Berlin, 24. Januar 2024

BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.

Reinhardtstraße 32
10117 Berlin

www.bdew.de

Stellungnahme

Gesetz des Bundesministeriums des Innern und für Heimat zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz von Betreibern kritischer Anlagen (KRITIS-Dachgesetz – KRITIS-DachG)

Schreiben des BMI vom 22. Dezember 2023
Verbändebeteiligung – KM4.51005/2#18

Transparenz-Register-ID des BDEW: 20457441380-38

I. Vorbemerkung

Der BDEW Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW) begrüßt grundsätzlich den Referentenentwurf eines Gesetzes des Bundesministeriums des Innern und für Heimat zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz von Betreibern kritischer Anlagen (KRITIS-DachG) vom 22. Dezember 2023 als einen wichtigen Schritt in Richtung eines bundeseinheitlichen Rechtsrahmens zur Steigerung des analogen Schutzes und der Resilienz von kritischen Infrastrukturen.

Der BDEW begrüßt im Vergleich zum letzten in die Verbändeanhörung gegebenen Entwurf des KRITIS-DachG vom 27. Juli 2023 dabei folgende Anpassungen ausdrücklich:

1. Bundeseinheitlicher Vollzug im Sektor Energie nach § 3 Abs. 3 KRIITS-DachG
2. Streichung des § 13 KRITIS-DachG (Einsatz kritischer Komponenten: Verordnungsermächtigung)

Der BDEW bedauert aber, dass der Beginn der Verbändeanhörung in die Weihnachts- und Neujahrszeit gelegt wurde. Mit der Versendung des zweiten Entwurfs am Nachmittag des 22. Dezember 2023 und der Frist zur Stellungnahme bis zum 24. Januar 2023 wurde es Unternehmen und Verbänden erschwert, sich umfassend zu dem Gesetzentwurf abzustimmen.

Übergreifend ist immer noch festzustellen, dass die Voraussetzungen noch nicht vorliegen, um eine vollständige Bewertung des Gesetzesentwurfes vorzunehmen. So fehlen etwa die nationale Risikoanalyse bzw. die Kenntnis auf welcher Detailtiefe welche Themenstellungen in dieser adressiert werden und somit auch die zu betrachtende Szenarien für die betrieblichen Risikoanalyse und deren Maßnahmenableitung und Kostenabschätzungen. Dass die Rechtsverordnung nach § 16 KRITIS-DachG noch nicht vorliegt, erschwert zusätzlich eine Gesamtbeurteilung. Der BDEW geht davon aus, dass dieses Gesetz die KRITIS-Betreiber betreffen wird, die zurzeit von der IT-Sicherheitsgesetzgebung betroffen sind (ca. 2.000 Unternehmen). Der BDEW bietet an, gemeinsam steuerbare Risiken und auch betroffene Branchen und kritischen Dienstleistungen zu identifizieren.

Der BDEW bedauert, dass der Kommentierungs-Entwurf zum NIS2UmsuCG immer noch nicht vorliegt, um erkennen zu können, ob diese beiden Gesetze in Sinne der zugrundeliegenden Richtlinien ineinandergreifen, sich ergänzen und vor allem nicht doppelt regulieren.

Es gibt keine Angaben zu den Bußgeldhöhen, weshalb hierzu keine detaillierte Betrachtung durch den BDEW erfolgen kann. Den Ansatz, erst zu einem späteren, noch nicht endgültig definierten Zeitpunkt Bußgelder einzuführen, kann der BDEW grundsätzlich nachvollziehen, sieht aber Verbesserungspotential.

Zur effektiven und kosteneffizienten Erhöhung der sektorübergreifenden physischen Sicherheit, weisen wir auf folgende Verbesserungsmöglichkeiten hin und hoffen auf eine

praxistaugliche nationale Umsetzung unter Einbeziehung der Wirtschaft unter anderem auch durch einen Anhörungstermin zu diesem Referentenentwurf.

II. Positionen des BDEW im Überblick

- Zuständigkeit der Bundesnetzagentur für den Sektor Energie und notwendige Regelung der Kostenanerkennung von Resilienzmaßnahmen
- Resilienz zukunftssicher und europäisch gestalten: Internationale Normung als verbindlichen und bewährten Bezugspunkt zur Ableitung von Resilienzmaßnahmen wählen
- Berücksichtigung von zeitlichen und inhaltlichen Abhängigkeiten sowie der betrieblichen Praxis bei der Auswahl und Festlegung von Maßnahmen zur Resilienz
- Verbundunternehmen und Betriebsführer werden durch verschiedene Anforderungsregime auf Bundes- und Landesebene überfordert
- Neue sicherheitspolitische Lage verlangt zwingende Anknüpfungspunkte für staatliche Unterstützung der Betreiber kritischer Anlagen durch die Gefahrenabwehrbehörden
- Transparenz- und Veröffentlichungspflichten dürfen Resilienz Kritischer Infrastrukturen nicht gefährden
- Im Sinne des Ansatzes „Ein Vorfall, eine Meldung“ muss eine Vereinheitlichung der Meldefristen in § 12 KRITIS-DachG mit den Fristen im NIS2UmsuCG erfolgen („24 Stunden“ statt unverzüglich“)
- Ungeregelte Anbindung der Landesbehörden an die Meldestelle nach § 12 KRITIS-DachG

III. Zuständigkeit der Bundesnetzagentur für den Sektor Energie und notwendige Regelung der Kostenanerkennung von Resilienzmaßnahmen

Mit der bundesbehördlichen Zuständigkeit für den Sektor Energie hat das Bundesministeriums des Innern und für Heimat (BMI) eine zentrale Position des BDEW berücksichtigt. Um die komplexen Herausforderungen bei der Regulierung sowie bei der Beurteilung der Systemsicherheit mit ihren komplexen Wechselwirkungen von analoger und digitaler Welt bewältigen zu können, sollte aber die Bundesnetzagentur analog zum Sektor Telekommunikation mit ihrer umfangreichen Erfahrung und Expertise für den Sektor Energie die bundesbehördliche Zuständigkeit erhalten. Insbesondere bei der zeitnahen Kostenanerkennung von Resilienzmaßnahmen, die zeitnah zum Inkrafttreten des KRITIS-DachG auch für nicht-regulierte Bereiche durch die Bundesnetzagentur zu klären ist, könnte die Zuständigkeit der Bundesnetzagentur durch

Erfahrungswerte, etablierte Prozesse und Synergienutzung aus der Informationssicherheit einen wesentlichen Beitrag zum schnellen Erfolg bei gleichzeitig praktikablem Vorgehen leisten.

IV. Resilienz zukunftssicher und europäisch gestalten: Internationale Normung als verbindlichen und bewährten Bezugspunkt zur Ableitung von Resilienzmaßnahmen wählen

In jenen Sektoren, in denen ein bundeseinheitlicher Vollzug aus bundesrechtlicher Sicht nicht durchsetzbar scheint, versucht der vorliegende Entwurf des KRITIS-DachG im Rahmen der gegebenen Kompetenz die drohenden Folgen eines bundesuneinheitlichen Vollzugs (z.B. für Verbundunternehmen und Betreiber kritischer Anlagen, die Infrastrukturen über einzelne Bundesländergrenzen hinaus betreiben) leider nur partiell zu begrenzen.

Um aber einem Auseinanderdriften von bundes- und landesrechtlichen Anforderungen an die Resilienz entgegenzuwirken, eine optimale Verzahnung von CER-Richtlinien- und NIS2-Richtlinienumsetzung zu erzielen sowie auf eine Harmonisierung von Anforderungen an den Schutz Kritischer Infrastrukturen im Unionsgebiet hinzuwirken, sollte die internationale Normung als bewährter Bezugspunkt für die Ableitung von konkreten Resilienzmaßnahmen bestimmt werden.

Dieses Vorgehen hat sich bei der Informationssicherheit von kritischen Infrastrukturen im Zusammenhang mit den IT-Sicherheitskatalogen der Bundesnetzagentur und den Branchenspezifischen Sicherheitsstandards, die im Geschäftsbereich des BSI liegen, sehr bewährt. Grundlage dafür bildet die ISO/IEC 27000-Familie. Diese stellt den Anwendern in allen Sektoren einen hinreichend umfassenden und allgemeinen Rahmen, um ein Informationssicherheitsmanagementsystem (ISMS) unter Berücksichtigung der meisten branchenspezifischen Herausforderungen und unternehmensspezifische Risikobewertungen rechtskonform zu implementieren und im Rahmen des international anerkannten Zertifizierungsrechts evident nachzuweisen.

Aufgrund der zunehmenden Bedeutung europäischer Gesetzgebung ist der Aspekt der internationalen Standards in seiner Relevanz nicht zu unterschätzen. So stellen schon heute europäische Gesetzgebungsinitiativen wie der Network Code on Cybersecurity auf die Umsetzung der ISO/IEC 27001 oder vergleichbarer internationaler bzw. europäischer Standards ab. Dieser Trend wird sich – nicht zuletzt aufgrund der Vorreiterrolle Deutschlands bei der Etablierung von zertifizierten ISMS – zukünftig noch verstärken.

Schließlich hat sich auf Seiten der zertifizierten Prüfstellen und Auditoren bezüglich der IT-Sicherheitskataloge der BNetzA und Nachweise nach § 8a BSIG in den vergangenen sieben Jahren ein Markt etabliert, auf dessen institutionelle und personelle Ressourcen -insbesondere vor dem Hintergrund des sich verschärfenden Fachkräftemangelns- unbedingt auch für etwaige Nachweisverfahren für Resilienzanforderungen zurückgegriffen werden sollte.

Idealerweise folgt daraus die Anerkennung der IT-Sicherheitskataloge der Bundesnetzagentur bzw. der einschlägigen Maßnahmen für die physische Sicherheit aus der ISO/IEC 27001 als

sektorübergreifende Mindestanforderungen und der Branchenspezifischen Sicherheitsstandards (B3S), sofern schon vorhanden, als Resilienzstandards durch das BBK nach § 10 Absatz 6 Satz 2 KRITIS-DachG. Hierdurch könnte auch eine größtmögliche Verzahnung von Informationssicherheit und Resilienz erzielt werden. Die einschlägigen Controls zur physischen Sicherheit der ISO/IEC 27001 könnten beispielsweise im Sinne des § 10 Absatz 4 KRITIS-DachG die sektorenübergreifenden Mindestanforderungen bilden. So beschreibt die Control 7 der ISO/IEC 27001:2022 u.a. folgende einschlägige Maßnahmen zum physischen Schutz und zur Resilienz kritischer Anlagen:

1. Physische Sicherheitsparameter
2. Physischer Zutritt
3. Sichern von Büros, Räumen und Einrichtungen
4. Physische Sicherheitsüberwachung
5. Schutz von physischen & umweltbedingten Bedrohungen
6. Arbeiten im Sicherheitsbereich
7. Aufgeräumter Arbeitsumgebung und Bildschirmsperre
8. Platzierung und Schutz von Geraten und Betriebsmitteln
9. Sicherheit von Werten außerhalb der Räumlichkeiten
10. […]

Die Maßnahmen dieser Controls sind aus Sicht des BDEW hinreichend allgemein, um als sektorübergreifende Mindestanforderungen zu dienen und ggf. durch sektorspezifische Sicherheits- und Resilienzstandards ergänzt zu werden. Mindestens sollte im ersten Zyklus des Gesetzes ausschließlich auf diese Maßnahmen aufgebaut werden. Die genannten Maßnahmen werden schon heute konsequent durch die Netz- und Energieanalagenbetreiber im Rahmen ihres ISMS umgesetzt und nachgewiesen.

Zusätzliche Anforderungen etwa an Fernwärme, Systembetreiber für die Bündelung und Steuerung elektrischer Leistung (Aggregatoren) oder Wasser und Abwasser könnten dann in sogenannten Branchenspezifischen Sicherheits- und Resilienzstandards durch den BDEW erarbeitet werden. Der BDEW hat in der Vergangenheit die Branchenspezifischen Sicherheitsstandards für Aggregatoren, Fernwärme sowie Wasser- und Abwasser erstellt. Auf diesen Branchenspezifischen Sicherheitsstandards sollte aufgebaut werden, um Resilienz- und Informationssicherheitsanforderungen branchengerecht abzubilden und die größtmögliche Verzahnung von physischer Sicherheit und Informationssicherheit nach KRITIS-DachG und NIS2UmsuCG zu erzielen.

Die Energiewirtschaft verfügt über umfangreiche Erfahrung bei der internationalen Normung sowie Erstellung Branchenspezifischer Sicherheitsstandards und steht für weitere Diskussionen und Arbeitstreffen wie Workshops gerne zur Verfügung.

V. Berücksichtigung von zeitlichen und inhaltlichen Abhängigkeiten sowie der betrieblichen Praxis bei der Auswahl und Festlegung von Maßnahmen zur Resilienz

Die in Abstimmung mit dem BDEW erstellte und im Rahmen der Stellungnahme des UP KRITIS mitgegebene „Zeitschiene“ zeigt sehr deutlich, dass die Umsetzung des Gesetzes in der vorliegenden Fassung in der betrieblichen Praxis nicht möglich ist. Die dort aufgezeigten Abhängigkeiten machen klar, dass betriebliche Notwendigkeiten bei der Gesamtausgestaltung zu berücksichtigen sind (Risikoidentifizierung, Maßnahmenidentifizierung und -planung, Budgetierung, Ausschreibungsverfahren, Beantragung von etwaigen baulichen Genehmigungen, bis zur Umsetzung). Erschwert wird das Thema in dem vorliegenden Referentenentwurf insbesondere durch die fehlende Planungssicherheit, die die angedachten, aber noch nicht existierenden behördlichen Vorgaben zur Ausgestaltung der Resilienzmaßnahmen nach § 10 Absatz 1 KRITIS-DachG mit sich bringen.

Aus Sicht des BDEW sollten somit die Rechtsverordnungen und Kataloge von Mindeststandards aus § 10 Absatz 4 KRITIS-DachG und § 10 Absatz 5 KRITIS-DachG, in den Artikel 2 ausgelagert und die Inkraftsetzung in Abhängigkeit zur Evaluierung gesetzt werden. Somit kann später deren Notwendigkeit im Rahmen der Evaluierung des Gesetzes geprüft werden. Dieses ist zurzeit schon für die sektorspezifischen Rechtsverordnungen der Länder so vorgehsehen und sollte auf Bundesvorgaben ausgeweitet werden. Somit würde das Thema der Ausgestaltung des § 10 Absatz 1 KRIITS-DachG für die Länder und den Bund in der ersten Fassung gleichbehandelt werden und dort keinen bis kaum Aufwand erzeugen.

Die Einführung des IT-Sicherheitsgesetzes hat nachweislich gezeigt, dass die Wirtschaft mit ihren Branchenverbänden auch ohne derartige Rechtsvorgaben oder Mindeststandards von behördlicher Seite geeignete Maßnahmen und Prozesse (branchenspezifischen Sicherheitsstandards) etablieren konnte. Bis auf die Rechtsverordnung zur Bestimmung von KRITIS-Betreibern nach BSI-KritisV wurde im Rahmen der Einführung des IT-Sicherheitsgesetzes auf die Nutzung dieses Rechtsmittels zur Vorgabe von Maßnahmen in den letzten acht Jahren verzichtet und insbesondere die Energiewirtschaft konnten im europäischen Vergleich ein sehr hohes Sicherheitsniveau erreichen. Es ist zusätzlich davon auszugehen, dass die zukünftig betroffenen Unternehmen auch schon heute aufgrund von bereits existierenden rechtlichen Rahmenbedingungen (aus IT-SIG oder UVV, etc.), insbesondere, auch im eigenen Interesse und nach Risikoabwägungen, ein geeignetes Maß an physischen Maßnahmen etabliert haben.

Es kann auf weitere Vorgaben zu Resilienzmaßnahmen von behördlicher Seite aus Sicht des BDEW auch verzichtet werden, da mit den in § 10 Absatz 6 KRITIS-DachG angedachten zu entwickelnden branchenspezifischen Mindeststandards, unter Berücksichtigung der „Leitplanken“ aus § 10 Absatz 1 KRITIS-DachG und § 10 Absatz 3 KRITIS-DachG ein praxisnaher und vor allem risikobasierten Ansatz ermöglicht würde. Zur Berücksichtigung der branchenspezifischen

Anforderungen haben sich in der Vergangenheit im Rahmen des bestehenden Informationssicherheitsrecht die vom BDEW erstellten Branchenspezifischen Sicherheitsstandards für Aggregatoren, Fernwärme sowie Wasser- und Abwasser bewährt.

Sollte das Instrument der Rechtsverordnung trotz unserer dringenden Empfehlung weiter angedacht sein, ist die Wirtschaft mit ihren Branchenverbänden zwingend in deren Erstellung einzubeziehen, damit deren Erfahrung hier einfließen kann und praxistaugliche Vorgaben zur Ausgestaltung des §10 Absatz 1 KRITIS-DachG entstehen können. Zudem sollte dieser Eingriff das letzte Mittel der Wahl sein. Des Weiteren ist auf der Zeitachse diese Einflussnahme in die betrieblichen Abläufe zu berücksichtigen und angemessene Umsetzungsfristen zur Berücksichtigung dieser Vorgaben vorzusehen. Dies kann bei baulichen Maßnahmen sehr schnell mehrere Jahre in Anspruch nehmen.

VI. Verbundunternehmen und technische Betriebsführer werden durch verschiedene Anforderungsregime auf Bundes- und Landesebene überfordert

Die zusätzliche Bestimmung von kritischen Anlagen, Schwellenwerten sowie Anforderungen durch die Bundesländer würde zu erheblichen Mehraufwänden bei Betreibern kritischer Anlagen führen. Viele dieser Betreiber haben entweder in mehreren Bundesländern kritische Anlagen, die kritischen Anlagen erstrecken sich über mehrere Bundesländer oder diese Betreiber übernehmen für Dritte in anderen Bundesländern die technische Betriebsführung. Auf die Dienstleistungen der technischen Betriebsführer sind hunderte kleine und meist kommunale Stadtwerke in Deutschland angewiesen. Durch das gleichzeitige Ansetzen verschiedener landesrechtlicher Regelungen droht, dass aufgrund des anfallenden Mehraufwandes die technischen Betriebsführer ihre Dienstleistung diesen kommunalen Stadtwerken nicht mehr wirtschaftlich anbieten können.

Besonders dramatisch wäre das gleichzeitige Anlegen von bundesrechtlichen und landesrechtlichen Regimen aber insbesondere für Verbundunternehmen, die neben bundesrechtlichen Regelungen etwa im Sektor Energie dann landesrechtliche Regelungen etwa für Wasser zu berücksichtigen hätten.

In den Fällen von Betreibern, die entweder kritische Anlagen in mehreren Bundesländern betreiben oder als technischer Betriebsführer für Unternehmen in anderen Bundesländern tätig sind, ist grundsätzlich fraglich, ob eine zuständige Landesbehörde den landesrechtlichen Vollzug, der sich nach § 3 Absatz 6 KRITIS-DachG durch den Hauptsitz des betroffenen Betreibers ergibt, in einem anderen Bundesland überhaupt leisten kann.

VII. Neue sicherheitspolitische Lage verlangt zwingende Anknüpfungspunkte für staatliche Unterstützung der Betreiber kritischer Anlagen durch die Gefahrenabwehrbehörden

In seiner Begründung zur Entscheidung, entgegen der Vereinbarung im Koalitionsvertrag dem Bundesamt für Sicherheit in der Informationstechnik (BSI) künftig lediglich begrenzte Freiheiten einräumen zu wollen, verweist das BMI auf die neue sicherheitspolitische Lage. Dieser neuen sicherheitspolitischen Lage muss auch das KRITIS-DachG gerecht werden. Sabotageakte wie z.B. auf NordStream haben gezeigt, dass die geopolitische Zeitenwende nicht nur im deutschen und europäischen Cyberraum zu spüren ist, sondern sich auch zunehmend in der analogen Welt manifestiert. Die kritischen Infrastrukturen in Deutschland und Europa stehen im Fadenkreuz hybrider Strategien von Drittstaaten. Deshalb muss der Anwendungsbereich des KRITIS-DachG so erweitert werden, dass neben Betreibern kritischer Anlagen auch Bund und Länder beim Schutz Kritischer Infrastrukturen in die Pflicht genommen werden. Die Betreiber kritischer Anlage können weder terroristischen noch militärischen Bedrohungen begegnen. Allein die Gefahrenabwehrbehörden auf Bundes- oder Landesebene können und dürfen die letzte Meile der Gefahrenabwehr gehen. Ohne eine entsprechende Erweiterung des Anwendungsbereichs und gegebenenfalls eine Neuregelung der Gefahrenabwehr insbesondere bei den Energienetzen, die sich über das ganze Bundesgebiet erstrecken, droht allein schon durch eine ungenügende Abschreckung eine offene Flanke gegenüber terroristischen oder hybriden Bedrohungen.

Der BDEW appelliert auch vor dem Hintergrund des Operationsplans Deutschland (OPLAN DEU), der vom Bundesministerium der Verteidigung und BMI unter Beteiligung der Länder erstellt wird, an das BMI, mindestens die notwendigen Anknüpfungspunkte für staatliche Unterstützung der verteidigungswichtigen Energieinfrastrukturen durch die Gefahrenabwehrbehörden im KRITIS-DachG zu schaffen. Nur durch die Kooperation von Wirtschaft, Gefahrenabwehrbehörden und Verteidigern kann die Resilienz eine Abschreckung entfalten und im Bündnis- oder Verteidigungsfall die Handlungsfähigkeit von Militär, Wirtschaft, Staat und Gesellschaft garantieren.

VIII. Transparenz- und Veröffentlichungspflichten dürfen Resilienz Kritischer Infrastrukturen nicht gefährden

Betreibern kritischer Anlagen sollte durch das KRITIS-DachG die Möglichkeit eingeräumt werden, eine Informationsherausgabe aus Transparenz- und Veröffentlichungspflichten zu Lage und Beschaffenheit kritischer Anlagen ablehnen zu können. Aufgrund der neuen sicherheitspolitischen Lage sollten kritische Anlagen als Belang von überragendem öffentlichem Interesse behandelt werden, da Geoinformationen zur Planung und Durchführung koordinierter Sabotageaktionen auf kritische Anlagen genutzt werden können.

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

IX. Ungeregelte Anbindung der Landesbehörden an die Meldestelle nach § 12 KRITIS-DachG

Aus § 12 KRITIS-DachG geht die Anbindung der Landesbehörden an die Meldestelle nicht hervor. Erfolgt eine Regelung zur Anbindung der Landesbehörden an die Meldestelle nicht, müssten bei landesgrenzüberschreitenden Vorfällen mehrere Behörden durch die Betreiber kritischer Anlagen informiert werden und diese Landesbehörden sich miteinander koordinieren. Dies würde im direkten Widerspruch zu dem Anspruch des KRITIS-DachG stehen, das Meldewesen so zu verschlanken, dass Betreiber kritischer Anlagen nur eine Meldung für einen Vorfall tätigen müssen. Ferner würde die Nichtanbindung die behördliche Koordination und Lagebilderstellung im Falle bundesweiter Vorfälle oder von umfassenden Sektor-Angriffen erheblich erschweren und einen Anstieg an Kosten auf Bundes- und Länderebene nach sich ziehen.

Ansprechpartner

Mathias Böswetter

Fachgebietsleiter IT-Sicherheit, Kritische Infrastrukturen

Telefon: 030 / 300 199 - 1526

Mathias.Boeswetter@bdew.de