Schutzzweck noch weitere Gesetzgebung zur Stärkung der Resilienz von Organisationen oder Einrichtungen treffen können. Aus Gründen der Gesetzgebungszuständigkeit ist diese Klarstellung sicherlich richtig, schafft aber in der Praxis ganz erhebliche Probleme.

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 17 verschiedenen Aufsichtsbehörden austauschen (16 Bundesländer + Bundesebene). Falls keine gute Abstimmung erfolgt, würde sich das gleiche auch für den Bereich der IT-Sicherheit ergeben. Es würde somit zu einer ähnlichen Situation wie im Datenschutz kommen, wo auch jedes Bundesland seine eigenen Regelungen und Aufsichtsbehörden hat. Ergänzend erlassen teilweise auch noch Landkreise ihre eigenen Regeln. Dies ist nicht praktikabel und führt zu enormen Mehraufwänden für die Unternehmen. Zudem leidet die Sicherheit insgesamt, da ein solch komplexes Zusammenspiel von keinem Unternehmen (und auch keiner Behörde) mehr durchdrungen werden kann. Es würden die dringend benötigen Ressourcen nicht in die Erhöhung der Sicherheit, sondern in Beratungsleistungen fließen, um herauszufinden welche Regelungen für das eigene Unternehmen gelten.

**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.**

**f. § 6 KRITIS-DachG – Anforderungen an Betreiber Kritischer Infrastrukturen**

Nach § 6 KRITIS-DachG können bestimmte Resilienzmaßnahmen auch von Betreibern von kritischen Infrastrukturen ergriffen werden, die nicht die maßgeblichen Schwellenwerte

erreichen und deshalb nicht im Anwendungsbereich des KRITIS-DachG sind (§ 6 Abs. 1 KRITIS-DachG). Auch können sie branchenspezifische Resilienzstandards berücksichtigen (§ 6 Abs. 2 KRITIS-DachG). Es ist unklar, welchen Regelungsgehalt diese Normen haben. Das Unternehmen zusätzliche Resilienzmaßnahmen treffen können, zu denen sie aber nicht verpflichtet sind, bedarf keiner gesetzlichen Regelung. Auch die Gesetzesbegründung bleibt vage. Es heißt dort: „So wird ein starker Appell dahingehend ausgesprochen, dass auch kleinere und mittlere Unternehmen Maßnahmen zur Stärkung ihrer Resilienz ergreifen."

**§ 6 KRITIS-DachG sollte mangels Regelungsgehalt ersatzlos gestrichen werden**
Will man auch nicht vom KRITIS-DachG erfasste Unternehmen dazu bringen, zusätzliche Resilienzmaßnahmen umzusetzen, kann dies beispielsweise über eine entsprechende finanzielle Förderung geschehen oder aber durch die Anerkennung dieser Kosten im Rahmen der Refinanzierung (siehe zu diesem Aspekt näher unter Nr. 11.b).

**5. § 8 KRITIS-DachG – Registrierung der kritischen Anlage**
Positiv zu bemerken ist zunächst, dass die Registrierung an einer einheitlich mit zwischen BBK und BSI betriebenen Registrierungsstelle vorgenommen werden kann. Hierdurch werden Doppelmeldungen vermieden und ein weniger an Bürokratie erzielt.

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 § 8 KRITIS-DachG, als auch in § 32 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. § 8 Abs. 2 KRITIS-DachG und § 32 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. 7 auf der einen Seite und die nur rudimentären Anforderungen aus § 8 Abs. 1 KRITIS-DachG). Auch finden sich die Passage der einheitlichen Kontaktstelle nur in § 8 Abs. 1 KRITIS-DachG und nicht in § 32 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.**

Soweit bekannt soll der Begriff des Betreibers der kritischen Infrastruktur aus dem aktuell geltenden § 2 Abs. 10 BSIG 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 über die erfolgte Übertragung der Betreibereigenschaft in das gemeinsame Register an den Betreiber der kritischen Anlage erfolgen**. So werden Doppelaufwände für die Unternehmen vermieden, zu denen es unweigerlich bei einer erneuten Registrierung kommen würden.

**6. § 9 KRITS-DachG - Nationale Risikoanalysen und Risikobewertungen**

Im Gesetz wird nicht angegeben, bis wann eine staatliche Risikoanalyse und Risikobewertung durchgeführt werden muss. Es lässt sich vermuten, dass eine solche Risikoanalyse und Risikobewertung in Umsetzung von Art. 5 Abs. 1 CER-Richtlinie bis zum 17. Januar 2026 erfolgen soll. Aus dem deutschen Gesetzestext ergibt sich dies jedoch nicht. **Es wird gefordert, den Zeitpunkt verbindlich im Gesetz festzulegen**. Dies ist insbesondere deshalb wichtig, da auf Grundlage dieser nationalen Risikoanalyse und Risikobewertung die Risikoanalyse und Risikobewertung der Betreiber stattfinden soll (vgl. zu den Problemen, falls eine solche nicht vorliegt, die Kommentierung zu § 10 KRITIS-DachG).

**Überdies muss im Gesetz 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**

**§ 9 Nationale Risikoanalysen und Risikobewertungen**

(1) Die für die Sektoren zuständigen Bundesministerien führen **nach Anhörung von Vertretern der betroffenen Betreiber und Einrichtungen und der betroffenen Wirtschaftsverbände erstmals bis zum 17. Januar 2026 und dann spätestens** alle vier Jahre oder auf Veranlassung für die auf der Grundlage der Rechtsverordnung nach § 15 bestimmten kritischen Dienstleistungen Risikoanalysen und -bewertungen gemäß ihren fachlichen und sektorspezifischen Zuständigkeiten durch, die mindestens […]

**Weiterhin ist eine 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.

Im Hinblick auf die durch die Bundesministerien durchzuführenden Risikoanalysen und Risikobewertungen stellt sich die Frage, warum diese nur dem BBK und nicht auch dem BSI zur Verfügung gestellt werden sollen und warum nicht eine explizite Zusammenarbeit von BBK und BSI festgeschrieben wird im Rahmen der Information der Betreiber von kritischen Anlagen (§ 9 Abs. 2 KRITIS-DachG).
**Es wird gefordert, dass die den Betreibern von kritischen Anlagen zu übermittelnden Informationen über die nationale Risikoanalyse und Risikobewertung in einer zwischen dem BBK und dem BSI abgestimmter Form übermittelt wird.** Im Rahmen der hybriden Bedrohungen können Bedrohungslagen aus dem Cyberraum und dem physischen Raum nicht getrennt werden, sondern müssen zusammen verarbeitet werden.

**Formulierungsvorschlag**

**§ 9 Nationale Risikoanalysen und Risikobewertungen**

(2) Die Bundesministerien stellen dem BBK **und dem BSI** die Risikoanalysen und -bewertungen zur Verfügung. Das BBK **und das BSI** werten die durch die Bundesministerien durchgeführten Risikoanalysen und -bewertungen **gemeinsam** sektorenübergreifend aus und stellen die entsprechenden Elemente der Risikoanalysen und -bewertungen den Betreibern kritischer Anlagen nach § 4 zur Verfügung.

## 7. § 10 KRITIS-DachG - Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen

### a. § 10 Abs. 1 KRITIS-DachG

Nach § 10 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 Informationsquellen erstmals neun Monate nach der Registrierung als kritische Anlage nach § 8 KRITIS-DachG, und dann spätestens alle vier Jahre erfolgen.

Zunächst stellt sich die Frage, ob Grundlage der Risikoanalyse und Risikobewertung der Betreiber zwangsläufig immer die staatliche Risikoanalyse und Risikobewertung nach § 9 KRITIS-DachG sein muss oder ob diese Informationen gleichrangig zu den „anderen Informationsquellen“ aus § 10 Abs. 1 KRITIS-DachG stehen. **Es wird gefordert, klarzustellen, ob die staatliche Risikoanalyse zwangsläufig berücksichtigt werden muss oder nicht.**

**Zudem darf die Frist zur Umsetzung betrieblichen Risikoanalyse und –bewertung erst anfangen zu laufen, wenn seinerseits die staatliche Risikoanalyse und –bewertung vorliegt.**

**Formulierungsvorschlag**

**§ 10 Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen**

**(1)** [S. 1 …] **Liegt im Zeitpunkt der Registrierung als kritische Anlage die nationale Risikoanalyse und Risikobewertung nach § 9 nicht vor, so beginnt die Frist nach S. 1 erst zu laufen, nachdem das BBK dem Betreiber der kritischen Anlage die entsprechenden Elemente der Risikoanalyse und Risikobewertung nach § 9 Abs. 2 zur Verfügung gestellt hat.** (S. 2 neu)

Hintergrund ist, dass im Gesetz nicht angegeben wird, wann eine staatliche Risikoanalyse und Risikobewertung vorliegt. Es lässt sich vermuten, dass eine solche Risikoanalyse und Risikobewertung in Umsetzung von Art. 5 Abs. 1 CER-Richtlinie bis zum 17. Januar 2026 erfolgen soll. Aus dem deutschen Gesetzestext ergibt sich dies jedoch nicht (siehe hierzu schon zuvor zu § 9 KRITIS-DachG). Es stellt sich jedoch die Frage, auf welcher Grundlage die Risikoanalyse und Risikobewertung durch die Betreiber vorgenommen werden soll, wenn zu diesem Zeitpunkt keine nationale Risikoanalyse und Risikobewertung vorliegt oder sie erst verspätet erfolgt. Die Unternehmen haben neun Monate nach der Registrierung Zeit ihre Risikoanalyse und Risikobewertung durchzuführen. Erfolgt die Registrierung am 02.01.2026 müssten Sie bis zum 02.10.2026 eine entsprechende Risikoanalyse und Risikobewertung durchführen. Dieser bereits nicht besonders lange Zeitraum könnte noch weiter verkürzt werden, wenn sich beispielsweise die staatliche Risikoanalyse und Risikobewertung verzögert.

Der Hinweis in der Gesetzesbegründung auf eine Mitteilung nach § 10 Abs. 8 KRITIS-DachG wird als Redaktionsversehen interpretiert. Es müsste wohl § 8 KRITIS-DachG heißen. **Dies muss jedoch klargestellt werden.**

Weiter spricht sowohl § 10 Abs. 1 Nr. 1 als auch Nr. 2 von Risiken, die die Wirtschaftsstabilität der Betreiber der kritischen Anlagen beeinträchtigen können. Zunächst stellt sich die Frage, was unter dem Begriff der Wirtschaftsstabilität zu verstehen ist. Dieser Begriff wird weder im KRITIS-DachG noch in der CER-Richtlinie definiert. Zudem ist fraglich, ob dieser Begriff überhaupt sinnvoll ist. In der Gesetzesbegründung wird wörtlich ausgeführt:

> „Dazu sieht die Vorschrift vor, Betreiber kritischer Anlagen zu verpflichten, diejenigen Risiken zu analysieren und zu bewerten, die die Aufrechterhaltung ihres Geschäftsbetriebs und damit die Erbringung ihrer kritischen Dienstleistung stören oder unterbrechen können."

Es ist wird nicht klar herausgearbeitet, ob es nun um Risiken geht, die insgesamt die Aufrechterhaltung des Geschäftsbetriebs betreffen, nur solche Risiken, die die wirtschaftliche Grundlage des Geschäftsbetriebs betreffen oder aber die Risiken, die speziell für die kritischen Dienstleistungen bestehen. Eine klare Entscheidung ist jedoch notwendig, um den Scope (auch genannt Geltungsbereich) der Risikobetrachtung zu bestimmen. Dabei wäre es konsequent nur die kritische Dienstleistung in den Blick zu nehmen und nicht den gesamten Geschäftsbetrieb. Ein solches Vorgehen ist im Bereich des IT-Sicherheitsrechts langjährige Praxis. **Es wird deshalb gefordert, dass nur die Risiken für die kritischen Dienstleistungen betrachtet werden müssen. Der Begriff der Wirtschaftsstabilität sollte nicht verwendet werden.**

**Formulierungsvorschlag**

**§ 10 Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen**

**(1)** […]
**1.** die entsprechenden**, die kritischen Dienstleistungen ~~Wirtschaftsstabilität~~ beeinträchtigenden,** naturbedingten, klimatischen und vom Menschen verursachten Risiken berücksichtigen, darunter solche sektorübergreifender oder grenzüberschreitender Art, Unfälle, Naturkatastrophen, gesundheitliche Notlagen, sowie hybride Bedrohungen oder andere feindliche Bedrohungen, einschließlich terroristischer Straftaten gemäß der Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates und

**2.** die entsprechenden, **die kritischen Dienstleistungen ~~Wirtschaftsstabilität~~ beeinträchtigenden**, Risiken berücksichtigen, die sich aus dem Ausmaß der Abhängigkeiten anderer Sektoren von der kritischen Dienstleistung, die von der kritischen Anlage - auch in benachbarten Mitgliedstaaten und Drittstaaten - erbracht wird, und dem Ausmaß der Abhängigkeit der kritischen Anlage von den kritischen Dienstleistungen, die von anderen Anlagen in anderen Sektoren - auch in benachbarten Mitgliedstaaten und Drittstaaten - erbracht wird, Rechnung tragen.

**Wird der Begriff der Wirtschaftsstabilität verwendet, so muss er definiert werden**. Es stellt sich beim Begriff der Wirtschaftsstabilität die Frage, ob die Wirtschaftsstabilität des Betreibers, die Wirtschaftsstabilität der Kunden oder die gesamtwirtschaftliche Wirtschaftsstabilität Deutschlands gemeint ist (siehe hierzu die ähnliche Kommentierung zu § 2 Nr. 2 KRITIS-DachG zum Begriff der wirtschaftlichen Tätigkeit). **Es wird gefordert, die Wirtschaftsstabilität nur auf die volkswirtschaftlichen Risiken zu beziehen. Sollte auf die Wirtschaftsstabilität des Betreibers abgestellt werden, so muss der Begriff eng definiert werden und sich ausschließlich auf existenzbedrohende Risiken beziehen, nämliche solche, die bei Verwirklichung zum Einstellen der kritischen Dienstleistung führen würden.**

Nicht weiter im Gesetz wird darauf eingegangen, wie diese Risikoanalyse– und Bewertung vorgenommen werden soll. Dies ist nicht sinnvoll, denn den Unternehmen muss die Prüfgrundlagen bekannt sein. **Zumindest sollte in der Gesetzesbegründung klargestellt werden, dass hierfür international anerkannte Standards wie z.B. die ISO 31000 („Risikomanagement – Grundsätze und Richtlinien“) oder auch die darauf aufbauenden Standards wie die ISO 27001 (ISMS), die ISO 9001 (Qualitätsmanagement oder die ISO 14001 (Umweltmanagement) herangezogen werden dürfen** (siehe hierzu bereits ausführlich die Kommentierung zu § 2 Nr. 8, 9 KRITIS-DachG)**.**

**b. § 10 Abs. 2 KRITIS-DachG**

Positiv zu bemerken ist, dass nach § 10 Abs. 2 KRITIS-DachG ein Betreiber einer kritischen Anlage die Anforderungen aus § 10 Abs. 1 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. 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 § 10 Abs. 2 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 § 10 Abs. 1 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 das BBK und die zuständige Aufsichtsbehörde des Bundes 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.**

Zusätzlich sind Auskunftspflichten und die Bereitstellungen von Dokumenten und Listen insbesondere im Rahmen von Zertifizierungsverfahren im Rahmen des KRITIS-Dachgesetzes kritisch zu hinterfragen. Bspw. wird zunehmend bei Zertifizierungsverfahren gemäß

IT-Sicherheitskatalog die Herausgabe von vollständigen Listen der kritischen Informationswerte (Hardwarelisten) und Listen nicht dauerhaft besetzter Standorte durch die Zertifizierer gefordert. Dies steht im Konflikt zum Schutz vertraulicher und sensibler Daten, da an zentralen Stellen sensible Daten mehrere Betreiber gesammelt werden und damit das Risiko einer unbeabsichtigten Veröffentlichung erhöht wird. Bereits den Auditoren wird im Regelfall lediglich ein Einsichtsrecht in den Räumlichkeiten der Unternehmen gewährt und die sensiblen Unterlagen nicht übermittelt. **Es wird gefordert, dass die vom Auditor bewertete Risikoanalyse und Risikobewertung alleine durch die Vorlage des Prüfvermerk als äquivalent angesehen wird.**

**Formulierungsvorschlag**

**§ 10 Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen**

**(2)** [S. 1, 2…] **Die Vorlage der bestehenden Risikoanalyse und Risikobewertung durch den Betreiber der kritischen Anlage an das BBK nach S. 2 ist freiwillig und lässt die Anrechnungsmöglichkeit für die Risikoanalyse und Risikobewertungen nach S. 1 unberührt. Wird die bestehenden Risikoanalysen und Risikobewertungen nach S. 2 durch den Betreiber der kritischen Anlage vorgelegt, so unterrichtet das BBK 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. Statt der Risikoanalyse und Risikobewertung können die Betreiber auch das Ergebnis eines Audits über die Risikoanalyse und Risikobewertung vorlegen. In einem solchen Fall gilt die Äquivalenzprüfung ebenfalls als positiv beschieden.**

**Zudem muss sichergestellt sein, dass auch der Staat (Bund/Länder/Kommune) die entsprechenden Schutzpflichten für die Informationssicherheit einhält, damit die sensiblen Daten der Unternehmen angemessen geschützt werden.**

**8. § 11 Kritis-DachG - Resilienzmaßnahmen der Betreiber kritischer Anlagen**

**a. § 11 Abs. 1 KRITIS-DachG**

Bei § 11 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 § 11 Abs. 1 KRTIS-DachG und aus § 30 Abs. 1 BSIG möglichst weitgehend aufeinander**

**abgestimmt werden und parallel laufen.**

Nach § 11 Abs. 1 KRITIS-DachG müssen sich die Maßnahmen zudem auf die staatliche Risikoanalyse nach § 9 KRITIS-DachG stützen. **Es wird gefordert, klarzustellen, ob die staatliche Risikoanalyse zwangsläufig berücksichtigt werden muss oder nicht. Zudem darf die Frist zur Umsetzung der Resilienzmaßnahmen erst anfangen zu laufen, wenn seinerseits die staatliche Risikoanalyse und Risikobewertung vorliegt**. Zur Begründung wird auf die entsprechenden Ausführungen in § 10 Abs. 1 KRITIS-DachG verwiesen. Ein Formulierungsvorschlag wird in der Kommentierung zu § 11 Abs. 13 KRITIS-DachG gegeben.

Für den Begriff des Stands der Technik existiert 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“[6] 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*

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

*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 § 11 Abs. 1 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**.

**b. § 11 Abs. 2 KRITIS-DachG**

Positiv zu bemerken ist, dass laut Gesetzesbegründung bei der Abwägung 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 unter 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. 2 BSIG geschehen.

**Formulierungsvorschlag**

**§ 11 Resilienzmaßnahmen der Betreiber kritischer Anlagen**

(1) […]
(2) Technische, sicherheitsbezogene und organisatorische Maßnahmen sind verhältnismäßig, wenn der Aufwand zur Verhinderung oder Begrenzung eines Ausfalls oder einer Beeinträchtigung der kritischen Dienstleistung zu den Folgen ihres Ausfalls oder ihrer Beeinträchtigung 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.**

**c. § 11 Abs. 3 KRITIS-DachG**

Zunächst ist dieser Absatz sprachlich anzupassen. Richtigerweise bezeichnet die Gesetzesbegründung die Nr. 1 – 6 als Ziele, die die Maßnahmen erreichen sollen. **Der Gesetzeswortlaut muss insofern angepasst werden.**

Es stellt sich weiterhin die Frage, ob die dort aufgezählten Ziele abschließend alle Ziele bezeichnet, die im Hinblick auf die Resilienz des Unternehmens betrachtet werden sollen, oder ob es sich lediglich um eine beispielhafte Aufzählung handelt. **Es wird gefordert klarzustellen, dass es sich lediglich um eine nicht abschließende Aufzählung der Ziele handelt.**

**Formulierungsvorschlag**

**§ 11 Resilienzmaßnahmen der Betreiber kritischer Anlagen**

(3) ~~**Zu den Maßnahmen zählen Maßnahmen, die erforderlich sind, um**~~ **Die Umsetzung der Maßnahmen nach Abs. 1 dienen insbesondere der Erreichung der folgenden Ziele:**

**d. § 11 Abs. 4 KRITIS-DachG und Anhang 1**

In § 11 Abs. 4 KRITIS-DachG erfolgt ein Verweis auf § 11 Abs. 2 KRITIS-DachG, während im Anhang 1 selbst ein Verweis auf § 11 Abs. 1 KRITIS-DachG erfolgt. **Der Verweis müsste richtigerweise auf § 11 Abs. 1 KRITIS-DachG lauten. Dies sollte angepasst werden.**

**e. § 11 Abs. 5 KRITIS-DachG**

Sehr positiv ist, dass gemäß § 11 Abs. 5 KRITIS-DachG die Möglichkeit eröffnet wurde, branchenspezifische Sicherheitsstandards zu erarbeiten. 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. 12 BSIG).

**Einzig § 11 Abs. 5 S. 2 Nr. 5 KRITIS-DachG sollte angepasst werden.** Dort wird der unbestimmte Artikel „einer“ genutzt, während der bestimmte Artikel „der“ deutlich mehr Sinn ergibt.

Zudem hebt die Gesetzesbegründung richtigerweise den UP Kritis als besonders wichtige Institution hervor. Allerdings werden nicht nur im UP Kritis branchenspezifische Standards entwickelt, sondern auch außerhalb des UP Kritis direkt über die Branchen- und Spitzenverbände der Unternehmen. **Dies sollte in der Gesetzesbegründung klargestellt werden.**

**f. § 11 Abs. 6 KRITIS-DachG**

§ 11 Abs. 6 KRITIS-DachG beschreibt zwei voneinander zu unterscheidende Pflichten: In § 11 Abs. 6 S. 1 KRITIS-DachG wird die Pflicht aufgestellt, dass Betreiber von kritischen Anlagen die Maßnahmen nach Abs. 1 in einem Resilienzplan darstellen müssen. In § 11 Abs. 6 S. 2 KRITIS-DachG wird dagegen die Pflicht aufgestellt, die Aufstellung dieses Resilienzplans gegenüber dem BBK nachzuweisen.

In Bezug auf § 11 Abs. 6 S. 1 KRITIS-DachG stellt sich die Frage, was genau in diesem Resilienzplan festgehalten werden soll, denn der Begriff des Resilienzplans wird nicht weiter definiert (siehe hierzu bereits die Kommentierungen zu § 2 Nr. 8, 9 KRITIS-DachG). 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 und um beides? Der Begriff des Resilienzplans spricht für die erste Möglichkeit. Auf der

anderen Seite stellt die Gesetzesbegründung auf „getroffenen Maßnahmen“ ab, was für eine Beschränkung auf bereits durchgeführte Maßnahmen spricht. **Es wird gefordert im Wortlaut des Gesetzes festzulegen, dass Inhalt des Resilienzplans (bzw. Risikobehandlungsplans) sowohl die bereits getroffenen Maßnahmen als auch die geplanten Maßnahmen zur Behandlung der erkannten Risiken umfassen.**

In Bezug auf § 11 Abs. 6 S. 2 KRITIS-DachG stellt sich die Frage, warum der Zeitpunkt des Nachweises des Resilienzplans bei der Registrierung als kritische Anlage anscheinend frei (also nach § 11 Abs. 13 KRITIS-DachG nach Ablauf von 10 Monaten nach Registrierung) vom BBK bestimmt werden kann. Dies ist nicht akzeptabel. **Es muss für die Unternehmen gesetzlich klar geregelt sein, bis wann die entsprechenden Nachweise erbracht werden müssen, insbesondere, weil Abhängigkeiten von der staatlichen Risikoanalyse und –bewertung bestehen.** Ein Formulierungsvorschlag zur Nachweisfrist wird in der Kommentierung zu § 11 Abs. 13 KRITIS-DachG gegeben.

Auch der anschließende Nachweis alle zwei Jahre ist nicht zielführend. **Wie auch im Bereich NIS2UmsuCG zu fordern ist, sollte der Nachweiszeitraum auf drei Jahre festgelegt werden, weil dies den internationalen Normen der ISO 27000-Reihe entspricht.** Anderenfalls kommt es zu Doppelaufwänden für die Unternehmen, weil sie die Nachweise zweimal erbringen müssen zu unterschiedlichen Zeitpunkten. **Von entscheidender Bedeutung ist, dass die Nachweiszeiträume im NIS2UmsuCG und im KRITIS-DachG parallel ausgestaltet werden, damit die Audits nur einmal und zwar gemeinsam durchgeführt werden müssen.**

**Formulierungsvorschlag**

**§ 11 Resilienzmaßnahmen der Betreiber kritischer Anlagen**

(6) Die Betreiber kritischer Anlagen müssen die **getroffenen und geplanten** Maßnahmen nach Absatz 1 in einem Resilienzplan darstellen. Der Resilienzplan ist dem BBK spätestens ~~**zu einem vom BBK bei der Registrierung im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik**~~ **zum gemäß § 11 Abs. 13 Kritis-DachG** festgelegten Zeitpunkt und anschließend alle ~~**zwei**~~ **drei** Jahre nachzuweisen.

**g. § 11 Abs. 7 KRITIS-DachG**

Positiv ist, dass gemäß § 11 Abs. 7 KRITIS-DachG in Bezug auf § 11 KRITIS-DachG der Verwaltungsaufwand reduziert werden soll und insbesondere Dokumente und ähnliche Nachweise aus anderen Bereichen der Resilienzsteigerung vorgelegt werden können. Allerdings ist der Regelungsbereich und Regelungsumfang unklar.

Zunächst stellt sich die Frage, welcher Fall genau mit § 11 Abs. 7 S. 1 Var. 1 KRITIS-DachG erfasst werden soll. So bleibt zunächst unklar, was genau mit Dokumenten gemeint ist. Es

kann sich hierbei wohl nicht um Nachweise zur Resilienzsteigerung handeln, denn dieser Fall ist spezieller in § 11 Abs. 7 S. 4 KRITIS-DachG geregelt und umfasst insbesondere die Dokumentenarten der Bescheide, Genehmigungen und Zertifizierungen. Nach § 11 Abs. 7 S. 1 Var. 1 KRITIS-DachG sollen die Dokumente zur Stärkung der Resilienz erstellt worden sein. Wahrscheinlich soll es sich um Teile des Resilienzplans nach § 11 Abs. 6 S. 1 KRITIS-DachG handeln. Hierfür spricht der Verweis in § 11 Abs. 7 S. 2 KRITIS-DachG auf § 11 Abs. 6 S. 2 KRITIS-DachG. Es bleibt im Grunde aber unklar, was genau hiermit gemeint ist, insbesondere, weil pauschal auf die nach § 11 KRITIS-DachG zu erfüllenden Anforderungen verwiesen wird und nicht die Anforderungen genau genannt werden. § 11 Kritis-DachG enthält jedoch eine Vielzahl von Anforderungen, so dass der Verweis unklar bleibt.

Ein ähnliches Problem stellt sich für die Maßnahmen zur Stärkung der Resilienz (§ 11 Abs. 7 S. 1 Var. 2 KRITIS-DachG). Auch hier ist nicht ganz klar, auf welche Pflichten dies angerechnet werden kann.

**Aus diesem Grund wird gefordert in der Gesetzesbegründung klarzustellen, welche Dokumente in § 11 Abs. 7 S. 1 KRITIS-DachG gemeint werden und in Bezug auf welche Pflichten in § 11 die vorhandenen Dokumente/Maßnahmen angerechnet werden können.**

§ 11 Abs. 7 S. 3 und S. 4 KRITIS-DachG nimmt Bezug auf die Maßnahmen und beschreibt wohl, wie die Maßnahmen nach § 11 Abs. 7 S. 1 KRITIS-DachG verwendet werden können. § 11 Abs. 7 S. 3 KRITIS-DachG adressiert wahrscheinlich nur Maßnahmen, über die kein Nachweis wie ein Bescheid, Genehmigung oder Zertifizierung erstellt wurde. Dies folgt aus der Spezialregelung des § 11 Abs. 7 S. 4 KRITIS-DachG, der diesen Fall regelt. Anscheinend soll nach § 11 Abs. 7 S. 3 für jede Maßnahme, die getroffen wurde ohne entsprechendes Zertifikat o.ä., eine Äquivalenzprüfung durchgeführt werden. Zudem würde dies wohl als Konsequenz heißen, dass das BBK selbst überprüfen müsste, ob ein Betreiber die technisch organisatorischen Maßnahmen einhält. Ob dies vom BBK geleistet werden kann, wird bezweifelt. Weiterhin ist unklar, ob die Maßnahmen nur anerkannt werden können, wenn eine entsprechende Äquivalenzprüfung vorgenommen wurde oder ob dies lediglich eine fakultative Möglichkeit darstellt (siehe hierzu auch die Ausführungen zu § 10 Abs. 2 KRITIS-DachG). **Es wird deshalb gefordert klarzustellen, welcher Fall der Maßnahmen in § 11 Abs. 7 S. 3 KRITIS-DachG gemeint ist. Ferner sollte klargestellt werden, dass die Äquivalenzprüfung lediglich ein durch die Unternehmen freiwillig zu beantragende Möglichkeit darstellt.**

**Formulierungsvorschlag**

**§ 11 Resilienzmaßnahmen der Betreiber kritischer Anlagen**

**(7)** [S. 1 -3 …] **Die Äquivalenzprüfung nach S. 3 wird nur auf Antrag des Betreibers der kritischen Anlage vorgenommen und lässt die Verwendung der Maßnahmen nach S. 1 unberührt. Wird durch den Betreiber ein Antrag auf Äquivalenzprüfung gestellt und die entsprechenden Unterlagen eingereicht, so unterrichtet das BBK 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.** [S. 4 – 6 neu]

Nach § 11 Abs. 7 S. 4 KRITIS-DachG kann der Betreiber einer kritischen Anlage Bescheide, Genehmigungen, Zertifizierungen oder ähnliche Nachweise zur Resilienzsteigerung von in anderem Zusammenhang zuständigen Behörden vorlegen und somit die darin beschriebenen Maßnahmen ohne weitere Überprüfung als nach § 11 festgelegten Anforderungen als erfüllt ansehen. Zunächst stellt sich die Frage, warum hierbei von den Nachweisarten aus der IT-Sicherheitsgesetzgebung gemäß § 34 Abs. 1 BSIG abgewichen wurde. Hier wird der Nachweis durch Sicherheitsaudits, Prüfungen und Zertifizierungen erbracht. Ferner ist auch der Begriff der Genehmigung nicht eindeutig. So hat sich beispielsweise im Bereich des Maßnahmenplans nach der Trinkwasserverordnung (vgl. § 50 Trinkwasserverordnung) ein informelles Verfahren ausgeprägt, bei dem der Plan lediglich zur Behörde gesendet wird und bei Nicht-Beanstandung davon auszugehen wird, dass eine Zustimmung erteilt wurde. Zudem sollen anscheinend nur Nachweise ausreichen, die von Behörden selbst erstellt wurden. Allerdings passt hier die Zertifizierung nicht ins Bild, da die Zertifizierung üblicherweise durch einen akkreditierten Dritten erbracht wird im Rahmen eines externen Audits. Das Zertifikat wird somit nicht durch eine Behörde, sondern einen privaten Dritten ausgestellt. Im Übrigen gibt es auch eine Vielzahl von anderen Formen der Nachweise, ob die erforderlichen Maßnahmen ergriffen wurden. Teilweise reicht z.B. auch eine Bescheinigung durch die interne Revision aus, um die Maßnahmen gegenüber dem BSI nachzuweisen (so z.B. aktuell im Rahmen der Systeme zur Angriffserkennung). Auch im Rahmen des Nachweises nach den B3S liegen teilweise andere Formen der Nachweise vor. **Es wird deshalb gefordert klarzustellen, welche Art von Nachweisen genau in welcher Form beigebracht werden dürfen, um die Erfüllung der Anforderungen nach § 11 nachzuweisen.**

**h. § 11 Abs. 8 KRITIS-DachG**

Es wird davon ausgegangen, dass der Resilienzplan und dessen Nachweis die zum Zeitpunkt des Inkrafttretens des Gesetzes bereits umgesetzten Maßnahmen, sowie die zukünftig geplanten Maßnahmen umfasst (siehe hierzu die Kommentierung zu § 11 Abs. 7 KRITIS-DachG). Dies angenommen umfasst der § 11 Abs. 8 KRITIS-DachG insbesondere

Maßnahmen, die im Resilienzplan geplant wurden und sodann umgesetzt wurden. **Es wird gefordert, diesen Zusammenhang deutlicher als bisher klarzustellen. Ferner darf die Frist zum Nachweis nicht in das Belieben der Behörden gestellt werden. Auch sind die Fristen den internationalen Normen entsprechend auf drei Jahre zu verlängern** (siehe bereits die Ausführungen zu § 11 Abs. 6 KRITIS-DachG). Ergänzende Ausführungen zur den Fristen finden sich in § 11 Abs. 13 KRITIS-DachG.

**Ferner muss die Möglichkeit bestehen, bereits durchgeführte Audits anrechnen zu lassen.** Diese sehr sinnvolle Regelung ist im restlichen Entwurf des KRITIS-DachG vorgesehen und sollte auch hier fortgeführt werden.

**Formulierungsvorschlag**

**§ 11 Resilienzmaßnahmen der Betreiber kritischer Anlagen**

(8) Betreiber kritischer Anlagen haben die Erfüllung der **nach Absatz 6 S. 1 geplanten Maßnahmen** ~~**Anforderungen nach Absatz 1**~~ spätestens ~~**zu einem vom BBK bei der Registrierung im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik**~~ **zum gemäß § 11 Abs. 13 Kritis-DachG** festgelegten Zeitpunkt und anschließend alle ~~**zwei**~~ **drei** Jahre dem BBK auf geeignete Weise nachzuweisen. Der Nachweis kann durch Audits erfolgen, **wobei auf bereits durchgeführte Audits in anderen Bereichen Bezug genommen werden kann.** […]

**Zudem wird gefordert, dass das BBK die nach § 11 Abs. 8 S. 7 KRITIS-DachG mögliche Ausgestaltung des Audits nur im Einvernehmen mit dem BSI vornimmt.** Beide Behörden müssen zusammenarbeiten, um möglichst einheitliche Anforderungen zu schaffen.

**i. § 11 Abs. 12 KRITIS-DachG**

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 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 Ländern abstimmt und gemeinsam genügend Kapazitäten aufbaut, um auch in solchen Fällen eine Sicherheitsüberprüfung anbieten zu können.**

**j. § 11 Abs. 13 KRITIS-DachG**

Gemäß § 11 Abs. 13 KRITIS-DachG sind die Verpflichtungen nach Absatz 1 bis 10 von den Betreibern der kritischen Anlagen frühestens nach Ablauf von zehn Monaten nach Registrierung als kritische Anlage nach § 4 KRITIS-DachG zu erfüllen.

Zunächst müsste der Verweis wohl auf § 8 KRTIS-DachG und nicht auf § 4 KRITIS-DachG lauten. In § 8 KRITIS-DachG ist die Registrierungspflicht geregelt. **Dies sollte angepasst werden.**

Weiter muss bedacht werden, dass die Absätze 1 bis 10 ganz unterschiedliche Verpflichtungen aufstellen. Grob kann unterschieden werden nach der Umsetzung der Maßnahmen und dem Nachweis über die Umsetzung der Maßnahmen. Beispielsweise wird in § 11 Abs. 1 KRITIS-DachG die Umsetzung von Maßnahmen gefordert, während die Pflicht zum Nachweis über die Umsetzung in § 11 Abs. 8 KRITIS-DachG aufgestellt wird. In § 11 Abs. 6 S. 1 KRITIS-DachG wird die Pflicht zur Aufstellung eines Resilienzplans aufgestellt, während § 11 Abs. 6 S. 2 KRITIS-DachG die Pflicht zum Nachweis über den Resilienzplan betrifft. Beide Pflichten sind nicht deckungsgleich, sondern müssen logisch getrennt werden. Dies ist z.B. bereits im Bereich der IT-Sicherheit lange geübte Praxis (siehe z.B. die Pflicht zur Umsetzung von Maßnahmen nach dem aktuell geltenden § 8a Abs. 1 BSIG im Vergleich zum zeitlich nachgelagerten Nachweis der Erfüllung der Maßnahmen nach dem aktuell geltenden § 8a Abs. 3 BSIG).

**Es wird gefordert, dass diese Pflichten im Rahmen der Umsetzungsfristen deutlicher voneinander unterschieden werden**. Bisher ist insbesondere unklar, ab wann die Pflicht zur Umsetzung gilt, denn die Festlegungsbefugnis des BBK in § 11 Abs. 6 S. 2 und Abs. 8 S. 1 KRITIS-DachG erfasst nur die Pflicht zum Nachweis der Umsetzung.

**Da auch die Umsetzung der Verpflichtungen nach § 11 Abs. 1- 10 KRITIS-DachG maßgeblich davon abhängt, dass die nationale Risikoanalyse und Risikobewertung nach § 9 KRITIS-DachG vorliegt, muss auch hier eine Abhängigkeit der Fristen geschaffen werden**. Auf die entsprechenden Ausführungen in der Kommentierung zu § 10 Abs. 1 KRITIS-DachG wird verwiesen.

**Formulierungsvorschlag**

**§ 11 Resilienzmaßnahmen der Betreiber kritischer Anlagen**

(13) Die Verpflichtungen nach Absatz 1 **und Absatz 6 S. 1** ~~**bis 10**~~ treffen die Betreiber der kritischen Anlage ~~**frühestens nach Ablauf von**~~ zehn Monate nach der Registrierung als kritische Anlage nach § **48**. **Liegt im Zeitpunkt der Registrierung als kritische Anlage die nationale Risikoanalyse und Risikobewertung nach § 9 nicht vor, so beginnt die Frist nach S. 1 erst zu laufen, nachdem das BBK dem Betreiber der kritischen Anlage die entsprechenden Elemente der Risikoanalyse und Risikobewertung nach § 9 Abs. 2 zur Verfügung gestellt hat. Die Betreiber der kritischen Anlagen haben die Nachweispflichten gemäß Absatz 6 S. 2 und Absatz 8 spätestens zwei Jahre nach dem in den Sätzen 1 und 2 genannten Zeitpunkt und anschließend alle drei Jahre gegenüber dem BBK zu erfüllen.**

**9. § 12 KRITIS-DachG - Meldewesen für Störungen**

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 eine gemeinsame Meldestelle von BSI und BBK geben soll. 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). Zudem sollte darüber nachgedacht werden, ob nicht auch die Information der Polizei und ggf. der Verfassungsschutzbehörden und anderer Landesbehörden (z.B. LKA) durch diese Meldung ausgelöst werden sollte.**

Nach § 12 Abs. 6 KRITIS-DachG übermittelt das BBK dem betreffenden Betreiber der kritischen Anlage im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes sachdienliche Folgeinformationen. Dies ist nicht ausreichend. **Vielmehr 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 vorsätzlichen Handlungen zu schützen bzw. diese bei Ihren Risikobetrachtung zu berücksichtigen.

**Formulierungsvorschlag**

**§ 12 Meldewesen für Störungen**

(6) Das BBK übermittelt dem betreffenden Betreiber der kritischen Anlage im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes 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 Cybersichersicht kann das BSI ein entsprechendes Computer-Notfallteam (CSIRT) zur Verfügung stellen (vgl. § 5 Abs. 3 Nr. 5 BSIG).

**10. § 13 KRITIS-DachG – Kritische Komponenten**

**Eine Regulierung von kritischen Komponenten wird abgelehnt.** Das bisherige Verfahren des § 9b BSIG hat sich weder im Telekommunikationssektor noch im Sektor Energie als geeignetes Mittel bewährt, um die technologische Abhängigkeit bei Schlüsseltechnologien bzw. kritischen IT-Komponenten spürbar und nachhaltig zu verringern. Es ist zudem unklar, welche Behörde die personellen Kapazitäten hätte, um die entsprechenden Prüfungen bei ca. 2000 Betreibern von kritischen Anlagen tatsächlich vornehmen zu können. Es drohen massive Verzögerungen bei Beschaffungsprozessen, die netto zu einem weniger an Sicherheit führen könnten und die Unternehmen zudem mit einer Vielzahl von bürokratischen Prozessen belasten.

**11. Übergreifendes zu den Pflichten aus §§ 9 – 13 KRTIS-DachG**

Die §§ 9 – 13 KRITIS-DachG legen die Hauptpflichten der Betreiber der kritischen Anlagen fest. Hierbei ist auf zwei 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 § 10 Abs. 1 Nr. 1 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 § 11 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.[7]

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[8] notwendig ist um staatliche Schutzpflichten auf privatwirtschaftlich strukturierte Unternehmen zu übertragen zu können.

Eng hiermit verwandt ist die Pflicht in § 10 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

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

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.**

**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[9]:


[9] 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;

In einem ersten Schritt wird das Ausgangsniveau durch die Kostenprüfung[10] 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

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 Anpassung der Erlösobergrenzen innerhalb einer Regulierungsperiode, wodurch eine unmittelbare Refinanzierung ermöglicht wird.

Auf Grund des kürzlich ergangenen EUGH-Urteils[11] 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.**

[10] Siehe näher zur Kostenprüfung: https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Netzentgelte/Anreizregulierung/WesentlicheElemente/Netzkosten/Netzkostenermittlung_node.html
[11] EuGH, Urteil vom 02.09.2021, Rs. C-718/18.

**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 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.

**12. § 15 KRITIS-DachG – Erlass von Rechtsverordnungen**
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.

Zunächst wird in § 57 Abs. 1 S. 1 (vor Nr. 1) BSIG die Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber, Einrichtungen und der betroffenen Wirtschaftsverbände explizit festgelegt, während diese Anhörungspflicht in § 15 S. 1 Abs. 1 S. 1 (vor Nr. 1) Kritis-DachG fehlt. **Es wird gefordert, auch in § 15 KRITIS-DachG eine Anhörungspflicht der o.g. Adressaten zu verankern. Zudem finden sich leichte Unterschiede im Satzaufbau, die ebenfalls angeglichen werden sollten.**

In § 15 S. 1 Abs. 1 S. 1 Nr. 1 Kritis-DachG wird das Bankenwesen explizit aufgeführt, während dies in § 57 Abs. 1 S. 1 Nr. 1 BSIG nicht der Fall ist**. Hier sollte eine einheitliche Regelung gefunden werden.** Zum Begriff der öffentlichen Verwaltung und zur Abweichung des Begriffs der kritischen Anlage siehe im Übrigen die Ausführungen zu § 2 Nr. 3 Kritis-DachG.

Nicht klar ist, wofür die Verordnungsermächtigungen zur Festlegung der besonders wichtigen Einrichtungen und der wichtigen Einrichtungen nach § 15 Abs. 1 S. 1 Nr. 2, 3 KRITIS-DachG gebraucht werden. Diese Begriffe werden lediglich im NIS2UmsuCG und nicht im KRITIS-DachG verwendet. **Diese Ziffern sollten gestrichen werden, da es sich um eine Doppelung handelt.**

Nach § 57 Abs. 1 S. 3 BSIG wird Zugang zu den Akten, die die Erstellung oder Änderung der Kritis-Verordnung betreffen, nicht gewährt. **Diese Formulierung fehlt in § 15 KRITIS-DachG und sollte ebenfalls aufgenommen werden.**

Schließlich sollte die bisherige Kritis-Verordnung und die nach dem KRITIS-DachG zu erlassende Verordnung einheitlich in einer gemeinsamen Verordnung geregelt werden. Es findet sich zwar in der Gesetzesbegründung zu § 2 Nr. 10 Kritis-DachG eine Andeutung in diese Richtung wieder. **Dies sollte aber auch unmissverständlich im Gesetzeswortlaut festgeschrieben werden. Insbesondere darf es keine abweichenden Definitionen der kritischen Anlagen im NIS2UmsuCG und im KRITIS-DachG geben.**

**13. § 19 KRITIS-DachG – Bußgeldvorschriften**
Positiv zu betrachten ist zunächst, dass das Verhängen eines Bußgeldes mit sehr hohen Hürden nach § 19 Abs. 4 KRITIS-DachG versehen wurde.

Unklar ist jedoch, wie das Verhältnis dieser Bußgelder gegenüber anderen Bußgeldern, insbesondere gegenüber den Bußgeldern aus dem NIS2UmsuCG ist. **Es wird gefordert,**

**dass festgelegt wird, 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 wurde**. Eine doppelte Bußgeldverhängung ist nicht verhältnismäßig. Eine vergleichbare Norm für das Verhältnis von BSIG zur Datenschutzgrundverordnung findet sich in § 60 Abs. 9 BSIG. Die Ausführungen in der Gesetzesbegründung sind dagegen nicht ausreichend, da sie unklar sind und sich nicht im Wortlaut der Norm wiederfinden.

**Formulierungsvorschlag**

**§ 19 Bußgeldvorschriften**

**(5) 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 Verweise in § 19 Abs. 1 Nr. 4 KRITIS-DachG sind nicht stimmig und müssen auf die korrekten Pflichten verweisen. Zudem erscheint eine Bußgeldandrohung auf Grund einer fehlenden Vorlage von Nachweisen gemäß § 11 Abs. 7 S. 4 KRITIS-DachG unlogisch und sollte gestrichen werden**. Es handelt sich hierbei um eine Obliegenheit der Betreiber von kritischen Anlagen und nicht um eine Pflicht. Erfüllen sie die Obliegenheit nicht, so können sie sich nicht auf die Fiktion der Erfüllung der Anforderungen nach § 11 KRITIS-DachG berufen. Hierfür noch zusätzlich ein Bußgeld zu verhängen ist unverhältnismäßig.

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.

**14. § 20 KRITIS-DachG – Inkrafttreten**

Es ist positiv zu vermerken, dass die Pflichten für die Betreiber der kritischen Anlagen erst am 01.01.2026 in Kraft treten und die Bußgeldvorschriften erst am 01.01.2027. Dies gibt den Betreibern ausreichend Zeit, sich auf die grundsätzlich neuen Regeln einzustellen und diese fristgerecht umzusetzen.

**VKU-Ansprechpartner**

Wolf Buchholz
Referent Recht der Digitalisierung
Abteilung Recht, Finanzen und Steuern

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