Energie. Wasser. Leben.

Berlin, 4. Juli 2025

BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.

Reinhardtstraße 32
10117 Berlin

www.bdew.de

Stellungnahme

Stellungnahme zum Referenten-entwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungs-gesetz vom 23. Juni 2025

Transparenz-Register-ID des BDEW: 20457441380-38

Der Bundesverband der Energie- und Wasserwirtschaft (BDEW), Berlin, und seine Landesorganisationen vertreten mehr als 2.000 Unternehmen. Das Spektrum der Mitglieder reicht von lokalen und kommunalen über regionale bis hin zu überregionalen Unternehmen. Sie repräsentieren rund 90 Prozent des Strom- und gut 60 Prozent des Nah- und Fernwärmeabsatzes, über 90 Prozent des Erdgasabsatzes, über 95 Prozent der Energienetze sowie 80 Prozent der Trinkwasser-Förderung und rund ein Drittel der Abwasser-Entsorgung in Deutschland.

Der BDEW ist im Lobbyregister für die Interessenvertretung gegenüber dem Deutschen Bundestag und der Bundesregierung sowie im europäischen Transparenzregister für die Interessenvertretung gegenüber den EU-Institutionen eingetragen. Bei der Interessenvertretung legt er neben dem anerkannten Verhaltenskodex nach § 5 Absatz 3 Satz 1 LobbyRG, dem Verhaltenskodex nach dem Register der Interessenvertreter (europa.eu) auch zusätzlich die BDEW-interne Compliance Richtlinie im Sinne einer professionellen und transparenten Tätigkeit zugrunde. Registereintrag national: R000888. Registereintrag europäisch: 20457441380-38

I. Einleitung

Der Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW) begrüßt die Möglichkeit, den Referentenentwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2UmsuCG) vom 23. Juni 2025 zu kommentieren.

Zum Prozess ist aus unserer Sicht anzumerken, dass Verbändeanhörungen ein zentrales Instrument zur Einbindung fachlicher Expertise und zur Berücksichtigung gesellschaftlicher Interessen im Gesetzgebungsverfahren sind. Sie tragen wesentlich zur Qualität, Praktikabilität und Akzeptanz von Gesetzesvorhaben bei. Um dieser Rolle gerecht werden zu können, ist eine angemessene Frist zur Auswertung des Entwurfs und zur Erarbeitung einer fundierten Stellungnahme unerlässlich. Der Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW) regt an, in Zukunft eine verträgliche Frist von vier Wochen für die wichtige Verbändeanhörung einzuräumen. Dies gilt auch für solche Gesetzgebungsverfahren, für die es bereits früher Anhörungen gegeben hat. Zum einen ändern sich bestimmte Bedingungen mit Zeitablauf und können zu neuen Bewertungen führen und zum anderen bedarf auch ein bereits konsultierter Entwurf eines Abgleichs auf Änderungen, der Zeit in Anspruch nimmt. Vor diesem Hintergrund behält sich der BDEW vor, ergänzende Vorschläge zu unterbreiten.

Der BDEW spricht sich dafür aus, die NIS-2-Richtlinie ohne zusätzliche nationale Verschärfungen in deutsches Recht zu überführen. Eine stringente Umsetzung dicht an den EU-Vorgaben und die Vermeidung nationaler Alleingänge erleichtern die Umsetzung für europaweit agierende Unternehmen. Sie vermeidet erhöhten Aufwand und damit einhergehende Wettbewerbsnachteile im europäischen Energiebinnenmarkt.

Insgesamt sieht der BDEW einige positive Entwicklungen:

- Regelungen zu Systemen zur Angriffserkennung, § 31 Abs. 2 BSIG
- Einrichtung einer zentralen Meldestelle zur Sicherstellung effizienter Informationsflüsse, § 32 BSIG
- Anwendung der Sicherheitsvorgaben nur auf informationstechnische Systeme, die für den Betrieb der kritischen Anlagen erforderlich sind, § 28 Absatz 5 BSIG

Allerdings besteht auch noch Verbesserungs- und Klarstellungsbedarf. Dies bezieht sich vor allem auf folgende Punkte:

- Harmonisierung und Erweiterung des Anwendungsbereichs von § 5c EnWG und § 28 BSIG auf Dienstleister und digitale Dienstleister
- Einführung von Übergangsregelungen für neue Vorgaben zu kritischen Komponenten
- Klarstellung der Definition eines „erheblichen Sicherheitsvorfalls“ nach § 2 Nr. 11 a) BSIG
- Inhaltliche und sprachliche Angleichung der Maßnahmenkataloge zum Risikomanagement in § 30 Absatz 2 BSIG und § 5c Absatz 4 EnWG

II. Zu begrüßende Punkte im neuen Referentenentwurf

1. Die Aufnahme der Systeme zur Angriffserkennung und ihre Beschränkung auf kritische Anlagen (§ 31 Abs. 2 BSIG)

Der BDEW begrüßt ausdrücklich die im NIS2UmsuCG vorgesehenen Regelungen zu Systemen zur Angriffserkennung. Sie schaffen die notwendige Rechtssicherheit für Unternehmen und fördern eine einheitliche regulatorische Umsetzung. Die Vermeidung von Doppelregulierungen ist aus Sicht des BDEW ein zentrales Anliegen, um Bürokratie abzubauen und unnötige Kostenbelastungen für die Wirtschaft zu vermeiden.

2. Einrichtung einer zentralen Meldestelle zur Sicherstellung effizienter Informationsflüsse (§ 32 BSIG)

Die Einrichtung einer zentralen, einheitlichen Meldestelle ist aus Sicht des BDEW ausdrücklich positiv zu bewerten und sollte zeitnah durch die Bundesverwaltung umgesetzt werden. Dabei ist sicherzustellen, dass die Meldeprozesse klar definiert und die Kommunikationswege verlässlich abgesichert sind. Der BDEW betont zudem die Notwendigkeit einer bidirektionalen Kommunikation: Eine strukturierte Rückmeldung an die Wirtschaft ist essenziell, um aktuelle Informationen zu erhalten und zeitnah auf neue Bedrohungslagen reagieren zu können.

3. Einbeziehung von Dienstleistern in den Adressatenkreis (§ 28 Abs. 1 Nr. 4 BSIG)

In § 28 Absatz 1 Nr. 4 BSIG sind Dienstleister adressiert, die Dienstleistungen erbringen, die einer Einrichtungsart nach Anlage 1 zugeordnet sind. Der BDEW geht davon aus, dass dies auch Dienstleister erfasst, die ihre Leistungen den in Anlage 1 genannten Marktteilnehmern und nicht den Endkunden selbst gegenüber erbringen. Dies würde auch folgende Dienstleistungen und Funktionen am Energiemarkt betreffen:

- KritisV-Aggregatoren (Handelsplattformen)
- Smart Meter Gateway Administration
- Steuerbox Administration
- CLS-Management
- Aggregation durch Sprachsteuerungsverfahren
- Zentrale eingeführte Kommunikationskomponenten im Energiemarkt:
- Smart Meter PKI
- Dataprovider (z.B. beim Redispatch)
- Dienstleistungen hinsichtlich von energiewirtschaftlichen Geräten (Wechselrichter, Speicher, Wärmepumpen, Wallbox, etc.)

Dies ist begrüßenswert. Allerdings bestehen weiterhin Unklarheiten hinsichtlich des genauen Anwendungsbereichs und der konkreten Adressaten der Regelung. Insbesondere sollte die Formulierung in § 28 Absatz 5 präzisiert werden. Sie bezieht sich auf Energieversorgungsnetze, Energieanlagen sowie digitale Energiedienste im Sinne des Energiewirtschaftsgesetzes. Das Energiewirtschaftsgesetz definiert den Begriff „digitale Energiedienstleister" allerdings nicht. Eine Definition findet sich dagegen in Anlage 1 der BSI-Verordnung-E. Danach ist ein digitaler Energiedienst „*eine Anlage oder ein System, das den zentralen, standortübergreifenden Zugriff auf die Steuerung oder die unmittelbare Beeinflussung von Energieanlagen oder zentralen, standortübergreifenden Zugriff auf die Steuerung oder die unmittelbare Beeinflussung de-zentralen Anlagen zum Verbrauch elektrischer Energie oder Gas ermöglicht*".

Durch die Verwendung der unterschiedlichen Begriffe und unklaren Verweise bleibt offen, welche Unternehmen oder Dienstleister durch die § 28 Absatz 1 Nr. 4 einerseits und § 28 Absatz 5 andererseits genau angesprochen werden sollen. Die Klarstellung ist essentiell, um für die betroffenen Unternehmen Klarheit über Handlungspflichten und -verantwortungen zu schaffen. Darüber hinaus müssen Rechts- und Planungssicherheit gewährleistet sein bzgl. zu erwartender Belastungen gewährleistet sein.

- **Der BDEW schlägt vor, den Gesetzestext in § 28 Absatz 1 Nr. 4 BSIG wie folgt zu ergänzen oder die Anwendung auf die Dienstleistungen, digitale Dienstleistungen und Funktionen zumindest in der Gesetzesbegründung klarzustellen:**

4. sonstige natürliche oder juristische Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen oder ***digitalen Dienstleistung*** anbieten, die einer der in Anlage 1 bestimmten Einrichtungsarten zuzuordnen sind und die a) mindestens 250 Mitarbeiter beschäftigen oder b) einen Jahresumsatz von über 50 Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen Euro aufweisen ***Dies gilt insbesondere, wenn es sich bei der Dienstleistung um eine kritische Dienstleistung oder digitale Dienstleistung handelt.***

III. Empfehlungen und Hinweise des BDEW zu kritischen Regelungsaspekten

1. Risiken eines rückwirkenden Verbots kritischer Komponenten (§ 41 Abs. 4 BSIG)

Der BDEW weist mit Nachdruck darauf hin, dass ein rückwirkendes Verbot bereits eingesetzter kritischer Komponenten die folgenden erhebliche Risiken und wirtschaftliche Belastungen für Betreiber kritischer Infrastrukturen mit sich bringt. Die beabsichtigten Sicherheitsgewinne im Umgang mit kritischen Komponenten müssen daher sorgfältig gegen die potenziell entstehenden Folgekosten und systemischen Auswirkungen, insbesondere auch auf die Versorgungssicherheit, abgewogen und ins Verhältnis gesetzt werden.

- *Marktabhängigkeiten und Wettbewerbsverzerrungen:*

Im Bereich besonders spezialisierter kritischer Komponenten besteht in vielen Fällen ein faktisches Oligopol mit sehr begrenzter Anbieteranzahl. Ein pauschales oder rückwirkendes Verbot kann zu massiven Beschaffungsengpässen, Lieferverzögerungen und erheblichen Preissteigerungen führen – mit unmittelbaren Auswirkungen auf Versorgungssicherheit, Ausbauprojekte und letztlich die Strom- und Energiepreise für Endkunden. Oligopole sind zudem aus einer systemischen Sicherheitsperspektive selbst als Klumpenrisiko zu bewerten.

- *Finanzielle und betriebswirtschaftliche Risiken:*

Ein rückwirkendes Verbot von Komponenten, die zum Zeitpunkt der Beschaffung rechtskonform eingesetzt wurden, führt zu einer erheblichen Rechts- und Investitionsunsicherheit. Betreiber müssten gegebenenfalls Rückstellungen für mögliche Untersagungen bilden, mit der Folge erheblicher bilanzieller Belastungen und Projektverzögerungen. Zusätzlich entstehen hohe Folgekosten für Ausbau, Ersatz und Neuplanung bestehender Anlagen.

- *IT-/OT-Sicherheitsarchitektur und Integrationsaufwand:*

Die betroffenen Komponenten sind regelmäßig tief in bestehende IT- und OT-Strukturen integriert. Ein Austausch erfordert nicht nur den physischen Ersatz der Hardware, sondern auch die vollständige sicherheitstechnische Neuintegration in bestehende Sicherheitsverfahren, einschließlich Systemintegration und Anlernverfahren (SzA), Risikoanalysen, Anomalieerkennungsverfahren und laufender Betriebsprozesse. Dies bindet personelle und finanzielle Ressourcen, die an anderer Stelle für operative Sicherheitsmaßnahmen fehlen würden und somit der Intention der Regelung entgegenstehen.

➢ **Der BDEW appelliert daher an die gesetzgebenden Stellen im Rahmen von § 41 Abs. 4 BSIG und unter Einbeziehung weiterer einschlägiger Regelungen wie z.B. dem Vergaberecht sicherzustellen, dass ein rückwirkendes Verbot ausschließlich auf Grundlage einer qualifizierten Gefährdungsanalyse erfolgt und unter**

Berücksichtigung der Folgen für die betroffenen Betreiber kritischer Anlagen umgesetzt wird.

2. Klare Übergangsregelungen für kritische Komponenten (§ 41 Abs. 2 BSIG)

Aus Sicht des BDEW bedarf es klarer Übergangsvorschriften hinsichtlich der Regelungen zu kritischen Komponenten gemäß § 41 Absatz 2 BSIG. Insbesondere fehlen der Branche derzeit nachvollziehbare Prozesse für die gleichmäßige initiale Bewertung und Einstufung solcher Komponenten.

Bisher sieht das Gesetz keine Übergangsfrist vor. Der BDEW schlägt daher die Aufnahme einer Übergangsregelung vor, die klar den Übergang von dem bisherigen Regimen nach § 9b BSIG zur neuen Regelung in § 41 BSIG regelt.

Die Regelung, dass jeder Betreiber eine vorliegende Garantieerklärung nachweisen muss, ist wenig effizient. Aus Sicht des BDEW wäre ein zentrales Blacklisting von nicht vertrauenswürdigen Herstellern bzw. die Schaffung einer zentralen Liste vertrauenswürdiger Hersteller beim BMI zielführender. Gleiches gilt für die Garantieerklärung der Hersteller, die so direkt an zentraler Stelle eingereicht werden könnten, um redundante Aufwände und Doppelbelastungen für alle Beteiligten zu vermeiden.

Darüber hinaus wäre mit Blick auf kritische Komponenten eine Harmonisierung wünschenswert. Komponenten, die in der europäischen Union zugelassen sind, sollten grundsätzlich auch in Deutschland eingesetzt werden können.

Zusätzlich sind Risiken im Hinblick auf die Komponentenbeschaffung im Rahme von Ausschreibungsverfahren und die damit einhergehenden Informationsveröffentlichungen zu Details kritischer Komponenten zu berücksichtigen. Um der Bedeutung und Kritikalität der kritischen Komponenten Rechnung zu tragen, müsste für kritische Komponenten eine Ausnahme von der Sektorenverordnung – ähnlich wie bei Behörden mit Verschlusssachen – umgesetzt werden. Hierdurch würden die Vertraulichkeit, Verfügbarkeit und Integrität von kritischen Komponenten gewahrt und der Prozess für Unternehmen umsetzbar gemacht werden

Der BDEW spricht sich daher für praktikable Übergangsfristen sowie transparente und schlanker Prozesse und Abläufe aus, um unnötige Bürokratie und Ressourcenbindung zu vermeiden und eine einheitliche Deutung des Themas innerhalb der Branche zu unterstützen. Ressourcen werden dringend für die aktive, operative Sicherheit unserer kritischen Infrastruktur benötigt.

- **Der BDEW schlägt vor,**
  - **Übergangsfristen für die Einführung von § 41 einzuführen,**

- **ein zentrales Register beim BMI für Garantieerklärungen nach § 41 Abs. 3 für Hersteller zu schaffen und**
- **Ausnahmeregelungen für die Beschaffung nach Sektorenverordnung hinsichtlich der Veröffentlichung zu treffen.**

3. Klarstellung der Definition eines „erheblichen Sicherheitsvorfalls“ nach § 2 Nr. 11 a) BSIG

Der BDEW spricht sich dafür aus, die Definition eines „**erheblichen** Sicherheitsvorfalls“ in § 2 Nr. 11 a BSIG eindeutig einzugrenzen. Die im Folgenden vorgeschlagene Klarstellung, dass ein „erheblicher Sicherheitsvorfall“ wie bei Betriebsstörungen auch nur bei ***schwerwiegenden*** finanziellen und nicht bei jeglichen Verlusten vorliegt, dient der rechtssicheren und verhältnismäßigen Anwendung der Meldepflichten.

Die bisherige Formulierung lässt offen, in welcher Höhe finanzielle Verluste als „erheblicher Sicherheitsvorfall“ zu bewerten sind. Ohne diese Eingrenzung besteht das Risiko, dass bereits geringfügige wirtschaftliche Beeinträchtigungen als meldepflichtige Sicherheitsvorfälle klassifiziert werden. Dies würde zu einer erheblichen Ausweitung des Meldevolumens führen, was weder den Zielen der NIS-2-Richtlinie entspricht noch einen sicherheitsrelevanten Mehrwert bietet.

Zudem würde eine derartige Interpretation zu einer unverhältnismäßigen Belastung sowohl für die betroffenen Unternehmen als auch für die zuständigen Behörden führen. Die Folge wären erhöhte Anforderungen an Meldeprozesse, Personalressourcen und Systemkapazitäten – ohne dass die Risikobewertung dadurch qualitativ verbessert würde.

Die vorgeschlagene Ergänzung stellt eine sachgerechte und systematisch konsistente Auslegung sicher. Ein Sicherheitsvorfall sollte nur dann erheblich sein, wenn eine „schwerwiegende“ Betriebsstörung“ oder ein „schwerwiegender“ finanzieller Verlust vorliegt.

➢ **Der BDEW schlägt vor, § 2 Nr. 11 a) BSIG wie folgt zu ergänzen:**

a) schwerwiegende Betriebsstörungen der Dienste oder ***schwerwiegende*** finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder

4. Klare Regelungen und Zuständigkeiten für Querverbundunternehmen (§ 28 BSIG)

Die Informationssicherheitspflichten innerhalb eines Mehrspartenunternehmens/Querverbundgesellschaften sind komplex und nicht gleichmäßig im Markt umgesetzt. Die aus dem Wortlaut des BSIG ableitbare Ausdehnung der Vorgaben des Energiewirtschaftsgesetzes auch auf die nicht für den Betrieb des Netzes / Anlage erforderlichen IT-Systeme (z.B.

„Office-IT“) wird In Mehrspartenunternehmen zu einer Verantwortungsdiffusion zwischen Bundesnetzagentur (BNetzA) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) führen. Es muss unbedingt klar geregelt sein, welche Zuständigkeiten und Regelungen für welchen Anwendungsbereich gelten

Für Querverbundgesellschaften, die in einer juristischen Gesellschaft Dienstleistungen für mehrere Sektoren erbringen (Querverbundgesellschaften), müssen daher geeignete und nachvollziehbare Regelungen der § 28 Abs. 5 BSIG und § 5c EnWG geschaffen werden, damit eine Regulierung aus einer Hand erfolgen kann.

Insbesondere muss eine analoge Übertragung der Dreistufigkeit aus der NIS-2-Richtlinie in die IT-Sicherheitskataloge der Bundesnetzagentur verbindlich festgeschrieben werden. Eine spätere Durchbrechung der Dreistufigkeit im Anwendungsbereich der IT-Sicherheitskataloge durch von anderen NIS-2-Sektoren abweichenden Maßnahmen und Anforderungen ist unbedingt für die Energiewirtschaft zu vermeiden.

Diese Anforderungen sieht der BDEW in der Regelung in § 28 Absatz 5 letzter Satz in Verbindung mit der Gesetzesbegründung als gegeben an, in der es auf Seite 158 heißt: „Von der Rückausnahme nicht erfasst wird demgegenüber Unternehmens-IT, die für die Tätigkeit in diesen weiteren Sektoren nicht erheblich ist (z.B. „Office-IT“ ohne Schnittstellen zu kritischen Anlagen“).

- **Der BDEW begrüßt die Regelung in § 28 Absatz 5 letzter Satz, die klarstellt, dass die Rückausnahme nur für solche informationstechnischen Systeme gilt, die für den Betrieb der weiteren kritischen Anlagen erforderlich ist.**

5. Abgrenzung Stand der Technik und Verhältnismäßigkeit für besonders wichtige und wichtige Einrichtungen (§ 30 Abs. 1 und 2 BSIG)

Die Verhältnismäßigkeit der Maßnahmen ist nach Absatz 1 für wichtige und besonders wichtige Einrichtungen unterschiedlich zu beurteilen. Zu den in Absatz 2 genannten Kriterien sollte in der Begründung klargestellt werden, dass der Stand der Technik auch branchenspezifisch zu beurteilen sein kann und möglichst beispielhaft branchenspezifische Sicherheitsstandards nennen.

- **Der BDEW schlägt daher vor, dass zumindest die Gesetzesbegründung für die Beurteilung der Verhältnismäßigkeit und des Stands der Technik klarstellt, dass auch sektorspezifisch Sicherheitsstandards wie der B3S zur Anwendung kommen können.**

6. Vermeidung von Verzögerungen durch neue Prozesse zur Aktualisierung der IT-Sicherheitskataloge (§ 5c Abs. 1 EnWG)

Zukünftig müssen die Aktualisierungen der IT-Sicherheitskataloge im Einvernehmen zwischen BSI und BNetzA beschlossen werden. Sie stellen eine wichtige Grundlage für die Cybersicherheit dar. Daher ist sicherzustellen, dass sich die notwendigen zweijährigen Aktualisierungen der Sicherheitskataloge durch das Abstimmungserfordernis nicht verzögern.

Gleichzeitig muss eine verlässliche und zielführende Zusammenarbeit zwischen der Branche, BSI und BNetzA gewährleistet sein.

Darüber hinaus ist zu beachten, dass die Aktualisierungszyklen der IT-Sicherheitskataloge mit den Zertifizierungszyklen der Unternehmen in Einklang stehen. Aktuell bestehen hier Inkonsistenzen: Die Aktualisierungen erfolgen alle zwei Jahre, die Rezertifizierung der Unternehmen dagegen im Dreijahresrhythmus. Dies führt zu Unsicherheiten bezüglich des Anwendungszeitpunkts neuer Vorgaben und kann unnötige Neu- und Rezertifizierungen verursachen, die wiederum Kosten nach sich ziehen und Ressourcen binden.

§ 5c EnWG sollte daher klarstellen, dass Änderungen der Sicherheitskataloge erst bei der nächsten Rezertifizierung der Unternehmen verbindlich anzuwenden sind. Damit würden unnötige Kosten und bürokratische Belastungen vermieden, die die Ressourcen für die aktive Sicherheit der Unternehmen belasten.

- **Der BDEW schlägt vor, die Regelung wie folgt anzupassen, um Regelungen zu Rezertifizierung zu ergänzen:**

> (1) […] Die Bundesnetzagentur überprüft den IT-Sicherheitskatalog alle zwei Jahre und aktualisiert ihn bei Bedarf. Ein angemessener Schutz nach Satz 1 liegt vor, wenn die Anforderung des IT-Sicherheitskatalogs eingehalten werden. ***Nach erfolgter Aktualisierung erfolgt die Anwendung der neuen Version nach angemessener Übergangsfrist bei der nächsten Rezertifizierung der Unternehmen.*** Die Einhaltung der Anforderungen des IT-Sicherheitskatalogs ist vom Betreiber zu dokumentieren. […]

7. Stärkung der Cybersicherheitspflichten für Dienstleister (§ 5c Abs. 1 bis 3 EnWG)

Der BDEW begrüßt ausdrücklich, dass bei der Beschaffung von Anlagengütern sowie bei der Beauftragung von Dienstleistungen sicherzustellen ist, dass angemessene Anforderungen an die Cybersicherheit berücksichtigt werden (§ 5c Abs. 2 EnWG). Dies stellt einen wichtigen Beitrag zur flächendeckenden Absicherung kritischer Infrastrukturen dar.

Vor dem Hintergrund der fortschreitenden Digitalisierung und der zunehmenden Abhängigkeit von externen IT- und Betriebsdienstleistern (z. B. Managed Service Provider, OT-

Support, spezialisierte Softwareanbieter) ist es aus Sicht des BDEW notwendig, die in § 5c Abs. 2 EnWG normierten Pflichten auch auf diese Dienstleister auszudehnen.

Insbesondere sollten Unternehmen, die sicherheitsrelevante Leistungen für Betreiber kritischer Infrastrukturen im Bereich Energie und Wasser erbringen – auch wenn sie nicht im direkten Kundenkontakt stehen –, entweder ausdrücklich in den Anwendungsbereich einbezogen oder zumindest durch eine klar definierte beidseitige Verantwortung zur Cybersicherstellung verpflichtet werden.

Der BDEW geht davon aus, dass auch solche rechtlichen und natürlichen Personen in den Anwendungsbereich der Regelung fallen, die Dienstleistungen im Bereich der Energie- und Wasserversorgung erbringen, die sich nicht an die Endkunden selbst richten, sondern an die Versorgungsunternehmen. Die Versorgungsunternehmen müssen gerade vor dem Hintergrund der fortschreitenden Digitalisierung eine Vielzahl von Dienstleistungen einkaufen, die für die Erbringung ihrer Leistungen unentbehrlich sind. Dienstleister, auf die sie angewiesen sind, müssen daher auch selbst der Anwendung von § 5c EnWG oder des BSI-Gesetzes unterliegen. Dies sollte im Gesetzestext oder zumindest in der Gesetzesbegründung klargestellt werden. Dies würde zur Harmonisierung regulatorischer Anforderungen beitragen, unverhältnismäßige Belastungen auf Seiten der Betreiber vermeiden und die gesamtwirtschaftliche Resilienz kritischer Versorgungsstrukturen erhöhen.

Bisher sind Betreiber digitaler Energiedienste von § 5c Absatz 1 bis 3 nur dann erfasst, wenn ihre Energieanlage an ein Energieversorgungsnetz angeschlossen ist. Betreiber digitaler Energiedienste, die keine an das Energienetz angeschlossene Energieanlage betreiben würden danach nicht in den Anwendungsbereich von § 5c EnWG fallen. Der BDEW geht davon aus, dass Betreiber digitaler Energiedienste, die keine Energieanlage betreiben dann in den Anwendungsbereich von § 28 BSIG fallen. Hier sieht der BDEW allerdings Klarstellungsbedarf.

- **Der BDEW schlägt vor, die Regelungen in § 5c Absatz 1 bis 3 EnWG und § 28 BSIG so zu harmonisieren, dass natürliche oder juristische Personen, die Dienstleistungen im Bereich der Energie und Wasserwirtschaft oder digitale Energiedienste erbringen direkt von den Vorgaben im EnWG bzw. im BSIG erfasst sind.**

8. Keine Regelung für kerntechnische Anlagen in EnWG und BSIG (z.B. § 5c Abs. 2 EnWG)

Der BDEW spricht sich mit Nachdruck dafür aus, keine Vorgaben zu kerntechnischen Anlagen – insbesondere im Rückbau – aus dem Anwendungsbereich des NIS2UmsuCG zu treffen.

Die Kernenergie ist in Deutschland per Gesetz (AtG) aus der Stromerzeugung ausgeschieden; der Rückbau der verbliebenen Kernkraftwerke erfolgt nach einem etablierten rechtlichen Rahmen. Für kerntechnische Anlagen bestehen bereits umfassende und

spezialgesetzlich geregelte Sicherheitsanforderungen, die auch die Informations- und Cybersicherheit vollständig abdecken. Diese Vorschriften gelten sowohl für Anlagen mit als auch ohne Kernbrennstoff und umfassen insbesondere physische und digitale Schutzmaßnahmen (Störmaßnahmen oder sonstige Einwirkungen Dritter – SEWD).

Für kerntechnische Anlagen finden insbesondere die folgenden untergesetzlichen Regelwerke Anwendung:

- **SEWD-RL LWR**: Richtlinie zum physischen Schutz von Kernkraftwerken mit Leichtwasserreaktoren
- **SEWD-RL IT**: Richtlinie zum Schutz von IT-Systemen in kerntechnischen Anlagen (Sicherungskategorien I und II)

Diese spezialgesetzlichen Vorschriften enthalten bereits detaillierte und behördlich überwachte Vorgaben zur Cybersicherheit. Eine zusätzliche Einbeziehung kerntechnischer Anlagen in die allgemeinen Anforderungen des EnWG oder des BSIG im Rahmen des NIS2UmsuCG würde zu einer doppelten Regulierung führen, ohne einen sicherheitsrelevanten Mehrwert zu erzielen.

Eine europarechtlich konsistente Ausgestaltung wäre durch einen Verweis auf den nationalen Rückbaubeschluss und die spezialgesetzliche Regelungslage herstellbar.

➢ **Der BDEW fordert klarzustellen, dass Kernkraftwerke nicht vom Anwendungsbereich der Regelungen im NIS2UmsuCG erfasst sind, da für sie eigene Regelungen gelten.**

9. Sprachlich verständlichere Formulierung von § 5c Abs. 4 Nr. 12 EnWG

Der BDEW weist darauf hin, dass § 5c Absatz 4 Nummer 12 EnWG in der aktuell vorliegenden Fassung (Arbeitsstand: 23.06.2025) sprachlich kaum nachvollziehbar ist.

➢ **Der BDEW regt daher an, § 5c Abs. 4 Nr. 12 EnWG sprachlich verständlicher zu fassen.**

10. Harmonisierung der Formulierungen in § 30 Abs. 2 Nr. 1 bis 10 BSIG und § 5c Abs. 4 Nr. 1 bis 10 EnWG

Unterschiedliche Formulierungen in systematisch vergleichbaren Regelungszusammenhängen (wie hier bei risikobezogenen Maßnahmenkatalogen im BSIG und EnWG) können zu Interpretationsunsicherheiten, Umsetzungsproblemen sowie rechtlicher Uneinheitlichkeit führen. Eine Harmonisierung verbessert die Rechtssicherheit für Betreiber Kritischer Infrastrukturen und vermeidet Mehraufwände durch divergierende Auslegungen oder redundante Compliance-Maßnahmen.

Der BDEW spricht sich nachdrücklich für eine inhaltliche und sprachliche Angleichung der Maßnahmenkataloge zum Risikomanagement in § 30 Absatz 2 BSIG und § 5c Absatz 4 EnWG aus. Aus Sicht des BDEW sollte dabei der Wortlaut des § 30 Absatz 2 BSIG – gemäß dem aktuellen Referentenentwurf zum NIS2UmsuCG – als Grundlage dienen. Dieser verwendet modernisierte und klar definierte Begriffe und verzichtet auf uneinheitlich verwendete oder auslegungsbedürftige Begriffe wie „Cyberhygiene“. Dies fördert nicht nur die Verständlichkeit, sondern auch die Praxistauglichkeit und Akzeptanz der Anforderungen in der Unternehmensumsetzung.

- **Der BDEW regt an, die Formulierungen des § 30 Abs. 2 Nr. 1 bis 10 BSIG auch im § 5c Abs. 4 Nr. 1 bis 10 EnWG wortgleich zu übernehmen.**

11. Verbändeanhörungen als unerlässlicher Mehrwert für praktikable und zielführende Gesetzgebung

Wie in der Einleitung bereits erwähnt, möchte der BDEW an dieser Stelle noch einmal dringend darauf hinweisen, dass die Beteiligung der Verbände im Gesetzgebungsprozess einen wichtigen Mehrwert darstellt. Im NIS2UmsuCG ist die Verbändeanhörung jedoch nicht durchgehend einheitlich geregelt.

Der BDEW appelliert daher eindringlich, Verbändeanhörungen, wie im Handbuch zur Vorbereitung von Rechts- und Verwaltungsvorschriften festgehalten, als sinnvolles und praxisnahes Instrument zu verstehen – insbesondere in hochregulierten Bereichen, die Zertifikate und Nachweise erfordern und bei unzureichender Umsetzung zu erheblichen Kosten sowie administrativen Aufwänden in der Energiewirtschaft führen können.

- **Der BDEW regt an, Verbändeanhörungen im NIS2UmsuCG vorzusehen und einheitlich für die verschiedenen Bereiche zu regeln.**

Ansprechpersonen

Laura Höltkemeier

Fachgebietsleitung Cybersicherheit und IT-Transformation

+49 30 300199 1677

laura.hoeltkemeier@bdew.de

Mathias Böswetter

Fachgebietsleitung KRITIS-, Cyber- und Sicherheitspolitik

+49 30 300199 1526

mathias.boeswetter@bdew.de