Deutscher Verein des
Gas- und Wasserfaches e.V.

www.dvgw.de

STELLUNGNAHME

vom 20. Oktober 2023 zum

Diskussionspapier der wirtschaftsbezogenen Regelung zur Umsetzung der NIS-2-Richtlinie

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; kirsten.wagner@dvgw.de

Zusammenfassung

Der DVGW e. V. begrüßt die Möglichkeit der Stellungnahme zum Diskussionspapier der wirtschaftsbezogenen Regelung zur Umsetzung der NIS-2-Richtlinie vom 27. September 2023.

Vor dem Hintergrund der zunehmenden und immer komplexer werdenden Cyberangriffen ist es dringend notwendig, den **rechtlichen Rahmen der IT-Sicherheit für den Schutz der Kritischen Infrastrukturen weiter auszugestalten**. Dabei ist es wichtig, dass die neu gefassten Regelungen und Definitionen in Übereinstimmung, mit denen im KRITIS-Dachgesetz formuliert werden, da nur durch einen umfassenden „All-Gefahren-Ansatz“, der die Risiken aus dem Cyberraum, dem Informationsraum und dem physischen Raum ganzheitlich berücksichtigt, die Resilienz der Kritischen Infrastrukturen in Deutschland erhöht werden kann.

Der DVGW fasst seine Kernforderungen wie folgt zusammen:

1. Der DVGW sieht eine **enge Verzahnung von NIS-2-Umsetzungsgesetz (NIS2UmsuCG) und KRITIS-DachG** als wichtige Voraussetzung, um eine effiziente, umsetzbare und wirtschaftlich abbildbare Gesetzgebung zum Schutz Kritischer Infrastrukturen zu gewährleisten. Die Regelungen der Rechtsverordnung sollten sektorenspezifisch zugeschnitten werden und auf bereits bestehende gesetzliche Regelungen der jeweiligen Sektoren aufbauen.
2. Die **Begriffsdefinitionen in allen Gesetzen und Verordnungen** (NIS2UmsuCG, KRITIS-Dachgesetz, ITSiG, EnWG, BSI-Gesetz, BSI-KritisV,…) für Kritische Infrastrukturen sollten **gleichlautend formuliert werden** und mit den dahinterliegenden EU-Richtlinien (NIS-2-Richtlinie, CER-Richtlinie) übereinstimmen.
3. Die in der **NIS-2-Richtlinie und in der EU-Empfehlung zur KMU-Definitionen** (2003/361/EG) enthaltenen Angaben sollten mit den **nationalen Definitionen für besonders wichtigen und wichtigen Einrichtungen übereinstimmen**, d.h. die bestehende „oder“ Verknüpfung im Diskussionsentwurfes muss durch eine „und“ Verknüpfung ersetzt werden.
4. Es wird begrüßt, dass die Branchenverbände weiterhin die Möglichkeit erhalten, **branchenspezifischen IT-Sicherheitsstandards** für die Erfüllung der Anforderungen in § 30 Absatz 2 zu erarbeiten. Die im Diskussionspapier aufgeführten Regelungen weisen unserer Ansicht nach eine wesentliche Lücke auf. Auch für **die wichtigen Einrichtungen sollte im NIS2UmsuCG präzise dargelegt werden, was der Gesetzgeber unter dem Stand der Technik zur Erfüllung der Anforderungen gemäß § 28 Absatz 2 versteht**. Sinnvoll wäre hier z. B. eine Öffnungsklausel, die es ermöglicht, Branchenstandards so zu gestalten, dass sie in einer Branche auch für die Erfüllung der Anforderungen von wichtigen Einrichtungen genutzt werden können. Es sollte außerdem geprüft werden, ob zur Klarstellung eine gesetzliche Vermutungsregelung aufgenommen wird.
5. Folgen der Zertifizierungspflichten von Komponenten und Prozessen sind gegenwärtig zur Abschätzung der Aufwendungen durch die Wirtschaft zu unbestimmt. **Zertifizierungen sind grundsätzlich problematisch für Beschaffung und Verfügbarkeit.**
6. Der vom BSI in Abstimmung mit BBK einzurichtende Meldeweg sollte über eine **zentrale Meldestelle** abgewickelt werden. Der notwendige Informationsaustausch aller Meldungen sollte gemäß NIS2UmsuCG und KRITIS-DachG über ein einheitliches Online-Meldeportal abgewickelt werden können.

Positionen des DVGW im Einzelnen

Das zukünftige NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) sollte aus Sicht des DVGW die im Folgenden genannten zusätzlichen Anforderungen aufnehmen, damit die Belange der Gas- und Wasserversorgung angemessen Berücksichtigung finden und unter Rückgriff auf bestehende und bewährte technische und rechtliche Ordnungsrahmen beim Schutz von Kritischen Infrastrukturen sowie im Sinne des All-Gefahren-Ansatzes die Sicherheit und die Resilienz tatsächlich erhöht werden können.

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

§ 2 Begriffsbestimmungen

Einheitliche Begriffsbestimmungen in allen nationalen und europäischen Gesetzestexten

Die Begriffsbestimmungen in allen Gesetzen und Verordnungen (NIS2UmsuCG, KRITIS-Dachgesetz, ITSiG, EnWG, BSI-Gesetz, BSI-KritisV,…), in denen die gesetzlichen Rahmenbedingungen für kritischen Infrastrukturen festgelegt werden, sollten gleichlautend formuliert werden und mit den dahinterliegenden EU-Richtlinien (NIS-2-Richtlinie, CER-Richtlinie) übereinstimmen.

Im § 2 des vorliegenden Diskussionsentwurfs fehlen aus DVGW-Sicht eine Reihe von wichtigen Begriffsdefinitionen, z.B. **kritische Infrastrukturen** und **kritische Dienstleistung**, während die Definition für **Betreiber kritischer Anlagen** im § 28 Absatz 5 gegeben wird, aber nicht im § 2 aufgeführt ist. Alle Begriffsdefinitionen sollten konsequent im § 2 aufgeführt werden.

§ 28 Besonders wichtige und wichtige Einrichtungen

Übernahme der KMU-Definitionen EU-Empfehlung (2003/361/EG)

Die Definitionen für die *besonders wichtigen* und *wichtigen Einrichtungen* im vorliegenden Diskussionspapier weichen von den Definitionen für *„important“* und *„essitial entities“* in der NIS-2-Richtlinie sowie in der EU-Empfehlung zu KMU-Definitionen (2003/361/EG) ab. Im Gegensatz zu den Definitionen in den europäischen Gesetzestexten für die beiden Einrichtungskategorien soll lt. § 28 Absatz 1 des Diskussionspapiers die Zuordnung mittels der Mitarbeiterzahl oder dem Jahresumsatz erfolgen. In den europäischen Gesetzestexten müssen dagegen beide Kriterien erfüllt sein (Mitarbeiterzahl und Jahresumsatz), um einer der beiden Kategorien zugeordnet zu werden. Hier sollten die europäischen Vorgaben übernommen werden, weil es sich sonst de facto um eine Verschärfung der Schwellenwerte handelt.

Keine Erweiterung des Scopes auf die gesamte Einrichtung bzw. das gesamte Unternehmen

Der bisherige Ansatz der Gesetzgebung den Scope, auf den sich die gesetzlichen Anforderungen beziehen, auf die kritischen Anlagen einer Einrichtung und damit eines Unternehmens zu beschränken, hat sich aus Sicht des DVGW bewährt und sollte in jedem Fall weiterhin bestehen bleiben.

Nach jetziger Lesart von § 28 in Verbindung mit § 30 des Diskussionspapiers sollen die gesetzlichen Anforderungen sowohl für die *besonders wichtigen Einrichtungen* wie auch für die *wichtigen Einrichtungen* auf die gesamte Einrichtung ausgeweitet werden. Die Erweiterung des Scops auf die gesamte Einrichtung, d.h. auch auf Teile der Unternehmens-IT-Infrastruktur, die nicht zur Erbringung der kritischen Dienstleistung notwendig sind, würde zu einem erheblichen administrativen,

personellen und wirtschaftlichen Mehraufwand für die Unternehmen führen, ohne dass für die Versorgungssicherheit der Bevölkerung ein wirklicher Mehrwert vorhanden ist.

Es muss bei der Festlegung des gesetzlichen Rahmens berücksichtigt werden, dass die bisherigen hohen Anforderungen in Bezug auf das Schutzniveau für die kritischen Anlagen eines Unternehmens zur Absicherung der kritischen Funktionen im Netz- und Anlagenbetrieb festgelegt wurden. Die Kritikalität dieser Anlagen ist nicht mit den unkritischen Businessprozessen im gesamten Unternehmen vergleichbar (z. B. für die IT-Systemen der Betriebskantine), die keinen unmittelbaren oder mittelbaren Einfluss auf den sicheren Netz- und Anlagenbetrieb haben. Aus DVGW-Sicht ist es daher unbedingt notwendig, eine Erweiterung des Scops zu vermeiden und den Scope für die Erbringung der gesetzlichen Anforderungen wie bisher ausschließlich auf die kritischen Anlagen zu beziehen, die zur Erbringung der kritischen Dienstleistung notwendig sind.

§ 30 Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtige Einrichtungen

Das zu implementierende Schutzniveau für besonders wichtige und wichtige Einrichtung muss im Gesetzestext präzise definiert werden

Aus Sicht des DVGW besteht eine Lücke in den Vorgaben für die *besonders wichtigen Einrichtungen* im Vergleich zu den *wichtigen Einrichtungen*. Gemäß § 30 Absatz 1 müssen beide Einrichtungskategorien ein Schutzniveau ihrer IT-Infrastruktur implementieren, dass dem Stand der Technik entspricht. Für die *besonders wichtigen Einrichtungen* kann die Implementierung eines Schutzniveaus durch vom BSI geprüfte und eignungsfestgestellte Branchenstandards erreicht werden (§ 30 Absatz 9). Für die *wichtigen Einrichtungen* ist dieser Weg lt. vorliegenden Diskussionspapier nicht vorgesehen, obwohl das BSI durch die Eignungsfeststellung bestätigt, dass die Branchenstandards dem Stand der Technik für die gesetzlichen Anforderung in § 30 Absatz 1 und 2 entsprechen. Deshalb stellt sich die Frage, ob das BMI, in Bezug auf den Stand der Technik, für die *besonders wichtigen* und die *wichtigen Einrichtungen* zwei verschiedene Schutzniveaus auferlegen will oder nicht. Im vorliegenden Diskussionspapier sind allerdings keine weiteren Angaben zu einem abweichenden Anforderungsprofil für *wichtige Einrichtungen* zu finden.

Um den Unternehmen Klarheit und Rechtssicherheit in Bezug auf die zu erfüllenden Anforderungen zu geben, bitten der DVGW hier um eine Präzisierung. Sinnvoll wäre z. B. eine Öffnungsklausel, die ermöglicht, dass ein Branchenstandard so gestaltet werden kann, dass er auch für die Erfüllung der Anforderungen von *wichtigen Einrichtungen* genutzt werden kann. Es sollte geprüft werden, ob zur Klarstellung eine gesetzliche Vermutungsregelung aufgenommen werden kann, z. B.: „Für *besonders wichtige Einrichtungen* und *wichtige Einrichtungen*, welche einen branchenspezifischen IT-Sicherheitsstandards nach § 30 Absatz 9 einhalten, deren Eignung das BSI festgestellt hat, gilt die Vermutung, dass sie den Stand der Technik nach § 30 Absatz 1 und Absatz 2 einhalten.“ Der Verweis auf allgemein anerkannte Regeln der Technik und die entsprechende Ausgestaltung und Schaffung von Standards durch die Technische Regelsetzung haben sich in der Abwasserentsorgung und Trinkwasserversorgung sowie in der Gas- und Stromversorgung bewährt.

Ergänzung des § 30, Absatz 2 um „nationale Normen“

Der BSI-Grundschutz ist aus DVGW-Sicht ebenfalls als Grundlage für die Implementierung des geforderten Schutzniveaus in § 30 Absatz 1 und 2 geeignet. Daher sollte der Absatz 2 erweitert werden, so dass zur Einhaltung des Standes der Technik nationale, europäische und internationale Normen herangezogen werden können.

Erweiterung der Gültigkeit einer Eignungsfeststellung auf 3 Jahre
Des Weiteren sollte der Zyklus der Eignungsfeststellung, dem der Nachweisepflicht (§ 38) angeglichen werden und auf 3 Jahre ausgedehnt werden.

§ 32 Meldepflichten

Keine Doppelmeldungen etablieren, stattdessen zentrale Meldewege vorsehen.
Der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in Abstimmung mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) einzurichtende Meldeweg sollte über eine zentrale Meldestelle abgewickelt werden. Entsprechend der Kommentierung unter § 6 sollte der notwendige Informationsaustausch aller Meldungen gemäß NIS2UmsuCG und KRITIS-DachG über ein einheitliches Online-Meldeportal abgewickelt werden können.

§ 33 Registrierungspflicht

Die verpflichtende Übermittlung von IP-Adressen erbringt der Wirtschaft grundsätzlich keinen nennenswerten Sicherheitszugewinn.
Die Machbarkeit der Forderung aus Absatz 2 ist zu hinterfragen, da gerade kleinere Betreiber, die keine festen IP-Adressen haben, bzw. Anlagen betreiben, da sie z. B. per Mobilfunk angebunden sind. Hier können keine sinnvollen IP-Adressbereiche gemeldet werden.
Entsprechend fraglich ist auch die diesbezügliche unverzügliche Meldungspflicht von Änderungen von dynamischen IP-Adressen aus Absatz 5.

§ 34 Besondere Registrierungspflicht für bestimmte Einrichtungen

Fehlender Bezug zu § 63 muss unbedingt zur vollständigen Bewertung zur Verfügung gestellt werden.
Hier wird Bezug genommen auf „bestimmte Einrichtungen“, die in § 63 Absatz 1 Satz 1 erläutert sein sollen. Auch der weitere Text nimmt auf § 63 Bezug, der nicht Bestandteil des Diskussionspapieres ist, und daher nicht bewertet werden kann.

§ 39 Nachweispflichten für Betreiber kritischer Anlagen

Anhebung der Nachweispflicht von 2 auf 3 Jahre.
Der DVGW begrüßt es, dass die Nachweisführung für die Betreiber kritischer Anlagen von 2 auf 3 Jahre angehoben wird. Die Anhebung vereinfacht es, die für die Nachweisführung notwendigen Audits in den Zyklus durchzuführender Sicherheitsaudits, Prüfungen und Zertifizierungen bestehender ISO-Managementsysteme der Unternehmen zu integrieren.

§ 40 Zentrale Melde- und Anlaufstelle

Der DVGW begrüßt die Einrichtung einer alleinigen und zentralen Melde- und Anlaufstelle im BSI.
Um die Verpflichtungen einheitlich und unkompliziert zu gestalten, ist es notwendig, diese für IT-Sicherheit und KRITIS einheitlich zu gestalten.

§ 57 Ermächtigung zum Erlass von Rechtsverordnungen

Die Unterscheidung zwischen Sicherheitszertifikat, IT-Sicherheitskennzeichen und Cybersicherheitszertifikat sollte eindeutig herausgearbeitet werden. Es muss sichergestellt sein, dass jede der drei der Verhältnismäßigkeit von Nutzen und Aufwand gerecht werden.
Absatz 1 räumt dem BMI das Recht ein, durch Rechtsverordnung „das Nähere über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen nach § 54 zu bestimmen". § 54 ist nicht Bestandteil des Diskussionspapiers. Damit ist trotz der Wichtigkeit des Aspektes keine Kommentierung möglich.
Absatz 2 bezieht sich auf ein IT-Sicherheitskennzeichen nach § 52. § 52 regelt die „Verpflichtung zur Zugangsgewährung" und scheint damit der falsche Bezug zu sein. Kein Abschnitt in dem Diskussionspapier scheint die Ausgestaltung des Kennzeichens zu regeln. Damit ist trotz der Wichtigkeit des Aspektes keine Kommentierung möglich.

Ungeachtet dessen, hält der DVGW es für sinnvoll ein europäisches IT-Sicherheitskennzeichen auf Basis europäischer Normen anzustreben, vergleichbar eines CE-Kennzeichens.
Absatz 3 räumt dem BMI das Recht ein, durch Rechtsverordnung zu bestimmen, welche durch eine besonders wichtige Einrichtung oder wichtige Einrichtung eingesetzten Produkte, Dienste oder Prozesse gemäß § 30 Absatz 9 über eine Cybersicherheitszertifizierung verfügen müssen; die Zertifizierungskriterien werden nicht benannt. Um eine einheitliche Zertifizierung sicherzustellen, sollten die Zertifizierungskriterien in Normen festgeschrieben werden. Insbesondere die Kriterien für Produkte sollten international oder europäisch festgelegt werden, da die meisten Produkte nicht in Deutschland hergestellt werden. Nationale Regelungen wären hier nicht zielführend. Durch den Bezug auf den Ausschluss aus § 30 gilt die Verpflichtung zur Cybersicherheitszertifizierung von Risikomanagementprozessen für Betreiber von Energieversorgungsnetzen und Energieanlagen nicht.
Absatz 4 räumt dem BMI das Recht ein, durch Rechtsverordnung zu bestimmen, welche Anlagen als kritische Anlagen im Sinne des Gesetzes gelten, um branchenspezifische Schwellenwerte festzulegen. Wie bereits zu § 28 Absatz 7 angegeben, wird die Kritikalität für Energieversorgungsnetze und Energieanlagen nach Verständnis des DVGW in der BSI-KritisV durch Schwellenwerte bereits ausreichend und etabliert definiert.
Zudem sei angemerkt, dass im geplanten KRITIS-DachG (Entwurf Juli 2023) angekündigt wird, dass künftig kritische Anlagen nur noch durch das KRITIS-DachG und die dazugehörige Rechtsverordnung festgelegt werden.

Anlage 1 – Sektoren mit hoher Kritikalität; hier Betreiber im Bereich Wasserstofferzeugung, -speicherung und -fernleitung (Ziffer 1.4.8)

Die Beschreibung der Einrichtungsart für Wasserstoff ist nicht vollständig.
Fernleitungen versorgen nicht zwingend und ausschließlich Endkunden. Zudem sollte die Begrifflichkeiten in der Strom- und Gasversorgung an das EnWG angelehnt werden. Der DVGW schlägt entsprechend der Gesamtsystematik vor, 1.4.8 umzubenennen und durch 1.4.9 und 1.4.10 zu ergänzen:

1.4.8 Betreiber von Wasserstofferzeugungsanlagen
1.4.9 Betreiber von Wasserstoffnetzen gemäß § 3 Nr. 10b EnWG
1.4.10. Betreiber von Wasserstoffspeicheranlagen gemäß § 3 Nr. 10c EnWG