Berlin, 3. Juli 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 24. Juni 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 und Positionen im Überblick

Der BDEW 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 vom 24. Juni 2024 kommentieren zu dürfen. Der vorliegende Referentenentwurf des NIS2UmsuCG weist im Vergleich zum Referentenentwurf vom 7. Mai 2024 Verbesserungen auf. Wir begrüßen dabei insbesondere:

- Die Berücksichtigung der vom BDEW geforderten weiteren Ausnahmen im § 28 Abs. 4 BSIG, um eine Doppelregulierung mit den Regelungen des § 5c EnWG zu vermeiden. **Allerdings führt der neu aufgenommene § 28 Abs. 4 S. 2 und 3 BSIG zu einer erheblichen und nicht praktikablen Komplexitätssteigerung in Verbundgesellschaften.** Hier muss unbedingt nachgebessert werden, da die vorliegende Regelung zur Überforderung der betroffenen Querverbundgesellschaften und unklaren Prüfgrundlagen führen wird.

Bei den folgenden Punkten sieht der BDEW aber noch dringenden Anpassungsbedarf:

- Für Querverbundgesellschaften, die in einer juristischen Gesellschaft Dienstleistungen für mehrere Sektoren erbringen (Querverbundgesellschaften), müssen geeignete und nachvollziehbare Regelungen der § 28 Abs. 4 BSIG und § 5c EnWG geschaffen werden. Insbesondere muss der **§ 28 Abs. 4 S. 2 und 3 BSIG vereinfacht und eine analoge Übertragung der Dreistufigkeit der NIS2-Richtlinie in die IT-Sicherheitskataloge der Bundesnetzagentur verbindlich festgeschrieben werden. Eine spätere Durchbrechung der Dreistufigkeit im Anwendungsbereich der IT-Sicherheitskataloge durch von anderen NIS2-Sektoren abweichenden Maßnahmen und Anforderungen ist unbedingt zu vermeiden.** Dies gilt insbesondere auch für die Anforderungen für Betreiber von Energieerzeugungsanlagen, die keine kritischen Anlagen sind, aber in Zukunft dennoch unter den Anwendungsbereich des IT-Sicherheitskatalogs gemäß § 5c Abs. 2 EnWG fallen sollen. Für diese sollte kein ISMS und Zertifikat erforderlich sein. **Dies gilt jedenfalls, soweit diese Anlagen ohnehin mittels der SMGW-Infrastruktur abgesichert sind und über den Messstellenbetreiber durch den Netzbetreiber netzdienlich im Falle von dezentralen Angriffen gesteuert werden können.**

- Das Prüfverfahren gemäß § 41 BSIG muss – wie auch in der BDEW-Stellungnahme vom 28. Mai gefordert und begründet - gestrichen und durch eine **Ausschlussliste generell nicht-vertrauenswürdiger Hersteller** ersetzt werden (siehe auch die Stellungnahme vom 28. Mai 2024: https://www.bdew.de/media/documents/1000_BDEW-Stellungnahme_NIS2UmsuCG.pdf).

- **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. Eine maximale Verzahnung ist schließlich auch beim Meldewesen unbedingt erforderlich. Ein einheitliches Meldeportal und eine einheitliche Meldestelle müssen daher zeitnah durch die Bundesverwaltung bereitgestellt werden. Die Anbindung von Landesbehörden an ein einheitliches Meldeportal und eine einheitliche Meldestelle gemäß §12 KRITIS-DachG muss darüber hinaus sichergestellt werden, da es für das KRITIS-DachG in einigen Sektoren zum Landesvollzug kommen wird (siehe auch die Stellungnahme vom 28. Mai 2024: https://www.bdew.de/media/documents/1000_BDEW-Stellungnahme_NIS2UmsuCG.pdf).

- Anlage 1 - Sektoren besonders wichtiger und wichtiger Einrichtungen. Anlage 1 verweist in Ziffer 1.1.9 noch immer auf die Ladesäulenverordnung (LSV) (siehe auch die Stellungnahme vom 28. Mai 2024: https://www.bdew.de/media/documents/1000_BDEW-Stellungnahme_NIS2UmsuCG.pdf).

II. Ausführliche Kommentierung § 28 Abs. 4 BSIG, Anlage 1 und § 5c EnWG

1 § 28 Abs. 4 S. 2 und 3 BSIG: Praxistauglichkeit erfordert Vereinfachung der Regelung

Gänzlich neu aufgenommen wurden im vorliegenden Referentenentwurf der § 28 Abs. 4 S. 2 und 3 BSIG. Hintergrund ist laut Gesetzesbegründung die besondere Stellung der Querverbundgesellschaften, also Unternehmen die neben dem Sektor der Energie auch noch in weiteren Sektoren (z.B. Wasser oder Telekommunikation) tätig sind. Zunächst begrüßt der BDEW, dass das Gesetz die spezielle Situation jener auch im BDEW organisierten Querverbundgesellschaften regeln soll. Querverbundgesellschaften sind nicht nur in verschiedenen Sektoren tätig, sondern müssen auch die verschiedenen sektorspezifischen Anforderungen an den Betrieb Kritischer Infrastrukturen erfüllen. Dies führt dazu, dass die Querverbundgesellschaften für den Sektor Energie neben den IT-Sicherheitskatalogen der BNetzA teilweise auch die Anforderungen aus den branchenspezifischen Sicherheitsstandards für die Bündelung und Steuerung elektrischer Leistung (Aggregatoren) oder für Fernwärme, Transport oder Wasser erfüllen und – abweichend von den IT-Sicherheitskatalogen der Bundesnetzagentur – dem BSI gegenüber nachweisen müssen. Darüber hinaus gelten in anderen Sektoren für Querverbundgesellschaften andere Anforderungen, die teilweise auch durch die Bundesnetzagentur etwa in einem eigenen Sicherheitskatalog für die Telekommunikation festgelegt wird oder wie im Sektor Wasser ebenfalls durch branchenspezifische Sicherheitsstandards beschrieben und in diesem Fall dem BSI gegenüber nachgewiesen werden müssen.

Der BDEW hat in diesem Zusammenhang und vor dem Hintergrund der Einführung des Einrichtungsbegriffs gemäß NIS2-Richtlinie in der Vergangenheit darauf hingewiesen, dass eine Ausweitung des Geltungsbereiches dieser aus den sektorspezifischen Anforderungen abgeleiteten KRITIS-Regelungen auch auf die nicht-kritischen IT-Prozesse der betroffenen Querverbundgesellschaften im weiteren Scope der besonders wichtigen Einrichtung zu konkurrierenden und gleichzeitig geltenden spezialrechtlicher Regelungen führen würde. Hier scheinen § 28 Abs. 4 S. 2 und 3 BSIG Abhilfe schaffen zu wollen.

Die Regelungen und die dazugehörige Gesetzesbegründungen zu § 28 Abs. 4 BSIG und § 5c EnWG sind zunächst nicht einfach zu lesen. Bildet man als Beispiel ein Querverbundgesellschaften, das in einer Gesellschaft folgende Anlagen betreibt:

- eine kritische Energieerzeugungsanlage (Schwellenwert der BSI-KritisV überschritten),
- eine kritische Trinkwassergewinnungsanlage (Schwellenwert der BSI-KritisV überschritten) und
- eine Anlage zur thermischen Behandlung von Siedlungsabfällen (Schwellenwert der BSI-KritisV wird nicht überschritten, d.h. es liegt insoweit nur eine wichtige Einrichtung vor)

so soll wohl Folgendes gelten:

- Die IT-Systeme, die für den sicheren Anlagenbetrieb der kritischen Energieerzeugungsanlage notwendig sind, werden über § 5c EnWG (bzw. der IT-Sicherheitskataloge) reguliert (§ 28 Abs. 4 S. 1 Nr. 2 BSIG)
- Die IT-Systeme, die für den sicheren Anlagenbetrieb der kritischen Trinkwassergewinnungsanlage notwendig sind, werden über das BSIG reguliert (§ 28 Abs. 4 S. 2 Var. 1, 3 BSIG)
- Die IT-Systeme, die für den sicheren Anlagenbetrieb der unkritischen Anlage zur thermischen Behandlung von Siedlungsabfällen notwendig sind, werden über das BSIG reguliert (§ 28 Abs. 4 S. 2 Var. 2, S. 3 BSIG)
- IT-Systeme, die für mehrere Sektoren erheblich sind, sollen sowohl der Regulierung durch die BNetzA als auch der Regulierung durch das BSI unterfallen
- Alle IT-Systeme in dieser Gesellschaft, die nicht für den sicheren Anlagenbetrieb unmittelbar notwendig sind (Office-IT ohne Schnittstellen zu den Anlagen) werden einheitlich über § 5c EnWG (bzw. der IT-Sicherheitskataloge) reguliert (Umkehrschluss aus § 28 Abs. 4 S. 3 BSIG bzw. die korrespondierende Gesetzesbegründung (S. 163, 216))

Aus dem oben gezeigten Beispiel sollte die Komplexität der Regelung ersichtlich werden. **Diese wird in der Praxis zur großen Überforderung der betroffenen Unternehmen und Prüfstellen führen.**

Auch ist sachlich nicht nachvollziehbar, warum die Bundesnetzagentur in Zukunft für die gesamte nicht-kritische IT in den Querverbundgesellschaften zuständig sein sollte. Diese IT-Systeme und IT-Prozesse wirken erstens nicht auf den sicheren Netz- oder Anlagenbetrieb ein,

noch haben diese zweitens im Einzelfall überhaupt mit den für die Bundesnetzagentur relevanten Sektoren Energie oder Telekommunikation zu tun. Hier ist eine Vereinfachung unbedingt erforderlich. Gegebenenfalls sollte die sogenannte Office-IT – wie auch vom BDEW in der Vergangenheit gefordert – in die Zuständigkeit des BSI fallen.

Darüber hinaus weisen wir darauf hin, dass die Rückausnahme von der Ausnahme ausschließlich einer Regelung für das BSIG trifft. Die Regelung sagt letztlich aus, dass die BSI-Vorgaben für wichtige oder besonders wichtige Einrichtungen doch Anwendung finden für die Aktivitäten auf anderen Sektoren nach Anlage 1 oder 2. § 5c EnWG trifft eine solche Ausnahme nicht und würde dann dazu führen, dass eben für Unternehmen, die unter § 5c EnWG fallen doch beide Gesetze gelten. Jede Ausnahme in § 28 BSIG muss daher auch in § 5c EnWG nachvollzogen werden.

2 Dreistufigkeit muss in den IT-Sicherheitskatalogen der Bundesnetzagentur analog zum BSIG umgesetzt

Die Dreistufigkeit sowie die Abstufung der Maßnahmen- und Nachweisregime muss in den IT-Sicherheitskatalogen der Bundesnetzagentur analog zum BSIG umgesetzt werden. Dabei ist darauf zu achten, dass lediglich für Energienetze und kritische Energieerzeugungsanlagen ein ISMS durch die Betreiber aufzubauen und zu zertifizieren ist. Der Aufbau eines ISMS und die Zertifizierung eines solchen bei kleinen und mittleren Energieerzeugungsanlagen ist weder verhältnismäßig, noch wird der Sicherheit in einem sich aufgrund der Energiewende verändernden Netzbetriebs gerecht. Vielmehr würde eine solche Anforderung den Ausbau von Erneuerbaren-Energie-Anlagen durch zusätzlichen Bürokratismus erschweren. Dagegen ermöglicht gerade die im Rollout befindliche Smart-Meter-Gateway-Infrastruktur jene für die Netzführung und Netzsicherheit notwendige Sichtbarkeit der kleinen und mittleren EE-Anlagen. Es sollte also geprüft werden, ob die Absicherung kleiner und mittlerer Anlagen im Rahmen des MsbG erfolgen kann, da gerade dezentrale und orchestrierte Angriffe nicht auf der Ebene der einzelnen Erzeugungsanlagen erkannt und mitigiert werden können. Dagegen könnte dem Messstellenbetreiber und dem Gateway-Administrator bei der Erkennung und Abwehr solcher Angriffe eine Schlüsselrolle zukommen.

Solange der Sektor Energie nicht vollständig im Zuständigkeitsbereich einer Behörde liegt, bleibt es auch zwingend erforderlich, dass alle Regelungen im Einvernehmen mit allen beteiligten Ressorts und Behörden erarbeitet werden.

3 Anlage 1 - Sektoren besonders wichtiger und wichtiger Einrichtungen

Anlage 1 verweist in Ziffer 1.1.9 noch immer auf die Ladesäulenverordnung (LSV). Die LSV wird in großen Teilen durch die Europäische Verordnung AFIR ersetzt. Der Begriff „Ladepunktbetreiber“ wird in der LSV zukünftig nicht definiert sein. Der Verweis in Anlage 1 auf § 2 Nr. 8 der LSV

würde daher ins Leere führen. In der LSV wird zukünftig auf die AFIR verwiesen für den Begriff „Betreiber“ in § 2 Nr. 2 und in § 2 Nr. 1 für den Begriff „Ladepunkt“. Der entsprechende Referentenentwurf für die LSV ist bereits in die Verbände- und Länderanhörung gegeben worden und soll demnächst beschlossen werden.

Ansprechpartner

Mathias Böswetter

Fachgebietsleiter KRITIS-, Cyber- und Sicherheitspolitik

+49 30 300199 1526

mathias.boeswetter@bdew.de