

# STELLUNGNAHME

vom 28. Mai 2024 zum

## Referentenentwurf zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

DVGW Deutscher Verein des  
Gas- und Wasserfaches e.V.

**Ansprechpartner**

**Frank Dietzsch (Gas)**

**Kirsten Wagner (Wasser)**

Josef-Wirmer-Straße 1-3

D-53123 Bonn

Tel.: +49 228 9188-914, +49 228 9188-868

E-Mail: [frank.dietzsch@dvgw.de](mailto:frank.dietzsch@dvgw.de); [kirsten.wagner@dvgw.de](mailto:kirsten.wagner@dvgw.de)

## Zusammenfassung

Der DVGW Deutscher Verein des Gas- und Wasserfaches e. V. begrüßt die Möglichkeit der Stellungnahme zum Referentenentwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) vom 07. Mai 2024.

Durch eine zunehmende Anzahl von immer komplexer werdenden Cyberangriffen, auch vor dem Hintergrund von geopolitischen Verschiebungen, ist **die weitere Ausgestaltung des rechtlichen Rahmens der IT-Sicherheit für den Schutz der Kritischen Infrastrukturen (KRITIS)** aus Sicht des DVGW unbedingt notwendig. Dabei ist eine **enge Verzahnung von NIS-2-Umsetzungsgesetz (NIS2UmsuCG) und KRITIS-Dachgesetzes (KRITIS-DachG)** im Sinne des All-Gefahren-Ansatzes der Schlüssel, um eine effiziente, umsetzbare und wirtschaftlich abbildbare Gesetzgebung zum Schutz Kritischer Infrastrukturen zu gewährleisten, die die Risiken aus dem Cyberraum, dem Informationsraum und dem physischen Raum ganzheitlich berücksichtigt.

Der DVGW hat sich aktiv an der Erarbeitung der Stellungnahme des UP KRITIS beteiligt und spricht sich klar für diese aus. Für die Sektoren der Gas- und Wasserversorgung hat der DVGW die folgenden Kernforderungen formuliert:

1. Die Anforderungen in der NIS2UmsuG an die deutschen Unternehmen sollten nicht strenger sein als in der NIS-2-Richtlinie vorgegeben. Es fällt auf, dass die NIS-2-Richtlinie vom „Beherrschen von Risiken für die Erbringung der Dienste“ (§ 21 (1) NIS2) spricht, während im vorliegenden Referentenentwurf der NIS2UmsuCG die strengere Formulierung vom „Vermeiden von Störungen in informationstechnischen Systemen, Komponenten und Prozesse, die für die Erbringung ihrer Dienste genutzt werden“ (§ 30 (1) BSIG) aufgenommen wurde. Aus Sicht des DVGW ist es nicht vertretbar, den deutschen Gas- und Wasserversorgungsunternehmen strengere Vorschriften aufzuerlegen.
2. Aus dem Referentenentwurf geht hervor, dass die Zuständigkeit für den Bereich der kritischen Anlagen und Netze im Energiesektor der Bundesnetzagentur (BNetzA) zu übertragen ist, während das Bundesamt für Sicherheit in der Informationstechnik (BSI) für den Bereich der besonders wichtigen Einrichtungen im Energiesektor zuständig sein soll. Aus Sicht des DVGW wird im Gesetzesentwurf nicht deutlich genug auf diese Trennung hingewiesen, da in § 28 (4) Nr. 2 BSIG die §§ 30, 33, 65, 66 BSIG für die betroffene Energieinfrastruktur nicht ausgenommen sind. Dies führt faktisch zu einer doppelten Verantwortung und Berichtspflicht der Betreiber in Richtung BNetzA und BSI.
3. Es wird begrüßt, dass die Branchenverbände weiterhin die Möglichkeit erhalten, **branchenspezifische Sicherheitsstandards** für die Erfüllung der Anforderungen der Betreiber Kritischer Infrastrukturen und der besonders wichtigen Einrichtungen in § 30 (2) BSIG und § 31 (2) BSIG zu erstellen. Entgegen den Zusagen des Bundesministerium des Inneren und für Heimat (BMI) beim Werkstattgespräch am 26. Oktober 2023 wurde im vorliegenden Referentenentwurf aber nicht ergänzt, in welcher Weise die Branchenstandards für die wichtigen Einrichtungen vom Gesetzgeber als geeignet angesehen werden, um die gesetzlichen Anforderungen zu erfüllen. Hier besteht dringender Nachbesserungsbedarf, um den wichtigen Einrichtungen klare Vorgaben und vor allem Rechtssicherheit in Bezug auf das vom Gesetzgeber geforderte Schutzniveau zu geben. Es wird daher vom DVGW vorgeschlagen, § 30 (8) BSIG dahingehend anzupassen, dass Branchenstandards auch zur Erfüllung der Anforderungen gemäß § 30 (2) BSIG für die wichtigen Einrichtungen verwendet werden können. Zumindest sollte aber in der Gesetzesbegründung der folgende Text aufgenommen werden: „Wichtige Einrichtungen

können sich angemessen und risikobasiert an den zukünftigen Branchensicherheitsstandards der besonders wichtige Einrichtungen für die Vorgaben aus § 30 (2) Nr. 1 bis 10 BSIG orientieren.“

4. Bei der Verwendung zertifizierter Komponenten und Prozesse gemäß § 30 (6) BSIG sowie dem Erlass nationaler technischer Spezifizierungen nach § 30 (5) BSIG ist darauf zu achten, dass keine dieser Maßnahmen eine Entstehung von Oligopolen oder Wettbewerbsnachteile auf europäischer Ebene bewirken.
5. In § 58 (4) BSIG fehlt in der Auflistung der beim Erlass oder der Änderung der Verordnung zur Identifizierung von Kritischen Anlagen zu beteiligenden Parteien, die Anhörung der „Vertretern der Wissenschaft, der betroffenen Betreiber und der Wirtschaftsverbände“. Der DVGW hält es für notwendig, dass die Anhörung der „Vertretern der Wissenschaft, der betroffenen Betreiber und der Wirtschaftsverbände“ an dieser Stelle ergänzt wird und zu jedem Zeitpunkt gewährleistet ist.

## Positionen des DVGW im Einzelnen

Aus Sicht des DVGW sollte bei der Finalisierung des zukünftigen NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) die im Folgenden genannten Änderungsvorschläge umgesetzt werden, um die Belange der Gas- und Wasserversorgung zu berücksichtigen und unter Rückgriff auf den bestehenden und bewährten technischen und rechtlichen Ordnungsrahmen beim Schutz von Kritischen Infrastrukturen sowie im Sinne des All-Gefahren-Ansatzes die Sicherheit und die Resilienz der Unternehmen der Gas- und Wasserversorgung tatsächlich zu erhöhen.

Im Folgenden sind die Positionen zu den Regelungsinhalten der einzelnen Rechtsparagrafen erläutert:

### § 28 Besonders wichtige und wichtige Einrichtungen

In der Gesetzesbegründung ist zukünftig eine klare Trennung der Zuständigkeiten der BNetzA und des BSI vorgesehen. Im engeren Sinne wird die Zuständigkeit für den Umfang kritischer Anlagen/Netze im Energiesektor der BNetzA zugeschrieben, wobei das BSI die *besonders wichtigen Einrichtungen* im Energiesektor verwalten soll. Im Gesetzesentwurf ist eine strikte Trennung nicht vorgesehen, sodass zwangsläufig eine doppelte Zuständigkeit für die Betreiber in Richtung BNetzA und BSI vorliegt. Um dem entgegenzuwirken, müssen in § 28 Absatz 4 Nr. 2 die §§ 30, 33, 65 und 66 BSIG ausgenommen werden. Der DVGW begrüßt die Trennung der Zuständigkeiten für die jeweiligen Behörden, sofern § 28 BSIG um die o.g. Bedingung erweitert wird.

### § 30 Risikomanagement besonders wichtiger Einrichtungen und wichtiger Einrichtungen

#### **Anforderungen in § 30 (1) BSIG an die Vorgaben im NIS-2-Richtlinie anpassen**

In Bezug auf das Anforderungsprofil an die Unternehmen sollte sich der Gesetzgeber an die Vorgaben in der NIS-2-Richtlinie orientieren und keine strengeren Vorgaben aufnehmen. Es ist auffällig, dass in der NIS-2-Richtlinie von der „Beherrschung von Risiken für die Erbringung der Dienste“ gesprochen wird, während sich das NIS2UmsuCG auf „die Vermeidung von Störungen in informationstechnischen Systemen, Komponenten und Prozesse, die für die Erbringung ihrer Dienste“ bezieht. Das ist ein großer Unterschied. In der deutschen Formulierung fehlt eine Abwägung, die miteinbezieht, ob die Störung überhaupt Relevanz für die Diensterbringung hat und es somit ein zu beherrschendes Risiko darstellt. Es ist nicht nachvollziehbar, warum deutsche Gas- und Wasserversorger an dieser Stelle stärker reguliert werden sollen als in den anderen europäischen Ländern. Der DVGW bittet um Prüfung und Anpassung.

#### **Zulassen der Umsetzung der Anforderungen in § 30 (2) BSIG für wichtige Einrichtungen durch branchenspezifische Sicherheitsstandards**

Aus Sicht des DVGW werden die Vorgaben für die *wichtigen Einrichtungen* im vorliegenden Referentenentwurf nicht ausreichend definiert. Die *wichtigen Einrichtungen* müssen gemäß § 30 (1) BSIG ebenso wie die *besonders wichtigen Einrichtungen* ein Schutzniveau implementieren, das dem Stand der Technik entspricht. Wenn der Stand der Technik durch die Implementierung eines vom BSI geprüften und eignungsfestgestellten Branchenstandards für die *besonders wichtigen Einrichtungen* erreicht werden kann (§ 30 (8) BSIG), stellt sich die Frage, warum dieser Weg nicht auch für die *wichtigen Einrichtungen* gesetzlich untermauert wird. Weder im Gesetzestext noch in der Begründung sind Vorgaben, Hinweise oder Erklärungen enthalten, die darlegen, wie und ob hier

unterschiedliche Schutzniveaus oder -tiefen für die beiden Einrichtungskategorien angedacht sind. Die Angaben zu einer Risikobetrachtung (§ 30 (1) BSIG) sind nicht ausreichend, weil diese Abwägung immer, d.h. auch bei Implementierung eines Branchenstandards oder der DIN ISO 27000 gemacht wird. Hier besteht eine Lücke, die absehbar zu Problemen und Fragen für die Kategorie der *wichtigen Einrichtungen* führt. In dem Sektor Wasser sind viele Unternehmen betroffen und werden künftig in die Kategorie der *wichtigen Einrichtungen* fallen. Deshalb ist es dem DVGW als technischen Regelsetzer der Branche ein besonderes Anliegen, dass die *wichtigen Einrichtungen* von Beginn an (nicht erst durch Orientierungshilfen und Leitfäden vom BSI) präzise Angaben zum Rahmen der gesetzlichen Verpflichtungen erhalten, die Rechtssicherheit in Bezug auf die zu erfüllenden Anforderungen geben.

Der DVGW hält eine Präzisierung des Gesetzestextes für unumgänglich. Sinnvoll wäre eine Öffnungsklausel, die es ermöglicht, Branchenstandards auch für die Erfüllung der Anforderungen von *wichtigen Einrichtungen* zu nutzen. Zumindest sollte in der Gesetzesbegründung aber eine Erklärung erfolgen die darlegt, dass wichtige Einrichtungen sich an den zukünftigen Branchensicherheitsstandards der besonders wichtige Einrichtungen für die Vorgaben aus § 30 (2) Nr. 1 bis 10 BSIG orientieren können.

## § 41 Untersagung des Einsatzes kritischer Komponenten

Im Sinne der Digitalisierung der Energiewende stellt der o.g. Paragraph eine Ausbremsung gegenwärtiger und zukünftiger Innovationen dar. Insbesondere für Smart Meter Gateways, die nach § 2 Absatz 1 Nr. 22 BSIG eine kritische Komponente repräsentieren und von Betreibern kritischer Anlagen wie beispielsweise Netzbetreiber genutzt werden, führt das in § 41 BSIG aufgeführte Prüfverfahren zu einer bürokratischen Hürde. Letztere wird in § 41 (3) BSIG ersichtlich, nach der ein Hersteller dazu verpflichtet ist, eine Garantieerklärung über seine Vertrauenswürdigkeit abzulegen. Aus diesem Grund spricht sich der DVGW für eine Anpassung des § 41 BSIG aus, welche den Einsatz und das Prüfverfahren für kritische IT-Komponenten insofern erleichtern, dass zukünftige Digitalisierungsvorhaben nicht durch bürokratische Prozesse beeinträchtigt werden.

## § 58 Ermächtigung zum Erlass von Rechtsverordnungen

Im Gegensatz zum Referentenentwurf der NIS2UmsuCG vom 22. Dezember 2023 wurde im § 58 (4) BSIG des vorliegenden Referentenentwurfs die Passage: „Die Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der Wirtschaftsverbände beim Erlass oder Änderung der Verordnung zur Identifizierung von Kritischen Anlagen“ gestrichen. Aus Sicht des DVGW wird nicht deutlich, warum der Gesetzgeber auf eine Anhörung der aufgeführten Parteien verzichten will. Wir halten die Beteiligung der Verbände und Wirtschaftsvertreter sowie im Erläuterungsteil des Referentenentwurfs auf S. 171 auch dargestellt, für absolut wichtig und notwendig.