Berlin, 23. August 2023

BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.

Reinhardtstraße 32
10117 Berlin

www.bdew.de

Stellungnahme

zum Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz – KRITIS-DachG)

Schreiben des BMI vom 27. Juli 2023
Verbändebeteiligung – KM 4 51005/2#13

Transparenz-Register-ID des BDEW: 20457441380-38

Energie. Wasser. Leben.

I. Zusammenfassung

Der BDEW Bundesverband der Energie- und Wasserwirtschaft e.V. begrüßt grundsätzlich den Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-DachG) vom 17. Juli 2023. Vor dem Hintergrund der geopolitischen Zeitenwende und der damit eingehenden Risiken von Sabotageakten und hybriden Bedrohungen muss der rechtliche Rahmen für den Schutz der Kritischen Infrastrukturen unter der Berücksichtigung des All-Gefahren-Ansatzes weiter fortgeschrieben werden. Nur durch einen umfassenden Ansatz, der Risiken aus dem Cyberraum, dem Informationsraum und dem physischen Raum ganzheitlich berücksichtigt, kann so die Resilienz der Kritischen Infrastrukturen in Deutschland und im Unionsgebiet auf ein vergleichbares Resilienzniveau erhöht werden. Dafür sieht der BDEW grundsätzlich geeignete Ansätze in dem vorliegenden Entwurf des KRITIS-DachG. Allerdings ist die Umsetzung der Ziele des KRITIS-DachG als zentralem Regelungsort nicht allein für Resilienzmaßnahmen, sondern darüber hinaus in Zukunft für alle Regelungsinhalte, die Betreiber kritischer Anlagen betreffen, von einer geeigneten Umsetzung der zu erlassenden Rechtsverordnung und vor allem von der engen Verzahnung mit dem NIS-2-Umsetzungsgesetzes (NIS2UmsuCG) abhängig. Eine nahtlose Verzahnung von KRITIS-DachG und NIS2UmsuCG ist die Voraussetzung für eine umsetzbare und wirtschaftlich abbildbare Gesetzgebung zum Schutz Kritischer Infrastrukturen.

Diese Erhöhung und Harmonisierung des Resilienzniveaus muss aber auch nach Maßgaben der Wirtschaftlichkeit der Resilienzmaßnahmen erfolgen, da die Stabilität des wirtschaftlichen Betriebs der vom KRITIS-DachG betroffenen Sektoren selbst als Resilienzfaktor der Wirtschaftsstabilität Berücksichtigung für Deutschland und den europäischen Binnenmarkt finden muss. Gerade in Deutschland zeigt sich, wie sehr die unternehmerische Freiheit und Verantwortung auf eine im europäischen Vergleich vorbildliche Versorgungsicherheit einzahlt und ein entscheidender Faktor für die systemische Resilienz des Sektors Energie ist. Deshalb begrüßt der BDEW auch den Anspruch des KRITIS-DachG ausdrücklich, die Belange der Wirtschaft zu berücksichtigen. Für die Mitigierung von Risiken, wie Sabotageakte durch terroristische Vereinigungen und Drittstaaten, muss der Bund daher auch ausreichende finanzielle, materielle und personelle Ressourcen zur Unterstützung der Betreiber kritischer Anlagen bereitstellen.

II. Zentrale Forderung: Anerkennung von IT-Sicherheitskatalogen und Branchenspezifischen Sicherheitsstandards als weitere spezialgesetzliche Regelungen nach § 5 KRITIS-DachG

Zentrale Forderung des BDEW, um den besonderen Belangen der Energiewirtschaft gerecht zu werden und dabei auf bestehenden sowie erprobten Frameworks für Energiewirtschaft, Behörden und akkreditierte Zertifizierungsstellen aufzubauen, ist es, die **IT-Sicherheitskataloge der Bundesnetzagentur (BNetzA)** - inklusive der in den Katalogen vorgegebenen ISMS-Zertifikate und ISO-Maßnahmen - und die **Branchenspezifischen Sicherheitsstandards der Sektoren Ener-**

gie und Wasser, die im **Geschäftsbereich des Bundesamtes für Sicherheit in der Informationstechnik (BSI)** liegen, für den Sektor Energie **im Sinne der weiteren spezialgesetzlichen Regelungen nach § 5 KRITIS-DachG** als **Grundlage für Risikoanalysen und -bewertungen der Betreiber kritischer Anlagen nach § 10 KRITIS-DachG** sowie für die **Resilienzmaßnahmen und ihre Nachweise** in Form von **Zertifikaten** nach **§ 11 KRITIS-DachG anzuerkennen**. Die Anerkennung der IT-Sicherheitskataloge der BNetzA im Sinne des § 5 KRITIS-DachG ist auch hinsichtlich der Kostenanerkennung von Resilienzanforderungen durch die BNetzA sinnvoll. Ferner sollten für die Risikoanalysen und -bewertungen nach § 9 und § 10 KRITIS-DachG die Sektorstudien des BSI herangezogen werden. Diese sollten aktualisiert werden.

III. Positionen des BDEW im Überblick

Ein zukünftiges KRITIS-DachG hat aus Sicht des BDEW weitere Anforderungen zu erfüllen, damit die Belange der Wirtschaft angemessen Berücksichtigung finden und im Sektor Energie unter Rückgriff auf bestehende und bewährte Frameworks beim Schutz von Kritischen Infrastrukturen sowie im Sinne des All-Gefahren-Ansatzes die Sicherheit und die Resilienz tatsächlich erhöht werden können (ausführliche Darlegung der Positionen Kommentierungen der Regelungsinhalte unter Abschnitt V dieser Stellungnahme):

§ 1 Zweck des Gesetzes:

- Ausreichende finanzielle, materielle und personelle Unterstützung durch Bund und Länder bei Risiken, wie Sabotageakten durch terroristische Vereinigungen und Drittstaaten.
- Vor dem Hintergrund hybrider Bedrohungen sollte das BBK im Falle nationaler Krisenlagen einen nationalen Krisenstab koordinieren.
- Die Grenzen eines Bundesgesetzes bei der Gefahrenabwehr dürfen nicht zulasten der Betreiber kritischer Anlagen gehen.
- Öffnungsklauseln für die Länder dürfen nicht zu uneinheitlichen Regelungen bzgl. Resilienzanforderungen in den Ländern führen. Regelungen der Länder müssen sich an den Bundesregelungen orientieren und die bestehenden Regelungen beim Schutz Kritischer Infrastrukturen (z.B. IT-Sicherheitskataloge) auch bezüglich der Kostenanerkennungen und Kostenerstattung berücksichtigen.
- Schaffung einer gesetzlichen Grundlage für eine erweiterte Zuverlässigkeitsüberprüfung des Personals unterhalb der Sicherheitsüberprüfung.

§ 2 Begriffsbestimmungen und § 4 Kritische Anlagen:

- Schätzungen zu den Aufwendungen der Wirtschaft vor dem Hintergrund von noch durch die zu erlassende Rechtsverordnung zu konkretisierenden Regelungsinhalten sind gegenwärtig nicht möglich. Die Konkretisierung des Begriffs kritische Anlage muss im Sektor

Energie in enger Abstimmung mit der BNetzA erfolgen, und es sollte auf bestehende Bestimmungen und Vorgaben (insbesondere BSI-KritisV) aufgesetzt werden.

- Einheitliche und konsistente Begriffsbestimmung und -verwendung (siehe uneinheitliche Begriffsansetzung kritische Anlagen bei KRITIS-DachG und NIS2UmsuCG) ist zwingend für eine nahtlose Verzahnung von KRITIS-DachG und NIS2UmsuCG sowie zur Vermeidung von überlappenden oder abweichenden Regelungsinhalten erforderlich.

§ 3 Nationale zuständige Behörde für die Resilienz kritischer Anlagen:

- Angemessene Ausstattung des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK) mit personellen, finanziellen und technischen Ressourcen.
- In Fällen von Cyber- bzw. Informationssicherheitsvorfällen mit nationaler Tragweite enge Abstimmung mit der Bundesnetzagentur (BNetzA) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI).

§ 5 Verhältnis zu weiteren spezialgesetzlichen Regelungen:

- Die IT-Sicherheitskataloge der BNetzA und die Branchenspezifischen Sicherheitsstandards sollten für den Sektor Energie im Sinne der spezialgesetzlichen Regelungen nach § 5 KRITIS-DachG anerkannt werden.
- Weiterentwicklung der IT-Sicherheitskataloge der BNetzA als Informationssicherheits- und Resilienzkataloge der BNetzA und der Branchenspezifischen Sicherheitsstandards im Sinne der Resilienzerhöhung.
- Ein nationales Vorgreifen mittels eines nationalen Ansatzes gegenüber der internationalen Normungsarbeit sollte unbedingt vermieden werden. Im Rahmen der europäischen Normungsarbeit sollten die internationalen Normen (insbesondere ISO 22300) weiterentwickelt werden.

§ 7 Kritische Anlagen von besonderer Bedeutung für Europa:

- Die Verzahnung der nationalen Risikoanalysen und -bewertungen nach § 9 KRITIS-DachG mit den europäischen Risikoanalysen und -bewertungen muss noch im KRITIS-DachG geregelt werden. Gegenwärtig ist insbesondere nicht geregelt, inwiefern die unter § 7 KRITIS-DachG fallenden Betreiber kritischer Anlagen die europäischen Risikoanalysen und -betrachtungen berücksichtigen müssen.
- Im Sinne der Umsetzbarkeit sollte die BNetzA die Schnittstelle zur Agentur für die Zusammenarbeit der Energieregulierungsbehörden (ACER) bilden. Es sollte vermieden werden, dass unter § 7 KRITIS-DachG fallende Betreiber kritischer Anlagen parallele Prozesse mit beiden Behörden führen müssen.

§ 8 Registrierung der kritischen Anlage:

- Doppelte Registrierungen von Betreibern kritischer Anlagen sind unbedingt zu vermeiden.
- Bestehende Registrierungen nach § 8b Abs. 3 Satz 2 BSIG sollten für die Registrierungen nach § 8 KRITIS-DachG ohne erneute Registrierung anerkannt und in ein neues Register übernommen werden.
- Die Liste registrierter Betreiber kritischer Anlagen muss vertraulich (Vertraulichkeit, Geheimhaltung) behandelt werden und darf nicht veröffentlicht werden. Das BBK sollte entsprechende Schutzmaßnahmen ergreifen, um die Vertraulichkeit zu gewährleisten.

§ 10 Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen i.V.m. § 9 Nationale Risikoanalysen und Risikobewertungen:

- Anerkennung von IT-Sicherheitskatalogen der BNetzA und die Branchenspezifischen Sicherheitsstandards nach § 5 KRITIS-DachG.
- Weiterentwicklung der IT-Sicherheitskataloge der BNetzA als Informationssicherheits- und Resilienzkataloge der BNetzA und der Branchenspezifischen Sicherheitsstandards im Sinne der Resilienzerhöhung.
- Es sollte dafür Sorge getragen werden, dass es durch verschiedene Risikobewertungen auf Landes- und Bundesebene nicht zu Dopplungen und damit zu Doppelarbeiten kommt.
- Gemäß § 10 Abs. 1 KRITIS-DachG sollen die Risikoanalysen und -bewertungen erstmals neun Monate nach der Registrierung als kritische Anlage durchgeführt werden. Diese Risikoanalyse und -bewertung erfolgt auf der Grundlage der staatlichen Risikoanalyse und -bewertung nach § 9 KRITIS-DachG. Für diese ist aber bisher keine Frist bestimmt. Es ist also gegenwärtig unklar, ob die Risikoanalyse und -bewertung nach § 9 KRITIS-DachG bis zu dem für uns verpflichtenden Termin überhaupt erstellt ist und mit ausreichendem zeitlichem Vorlauf vorliegt. Das ist im Gesetz zu präzisieren.
- Bewertung geopolitischer Abhängigkeiten von Drittländern können nur durch oder mit Unterstützung von Behörden erfolgen. Dies gilt auch für die Analyse und Bewertung der Risiken von Sektorabhängigkeiten nach § 10 Abs. 1 Nr. 2 KRITIS-DachG.

§ 11 Resilienzmaßnahmen der Betreiber kritischer Anlagen:

- Anerkennung von IT-Sicherheitskatalogen der BNetzA und der Branchenspezifischen Sicherheitsstandards nach § 5 KRITIS-DachG.
- Weiterentwicklung der IT-Sicherheitskataloge der BNetzA als Informationssicherheits- und Resilienzkataloge der BNetzA und der Branchenspezifischen Sicherheitsstandards im Sinne der Resilienzerhöhung.

- In § 11 Abs. 13 KRITIS-DachG sollte ergänzt werden, dass die Verpflichtungen frühestens nach Ablauf von 10 Monaten nach der Registrierung und der Veröffentlichung der Anforderungen nach § 11 Abs. 8 KRITIS-DachG gelten.

§ 12 Meldewesen für Störungen:

- Die IT-technische Umsetzung eines zentralen Melde- und Informationsportals sollte am Stand der Technik für Portale und ihrer Absicherung erfolgen. Grundlage für die Meldungen im Sinne eines ganzheitlichen Ansatzes könnte z.B. das BSI-Meldeformular sein, das um einen Abschnitt zu physischen Vorfällen ergänzt werden könnte.
- Nachgelagerte Behördenprozesse sollten reibungslos aufgesetzt sein.
- Alle verfügbaren Informationen zu einem Vorfall können nicht bereitgestellt werden. Die Betreiber kritischer Anlagen können aber alle für den Vorfall relevanten Daten bereitstellen.
- Es müssen eindeutige und klare Kriterien vorliegen, welche Art von Vorfällen – insbesondere zum physischen Schutz gemeldet werden müssen (z. B. sind Hobbydrohnen oder Personenansammlungen vor der Station meldepflichtig ja/nein?)

§ 13 Einsatz kritischer Komponenten: Verordnungsermächtigung:

- Keine Übertragung des Verfahrens nach § 9b BSIG i.V.m. § 11 Abs. 1g EnWG auf kritische Komponenten im Sinne des § 13 KRITIS-DachG.

§ 14 Berichtspflichten:

- Umfassende Berichtspflicht gegenüber Kommission birgt nicht unerhebliches Klumpen risiko bezüglich sensitiver Daten.
- Betreiber kritischer Anlagen müssen beim Vorliegen von Entwicklungen oder Vorfällen von europäischer Relevanz Zugang zu relevanten Informationen aus dem Berichtswesen an die Kommission erhalten.

§ 15 Ermächtigung zum Erlass von Rechtsverordnung:

- Die zu erlassende Rechtsverordnung sollte auf den Sektorstudien des BSI und der daraus abgeleiteten BSI-KritisV aufbauen und die dort erarbeiteten Methoden zur Bestimmung von Schwellenwerten und Anlagenkategorien übernehmen.
- Es sollte zu einer frühzeitigen und umfassenden Einbindung der Branchen und ihrer Verbände kommen.

§ 16 Ausnahmebescheid:

- Es sollte keine Ausnahmen für Behörden geben, die zu einem abweichenden und im Vergleich zur Wirtschaft niedrigeren Schutzniveau bei der Resilienz und der Informations-

sicherheit (siehe auch § 12 KRITIS-DachG insbesondere zentrales Melde- und Informationsportal) führen.

- Ausnahmen sollten nicht für die Dienstleister der Verwaltung gelten.

Anhang 1:

- Der BDEW wird das BBK bei der Erstellung der Vorlagen und Muster zur Unterstützung der Betreiber kritischer Anlagen unterstützen.

IV. Gesamtbewertung aus energiewirtschaftlicher Sicht

a. Keine Wirtschaftsstabilität ohne Wirtschaftlichkeit der Resilienzanforderungen

Die Gesetzgebungskompetenz des Bundes für das KRITIS-DachG ergibt sich aus Art. 74 Abs. 1 Nr. 11 Grundgesetz (Recht der Wirtschaft). Daraus ergibt sich auch die besondere Verantwortung des zuständigen Ressorts (Bundesministerium des Innern und für Heimat) zur Berücksichtigung der Belange der Wirtschaft. Das KRITIS-DachG ist kein Sicherheitsgesetz, sondern ein Wirtschaftsgesetz. Als Wirtschaftsgesetz sollte das KRITIS-DachG deshalb der Wirtschaft auch nur Leitplanken zur Erhöhung der Resilienz von Kritischen Infrastrukturen geben, die durch die Wirtschaft dann mittels eines risikobasierten Ansatzes in geeignete Maßnahmen übersetzt und schließlich umgesetzt werden können. Der Wirtschaftlichkeit der Maßnahmen kommt dabei eine überragende Bedeutung zur Erreichung des Zieles des KRITIS-DachG und der ihm zu-grundliegenden EU-Richtlinien zum Schutz Kritischer Infrastrukturen (CER-Richtlinie) zu, die Wirtschaftsstabilität Deutschlands und des europäischen Binnenmarkts durch die Erhöhung der Resilienz von Kritischen Infrastrukturen zu erhöhen. Erstens können begrenzte finanzielle und personelle Ressourcen nur durch einen risikobasierten Ansatz optimal zum Schutz Kritischer Infrastrukturen genutzt werden. Zweitens muss die Stabilität des wirtschaftlichen Betriebs der vom KRITIS-DachG betroffenen Sektoren selbst als Resilienzfaktor der Wirtschaftsstabilität Berücksichtigung für Deutschland und den europäischen Binnenmarkt finden. Übermäßiger Bürokratismus und Planungsunsicherheiten - etwa durch Beschaffungsvorbehalte bei kritischen Komponenten - gefährden dabei nicht nur die Wirtschaftlichkeit der betroffenen Sektoren, sondern dadurch auch die Versorgungssicherheit selbst.

b. Bereitstellung kritischer Dienstleistungen (kDL) und nicht einer Versorgungssicherheit maßgeblicher Rahmen für Anforderungen an Betreiber kritischer Anlagen

Gerade die hohe Versorgungssicherheit in der Energieversorgung ist aber im Wesentlichen das Ergebnis unternehmerischer Freiheit und unternehmerischer Verantwortung, der die Energiewirtschaft seit Jahrzehnten nachkommt. Die hohe und im europäischen Vergleich vorbildliche Versorgungssicherheit Deutschlands kann aber selbst nicht zur bindenden Maßgabe für die Betreiber werden. Sollten also im Rahmen der nationalen Risikoanalysen und -bewertungen nach § 9 KRITIS-DachG gesamtsystemische Risiken identifiziert werden, die über die im Rahmen der

Energie. Wasser. Leben.

Risikoanalysen- und -bewertungen nach § 10 KRITIS-DachG identifizierten Risiken für die sichere und resiliente Bereitstellung von kDL hinausgehen. So muss der Bund die materiellen, finanziellen und personellen Mittel zu ihrer Mitigierung bereitstellen und die Betreiber kritischer Anlagen auch im Sinne der CER-Richtlinie so unterstützen, dass die Risiken mitigiert werden können. Diese Forderung wirft gleichwohl grundlegende Fragen auch nach den gesetzgeberischen Grenzen des Bundes bei der Unterstützung der Betreiber kritischer Anlagen auf. Es ist schon jetzt davon auszugehen, dass bestimmte - durch die nationalen Risikoanalysen und -bewertungen identifizierte - Risiken (z.B. Sabotageakte, die durch terroristische Vereinigungen oder durch Drittstaaten verübt werden) Maßnahmen zu ihrer Mitigierung erforderlich machen, die in den Bereich der Gefahrenabwehr fallen. Gefahrenabwehr ist aber Sache der Länder. Hier scheint in Zukunft ggf. auch eine grundlegende Neuregelung der Gefahrenabwehr notwendig, damit der Bund und/oder die Länder die notwendige Unterstützung für die Betreiber kritischer Anlagen leisten kann/können.

c. Anforderungen und Nachweise für Resilienz im Sektor Energie auf den bewährten IT-Sicherheitskatalogen und Branchenspezifischen Sicherheitsstandards aufbauen

Der unternehmerischen Freiheit und Verantwortung kommt die Energiewirtschaft seit vielen Jahren insbesondere schon dort nach, wo es um den Schutz der Netz- und Erzeugungsinfrastruktur gegenüber Bedrohungen aus dem Cyber- und Informationsraums geht. Mit den IT-Sicherheitskatalogen der BNetzA, aber auch mit den Branchenspezifischen Sicherheitsstandards der Sektoren Energie und Wasser, die im Geschäftsbereich des BSI liegen, wurde beim Schutz Kritischer Infrastrukturen ein gleichermaßen robustes wie anpassungsfähiges Fundament gelegt, auf dem die Anforderungen an die Resilienz Kritischer Infrastrukturen Hand in Hand mit neuen Anforderungen aus der Informationssicherheit aufbauen sollten. Das kann auch dazu beitragen, insbesondere mit personeller Ressourcenknappheit konfrontierte Betreiber kritischer Anlagen, Bundesbehörden und akkreditierte Zertifizierungsstellen bei den anfallenden Umsetzungsaufwänden zu entlasten.

d. Grundsätzliche Berücksichtigung der Belange der Energiewirtschaft im KRITIS-DachG

Dem Anspruch eines Wirtschaftsgesetzes wird der Entwurf des KRITIS-DachG in entscheidenden Teilen grundsätzlich gerecht. Im Einzelnen begrüßt der BDEW ausdrücklich:

- **Ausreichend lange Frist zur Stellungnahme:** Dadurch wird den Branchen und ihren Branchenverbänden die Möglichkeit gegeben, eine fundierte und repräsentative Kommentierung des KRITIS-DachG einzureichen.
- **Gegenüber NIS2UmsuCG geringerer Anwendungsbereich und geringere Regelungsintensität nach § 1 KRITIS-DachG:** Eine Ausweitung des Anwendungsbereiches des KRITIS-DachG auf…

1. …alle Business-Prozesse, die nicht in den Anwendungsbereich der kritischen Anlagen, sondern in den nach NIS2UmsuCG geltenden Anwendungsbereich der besonders wichtigen Einrichtungen fallen, …
2. …den besonders wichtigen Einrichtungen, die keine Betreiber kritischer Anlagen sind…
3. …und schließlich den wichtigen Einrichtungen…

…hätte in Qualität und Quantität bei den betroffenen Unternehmen zu einer für Wirtschaft und Verwaltung nicht mehr beherrschbaren und wirtschaftlich abbildbaren Vervielfachung der betroffenen Betreiber geführt.

- **Geeignetheit und Verhältnismäßigkeit technischer, sicherheitsbezogener und organisatorischer Maßnahmen zur Gewährleistung der Resilienz § 11 KRITIS-DachG:** Der BDEW begrüßt grundsätzlich, dass der Entwurf des KRITIS-DachG die Bestimmung und Umsetzung von Resilienzmaßnahmen nach der Maßgabe der Geeignetheit und Verhältnismäßigkeit fordert. Im Sinne des Referentenentwurfes sind technische, sicherheitsbezogene und organisatorische Maßnahmen nach § 11 KRITIS-DachG 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. Dabei muss die Verhältnismäßigkeit aber ihre Grenzen in der Bereitstellung der kDL finden.
- **Möglichkeit der Anerkennung von bestehenden und als gleichwertig angesehenen Risikoanalysen und -bewertungen nach § 10 KRITIS-DachG sowie von Nachweisen und Zertifikaten aus bestehenden Sicherheitsmanagementsystemen in Abstimmung von BBK mit BNetzA oder BSI nach § 11 KRITIS-DachG:** Der Entwurf eröffnet in § 11 Abs. 2 KRITIS-DachG und § 11 Abs. 7 KRITIS-DachG die Möglichkeit, dass die mit der ISMS-Umsetzung nach den IT-Sicherheitskatalogen nach § 11 Abs. 1a und § 11 Abs. 1b EnWG oder mit der Umsetzung eines Branchenspezifischen Sicherheitsstandards erstellten Risikoanalysen und -bewertungen sowie erworbene Dokumente (etwa bei Zertifikaten nach den IT-Sicherheitskatalogen nach § 11 Abs. 1a und § 11 Abs. 1b EnWG) und ergriffene Maßnahmen in Abstimmung mit der BNetzA (etwa bei Zertifikaten nach den IT-Sicherheitskatalogen nach § 11 Abs. 1a und § 11 Abs. 1b EnWG) oder dem BSI (etwa Nachweise nach § 8a Abs. 5 EnWG) durch das BBK vollständig oder teilweise anerkannt werden können. Dies begrüßt der BDEW grundsätzlich, schlägt aber vor, die IT-Sicherheitskataloge der BNetzA und die Branchenspezifischen Sicherheitsstandards als weitere spezialgesetzliche Regelungen im Sinne des § 5 KRITIS-DachG zu behandeln.
- **Möglichkeit der Erstellung von Branchenspezifischen Resilienzstandards durch Branche und ihre Branchenverbände nach § 11 KRITIS-DachG:** Der BDEW begrüßt grundsätzlich, dass den Betreibern kritischer Anlagen und ihren Branchenverbänden die Möglichkeit zur Erstellung eigener und Branchenspezifischer Resilienzstandards gegeben werden soll. Der

BDEW hat mit den Branchenspezifischen Sicherheitsstandards der Sektoren Energie und Wasser im Rahmen der Informationssicherheit in der Vergangenheit gute Erfahrungen mit Branchenspezifischen Standards gemacht. Entscheidend für eine zukunftsfähige Umsetzung ist aber insbesondere vor dem Hintergrund der Harmonisierung im Unionsgebiet dabei, dass diese Resilienz-Branchenstandards auf der Grundlage europäischer Normungsarbeit und den für Sicherheitsmanagementsysteme etablierten internationalen Normen aufbaut. Vor diesem Hintergrund und dem Hintergrund der Berücksichtigung des All-Gefahren-Ansatzes schlägt der BDEW daher vor, die IT-Sicherheitskataloge der BNetzA und die Branchenspezifischen Sicherheitsstandards als weitere spezialgesetzliche Regelungen im Sinne des § 5 KRITIS-DachG zu behandeln.

- **Zentrales Melde- und Informationsportal nach § 12 KRITIS-DachG:** Der BDEW begrüßt ein zentrales Melde- und Informationsportal nach dem von ihm geforderten Prinzip „Ein Vorfall, eine Meldung“ ausdrücklich. Eine IT-technische Umsetzung sollte aber am Stand der Technik für Portale und ihre Absicherung erfolgen. Es müssen für die Betreiber kritischer Anlagen eindeutige und klare Kriterien vorliegen, welche Art von Vorfällen – insbesondere zum physischen Schutz gemeldet werden müssen (z. B. sind Hobbydrohnen oder Personenansammlungen vor der Station). Das IT-Sicherheitsgesetz sieht z.B. vor, dass für die Meldung von IT-Sicherheitsvorfällen mit dem BSI eine zentrale Meldestelle besteht, die diese dann unter der Berücksichtigung sektorspezifischer Merkmale von Vorfällen an die zuständigen Fachbehörden auf Bundes- oder Landesebene weiterleitet. Dieses Vorgehen hat sich bisher bewährt und muss in ähnlicher Weise in einem Ansatz fortgeschrieben werden, in dem physischer Schutz und Cyberschutz in einem ganzheitlichen Melde- und Lagebildwesen zusammengeführt werden. In diesem Zusammenhang ist auch die Einrichtung eines behördenübergreifenden nationalen Sicherheitslagezentrums in Erwägung zu ziehen. Grundlage für die Meldungen im Sinne eines ganzheitlichen Ansatzes könnte z.B. das BSI-Meldeformular sein, das um einen Abschnitt zu physischen Vorfällen ergänzt werden könnte.

e. Schärfung und Konkretisierung von KRITIS-DachG und der zu erlassenden Rechtsverordnung erforderlich

Der Entwurf des KRITIS-DachG und die zu erlassende Rechtsverordnung müssen aber bezüglich der folgenden Aspekte geschärft und konkretisiert werden, damit das KRITIS-DachG sowie die zu erlassende Rechtsverordnung im Sinne des All-Gefahren-Ansatzes die größte Wirksamkeit entfalten und im Sinne der optimalen Nutzung begrenzter Ressourcen bei Bundesverwaltung und Wirtschaft die größten Synergien heben kann:

- **Realistische Schätzung der Erfüllungsaufwände bei Wirtschaft und Verwaltung entscheidend für Bemessung umsetzbarer Anforderungen.**

  Konkretisierung wesentlicher Regelungsinhalte in erst zu erlassender Rechtsverordnung problematisch: Voraussetzung für eine realistische Schätzung der Erfüllungsaufwände der

Wirtschaft ist die Kenntnis der erst in der zu erlassenden Rechtsverordnung bestimmten Schwellenwerte und Anlagentypen. Zur realistischen Einschätzung der Erfüllungsaufwände müssen die Anforderungen in der Praxis auch umsetzbar sein und dürfen nicht weitere bürokratische Hürden mit sich bringen. Daher ist es erforderlich, zeitnah konkrete und praktikable Anforderungen klar zu definieren. Darüber hinaus sollten wesentliche, bisher gesetzlich geregelte Regelungsinhalte (kritische Komponenten nach § 13 KRITIS-DachG) erst durch die zu erlassende Rechtsverordnung geregelt werden.

V. Ausführliche Positionen des BDEW

§ 1 Zweck des Gesetzes: Die Anforderungen an die Betreiber kritischer Anlagen im Sektor Energie messen sich an der Maßgabe der Bereitstellung von kDL und können sich nicht an der Maßgabe der Versorgungssicherheit orientieren (siehe dazu auch Abschnitt II dieser Stellungnahme). Daraus ergibt sich auch, dass bestimmte im Rahmen der nationalen Risikoanalysen und -bewertungen nach § 9 KRITIS-DachG identifizierten Risiken (z.B. Sabotageakte, die durch terroristische Vereinigungen oder durch Drittstaaten verübt werden) durch die Betreiber nicht berücksichtigt werden können und in diesem Fall Bund und Länder auch im Sinne der EU-Richtlinien zum Schutz Kritischer Infrastrukturen (CER-Richtlinie) die Betreiber kritischer Anlagen angemessen finanziell und personell unterstützen müssen. Die Grenzen eines Bundesgesetzes dürfen ferner auch nicht zulasten der Betreiber kritischer Anlagen gehen: Im Rahmen der nationalen Risikoanalysen und -bewertungen nach § 9 KRITIS-DachG identifizierten Resilienzrisiken, deren Mitigierung Maßnahmen der Gefahrenabwehr enthalten, müssen aufgrund der Zuständigkeit der Länder auch durch die Länder getragen werden. Im Sinne einer bundesweit einheitlichen Regelung zur Erhöhung der Resilienz (gerade für Energieversorgungsunternehmen, die in mehreren Bundesländern geschäftstätig sind) dürfen die Öffnungsklauseln für die Länder nicht zu Anforderungsabweichungen auf Länderebene führen.

Darüber hinaus sollte ein KRITIS-DachG die gesetzliche Grundlage für eine erweiterte Zuverlässigkeitsüberprüfung des Personals unterhalb der Sicherheitsüberprüfung schaffen. Die Vertrauenswürdigkeit des Personals trägt in einem erheblichen Maße zur Resilienz kritischer Anlagen bei. Betreiber kritischer Anlagen sollten daher das Recht eingeräumt bekommen, eine erweiterte Zuverlässigkeitsüberprüfung des Personals unterhalb der Sicherheitsüberprüfungen im Umfeld kritischer Funktionen durchführen zu können. Unternehmen sollten bei Bedarf auf diesen Regelungsinhalt zurückgreifen können.

§ 2 Begriffsbestimmungen und § 4 Kritische Anlagen: Mit dem Regelungsinhalt kritische Anlage soll im vorliegenden Entwurf des KRITIS-DachG ein Regelungsinhalt kommentiert werden, der erst im Rahmen der zu erlassenden Rechtsverordnung abschließend geregelt werden soll (siehe dazu auch §§ 13 und 15 KRITIS-DachG). Darüber hinaus sind kritische Anlagen im Entwurf des KRITIS-DachG abweichend vom Referentenentwurf des NIS-2-Umsetzungsgesetzes (NIS2UmsuCG) bestimmt. Eine einheitliche und konsistente Begriffsbestimmung und -verwen-

dung ist aber zwingend für eine nahtlose Verzahnung von KRITIS-DachG und NIS2UmsuCG sowie zur Vermeidung von überlappenden oder abweichenden Regelungsinhalten erforderlich. Um die Umsetzbarkeit und Wirtschaftlichkeit gesetzlicher Regelungsinhalte schon früh genug auch im Sinne von Rechts- sowie Planungssicherheit bewerten zu können, sollten grundsätzlich wesentliche Regelungsinhalte daher nicht erst in der zu erlassenden Rechtsverordnung konkretisiert werden. Der Zweck der zu erlassenden Rechtversordnung sollte darin bestehen, die Regelungsinhalte weiter auszugestalten.

§ 3 Nationale zuständige Behörde für die Resilienz kritischer Anlagen: Damit das BBK seiner neuen Rolle als nationale zuständige Behörde für kritische Anlagen nachkommen kann, muss diese mit angemessenen personellen, finanziellen und technischen Ressourcen ausgestattet werden. Da das BBK in Zukunft nicht allein die zuständige Behörde für die Resilienz kritischer Anlagen, sondern für kritische Anlagen und die für diese nach dem All-Gefahren-Ansatz identifizierten Risiken überhaupt sein wird, muss auch bei Cyber- bzw. Informationssicherheitsvorfällen von nationaler Tragweite die Abstimmung mit der BNetzA und dem BSI so eng und effizient wie möglich erfolgen. In diesem Zusammenhang ist auch die Einrichtung eines behördenübergreifenden nationalen Sicherheitslagezentrums in Erwägung zu ziehen.

§ 5 Verhältnis zu weiteren spezialgesetzlichen Regelungen: Die IT-Sicherheitskataloge der BNetzA und die Branchenspezifischen Sicherheitsstandards sollten für den Sektor Energie im Sinne der spezialgesetzlichen Regelungen nach § 5 KRITIS-DachG gelten. Insbesondere auf Seiten der akkreditierten Zertifizierungsstellen könnte dadurch auf bestehende Erfahrungen und bewährte Routinen für die Sektoren Energie und Wasser aufgebaut werden. Dadurch können neue Anforderungen an Sicherheit und Resilienz schnell in bestehende Zertifizierungsregime integriert werden. Dieser Ansatz für den Sektor Energie ist auch deshalb sinnvoll, weil dadurch zeitnah akkreditierte Zertifizierungsstellen zur Verfügung stehen würden und sich die Aufwendungen bei Wirtschaft und Verwaltung minimieren ließen.

Die Anerkennung der IT-Sicherheitskataloge der BNetzA im Sinne des § 5 KRITIS-DachG ist auch aus Sicht der Kostenanerkennung von Resilienzanforderungen durch die BNetzA sinnvoll und geboten. Ansonsten können im regulierten (Netz-)Geschäft anfallende Kosten aus Resilienzanforderungen nicht wirtschaftlich abgebildet werden.

Die IT-Sicherheitskataloge der BNetzA sollten als Informationssicherheits- und Resilienzkataloge der BNetzA entsprechend den identifizierten Bedarfen bei der Resilienz weiterentwickelt werden. Die Branchenspezifischen Sicherheitsstandards, die im Geschäftsbereich des BSI liegen, sollten als Branchenspezifische Informationssicherheits- und Resilienzstandards in Abstimmung mit dem BBK entsprechend der identifizierten Bedarfe bei der Resilienz weiterentwickelt werden.

Im Rahmen der europäischen Normungsarbeit sollte die Energiewirtschaft ferner darauf hinwirken, die Normengrundlage der IT-Sicherheitskataloge und Branchenspezifischen Sicherheitsstandards nach den identifizierten Bedarfen der Resilienzanforderungen entsprechend und

entlang der einschlägigen internationalen Normen (insbesondere ISO 22300) weiterzuentwickeln. Im Sinne einer Harmonisierung des Resilienzniveaus im Unionsgebiet sollte ein nationales Vorgreifen mittels eines nationalen Ansatzes gegenüber der internationalen Normungsarbeit unbedingt vermieden werden.

§ 6 Anforderungen an Betreiber Kritischer Infrastrukturen: Mit den IT-Sicherheitskatalogen der BNetzA werden schon heute besonders hohe Anforderungen an die Resilienz von Netz- und Erzeugungsanlagen gestellt. Im Falle der Netzbetreiber ist dabei schon heute das Erreichen eines bestimmten Schwellenwertes keine Voraussetzung für die Pflicht zur Umsetzung der Anforderungen aus dem IT-Sicherheitskatalog der BNetzA. Die IT-Sicherheitskataloge der BNetzA und die Branchenspezifischen Sicherheitsstandards sollten deshalb für den Sektor Energie auch als weitere spezialgesetzliche Regelungen im Sinne des § 5 KRITIS-DachG anerkannt werden, weil sie schon heute schärfere Anforderungen an die Betreiber Kritischer Infrastrukturen im Sektor Energie stellen.

§ 7 Kritische Anlagen von besonderer Bedeutung für Europa: Da der deutsche Anteil der im Synchrongebiet Kontinentaleuropa benötigten Primärregelreserve (auch Frequenzhaltungsreserve genannt) aktuell 570 MW beträgt, geht der BDEW gegenwärtig davon aus, dass analog zur Sicherheitsüberprüfungsfeststellungsverordnung vom 6. Februar 2023 (SÜFV) viele Verteilnetzbetreiber in den Anwendungsbereich des § 7 KRITIS-DachG fallen werden. Im Sinne der Umsetzbarkeit sollte die BNetzA die Schnittstelle zur Agentur für die Zusammenarbeit der Energieregulierungsbehörden (ACER) bilden. Es sollte vermieden werden, dass unter § 7 KRITIS-DachG fallende Betreiber kritischer Anlagen parallele Prozesse mit beiden Behörden führen müssen.

§ 8 Registrierung der kritischen Anlage: Doppelte Registrierungen von Betreibern kritischer Anlagen sind unbedingt zu vermeiden. Bestehende Registrierungen nach § 8b Abs. 3 Satz 2 BSIG sollten für die Registrierungen nach § 8 KRITIS-DachG ohne erneute Registrierung anerkannt und in ein neues Register übernommen werden. Die Liste registrierter Betreiber kritischer Anlagen sollte vertraulich (Vertraulichkeit, Geheimhaltung) behandelt werden und darf nicht veröffentlicht werden. Das BBK sollte entsprechende Schutzmaßnahmen ergreifen, um die Vertraulichkeit zu gewährleisten. Deshalb sollte es nach § 16 KRITIS-DachG auch keine Ausnahmebescheide für das BBK und die beteiligten Behörden geben, die hinreichend hohen Vorgaben für die Vertraulichkeit im Wege stehen.

§ 9 Nationale Risikoanalysen und Risikobewertungen: Bestimmte durch die nationalen Risikoanalysen und -bewertungen nach § 9 KRITIS-DachG identifizierte Risiken (z.B. Sabotageakte, die durch terroristische Vereinigungen oder durch Drittstaaten verübt werden) können durch die Betreiber kritischer Anlagen in ihren Resilienzplänen nur bedingt berücksichtigt werden. In diesen Fällen sollten Bund und Länder auch im Sinne der EU-Richtlinien zum Schutz Kritischer Infrastrukturen (CER-Richtlinie) die Betreiber kritischer Anlagen angemessen finanziell, materiell und personell unterstützen. Denn je nach Schutzbedarf, der sich auch aus dem Täterprofil ableitet

(bisher Gelegenheitstäter), ergeben sich auch deutliche Kostenunterschiede für Sicherungsmaßnahmen, die die Unternehmen tragen müssen.

§ 10 Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen: Die IT-Sicherheitskataloge der BNetzA und die Branchenspezifischen Sicherheitsstandards sollten für den Sektor Energie im Sinne der weiteren spezialgesetzlichen Regelungen nach § 5 KRITIS-DachG als Grundlage für Risikoanalysen und Risikobewertungen anerkannt werden. Im Rahmen der europäischen Normungsarbeit sollte die Energiewirtschaft ferner darauf hinwirken, die Normengrundlage der IT-Sicherheitskataloge und Branchenspezifischen Sicherheitsstandards nach den identifizierten Bedarfen der Risikoanalysen und -bewertungen entsprechend und entlang der einschlägigen internationalen Normen (insbesondere auch ISO 22300) weiterzuentwickeln.

Die Bewertung der Abhängigkeiten insbesondere nach geopolitischen Maßgaben von Drittländern kann nicht durch die Risikoanalyse und -bewertung der Betreiber kritischer Anlagen erfolgen. Über die dafür notwendigen Informationskanäle und Kompetenzen verfügen nur das Auswärtige Amt sowie die geheimdienstlichen Behörden. Die Analyse und Bewertung für die Zuverlässigkeit und Sicherheit komplexer IT-Produkte übersteigt die Möglichkeiten der KRITIS-Betreiber. Deshalb sollte die Risikoanalyse und -bewertung bezüglich der Abhängigkeit von Drittländern auch ausschließlich Aufgabe der nationalen Risikoanalyse und -bewertung nach § 9 KRITIS-DachG sein.

§ 11 Resilienzmaßnahmen der Betreiber kritischer Anlagen: Die IT-Sicherheitskataloge der BNetzA und die Branchenspezifischen Sicherheitsstandards sollten für den Sektor Energie im Sinne der weiteren spezialgesetzlichen Regelungen nach § 5 KRITIS-DachG als Grundlage für Resilienzmaßnahmen und Nachweise anerkannt werden. Im Rahmen der europäischen Normungsarbeit sollte die Energiewirtschaft ferner darauf hinwirken, die Normengrundlage der IT-Sicherheitskataloge und Branchenspezifischen Sicherheitsstandards nach den identifizierten Bedarfen bei Resilienzmaßnahmen entsprechend und entlang der einschlägigen internationalen Normen (insbesondere ISO 22300) weiterzuentwickeln.

Im Sinne der Hebung von Synergien und Effizienzen sollten bestehende Dokumente, Zertifikate und Maßnahmen aus der Informationssicherheit so weit wie möglich anerkannt werden. Schon heute werden über Informationssicherheitsmanagementsysteme, die dafür auf etablierte und bewährte Normen zurückgreifen, Resilienz-Risiken im Sinne des All-Gefahren-Ansatzes erfasst und geeignete Maßnahmen zu ihrer Mitigierung beschrieben sowie umgesetzt. Im Sinne des Ziels, die Resilienz Kritischer Infrastrukturen im gesamten Unionsgebiet auf gemeinsames und nachhaltiges Niveau zu erhöhen, des All-Gefahren-Ansatzes und nicht zuletzt, um nationale Sonderwege zu vermeiden, sollte bei der Entwicklung von Branchenspezifischen Resilienzstandards auf den bestehenden und bewährten Normen-Reihen aufgebaut werden dürfen, und es sollte im Rahmen der internationalen Normungsarbeit die ISO 22300 entsprechend der identifizierten Bedarfe bei Resilienz und physischem Schutz weiterentwickelt werden. Es sollte in

jedem Fall ein nationales Vorgreifen mittels eines nationalen Ansatzes gegenüber der internationalen Normungsarbeit vermieden werden.

§ 12 Meldewesen für Störungen: Der BDEW begrüßt ein zentrales Melde- und Informationsportal ausdrücklich. Eine IT-technische Umsetzung sollte aber am Stand der Technik für Portale und ihre Absicherung erfolgen. Ferner sollten die nachgelagerten Behördenprozesse reibungslos aufgesetzt werden, um gerade im Zusammenhang mit ausführlichen Berichten nicht zur Überlastung des Meldeprozesses zu führen. Grundlage für die Meldungen im Sinne eines ganzheitlichen Ansatzes könnte z.B. das BSI-Meldeformular sein, das um einen Abschnitt zu physischen Vorfällen ergänzt werden könnte.

§ 13 Einsatz kritischer Komponenten: Verordnungsermächtigung: 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 verringen. Der BDEW fürchtet daher, dass dieses gegenwärtig ungeeignete Verfahren nun auch für die kritischen Komponenten im Sinne des KRITIS-DachG zum Einsatz kommen soll. IT-Produkte, sowohl Hard- als auch Software, sind in der Regel Produkte mit einer komplexen Aufbau-Hierarchie. Was innerhalb dieser Hierarchie als „Komponente“ anzusehen ist und damit einer Bewertung unterliegen soll, kann nicht vom KRITIS-Betreiber als Anwender geleistet werden. Auch eine Bewertung der Zuverlässigkeit und Sicherheit der Komponenten innerhalb der Hierarchie bzw. der fertigen Zusammensetzungen kann, ggf. sogar notwendigerweise im Vorfeld einer Verwendung, nicht vom KRITIS-Betreiber geleistet werden. Damit aber Netzausbau und Energiewende nicht weiter ausgebremst werden und die Versorgungssicherheit durch bürokratisch induzierte Beschaffungsengpässe nicht gefährdet werden, spricht sich der BDEW daher gegen eine Übertragung des Verfahrens auf kritische Komponenten im Sinne des § 13 KRITIS-DachG aus.

§ 14 Berichtspflichten: Der Nutzen umfassender Berichtspflichten an die Kommission ist vor dem Hintergrund der Fülle von Berichten aus allen Unionsmitgliedstaaten fraglich. Vielmehr besteht sogar das nicht unerhebliche Klumpenrisiko, da eine Fülle sehr sensitiver Daten zur Resilienz kritischer Anlagen an eine Institution übergeben werden soll. Gegenwärtig ist auch kein Feedback-Prozess Richtung Betreiber kritischer Anlagen angedacht, der einen echten Mehrwert etwa in Bezug auf Entwicklungen von europäischer Relevanz für die Betreiber kritischer Anlagen bieten könnte.

§ 15 Ermächtigung zum Erlass von Rechtsverordnung: Die zu erlassende Rechtsverordnung sollte im Sinne des All-Gefahren-Ansatzes auf den Sektorstudien des BSI und der BSI-KritisV aufbauen und die dort erarbeiteten Methoden zur Bestimmung von Schwellenwerten übernehmen. Die Erfahrung mit der Erarbeitung und Umsetzung der BSI-KritisV haben darüber hinaus gezeigt, dass eine frühzeitige und umfassende Einbindung der Branchen und ihrer Verbände sinnvoll ist.

§ 16 Ausnahmebescheid: Ausnahmen sollten nicht für die Dienstleister der Verwaltung gelten. Es sollte ferner grundsätzlich keine Ausnahmen für Behörden geben, die zu einem abweichenden und im Vergleich zur Wirtschaft niedrigeren Schutzniveau bei der Resilienz führen. Insbesondere (kommunale) Verwaltungen haben sich in den letzten Jahren dem Angriffsgeschehen aus dem Cyberraum teilweise als nicht gewachsen gezeigt. Sie stellten damit im Cyber- und Informationsraum das „Einfallstor" für die Verbreitung von Angriffen auf (kommunale) Unternehmen der Daseinsvorsorge dar. Diesem Risiko muss auch bei der Resilienz durch vergleichbare Sicherheits- bzw. Resilienzniveaus begegnet werden.

§ 17 Verarbeitung personenbezogener Daten: Der BDEW stellt fest, dass für die Erstellung von Risikoanalysen und -bewertungen bzw. für die Ableitung von Resilienzmaßnahmen keine personenbezogenen Daten benötigt werden.

Anhang 1: Der BDEW wird das BBK bei der Erstellung der Vorlagen und Muster unterstützen.

Möglichkeit zur Risikoabwägung bei der Erfüllung von Transparenzpflichten

Betreibern Kritischer Infrastrukturen sollte zusätzlich mit diesem Gesetz die Möglichkeit eingeräumt werden, eine Informationsherausgabe auf Grund von gesetzlichen Transparenzpflichten, von der ein Risiko für die Kritische Infrastruktur ausgehen könnte, nach einer Risikoabwägung ablehnen zu können.

Der Aufbau von einem zentralen Register der Kritischen Infrastrukturen sollte - aus Gründen der Risikominimierung - vermieden werden.

Ansprechpartner

Mathias Böswetter
Fachgebietsleiter IT-Sicherheit, Kritische Infrastrukturen
Telefon: 030 / 300 199 - 1526
Mathias.Boeswetter@BDEW.de