BDEW Bundesverband der Energie- und Wasserwirtschaft e. V.
Reinhardtstraße 32
10117 Berlin

www.bdew.de

Berlin, 20. Oktober 2023

Stellungnahme zum Diskussionspapier des Bundesministeriums des Innern und für Heimat „Wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland“ vom 27. September 2023

Transparenz-Register-ID des BDEW: 20457441380-38

I. Zusammenfassung und Positionen des BDEW im Überblick

Der BDEW begrüßt das Angebot des Diskussionspapiers des Bundesministeriums des Innern und für Heimat „Wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland“ vom 27. September und eines anstehenden Werkstattgesprächs ausdrücklich. Nur durch die frühzeitige und intensive Einbindung der Wirtschaft kann eine geeignete Weiterentwicklung des Cybersicherheitsrechts in Deutschland gelingen. Der BDEW hofft daher, dass im Zusammenhang mit dem KRITIS-DachG eine vergleichbare Einbindung der Branchen und ihrer Verbände erfolgen wird.

Auch begrüßt der BDEW die Erweiterung des Nachweiszyklus auf drei Jahre als einen wichtigen Schritt in Richtung Internationalisierung des nationalen Cybersicherheitsrechts entlang der einschlägigen europäischen und internationalen Normen im Bereich der Informationssicherheit. In Zukunft werden europäische Regulierungsframeworks wie etwa der Network Code on Cybersecurity diese Entwicklung gerade im Sektor Energie erheblich verstärken. Das vorliegende Diskussionspapier trägt dieser Entwicklung etwa in § 30 NIS2UmsuCG grundsätzlich Rechnung. Deshalb sollte die Internationalisierung auch andere wesentliche Regelungsinhalte des NIS2UmsuCG erfassen und nationale Alleingänge (etwa bei der Einführung von abweichenden Schutzzielen oder bei der Neuregelung der Prüfung von Konformitätsbewertungsprogrammen) vermieden werden. Nationale Alleingänge bei der Umsetzung europäischer Vorgaben können in Zukunft aufgrund steigender Harmonisierungsanforderungen im Unionsgebiet einen aufwändigen Rückbau erforderlich machen. Nicht zuletzt hat die Vergangenheit gezeigt, dass nationale Alleingänge (wie beim IT-Grundschutz des BSI oder bei der Smart-Meter-Gateway-Infrastruktur) leider keinen nennenswerte „Leuchtturm-Charakter“ mit Nachahmungswirkung im Unionsgebiet entfalten konnten.

II. Positionen im Überblick

Folgende Punkte sollte das NIS2UmsuCG im Sinne einer geeigneten Weiterentwicklung des Cybersicherheitsrechts und einer Harmonisierung mit dem KRITIS-DachG berücksichtigen:

1. Öffentliche Ladeinfrastruktur, Gateway-Administratoren, Anlagen zur Bündelung elektrischer Leistung, Handelssysteme sowie Fernwärme sollten im Zuge des neuen § 5c EnWG durch eigenständige Informationssicherheitskataloge (der BNetzA) für den Scope *kritische Anlage* erfasst werden.

2. Die Regime der IT-Sicherheitskataloge der BNetzA und der Branchenspezifischen Sicherheitsstandards - mit ihren besonders hohen Anforderungen an den sicheren Netz- und Anlagenbetrieb - müssen auf den Scope *kritische Anlage* beschränkt bleiben und dürfen nicht auf den Scope *besonders wichtige Einrichtung* ausgeweitet werden.

3. NIS2UmsuCG und KRITIS-DachG sollten stärker aufeinander abgestimmt, wesentliche Regelungsinhalte im Sinne des All-Gefahren-Ansatzes harmonisiert und beide Gesetze gleichzeitig in den Bundestag eingebracht werden.

4. Zur Vermeidung einer potenziellen „Resilienz-Lücke“ sollten Bund und Länder die Betreiber kritischer Anlagen mit ausreichenden finanziellen, materiellen und personellen Mitteln zur Mitigierung terroristischer, paramilitärischer und militärischer Risiken unterstützen.

5. Konformitätsbewertung und die fachliche Qualifikation der Prüfstellen sollten im Sinne der Internationalisierung des nationalen Cybersicherheitsrechts auf Grundlage internationalen Standards erfolgen.

6. Das Prüfverfahren zu den kritischen Komponenten nach § 9b BSIG sollte in § 41 NIS2UmsuCG [trotz großer Relevanz für die Wirtschaft nicht im Diskussionspapier enthalten] durch ein öffentliches Blacklisting ersetzt oder zumindest ergänzt werden. Dieses Verfahren sollte auch für die Bestimmung und die Untersagung des Einsatzes von kritischen Komponenten nach KRITIS-DachG gelten.

7. Die Folgen der in §30 Absatz 2 NIS2UmsuCG definierten geplanten Zertifizierungspflichten von Komponenten und Prozessen sind gegenwärtig für die verlässliche Abschätzung der Aufwendungen durch die Wirtschaft zu unbestimmt. Die Verpflichtung zur Nutzung von zertifizierten Komponenten und Prozessen sowie die Möglichkeit zum Erlass nationaler technischer Spezifizierungen dürfen nicht zu Beschaffungsengpässen und zur Bildung von Oligopolen führen.

8. Abschätzung der Erfüllungsaufwendungen durch die Betreiber kritischer Anlagen ist gegenwärtig nur eingeschränkt möglich. Erst die nach KRITIS-DachG zu erlassende Rechtsverordnung bestimmt wesentliche zur Abschätzung der Erfüllungsaufwende der Wirtschaft notwendige Regelungsinhalte.

9. Das Schutzziel *Authentizität* sollte im international etablierten Schutzziel *Integrität* integriert werden, um nicht von internationalen Standards abzuweichen.

10. Es sollten aus Gründen von Sicherheit und Vertraulichkeit nur öffentliche IP-Adressen und keine internen Netzwerk-IP-Adressen als „digitaler Fußabdruck" (im Rahmen der Registrierung) übermittelt werden (müssen).

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

III. Begründung der Positionen

Fortschreiben und Weiterentwicklung der IT-Sicherheitskataloge (der BNetzA) für den Scope *kritische Anlage*: Die Komplexität der Energiewende sowie die daraus resultierenden komplexen Wechselwirkungen zwischen Informationssicherheit und Systemsicherheit verlangen das Fortbestehen und die Harmonisierung der IT-Sicherheitskataloge der BNetzA sowie die Integration der Anlagenkategorien öffentliche Ladeinfrastruktur, Gateway-Administratoren, Anlagen zur Bündelung elektrischer Leistung und Handelssysteme in einem neuen Informationssicherheitskatalog oder jeweils eigenständigen Informationssicherheitskatalogen (der BNetzA) für den Scope *kritische Anlage*. Im Sinne eines einheitlichen Informationssicherheits-Risikomanagementverfahrens für den Sektor Energie sollte auch die Fernwärme in einem eigenständigen IT-Sicherheitskatalog der BNetzA berücksichtigt werden. Das Fortschreiben und die Weiterentwicklung der IT-Sicherheitskataloge (der BNetzA) könnte dabei im Rahmen des im Diskussionspapier angelegten (neuen) § 5c EnWG erfolgen.

Die Regime der IT-Sicherheitskataloge der BNetzA und der Branchenspezifischen Sicherheitsstandards - mit ihren besonders hohen Anforderungen an den sicheren Netz- und Anlagenbetrieb - müssen auf den Scope *kritische Anlage* beschränkt bleiben und dürfen nicht auf den Scope *besonders wichtige Einrichtung* ausgeweitet werden. Zusätzliches birgt eine solche Ausweitung das Risiko der unverhältnismäßigen Ausweitung des Anwendungsbereichs für Resilienz-Anforderungen nach KRITIS-DachG und der zu erlassenden Rechtsverordnung: Nach § 28 NIS2UmsuCG i.V.m. § 30 NIS2UmsuCG sollten für Betreiber von kritischen Anlagen im Scope *besonders wichtige Einrichtung* abweichend vom Scope *kritische Anlage* die Maßnahmen aus § 30 Abs. 2 NI2UmsuCG sowie Nachweispflichten im Schadensfall gegenüber dem BSI gelten. Die Ausweitung der sehr hohen Anforderungen für Betreiber kritischer Anlagen in den Regimen der IT-Sicherheitskataloge der BNetzA und der Branchenspezifischen Sicherheitsstandards auf den Scope *besonders wichtige Einrichtung* ist unverhältnismäßig und würde zu einem erheblichen administrativen, personellen und wirtschaftlichen Mehraufwand führen, der für die Wirtschaft selbst mehr Sicherheitsrisiken als nennenswerte Sicherheitszugewinne birgt. Die besonders hohen Anforderungen im Scope *kritische Anlagen* wurden im Rahmen der IT-Sicherheitskataloge der BNetzA oder der Branchenspezifischen Sicherheitsstandards auf die Absicherung der kritischen Funktionen im Netz- und Anlagenbetrieb hin festgelegt. Deren Kritikalität und Spezifizität kann nicht mit den für Netz- und Anlagenbetrieb unkritischen Businessprozessen im Scope *besonders wichtige Einrichtung* verglichen werden (z.B. für die IT-Systemen der Betriebskantine). Diese unkritischen Businessprozesse haben keinen unmittelbaren oder mittelbaren Einfluss auf den sicheren Netz- und Anlagenbetrieb. Auch sind die kritischen Funktionen im Netz- oder Anlagenbetrieb und die unkritischen Businessprozesse IT-seitig hinreichend segregiert. Durch eine deutliche Ausweitung des Anwendungsbereiches der Regime der IT-Sicherheitskataloge der BNetzA und der Branchenspezifischen Sicherheitsstandards besteht deshalb das erhebliche Risiko, dass vor allem knappe personelle Ressourcen durch administrative Prozesse gebunden werden und dadurch der operativen Informationssicherheit nicht ausreichend zur Verfügung

stehen können. Dieses Risiko ist besonders vor dem Hintergrund des sich weiter verschärfenden Fachkräftemangels sehr ernst zu nehmen. Auch aus behördlicher Sicht ergibt die vorgeschlagene Lösung Sinn, da das BSI die IT-Vorfälle im Scope *besonders wichtige Einrichtung* mit seiner umfassenden Erfahrung sowie Expertise schnell erfassen und bewerten kann, während die BNetzA in Abstimmung mit dem BSI Vorfälle im Scope *kritische Anlage* aus umfassender Sicht auf die Sicherheit im Energiesystem beurteilen kann.

Zusätzlich besteht durch die Ausweitung der hohen Anforderungen des Scopes *kritische Anlage* auf den Scope *besonders wichtige Einrichtung* das Risiko, dass die zukünftigen Anforderungen aus dem KRITIS-DachG und der zu erlassenden Rechtsverordnung an Betreiber kritischer Anlagen dann auch im Scope *besonders wichtige Einrichtung* umzusetzen sind. Eine solche unverhältnismäßige Ausweitung des Anwendungsbereichs für Resilienz-Anforderungen nach KRITIS-DachG und der zu erlassenden Rechtsverordnung muss unbedingt im Sinne der Umsetzbarkeit vermieden werden.

Größtmögliche Harmonisierung NIS2UmsuCG und KRITIS-DachG: 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.

Potenzielle „Resilienz-Lücke“ (nach All-Gefahren-Ansatz) gefährdet Wirtschaftlichkeit und rechtskonforme Umsetzung von Anforderungen für Betreiber kritischer Anlagen: Die hohe Versorgungssicherheit in der Energieversorgung ist im Wesentlichen das Ergebnis unternehmerischer Freiheit und unternehmerischer Verantwortung, der die Energiewirtschaft seit Jahrzehnten durch die Bereitstellung kritischer Dienstleistungen nachkommt. Die hohe und im europäischen Vergleich vorbildliche Versorgungssicherheit Deutschlands kann aber selbst nicht zur bindenden Maßgabe für die Betreiber werden. Die Bereitstellung der kritischen Dienstleistungen muss sich dagegen an der Wirtschaftlichkeit der zu ergreifenden Schutz- und Sicherheitsmaßnahmen messen lassen. Der Mitigierung terroristischer oder (para-)militärischer Bedrohungen können daher die Betreiber kritischer Infrastrukturen -ohne Unterstützung durch den Bund oder die Länder- weder wirtschaftlich nachkommen, noch dürfen sie den hoheitlichen und bei den Ländern liegenden Auftrag der

Gefahrenabwehr im Cyberraum oder im physischen Raum erfüllen. Um dieser drohenden „Resilienz-Lücke“ zu begegnen, müssen der Bund und die Länder ausreichende Mittel zur Unterstützung der Betreiber kritischer Infrastrukturen bereitstellen und eine erweiterte Zuständigkeit der Bundespolizei beim Schutz kritischer Infrastrukturen in Erwägung ziehen. Nicht zuletzt haben die der NIS2-UmsuCG und KRITIS-DachG zugrundeliegenden EU-Richtlinien deshalb die ausreichende finanzielle, materielle und personelle Unterstützung der Betreiber kritischer Anlagen durch die Mitgliedsstaaten -explizit- vorgesehen.

Prüfung von Konformitätsbewertungsprogrammen durch DAkkS und fachliche Qualifikation der Prüfstellen im Sektor Energie: Die Konformitätsbewertung und die sektorspezifische Qualifikation der Prüfstellen sollten im Sinne der Internationalisierung des nationalen Cybersicherheitsrechts unter Berücksichtigung internationaler Standards erfolgen. Insbesondere aus EU-rechtlicher Sicht sollte die Prüfung von Konformitätsbewertungsprogrammen im Sektor Energie damit -auch in Zukunft- durch die Deutschen Akkreditierungsstelle (DAkkS) erfolgen.

Anpassung des Prüfprozesses bei kritischen Komponenten in § 41 NIS2UmsuCG und ein gemeinsames Verfahren für NIS2UmsuCG und KRITIS-DachG: Das bisherige Verfahren des § 9b BSIG hat sich weder im Telekommunikationssektor noch im Sektor Energie als wirkungsvolles Mittel bewährt, um die technologische Abhängigkeit bei Schlüsseltechnologien bzw. kritischen IT-Komponenten spürbar und nachhaltig zu verringen. Der BDEW fürchtet daher, dass dieses gegenwärtig ungeeignete Prüfverfahren zur Untersagung des Einsatzes von kritischen Komponenten nun auch für die kritischen Komponenten im Sinne des neuen § 41 NIS2UmsuCG und des § 13 KRITIS-DachG zum Einsatz kommen könnte. Damit Netzausbau und Energiewende aber nicht weiter ausgebremst und die Versorgungssicherheit durch bürokratisch induzierte Beschaffungsengpässe nicht gefährdet werden, spricht sich der BDEW dafür aus, für NIS2UmsuCG und das KRITIS-DachG das bestehende Prüfverfahren durch ein öffentliches „Blacklisting“ von Herstellern, die als nicht-vertrauenswürdigt eingestuft werden, zu beerben.

Zertifizierungspflichten von Komponenten und Prozessen nach § 30 Absatz 2 NIS2UmsuCG dürfen nicht zu Beschaffungsengpässen und zur Bildung von Oligopolen führen: Nach dem vorliegenden Diskussionspapier zum NIS2UmsuCG sind die Folgen der Zertifizierungspflichten von Komponenten und Prozessen zur Abschätzung der Aufwendungen durch die Wirtschaft noch zu unbestimmt. Die Erfahrungen (etwa mit der Smart-Meter-Gateway-Infrastruktur) haben gezeigt, dass insbesondere nationale Zertifizierungsframeworks der zügigen Einführung sicherer digitaler Infrastrukturen im Sektor Energie im Wege stehen und die Bildung von Oligopolen begünstigen können. Diese Oligopole sind aus einer systemischen Sicherheitsperspektive selbst als potenzielles Klumpenrisiko zu bewerten. Auch im Sinne der internationalen Wettbewerbsfähigkeit deutscher Hersteller sollte der Stand der Technik nicht durch Dokumente und technische Richtlinien einer Bundesbehörde festgelegt werden. Eine rein nationale Zertifizierung ist deshalb auch nicht im Sinne der NIS2-Richtlinie, da diese auf einen gemeinsamen europäischen Binnenmarkt ohne Zutrittsbarrieren für Hersteller

aus den Unionsstaaten abzielt. Es kann ferner nicht davon ausgegangen werden, dass Hersteller zwingend ein Interesse an den Aufwänden einer Zertifizierung bei einer ausschließlich deutschen Zertifizierung haben.

Integration des Schutzziels *Authentizität* in das international etablierte Schutzziel *Integrität*, um nicht von internationalen Normen abzuweichen: Die ISO/IEC 27001 und die im Sektor Energie nach IT-Sicherheitskatalogen der BNetzA etablierten Informationssicherheitsmanagementsysteme berücksichtigen bisher nicht das Schutzziel *Authentizität*. Es ist nicht davon auszugehen, dass eine entsprechende Erweiterung um das Schutzziel *Authentizität* im nationalen Cybersicherheitsrechts sich in der europäischen und internationalen Normungsarbeit niederschlagen wird. Aus sachlicher Sicht ließen sich die wesentlichen Aspekte des Schutzziels *Authentizität* aber auch im Schutzziel *Integrität* identifizieren, das in der ISO/IEC 27001 etabliert ist.

Verpflichtende Weitergabe von IP-Adressen bringt keinen nennenswerten Sicherheitszugewinn: Es sollten aus Gründen von Sicherheit und Vertraulichkeit ausschließlich öffentlich erreichbar IP-Adressen und keine internen Netzwerk-IP-Adressen übermittelt werden. Die verpflichtende Übermittlung von IP-Adressen birgt für die Wirtschaft eher mehr Sicherheitsrisiken als einen nennenswerten Sicherheitszugewinn. Auf freiwilliger Basis einen „IP-Adressen-Fußabdruck“ bereitzustellen, ist als Alternative grundsätzlich der geeignetere Ansatz, um die Informationssicherheit zu stärken.

Notwendige Begriffsbestimmung im § 2 Abs. 1 Nr. 9 BSIG (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. Verstärkt wird dies dadurch, dass nach dem Wortlaut der Norm der finanzielle Verlust gar nicht eingetreten sein muss, sondern allein die Möglichkeit des Eintritts ausreicht. Deshalb sollten *finanzielle Verluste* durch *erhebliche finanzielle Verluste* in der Norm Ersetzung finden.

Ansprechpartner

Mathias Böswetter

Fachgebietsleiter IT-Sicherheit, Kritische Infrastrukturen

+49 30 300199 1526

mathias.boeswetter@bdew.de