Berlin, 28. Mai 2024

BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.

Reinhardtstraße 32
10117 Berlin

www.bdew.de

Stellungnahme zum Referentenentwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz vom 7. Mai 2024

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 BDEW Bundesverband der Energie- und Wasserwirtschaft e.V. (BDEW) begrüßt grundsätzlich den Referentenentwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung vom 7. Mai 2024 und die Möglichkeit zur mündlichen Anhörung der Branchenverbände am 3. Juni 2024. Das Bundesministerium des Innern und für Heimat löst damit das im Rahmen des Werkstattgesprächs vom 26. Oktober 2023 gegebene Versprechen ein, den Branchenverbänden noch einmal die Möglichkeit zur Stellungnahme zu geben.

Darüber hinaus wird durch eine Anhörung von Verbänden und Ländern vor der Sommerpause eine schnelle und fristgerechte Umsetzung der NIS2-Richtlinie befördert. Eine schnelle und fristgerechte Umsetzung ist auch vor dem Hintergrund einer veränderten sicherheitspolitischen Lage erforderlich. Es ist aus Sicht des BDEW daher gleichwohl auch nicht nachvollziehbar, dass eine erneute Anhörung der Branchenverbände einerseits erst im Juni 2024 erfolgen wird und andererseits das Gesetz seit der letzten Verbändebeteiligung in wesentlichen Teilen unverändert geblieben ist.

Diese Umsetzung der NIS2-Richtlinie muss dazu geeignet sein, um einerseits der neuen Bedrohungslage gerecht zu werden, dabei aber andererseits den bürokratischen Aufwand für die Unternehmen der Energie- und Wasserwirtschaft so gering wie möglich zu halten. Sicherheit wird in Zeiten knapper personeller Ressourcen durch Bürokratie nicht gestärkt. Die Unternehmen der Energie- und Wasserwirtschaft tragen schon seit vielen Jahren zum Schutz der kritischen Infrastrukturen bei. Dabei konnten sich diese Unternehmen bisher auf einen geeigneten Rechtsrahmen insbesondere für Cybersicherheit verlassen.

Wir sehen mit großer Sorge, dass diese Verlässlichkeit aufgrund von Bürokratismus, unklarer Zuständigkeiten und unzureichender Harmonisierung zwischen Gesetzgebungsinitiativen (insbesondere zum KRITIS-DachG) gefährdet ist. Vor dem Hintergrund einer veränderten sicherheitspolitischen Lage benötigen die Unternehmen der Energie- und Wasserwirtschaft dringend eine umfassende, ineinandergreifende sowie verlässliche Sicherheitsarchitektur in Deutschland und Europa.

Der vorliegende Referentenentwurf des NIS2UmsuCG leistet in Teilen einen Beitrag zu klaren gesetzlichen Rahmenbedingungen. Wir begrüßen dabei insbesondere:

- Die Bereichsausnahmen für den Sektor Energie und die spezialrechtliche Regelung des § 5c EnWG versuchen den bewährten Rechtsrahmen der IT-Sicherheitskataloge der Bundesnetzagentur für den sicheren Netz- und Anlagenbetriebs fortzuschreiben. Allerdings müssen die Bereichsausnahmen und die spezialrechtlichen Regelungen verbessert

werden, damit eine Doppelregulierung der Betreiber von Energienetzen, die nicht unter die Schwellenwerte der BSI-KritisV fallen, im Scope der OT vermieden wird (siehe unten).

- Im Sinne der Internationalisierung ist zu begrüßen, dass das Schutzziel Authentizität bereits weitgehend entfallen ist. Eine vollständige Streichung des Schutzzieles Authentizität muss allerdings im Sinne eines konsistenten Gesetzes noch erfolgen (z.B. in §2 Abs. 13 BSIG).

Damit das NIS2UmsuCG über die genannten Punkte hinaus zu einer umfassenden, ineinandergreifenden sowie verlässlichen Sicherheitsarchitektur beitragen kann, fordert der BDEW die Berücksichtigung folgender Punkte:

- Das Prüfverfahren gemäß § 41 BSIG muss gestrichen und durch eine **Ausschlussliste generell nicht-vertrauenswürdiger Hersteller** ersetzt werden.

- Die Normen zur **Abgrenzung des BSIG zu den spezialgesetzlichen Normen des EnWG müssen überarbeitet** werden. Im Moment kommt es zu unklaren Doppelregulierungen von Unternehmen der Energiewirtschaft (siehe die Ausführungen zu § 28 Abs. 4 BSIG).

- Auch die **spezialgesetzlichen Regelungen des EnWG müssen geändert werden.** Insbesondere muss aus den Normen klar hervorgehen, dass die bisherige Logik des § 11 EnWG nicht geändert werden soll. Nicht alle Energieanlagen, sondern nur kritische Energieanlagen dürfen in den Anwendungsbereich des EnWG mit seinen IT-Sicherheitskatalogen fallen. In seiner aktuellen Fassung würden auch solche Unternehmen unter die Regelung des EnWG fallen, wenn diese aufgrund von Umsatz und Mitarbeitendenzahl in einem nicht-energiewirtschaftlichen Geschäftsfeld unter die NIS2-Size-Cap fallen und etwa zur Förderung der Dekarbonisierung des Geschäftsbetriebs Erneuerbare-Erzeugungs-Anlagen mit Einspeisung ins öffentliche Stromnetz betreiben würden. **Diese Unternehmen hätten dann ein ressourcen- und kostenaufwendiges ISMS-Zertifikat zu beschaffen, ohne für den sicheren Netzbetrieb kritisch zu sein. Die IT-Sicherheitskataloge für die Energieversorgungsnetze und Energieanlagen dürfen sich zudem nur auf die (kritischen) Anlagen beziehen und nicht auf die Office-IT (siehe die Ausführungen zu § 5c EnWG).** Ansonsten drohen in Querverbundsunternehmen auch Herausforderungen bezüglich der Vorrangigkeit geltender spezialrechtlicher Regelungen, die im weiteren Scope der besonders wichtigen Einrichtung miteinander konkurrieren würden.

- **NIS2UmsuCG und KRITIS-DachG sollten stärker miteinander abgestimmt**, wesentliche Regelungsinhalte des KRITIS-DachG mit Relevanz für die Beurteilung des NIS2UmsuCG den Branchenverbänden zur Kommentierung zugänglich gemacht und beide Gesetze schließlich gleichzeitig in den Bundestag eingebracht werden.

- Anlage 1 Sektoren besonders wichtiger und wichtiger Einrichtungen: **NIS2-Richtlinien-konforme Beschränkung auf Ladepunktbetreiber LSV im Sinne der AFIR**, die gegenüber Endnutzern Elektromobilitätsdienstleistungen erbringen.

- Geeignetes Meldewesen (Massenfähigkeit)

- Im Sinne einer notwendigen Begriffsbestimmung im § 2 Abs. 1 Nr. 9 BSIG sollten *finanzielle Verluste* durch *erhebliche* ***oder existenzbedrohende*** *finanzielle Verluste* in der Norm Ersetzung finden. Ebenso sollten hier immaterielle Schäden ausgeschlossen werden.

- § 38 Abs. 2 BSIG – Haftungsverzicht / Vergleich über die Haftung

II. Begründung der einzelnen Positionen

1 Prüfverfahren zu den kritischen Komponenten gemäß § 41 BSIG

1.1 Energiewende und Digitalisierung schaffen neue geopolitische Risiken

Die Energiewende zahlt vor dem Hintergrund der sicherheitspolitischen Zeitenwende auf die Energieunabhängigkeit und damit die Energiesicherheit in Deutschland und Europa ein. Das führt auch zunehmend zu einer Verschiebung im sogenannten energiepolitischen Zieldreieck: Versorgungssicherheit und Umweltverträglichkeit stehen immer weniger in einem Spannungsverhältnis, sondern in einem ergänzenden Verhältnis.

Gleichwohl ist aus Sicht des BDEW darauf zu achten, dass die eine geopolitische Abhängigkeit bei den Energieträgern nicht um eine neue geopolitische Abhängigkeit bei den Komponenten von Energiewende und Digitalisierung eingetauscht wird. Technologische Souveränität, aber auch verlässliche Partner für die Diversifizierung der Lieferketten sind hier gleichermaßen entscheidende Faktoren, um dieser Abhängigkeit entgegenzuwirken.

Aufgrund des steigenden Digitalisierungsbedarfes der Energiewende und neuen Geschäftsmodellen sollte darüber hinaus auch die zunehmende Bedeutung digitaler Energiedienstleistungen regulatorisch berücksichtigt werden. Schon heute nehmen in vielen Mitgliedsstaaten der Europäischen Union einzelne Hersteller aus Nicht-EU-Ländern im Segment der Heimspeicher Marktanteile nah an einer marktbeherrschenden Stellung ein. Die Stabilität des Stromnetzes wird heute sowohl von einzelnen großen Kraftwerken als auch zu einem immer größeren Teil von vielen kleinen Anlagen erbracht, die gebündelt wie ein großes „virtuelles“ Kraftwerk agieren. Von beiden kann grundsätzlich im gleichen Maße eine Gefährdung für die Sicherheit der Energieversorgung ausgehen. Durch die Transformation des Energiesystems im Zuge der

Energiewende sind im letzten Jahr etwa 5,3 GW Heimspeicher in Deutschland installiert worden. Gegenwärtig fallen Anlagen oder Systeme zur Steuerung oder Bündelung elektrischer Leistung zwar unter die BSI-KritisV, nicht aber unter den Anwendungsbereich des § 41 BSIG i. V. m. § 5c Abs. 9 EnWG. Hier sollte im Sinne der Versorgungssicherheit regulatorisch vorgebeugt werden, damit Hersteller eine annähernd marktbeherrschende Stellung zukünftig nicht in eine das Stromnetz beherrschende Macht ummünzen können.

1.2 Berechtigtes politisches Interesse darf nicht zum rechtlichen und wirtschaftlichen Betreiberrisiko werden

Das berechtigte politische Interesse, den Einsatz von IT-Komponenten jener Hersteller untersagen zu können, die aus geopolitischer Sicht keine verlässlichen oder vertrauenswürdigen Partner sind, darf aber nicht zu einem erheblichen rechtlichen und wirtschaftlichen Risiko für die Betreiber Kritischer Infrastrukturen werden. Durch den Duldungscharakter des Prüfverfahrens gemäß § 41 BSIG entstehen betriebliche Risiken im Rahmen der Betriebsführung und möglicher nachträglicher Ausbauverpflichtungen. Dies kann zu längerfristigen Ausfällen von für den Betrieb essenziellen Komponenten im Leitsystem oder im Umfeld der Fernwartung führen. Das Prüfverfahren gemäß § 41 BSIG verlangt die umfassende Anpassung, Bildung von Rückstellungen und langfristige Ausrichtung von Beschaffungs- und Einsatzprozessen bei den Betreibern. Ferner werden sich die durch den Prüfprozess gemäß § 41 BSIG anfallenden Mehrkosten im Rahmen der Energieerzeugung bei den Erzeugungspreisen niederschlagen müssen. Geschieht dies nicht, droht eine Schwächung des energiewirtschaftlichen Standort Deutschland, da hierdurch indirekt Marktkapazitäten an das europäische Ausland verloren gehen. Deshalb sind die Betreiber im Sinne von Rechts- und Planungssicherheit auf ein transparentes, verlässliches sowie schnelles Verfahren angewiesen. Auch muss vermieden werden, dass die Regelungen des § 41 BSIG im Widerspruch stehen zum europäischen Ausschreibungsrecht.

Der BDEW befürchtet vor diesem Hintergrund, dass das Prüfverfahren des § 41 BSIG nicht dazu geeignet ist, die zu erwartende Fülle an Meldungen von kritischen Komponenten durch die betroffenen KRITIS-Betreiber im Sektor Energie zu bewältigen. Denn das Ziel des Prüfverfahrens gemäß § 41 BSIG, das der Katalog gemäß § 5c Abs. 9 EnWG geerbt hat, ist die Erfassung und Bewertung der Meldungen über kritische Komponenten, die durch lediglich vier TK-Netzbetreiber an das BMI übermittelt werden - und dies ausschließlich im Rahmen ihres 5G-Netzbetriebs, nicht aber ihres ganzen Netzbetriebs. Dies steht im Gegensatz zum Regelungsgegenstand des § 5c Abs. 9 EnWG i. V. m. §41 BSIG, der sich spartenübergreifend auf alle Netzbetreiber und Erzeugungsanlagenbetreiber erstreckt, die unter die in der BSI-KritisV bestimmten Versorgungsgrade bzw. Schwellenwerte fallen.

Darüber hinaus ist der Regelungsgegenstand des § 5c Abs. 9 EnWG auch nicht wie im Falle der Regelung im Sektor Telekommunikation auf einen bestimmten und als besonders kritisch bewerteten Netzbetriebsaspekt beschränkt. Bestimmt sich die Kritikalität und damit die

Begründung der Regelung im Sektor Telekommunikation aus der Sorge um die erhebliche Abhängigkeit bei einer als strategisch wichtig identifizierten Schlüsseltechnologie (5G), so zielt der § 5c Abs. 9 EnWG i. V. m. § 41 BSIG auf den sicheren Netzbetrieb im Ganzen und verschiebt damit die Qualität der ursprünglichen Begründung des Prüfverfahrens: Anstatt der technologischen Abhängigkeit bei einer Schlüsseltechnologie entgegenzuwirken, die einen Zugewinn an Versorgungsqualität verspricht, zielt der § 5c Abs. 9 EnWG auf die Versorgungssicherheit überhaupt – und dies unabhängig davon, ob diese in Zukunft von einer bestimmten Schlüsseltechnologie oder von einer Reihe an Schlüsseltechnologien mutmaßlich abhängen mag.

Im Ergebnis konfrontiert der Katalog kritischer Funktionen gemäß § 5c Abs. 9 EnWG das Prüfverfahren gemäß § 41 BSIG mit einer Aufgabe, für die die Regelung nicht erdacht wurde, weil das BMI in Zukunft die Meldungen tausender KRITIS-Betreiber bearbeiten bzw. bewerten müsste. Gerade aber die Bewertung der Vertrauenswürdigkeit eines Herstellers wird sich als eine ressourcenintensive Herausforderung darstellen, weil der großen und heterogenen Akteurslandschaft der KRITIS-Betreiber im Sektor Energie und insbesondere im Bereich der Erzeugung eine auch ebenso heterogene sowie kleinteilige Herstellerlandschaft gegenübersteht.

1.3 Risiken für Netzausbau und Energiewende

Netzausbau und Energiewende sind ambitionierte Projekte, die auf die Klimaziele, die nachhaltigen Versorgungssicherheit und aus geopolitischer Sicht auf die Energiesicherheit sowie Energieunabhängigkeit einzahlen. Schon jetzt führen Bürokratie und Genehmigungsverfahren zu einem Ausbremsen beider Projekte. Mit dem steigenden Digitalisierungsgrad bei beiden Projekten ergibt sich zwar einerseits eine gewisse Abhängigkeit bei IT-Komponenten, die bei mangelnder Diversifizierung sowie technologischer Souveränität zu einer Verschiebung der geopolitischen Abhängigkeiten bei Energieträgern hin zu IT-Komponenten führen könnte. Andererseits darf die für das Gelingen von Netzausbau und Energiewende essenzielle IT-Beschaffung nicht unverhältnismäßig erschwert werden und es sollte Planungssicherheit bei Beschaffung und Betrieb von IT-Komponenten bestehen.

1.4 Gefährdung der Versorgungssicherheit durch Beschaffungsengpässe

Die Versorgungssicherheit hängt von der Aufrechterhaltung genau jener kritischen Funktionen ab, die in Zukunft im Regelungsbereich des Beschaffungsvorbehalts mit Duldungswirkung bei kritischen IT-Komponenten des § 5c Abs. 9 EnWG i. V. m. § 41 BSIG liegen werden.

Im Sinne der Versorgungsicherheit sollte daher sichergestellt werden, dass der Weiterbetrieb von beanstandeten kritischen IT-Komponenten bestimmter Hersteller immer dann möglich bleiben muss, wenn eine anderweitige Beschaffung der betroffenen IT-Komponenten aufgrund von Beschaffungsengpässen nicht erfolgen kann.

Insbesondere die Beschaffungsengpässe können Folge einer künstlichen und politisch motivierten Marktverknappung sein. Gerade in der künstlichen Marktverknappung – nicht aber in der „Sabotage by Design" der IT-Komponenten – sieht der BDEW gegenwärtig den wahrscheinlichen und mächtigsten Hebel, über den die Hersteller aus Drittländern effektiv und nachhaltig eine Abhängigkeit zum Schaden der Versorgungsicherheit ausspielen könnten. Vor dem Hintergrund dieses Szenarios sollte ein Weitebetreib von IT-Komponenten möglich bleiben, wenn keine konkreten Erkenntnisse über die Sabotage der Komponenten ab Werk vorliegen und bis eine alternative Beschaffung wieder möglich ist.

- **Der BDEW fordert daher, das Prüfverfahren zu den kritischen Komponenten gemäß § 41 BSIG durch eine Ausschlussliste von generell nicht-vertrauenswürdigen Herstellern zu ersetzen.**

2 Doppelregulierung von § 28 Abs. 4 BSIG mit dem § 5c EnWG vermeiden / Abschichtung der Anforderungstiefe nach engem KRITIS-Scope (IT-Sicherheitskataloge der BNetzA) sowie weiterem Scope der wichtigen Einrichtung (BSIG) eines Betreibers kritischer Anlagen

Nach § 28 Abs. 4 Nr. 2 BSIG gelten § 31 (Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen), § 32 (Meldepflichten), § 35 (Unterrichtungspflichten) und § 39 (Nachweispflichten für Betreiber kritischer Anlagen) nicht für Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des EnWG, soweit sie den Regelungen des § 5c des EnWG unterliegen. Nach der Gesetzesbegründung soll Abs. 4 den bisherigen § 8d Abs. 2 BSIG fortführen. Mit dem hier vorgeschlagenen Gesetzeswortlaut gelingt dies jedoch nicht. Vielmehr kommt es zu Widersprüchen mit dem neuen § 5c EnWG.

Besonders deutlich wird dies zunächst beispielhaft für Erzeugung in § 5c Abs. 2 EnWG. Diese Norm statuiert die IT-Sicherheitspflichten für die Betreiber von Energieanlagen in Bezug auf die IT-Infrastrukturen des Anlagenbetriebs. Während der bisherige § 11 Abs. 1b BSIG diese Pflichten nur für die Betreiber von kritischen Infrastrukturen (zukünftig Betreiber von kritischen Anlagen) statuiert, erweitert der § 5c Abs. 2 EnWG diese Pflichten auf alle Betreiber von Energieanlagen, die besonders wichtige / wichtige Einrichtungen sind. Da eine Einrichtung bereits ab 50 Mitarbeitenden eine wichtige Einrichtung ist (vgl. § 28 Abs. 2 Nr. 3 BSIG), wären zukünftig faktisch fast alle Betreiber von Energieanlagen von den neuen Regelungen erfasst. Dies ist abzulehnen und passt auch nicht zur sonstigen Systematik des § 5c EnWG. Damit findet eine massive Ausweitung des Anwendungsbereichs der IT-Sicherheitskataloge und die Verwässerung ihres Zweckes statt. Zweck der IT-Sicherheitskataloge für Energienetzbetreiber und Erzeugungsanlagenbetreiber ist der sichere Netz- und Anlagenbetrieb. Eine so unverhältnismäßige Ausweitung des Anwendungsbereiches der IT-Sicherheitskataloge auf unkritische Assets in der Erzeugung und in Konsequenz auch auf Business-Prozesse im Scope der besonders wichtigen Einrichtung (z.B. Office-IT), die keinen unmittelbaren oder kritisch mittelbaren Einfluss auf den sicheren Netz- oder Anlagenbetrieb haben, ist zwingend zu vermeiden. Vielmehr

sollten der Anwendungsbereich der IT-Sicherheitskataloge auf den klaren und bewährten Scope der kritischen Anlage begrenzt bleiben. Sie sollten diesen Pflichten auch nur „insoweit" unterliegen, als dass sich diese Pflichten auf die kritischen Anlagen beziehen. Nicht erfasst sein dürfen dadurch die Pflichten für die sonstigen IT-Systeme außerhalb des Scopes der kritischen Anlagen, wie z.B. die reguläre Office-IT. Für diese IT-Systeme muss es bei den allgemeinen Regeln des BSIG verbleiben, ohne das die Pflichten nach EnWG (bzw. den IT-Sicherheitskatalogen) einschlägig sind (vgl. die Ausführungen zu § 28 Abs. 4 bzw. zu §§ 30, 31 BSIG).

Nicht ausgeschlossen wird zum einen § 30 BSIG, der die Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen regelt. Die Begründung zu § 5c EnWG weist darauf hin, dass die Anforderungen von § 30 BISG in § 5c EnWG ergänzt worden sind. Der BDEW geht daher davon aus, dass hier fehlerhaft nicht auch § 30 BSIG in die Aufzählung in § 28 Absatz 4 BSIG aufgenommen wurde. Betreiber von Energieversorgungsnetzen oder Energieanlagen müssten sonst neben dem § 5c EnWG immer auch den § 30 BSIG beachten. § 5c EnWG regelt teilweise auch Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen, so dass hier eine Doppelung entstünde, die zumindest zu Unklarheiten führt, in welchem Verhältnis § 30 BSIG zu § 5c Abs. 1 – 3 EnWG steht.

Weiterhin käme es zu Doppelungen im Bereich der Dokumentationen der ergriffenen Maßnahmen bzw. des Nachweises dieser Dokumentationen für Betreiber von Energieversorgungsnetzen. So müssen nach § 5c Abs. 1 letzter Satz EnWG und § 5c Abs. 4 EnWG alle Betreiber von Energieversorgungsnetzen ihre Maßnahmen dokumentieren (Abs. 1) und diese Dokumentation der BNetzA übermitteln bzw. nachweisen (Abs. 4). §§ 65, 66 BSIG wiederum regelt für die besonders wichtigen und wichtigen Einrichtungen ebenfalls Dokumentations- und Nachweispflichten. §§ 65, 66 BSIG sind allerdings durch § 28 Abs. 4 Nr. 2 BSIG ebenfalls nicht ausgeschlossen, sodass diese Pflichten nebeneinanderstünden. Da sich die Dokumentation auf die Pflichten nach § 30 BSIG bezieht. Entstünde auch dieses Problem nicht, wenn auch § 30 BSIG nicht anwendbar wäre, soweit § 5c EnWG Anwendung findet.

- **Der BDEW fordert daher, auch die Anwendbarkeit von § 30 BSIG durch § 28 Abs. 4 Nr. 2 BSIG im Scope der kritischen Anlage auszuschließen, soweit Betreiber von Energieversorgungsnetzen oder Energieanlagen von § 5c EnWG erfasst werden.**

Gleiches gilt für die Pflicht zur Registrierung. So schreibt zum einen § 5c Abs. 8 S. 1, 2 EnWG die Registrierung von (allen) Betreibern von Energieversorgungsnetzen vor. Gleiches gilt für die Betreiber von Energieanlagen, die besonders wichtige Einrichtungen sind. Diese unterlägen in der vorliegenden Fassung allerdings auch den Registrierungspflichten nach § 33 BSIG. Die Pflichten stünden nebeneinander.

- **Der BDEW fordert daher, auch die Anwendbarkeit von § 33 BSIG durch § 28 Abs. 4 Nr. 2 BSIG im Scope der kritischen Anlage auszuschließen, soweit Betreiber von**

Energieversorgungsnetzen oder Energieanlagen bereits von § 5c EnWG erfasst werden.

Sollten diese Argumente für die wichtigen Einrichtungen und besonders wichtigen Einrichtungen nach § 28 Absatz 4 Nr. 1 nicht gelten, sollte für die Betreiber von Energieversorgungsnetzen oder Energieanlagen ein eigener Absatz geschaffen werden.

BDEW-Formulierungsvorschlag:

Der BDEW schlägt vor, einen neuen Absatz 5 einzufügen:

(5neu) Die §§ **30**, 31, 32, **33**, 35 und 39 gelten nicht für Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetz vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 1 des Gesetzes vom 5. Februar 2024 (BGBl. 2024 I Nr. 32) geändert worden ist, soweit sie den Regelungen des § 5c des Energiewirtschaftsgesetzes unterliegen.

3 § 5c EnWG - Notwendige Anpassungen der spezialrechtlichen Regelungen des Energiewirtschaftsgesetzes

Mit den für das EnWG vorgeschlagenen Regelungen geht die vorliegende Fassung des Gesetzes deutlich über die Anforderungen der NIS2-Richtlinie hinaus, ohne dies sachgerecht zu begründen. Die Ergänzung der ursprünglichen Vorgaben aus § 11 EnWG durch die Vorgaben der die NIS2 Richtlinie ist nicht immer stringent umgesetzt.

3.1 § 5c Abs. 2 EnWG – Anforderungen an die Betreiber von Energieanlagen

§ 5c Abs. 2 EnWG regelt die IT-Sicherheitspflichten für die Betreiber von Energieanlagen in Bezug auf die IT-Infrastrukturen des Anlagenbetriebs. Der bisherige § 11 Abs. 1b BSIG sah Pflichten nur für die Betreiber der Energieanlagen vor, die durch Rechtsverordnung als kritischen Infrastrukturen (zukünftig Betreiber von kritischen Anlagen) bestimmt wurden. § 5c Abs. 2 EnWG erweitert diese Pflichten auf alle Betreiber von Energieanlagen, die besonders wichtige oder wichtige Einrichtungen sind und weitet den Anwendungsbereich damit deutlich über das nach der NIS2-Richtlinie erforderliche hinaus aus. Unabhängig von der entstehenden Unsicherheit würde die Erweiterung insbesondere auf eine Vielzahl insbesondere von kleinen Betreibern von Energieanlagen zu einer erheblichen Erweiterung der Aufwände führen, die sich mittelbar in höheren Strompreisen ausdrücken werden.

Im Übrigen würde die Erweiterung auch nicht zur Systematik des Kritis-Dachgesetzes passen, denn der dortige Anwendungsbereich erfasst nur die Betreiber von kritischen Anlagen. Zudem müssten auch die Betreiber ihre wertvollen Ressourcen zunächst in die Klärung ihrer

Betroffenheit vom NIS2-Umsetzungsgesetz / Kritis-Dachgesetz stecken, anstatt in die Sicherheit investieren zu können.

Einrichtungen ab 50 Mitarbeitern sind bereits als eine wichtige Einrichtung nach § 28 Abs. 2 Nr. 3 BSIG anzusehen. Zukünftig wären fast alle Betreiber von Energieanlagen von den neuen Regelungen erfasst, unabhängig davon, ob sie als kritische Infrastruktur oder Anlage eingestuft wurden. Auch größere Unternehmen, die lediglich kleine bisher nicht als kritisch eingestufte Anlagen betreiben und z. B. Reststrom aus einer eigenen PV-Anlage einspeisen, würden unter den Wortlaut der Regelung gefasst werden können, z. B. von § 28 Absatz 2 Nr. 3 BSIG.

Nicht verständlich ist auch die Bezugnahme auf § 28 Abs. 2 Satz 1 BSIG. Diese Regelung umfasst nur Vertrauensdiensteanbieter und den Telekommunikationssektor. Erst Satz 2 würde auch Energieversorgungsunternehmen oder Unternehmen, die Energie oder entsprechende Dienstleistungen verkauften einschließen. Entsprechend der Systematik des § 5c EnWG sollten weiterhin ausschließlich Betreiber von Energieanlagen, die Betreiber von kritischen Anlagen sind, den speziellen Regelungen des EnWG unterliegen. Darüber hinaus sollten sie diesen Pflichten auch nur „insoweit“ unterliegen, als sich diese Pflichten auf die kritischen Anlagen beziehen.

Nicht erfasst sein dürfen die Pflichten für die sonstigen IT-Systeme, die sich auf die kritischen Anlagen, nicht auswirken wie z. B. die reguläre Office-IT. Für diese IT-Systeme muss es bei den allgemeinen Regeln des BSIG verbleiben, ohne dass die Pflichten nach dem EnWG und den IT-Sicherheitskatalogen anzuwenden sind (vgl. die Ausführungen zu § 28 Abs. 4 bzw. zu §§ 30, 31 BSIG).

Dieser Hintergrund sollte auch in der Gesetzesbegründung erläutert werden. Anderenfalls bleibt unklar, welche Anforderungen für Unternehmen zu erfüllen sind, die zwar wichtige oder besonders wichtige Unternehmen sind, beispielsweise auf Grund ihrer Größe, die aber keine kritischen Anlagen (Energieanlagen) betreiben.

BDEW-Formulierungsvorschlag:

Vor diesem Hintergrund schlägt der BDEW folgende Änderung vor in § 5c Abs. 2 EnWG:

(2) Betreiber von Energieanlagen**, die kritische Anlagen nach § 2 Absatz 1 Nummer 21 des BSI-Gesetzes sind**, ~~die besonders wichtige Einrichtungen nach § 28 Absatz 1 Satz 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von kritischen Anlagen und Einrichtungen (BSI-Gesetz) vom […] oder wichtige Einrichtungen nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes sind~~ und **die** ~~und~~ an ein Energieversorgungsnetz angeschlossen sind, haben einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische

Datenverarbeitungssysteme zu gewährleisten, die für einen sicheren Anlagenbetrieb notwendig sind […].

3.2 § 5c Abs. 3 EnWG – Inhalt der IT-Sicherheitskataloge

§ 5c Abs. 3 BSIG regelt die Inhalte der IT-Sicherheitskataloge näher. Die jetzige Fassung ist nicht konsistent und würde durch den generellen Verweis auf § 5c Abs. 1 und Abs. 2 EnWG auch für wichtige und besonders wichtige Einrichtungen gelten, die keine Energieanlagen betreiben, die als kritische Anlagen einzustufen wären. Die Norm lehnt sich dabei zwar erkennbar an die §§30, 31 BSIG an, vollzieht aber dessen Abstufung hinsichtlich der Pflichtentiefe von Betreibern kritischer Anlagen, von besonders wichtigen Einrichtungen und von wichtigen Einrichtungen nicht hinreichend nach und geht so deutlich über die Richtlinie und das BSIG hinaus.

Dies betrifft zunächst § 5c Abs. 3 S. 2 EnWG, der bei der **Bewertung** der Angemessenheit der IT-Sicherheitsmaßnahmen im Vergleich mit § 30 Abs. 1 S. 2 BSIG. nicht ausdrücklich auf die Umsetzungskosten verweist. Diese Umsetzungskosten werden in § 30 Abs. 1 S. 2 BSIG explizit genannt. Auch für den Bereich der kritischen Anlagen sind die Umsetzungskosten ein maßgeblicher Faktor, der bei der Bewertung der Angemessenheit der Maßnahmen berücksichtigt werden kann. Zwar sind die Umsetzungskosten in § 5c Absatz 3 Satz 1 EnWG erwähnt. Die fehlende Berücksichtigung bei der Bewertung könnte jedoch dazu führen, dass die Umsetzungskosten nicht ausreichend berücksichtigt werden.

Die Gesetzesbegründung sollte dies auch deutlicher darstellen, um Missverständnisse zu vermeiden und Sicherheit in der Umsetzung zu geben.

Zudem weist der BDEW darauf hin, dass durch den jetzigen § 5c Abs. 3 S. 3 Nr. 11 EnWG faktisch alle Betreiber von Energieanlagen **Systeme mit Angriffserkennung** umsetzen müssten. Dies widerspricht dem § 31 Abs. 2 BSIG, der diese Pflicht auf die Betreiber von kritischen Anlagen beschränkt. Auch aus diesem Grund muss § 5c Abs. 2 EnWG auf die Betreiber von kritischen Anlagen beschränkt werden (siehe hierzu die Ausführungen zu § 5c Abs. 2 EnWG).

BDEW-Formulierungsvorschlag:

Der BDEW schlägt vor, § 5c Abs. 3 EnWG wie folgt zu ändern:

(3) Die IT-Sicherheitskataloge nach den Absätzen 1 und 2 sollen den Stand der Technik einhalten und unter Berücksichtigung der einschlägigen europäischen und internationalen Normen sowie der Umsetzungskosten ein Sicherheitsniveau der informationstechnischen Systeme, Komponenten und Prozesse gewährleisten, das dem bestehenden Risiko angemessen ist. Bei der Bewertung, ob Maßnahmen dem bestehenden Risiko

angemessen sind, sind **neben den Umsetzungskosten** das Ausmaß der Risikoexposition**,** ~~**und**~~ die Größe des Betreibers**,** sowie die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen, zu berücksichtigen.

3.3 § 5c Abs. 4, 5 EnWG – Nachweiserbringung

Zunächst ist positiv zu bemerken, dass lediglich (alle) Betreiber von Energieversorgungsnetzen und Betreiber von kritischen Energieanlagen der BNetzA die Dokumentation der IT-Sicherheitsmaßnahmen übermitteln bzw. nachweisen müssen. Keine ex ante (also eine proaktive) Nachweispflicht haben dagegen die Betreiber von Energieanlagen, die lediglich eine besonders wichtige oder wichtige Einrichtung sind, aber nicht gleichzeitig eine kritische Anlage betreiben. (vgl. § 5c Abs. 4 EnWG).

Die Regelung in § 5c Abs. 5 EnWG ist nicht konsistent mit den übrigen Vorgaben in § 5c Absatz 2 und 4. Danach kann die BNetzA im Einzelfall von Betreibern von Energieanlagen, die wichtige Einrichtungen sind, ebenfalls die Maßnahmen nach § 5c Abs. 4 durchführen, also Mängelbeseitigungspläne anfordern. Betreiber von Energieanlagen, die besonders wichtige Einrichtungen sind, erwähnt die Regelung allerdings nicht. Die Norm müsste also – wenn diese Einrichtungen auch umfasst sein sollen – um die besonders wichtigen Einrichtungen ergänzt werden. Insgesamt sollten in den Regelungsbereich des § 5c EnWG allerdings ohnehin nur Betreiber von Energieanlagen fallen, die auch kritische Anlagen betreiben. Aus Sicht des BDEW wäre diese Regelung also entbehrlich. Hinzuweisen ist vor diesem Hintergrund darauf, dass zwar jeder Betreiber einer kritischen Anlage gleichzeitig eine besonders wichtige Einrichtung ist (vgl. § 28 Abs. 1 S. 1 Nr. 1 BSIG) aber nicht jede besonders wichtige Einrichtung auch gleichzeitig ein Betreiber einer kritischen Anlage ist.

BDEW-Formulierungsvorschlag

Der BDEW schlägt vor § 5c Absatz 5 zu streichen.

~~**(5) Erlangt die Bundesnetzagentur Kenntnis über Hinweise oder Informationen, wonach ein Betreiber von Energieanlagen, der eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist, die Anforderungen aus Absatz 2 nicht oder nicht richtig umsetzt, so kann sie Maßnahmen nach Absatz 4 durchführen. Die Bundesnetzagentur kann Informationen anfordern, um die Einhaltung der Sicherheitsanforderungen nach Absatz 2 zu überprüfen.**~~

Es wird ferner darauf hingewiesen, dass im Rahmen der Nachweiserbringung eine Formulierung vergleichbar § 39 Abs. 3 BSIG fehlt. In dieser Norm wird geregelt, dass für Bestandsanlagen für

den ersten Nachweis nach dem neuen Gesetz der letzte Nachweis nach dem alten Gesetz maßgeblich ist. Zudem wird dem BSI eine entsprechende Befugnis erteilt, diese Pflichten dann im Einzelfall festzulegen. **Es wird angeregt eine entsprechende Regel auch in das EnWG einzufügen**. Dies dient, wie in der Gesetzesbegründung beschrieben, der Entzerrung der Nachweisprüfung. Hierbei sollte zusätzlich festgelegt werden, dass die Nachweiserbringung auch in Bezug auf die Systeme zur Angriffserkennung einheitlich gefordert werden. Es muss verhindert werden, dass die Zyklen für die Nachweise der Systeme zur Angriffserkennung von den restlichen Nachweisen abweichen.

3.4 § 5c Abs. 8 – Registrierung

Wie mit Blick auf § 5c Absatz 2, und Absatz 5 festgestellt wurde, müssen aus den gleichen Gründen auch die Regelungen in Absatz 8 auf solche Betreiber von Energieanlagen begrenzt werden, die kritische Anlagen betreiben. Betreiber von Energieanlagen, die keine kritischen Anlagen betreiben aber wichtige oder besonders wichtige Einrichtungen sind, sollten in den Anwendungsbereich des BSI-Gesetzes fallen.

BDEW-Formulierungsvorschlag

> Der BDEW schlägt vor § 5c EnWG wie folgt zu ändern:
>
> (8) Betreiber von Energieversorgungsnetzen und solche Betreiber von Energieanlagen, **die kritische Anlagen nach § 2 Absatz 1 Nummer 21 des BSI-Gesetzes sind**~~, die besonders wichtige Einrichtungen nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder wichtige Einrichtungen nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes sind~~, sind verpflichtet, spätestens bis zum 1. April, erstmalig oder erneut, sich beim Bundesamt für Sicherheit in der Informationstechnik zu registrieren. […]

3.5 Weitere Hinweise zu § 5c EnWG

Der BDEW weist darauf hin, dass im Rahmen der Nachweiserbringung eine mit § 39 Abs. 3 BSIG vergleichbare Formulierung fehlt. Die Norm regelt, dass für Bestandsanlagen für den ersten Nachweis nach dem neuen Gesetz der letzte Nachweis nach dem alten Gesetz maßgeblich ist. Außerdem erhält das BSI eine entsprechende Befugnis, diese Pflichten dann im Einzelfall festzulegen. Dies würde, wie in der Gesetzesbegründung zum BSIG beschrieben, der Entzerrung der Nachweisprüfung dienen. Hierbei sollte zusätzlich festgelegt werden, dass die Nachweiserbringung auch in Bezug auf die Systeme zur Angriffserkennung einheitlich gefordert werden. Es muss verhindert werden, dass die Zyklen für die Nachweise der Systeme zur Angriffserkennung von den restlichen Nachweisen abweichen.

- **Der BDEW regt an eine entsprechende Regel auch in das EnWG einzufügen**.

4 § 2 Abs. 1 Nr. 10 BSIG - Definition erheblicher Sicherheitsvorfall

Der Wortlaut der Norm kann so verstanden werden, dass jeder nur mögliche finanzielle Verlust - ganz gleich wie groß er ist - zu einem erheblichen Sicherheitsvorfall führt. Da jeder Sicherheitsvorfall allein durch die Behebung zu einem finanziellen Verlust führt, wäre somit diese Regelung uferlos und unverhältnismäßig. Aus diesem Grund erläutert Erwägungsgrund 101 der NIS2-Richtlinie auch, dass solche Gefahren vermieden werden sollen, die erhebliche materielle oder immaterielle Schäden verursachen können.

Eine entsprechende Klarstellung sollte in der Begründung oder im Gesetzestext bzw. spätestens in einer Verordnung nach § 2 Absatz 2 BSIG auch deswegen erfolgen, weil nach dem Wortlaut der Norm der finanzielle Verlust gar nicht eingetreten sein muss, sondern allein die Möglichkeit des Eintritts ausreicht.

- **BDEW-Forderung:**

  Klarstellung, zumindest in der Gesetzesbegründung, dass nicht jeder finanzielle Verlust, sondern nur erhebliche finanzielle Verluste einen erheblichen Sicherheitsvorfall darstellen können.

5 Anlage 1 Sektoren besonders wichtiger und wichtiger Einrichtungen

In der Anlage 1 sind in Zeile 1.1.9 Ladepunktbetreiber gemäß § 2 Nr. 8 LSV als Einrichtungsart aufgeführt. Die Ladesäulenverordnung (LSV) wird derzeit geändert. Sie ist zu großen Teilen durch die AFIR ersetzt worden. Daher wäre es sinnvoller auf Art. 2 Nr. 49 AFIR zu verweisen. Erfasst wären alle Ladepunkte, auch private Ladepunkte für den Eigengebrauch. Die NIS2 RL zielt dagegen ausweislich der Anlage 1 auf Betreiber von Ladepunkten ab, die Endnutzern einen Aufladedienst erbringen, auch im Namen und Auftrag eines Mobilitätsdienstleisters die also vor allem Ladepunktbetreiber öffentlich zugängliche Ladepunkte betreiben. Zu überlegen wäre auch eine Einschränkung auf öffentlich zugängliche Ladepunkte.

BDEW-Formulierungsvorschlag:

Anlage 1 Sektoren besonders wichtiger und wichtiger Einrichtungen sollte in Zeile 1.1.4 ergänzt werden:

„Ladepunktbetreiber ~~gemäß § 2 Nr. 8 LSV~~ **im Sinne von Art. 2 Nr. 49 AFIR, die gegenüber Endnutzern Elektromobilitätsdienstleistungen erbringen.“**

6 NIS2UmsuCG und KRITIS-DachG: Abhängigkeiten und notwendige Harmonisierung

Im Verhältnis des NIS2-Umsetzungsgesetzes und des KRITIS-Dachgesetzes gibt es Harmonisierungsbedarf, der zwar absehbar aber derzeit noch nicht vollständig bewertet werden kann. Folgende Punkte sind dabei wesentlich:

6.1 Abschließende Beurteilung des NIS2UmsuCG aufgrund nicht bewertbarer Bezüge zum KRITIS-DachG nicht möglich

NIS2UmsuCG und KRITIS-DachG sollten stärker miteinander abgestimmt, wesentliche Regelungsinhalte des KRITIS-DachG mit Relevanz für die Beurteilung des NIS2UmsuCG den Branchenverbänden zur Kommentierung zugänglich gemacht und beide Gesetze schließlich gleichzeitig in den Bundestag eingebracht werden.

Die kohärente Umsetzung der CER-Richtlinie und der NIS2-Richtlinie verlangt eine größtmögliche Harmonisierung und Verzahnung von NIS2UmsuCG und KRITIS-DachG. Diese Verzahnung sollte bei einer einheitlichen Begriffsbestimmung (z. B. kritische Anlagen) beginnen und mit der engen Abstimmung der Regelungsinhalten (insbesondere gemeinsamer Nachweispflichten) fortfahren. Nur so können Doppelaufwendungen vermieden und eine Cyberraum und physischen Raum integrierende Sicherheit im Sinne des All-Gefahren-Ansatzes realisiert werden. Die zu erlassende Rechtsverordnung sollte im Sinne einer größtmöglichen Harmonisierung zwischen NIS2UmsuCG und KRITIS-DachG auf aktuellen Sektorstudien des BSI und auch der BSI-KritisV aufbauen und die dort erarbeiteten sowie bewährten Methoden zur Bestimmung von Schwellenwerten kritischer Anlagen übernehmen. Die Konkretisierung des Begriffs *kritische Anlage* sollte im Sektor Energie in enger Abstimmung mit der BNetzA erfolgen. Die Erfahrung mit der Erarbeitung und Umsetzung der BSI-KritisV haben gezeigt, dass eine frühzeitige und umfassende Einbindung der Branchen und ihrer Verbände sinnvoll und zielführend ist. Abschließend sollten NIS2UmsuCG und KRITIS-DachG -im Sinne einer größtmöglichen Harmonisierung- auch gleichzeitig im Bundestag eingebracht werden. Schließlich ist eine abschließende Beurteilung des NIS2UmsuCG aufgrund der fehlenden Referenzen zum aktuellen und der Wirtschaft nicht vorliegenden Referentenentwurfs des KRITIS-DachG und etwaiger zukünftiger Änderungen im KRITIS-DachG zurzeit nicht möglich.

6.2 Anbindung von Landesbehörden an einheitliches Meldeportal und einheitliche Meldestelle gemäß §12 KRITIS-DachG

§ 12 KRITIS-DachG des Referentenentwurfs vom 21. Dezember 2023 sieht nach dem Grundsatz „ein Vorfall, eine Meldung“ ein einheitliches Meldeportal sowie eine einheitliche Meldestelle

für Vorfälle gemäß KRITIS-DachG und NIS2UmsuCG vor. Ein nicht-bundeseinheitlicher Vollzug des KRITIS-DachG in den Sektoren Wasser, Abfallwirtschaft und ÖPNV führt in diesen Sektoren – und damit auch in Querverbundsunternehmen – allerdings zu einer Zersplitterung der behördlichen Zuständigkeit und des Meldewesens nicht nur bei der Resilienz, sondern auch bei der Cybersicherheit. Denn aus § 12 KRITIS-DachG des Referentenentwurfs vom Dezember 2023 geht die Anbindung der für die benannten Sektoren zuständigen Landesbehörden an die gemeinsame Meldeportal und einheitliche Meldestelle noch nicht hervor. Ein Vorfall, der zunächst als physischer Vorfall durch einen Betreiber in einem Sektor mit behördlicher Zuständigkeit auf Landesebene eingeordnet und an die zuständige Landesbehörde gemeldet wird, müsste im Falle einer späteren Qualifizierung als Informationssicherheitsvorfall auf Grundlage weiterführender Erkenntnisse dann erneut und dieses Mal an das Bundesamt für Sicherheit in der Informationstechnik gemeldet werden. Erfolgt eine Regelung zur Anbindung der Landesbehörden an das einheitliche Meldeportal und die einheitliche Meldestelle nicht, müssten bei landesgrenzüberschreitenden Vorfällen darüber hinaus auch mehrere Behörden durch die Betreiber kritischer Anlagen informiert werden und diese Landesbehörden sich miteinander koordinieren. Beide Szenarien würden im direkten Widerspruch zum Zweck des § 12 KRITIS-DachG stehen, das Meldewesen so zu verschlanken, dass Betreiber kritischer Anlagen nur eine Meldung für einen Vorfall abgeben müssen und die Behörden eine schnelle und umfassende Erstellung von Lagebildern vornehmen können. Schließlich 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.

- **Der BDEW fordert aus diesen Gründen eine Regelung zur Anbindung der für die einschlägigen Sektoren zuständigen Landesbehörden in § 12 KRITIS-DachG. Zudem müssen die Landesbehörden die Datenhaltung und die Datenübertragung des Meldewesens auf dem gleichen Niveau wie das Bundesamt für Sicherheit in der Informationstechnologie absichern.**

7 Geeignetes Meldewesen (Massenfähigkeit)

Nach der Inkraftsetzung des NIS2UmsuCG werden voraussichtlich etwa 29.000 bis 30.000 Unternehmen betroffen sein. Diese Unternehmen müssen künftig dem BSI erhebliche Sicherheitsvorfälle melden. Dies führt dazu, dass das BSI eine Art „manuelles bundesweites Sensorsystem“ aufbaut und durch neue Meldefristen relativ schnell über Cyberangriffe und Sicherheitslücken informiert wird. Ähnliches muss auch in den anderen europäischen Mitgliedsstaaten umgesetzt werden.

Unter der Annahme, dass jedes dieser deutschen Unternehmen alle 2 Monate einen meldepflichtigen Vorfall hat (Annahme aus IT-SIG 1.0), handelt es sich um ca. 180.000 Erst-Meldungen pro Jahr (das wären ca. 500 Meldungen pro Tag) dazu kommen noch bis zu 3 Folgemeldungen pro Vorfall.

Falls die anderen Mitgliedsstaaten ähnlich hohe Fallzahlen haben und das BSI zumindest über mögliche grenzüberschreitende Vorfälle informiert wird, erhöht das die Summe der Meldungen. Darüber hinaus wird in naher Zukunft der Cyber Resilience Act (CRA) in Kraft treten. Dabei müssen auch Hersteller, Importeure und Distributoren hilfreiche Informationen an die nationalen Behörden melden. Nimmt man das alles zusammen, sind viele 100 Meldungen pro Tag zu erwarten. Dabei fehlen noch die Meldungen von Bundes- und Landesverwaltungen, welche in den Meldeprozessen zurzeit noch nicht integriert sind, welche aber für ein Gesamtbild auch relevant wären.

Das Bundesamt benötigt geeignete Technologien und Prozesse, um diese „Meldeflut“ zu bewältigen (E-Mails oder Portale mit ausschließlich manueller Verarbeitung sind ungeeignet) und, was noch wichtiger ist, relevante Meldungen/Informationen zu identifizieren und an die zuständigen Stellen und die betroffenen Unternehmen weiterzuleiten damit diese ihre eigene Betroffenheit prüfen und gegebenenfalls Maßnahmen ergreifen können.

8 § 38 Abs. 2 BSIG – Haftungsverzicht / Vergleich über die Haftung

Die NIS2-Richtlinie sieht in Art. 20 Abs. 1 vor, dass Leitungsorgane für Verstöße gegen diesen Artikel durch die betreffenden Einrichtungen verantwortlich gemacht werden können. Das ist in Deutschland bereits durch den § 43 GmbHG gewährleistet. Insofern bedarf es für die Umsetzung der Richtlinie keine weiteren Regelungen, wie in § 38 Abs. 2 BSIG aktuell vorgesehen.

Ansprechpartner

Mathias Böswetter

Fachgebietsleiter KRITIS-, Cyber- und Sicherheitspolitik

+49 30 300199 1526

mathias.boeswetter@bdew.de