Deutscher Verein des
Gas- und Wasserfaches e.V.

www.dvgw.de

STELLUNGNAHME

vom 19. März 2021 zur

Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-Richtlinie 2.0)

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

Ansprechpartner
Dipl.-Ing. Kirsten Wagner
Josef-Wirmer-Straße 1-3
D-53123 Bonn
Tel.: +49 228 9188-868
E-Mail: kirsten.wagner@dvgw.de

Verm.-Ass. Dipl.-Ing. Frank Dietzsch
Josef-Wirmer-Straße 1-3
D-53123 Bonn
Tel.: +49 228 9188-914
E-Mail: frank.dietzsch@dvgw.de

Am 16. Dezember 2020 wurde der Vorschlag der Europäischen Kommission für die NIS-Richtlinie 2.0 zur Erhöhung des Cybersicherheitsniveau in der Union veröffentlicht. Der DVGW begrüßt die Möglichkeit eine Stellungnahme zur NIS-Richtlinie 2.0 einreichen zu können. Im Folgenden werden die drei wichtigsten Punkte aufgeführt, bei denen aus Sicht der Gas- und Wasserversorgungsunternehmen Anpassungsbedarf gesehen wird.

1) Anwendungsbereich (Artikel 2)

Die Festlegung von Kriterien und Schwellenwerten für Unternehmen bzw. Anlagen, die als KRITIS-Betreiber eingestuft werden, sollte weiterhin durch die Mitgliedstaaten unter Berücksichtigung der branchenspezifischen und nationalen Eigenschaften und Strukturen der Sektoren erfolgen.

Die vorgeschlagene Ausweitung des Anwendungsbereichs sollte nur Unternehmen von systemischer Relevanz umfassen und auf Basis der Versorgungskritikalität der Unternehmen für das staatliche Gemeinwesen erfolgen.

Der in Deutschland vorgeschriebene Schwellenwert von 500.000 versorgten Einwohnern sowie die Zuordnung des Schwellenwertes zu Anlagenkategorien (und nicht dem Unternehmen) hat sich als äußerst praktikabel erwiesen. Die Festlegung von Schwellenwerten auf europäischem Niveau auf Basis der EU-Empfehlung 2003/361/EG ist nicht zielführend und würde aufgrund der unterschiedlichen Strukturen der Sektoren in den Mitgliedsstaaten eine Ungleichbehandlung mit sich bringen.

2) Stand der Technik im Bereich der Netz- und Informationssicherheit (Artikel 18)

Die Formulierung des Artikel 18 Abs. 1 und Abs. 5 sollte dahingehend präzisiert werden, dass die Festlegung des Standes der Technik ausschließlich auf Basis internationaler, europäischer oder nationaler Standards erfolgt, die die jeweiligen branchenspezifischen Gegebenheiten berücksichtigen.

Ein Stand der Technik sollte nicht durch den Erlass von Durchführungsakten der EU-Kommissionen festgelegt werden, sondern muss auf der Basis von anerkannten Normen, Standards und Spezifikationen erfolgen. Eine Doppelregulierung ist unbedingt zu vermeiden. Die Möglichkeit auf Basis der spezifischen Eigenschaften von IT-Infrastruktur und IT-Architektur der Sektoren branchenspezifische IT-Sicherheitsstandards zu definieren, muss in jedem Fall weiter gewährleistet sein.

3) Nutzung der europäischen Systeme für die Cybersicherheitszertifizierung (Artikel 21)

Die Formulierung des Artikel 21 Abs. 1 sollte nicht dazu führen, dass es durch die Betreiberverpflichtung zertifizierte IKT-Produkte, -Dienste und -Prozesse einzusetzen, zu einer Verknappung bei deren Beschaffung und ihrem Betrieb kommt. Das hätte eine Monopolbildung einzelner Produkte, Dienste und Prozesse zur Folge, die unbedingt zu vermeiden ist und neue systemische und grenzüberschreitende Risiken in sich birgt.

Vorbemerkung

Der **DVGW Deutscher Verein des Gas- und Wasserfaches e. V.** – Technisch-wissenschaftlicher Verein – fördert das Gas- und Wasserfach mit den Schwerpunkten Sicherheit, Hygiene und Umweltschutz. Mit seinen rund 13.000 Mitgliedern erarbeitet der DVGW die allgemein anerkannten Regeln der Technik für Gas und Wasser. Der DVGW ist wirtschaftlich unabhängig und politisch neutral.

Der DVGW bedankt sich für die Möglichkeit, zum Entwurf der Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-Richtlinie 2.0) vom 16. Dezember 2020 Stellung nehmen zu können. Wir begrüßen innerhalb der NIS-Richtlinie 2.0 die Weiterentwicklung der Maßnahmen, mit denen die Resilienz und die Kapazitäten zur Reaktion auf Sicherheitsvorfälle öffentlicher und privater Einrichtungen, zuständiger Behörden und der Union als Ganzer auf dem Gebiet der Cybersicherheit und des Schutzes kritischer Infrastrukturen weiter verbessert werden sollen. Vor dem Hintergrund der zunehmend komplexer werdenden Cyberangriffe wird die ständige Verbesserung der IT-Sicherheit der Kritischen Infrastrukturen vom DVGW für eine wichtige gesellschaftliche, national wie europäisch, Aufgabe angesehen.

Zu diesem Zweck befürworten wir ausdrücklich, dass Hersteller von IT-Produkten und Anbieter digitaler Dienste zukünftig verbindlich verpflichtet werden, einen Beitrag zu den Schutzzielen der Informationssicherheit von Kritischen Infrastrukturen zu leisten. Bei einer Reihe der neuen Regelungsvorschläge bedarf es aus Sicht des DVGW einer Anpassung oder Konkretisierung (vgl. Artikel 2, 18, 20 und 21).

Im Sinne eines kontinuierlichen Verbesserungsprozesses sind die Betreiber von Gas- und Wasserversorgungsinfrastrukturen grundsätzlich angehalten, ihre systemkritischen Prozesse und Systeme einem ganzheitlichen Sicherheitskonzeptes auf Grundlage von gesetzlichen und untergesetzlichen Vorgaben zu unterwerfen, wie auch dem DVGW-Regelwerk, und an die aktuelle Bedrohungslage anzupassen.

Zu den Regelungen des Gesetzesentwurfes im Einzelnen

Zu Artikel 2 „Anwendungsbereich“

Die Festlegung von Kriterien und Schwellenwerten für Unternehmen bzw. Anlagen, die als KRITIS-Betreiber eingestuft werden, sollte weiterhin durch die Mitgliedstaaten unter Berücksichtigung der branchenspezifischen und nationalen Eigenschaften und Strukturen der Sektoren erfolgen.

Gemäß Artikel 2 des vorliegenden Vorschlags der EU-Kommission sollen zukünftig alle Unternehmen der KRITIS-Sektoren mit Ausnahme der Kleinst- und Kleinunternehmen gemäß Empfehlung 2003/361/EG unter das Regime der NIS-Richtlinie 2.0 fallen. Damit würden die Kriterien und Schwellenwerte zur Bestimmung der KRITIS-Betreiber nicht, wie bisher, durch die Mitgliedsstaaten, sondern durch die EU-Kommission erfolgen und weder sektoren- oder branchenspezifische Gegebenheiten noch nationale Eigenschaften und Strukturen berücksichtigt werden. Die KMU-Definition in der Empfehlung 2003/361/EG stützt sich auf die Mitarbeiterzahl und den Gesamtumsatz der Unternehmen. Diese Kriterien sind keine geeignete Grundlage, um die Kritikalität eines Unternehmens für das staatliche Gemeinwesen zu bestimmen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe eintreten würden.

Des Weiteren berücksichtigt die EU-Empfehlung 2003/361/EG Unternehmen, die zu mehr als 25 % in öffentlicher Hand liegen, nicht. Der Verweis auf die Empfehlung 2003/361/EG (Artikel 16 Ziffer 11) hätte zur Folge, dass die Ausnahmeregelung auf zahlreiche kommunale Unternehmen in Deutschland nicht anwendbar ist und würde damit viele Wasserversorgungsunternehmen treffen. Der Anteil der öffentlich-rechtlichen Organisationsformen bei den Wasserversorgungsunternehmen liegt zurzeit bei ca. 67 % (von insgesamt 5.845 Wasserversorgungsunternehmen). Die Regulierung der Kleinst- und Kleinunternehmen würde zu einem nicht vertretbaren Aufwand für diese Unternehmen führen.

Die bisher in der BSI-KritisV verwendete Herangehensweise, anlagenbezogene Schwellenwerte zu definieren, hat sich in Deutschland bewährt. Sie berücksichtigt die individuellen Rahmenbedingungen der einzelnen Branchen und führt zu einer fundierten Einschätzung in Bezug auf die Versorgungskritikalität der Unternehmen. Aus Sicht der Gas- und Wasserversorgung wäre es nicht sinnvoll und zielführend von dieser Herangehensweise abzuweichen und EU-einheitliche Kriterien zu definieren. Eine Überregulierung sollte in jedem Fall vermieden werde. Des Weiteren bleibt anzumerken, dass die deutsche Wasserwirtschaft im Gegensatz zu der in anderen Mitgliedstaaten sehr kleinteilig ist. Die Festlegung von Schwellenwerten auf Basis der Empfehlung 2003/361/EG hätte damit eine Ungleichbehandlung zur Folge.

Vor diesem Hintergrund setzt sich der DVGW dafür ein, die Festlegung der Rahmenbedingungen für die Einstufung der Unternehmen als KRITIS-Betreiber weiterhin den Mitgliedstaaten zu überlassen und den Artikel 2 dahingehend zu ändern.

Zu Artikel 18 „Risikomanagementmaßnahmen im Bereich der Cybersicherheit“

Die Formulierung des Artikel 18 Abs. 1 und Abs. 5 sollte dahingehend präzisiert werden, dass die Festlegung des Standes der Technik ausschließlich auf Basis internationaler, europäischer und nationaler sowie branchenspezifischer Standards zu erfolgen hat, die ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, welches dem bestehenden Risiko angemessen ist.

Die EU-Kommission erhält mit dem Artikel 18 Abs. 5 die Möglichkeit, Durchführungsrechtsakte zu erlassen, um die technischen und methodischen Spezifikationen für die in Absatz 2 genannten Elemente festzulegen. Dadurch erhält die EU-Kommission weitreichende Eingriffsmöglichkeiten, ohne dass diese weiter spezifiziert und ausformuliert werden. Die Entwicklung und Veröffentlichung von sicherheitstechnischen Anforderungen müssen sich aber *ausschließlich* auf Basis anerkannter Normen und Standards stützen, an deren Erarbeitung die betroffenen Sektoren der Kritischen Infrastrukturen und deren Wirtschaftsverbände beteiligt sind. Es sollte außerdem weiterhin die Möglichkeit bestehen, die gesetzlichen Anforderungen durch die Verwendung von branchenspezifischen IT-Sicherheitsstandards zu erfüllen, so wie zurzeit gemäß § 8a Abs. 2 BSIG vorgesehen. Die Definition von branchenspezifischen IT-Sicherheitsstandards, die auf den spezifischen Rahmenbedingungen und Besonderheiten der IT-Infrastruktur und IT-Architektur eines Sektors aufbauen, hat sich als wichtiger Baustein etabliert, um das Cybersicherheitsniveau in den Sektoren deutlich anzuheben.

Wir bitten daher um Streichung des Teilsatzes „…dabei so weit wie möglich …“ im Absatz 5. Die Ausarbeitung eines „Stands der Technik“ sollte ausschließlich unter Berücksichtigung internationaler, europäischer oder nationaler Standards und unter Beteiligung der betroffenen Sektoren Kritischer Infrastrukturen und deren Wirtschaftsverbände erarbeitet werden.

Zu Artikel 20 „Meldepflichten“

Artikel 20 sollte dahingehend präzisiert werden, dass sichergestellt ist, dass die Meldepflichten, die den Betreibern kritischer Infrastruktur auferlegt werden, sich ausschließlich auf die Meldung von definierten, erheblichen Sicherheitsvorfällen gegenüber den nationalen Sicherheitsbehörden beziehen und doppelte Meldepflichten mit ggf. konkurrierenden Zuständigkeiten nachdrücklich vermieden werden.

Vor dem Hintergrund der zunehmenden Cybersicherheitsvorfällen wird eine Meldepflicht von Sicherheitsvorfällen ausdrücklich begrüßt. Allerdings benötigen die Unternehmen in Bezug auf die behördlichen Zuständigkeiten für die Meldepflichten sowie der eindeutigen Eingrenzung und Definition der zu meldenden Sicherheitsvorfälle Rechtssicherheit. Die Meldepflichten sollten auf IT-Sicherheitsvorfälle mit überregionaler, nationaler oder europäischer Bedeutung beschränkt bleiben. Es muss eindeutig formuliert werden, was als erheblicher Sicherheitsvorfall im Hinblick auf eine erhebliche Betriebsstörung oder ein erheblicher materieller oder immaterieller Verlust (Artikel 20, Abs. 3) gemeint ist. In jedem Fall sollten doppelte Meldepflichten (an eine europäische und nationale Behörde) vermieden werden.

Bei den Vorgaben für die Meldepflichten sollten außerdem Rahmenbedingungen gewählt werden, die für die Unternehmen im Falle eines Sicherheitsvorfalls handhabbar sind und nicht zu einer Behinderung oder einer zusätzlichen schwer leistbaren Belastung führen, die ggf. einer Behebung des Sicherheitsvorfalls entgegenwirken. Vor diesem Hintergrund wird z.B. der gewählte Zeitraum von 24 Stunden, innerhalb dem gemeldet werden muss, ob der Sicherheitsvorfall auf eine rechtswidrige oder böswillige Handlung zurückgeht sowie die Festlegung, dass auf Ersuchen einer zuständigen Behörde oder eines CSIRT einen Zwischenbericht über relevante Statusaktualisierungen als problematisch und unter Praxisbedingungen schwer leistbar angesehen (Artikel 20 Abs. 4a/b). Die Auswertung von erheblichen Sicherheitsvorfälle benötigt nach unserer Erfahrung einige Zeit, bevor die Betreiber die notwendigen IT-forensischen Analysen durchgeführt haben, um eine fundierte Rückmeldung an die zuständigen Behörden zu geben.

Zu Artikel 21 „Nutzung der europäischen Systeme für die Cybersicherheitszertifizierung“

Die Formulierung des Artikel 21 Abs. 1 sollte nicht dazu führen, dass ein Wettbewerbsnachteil durch unterschiedliche Zertifizierungsniveaus in den Mitgliedsstaaten entsteht. Eine Verknappung bei der Beschaffung und dem Betrieb von wesentlichen IKT-Produkten, die zu einer Monopolbildung von einzelnen Produkten, -Diensten und -Prozessen führen kann, sollte vermieden werden.

Die Mitgliedstaaten können wesentliche und wichtige Einrichtungen dazu verpflichten, bestimmte IKT-Produkte, -Dienste und -Prozesse im Rahmen spezifischer europäischer Systeme für die Cybersicherheitszertifizierung, zertifizieren zu lassen.

Allerdings werden die betroffenen Einrichtungen maßgeblich bei der Auswahl der passenden Lösungen eingeschränkt. Dadurch wird der Einsatz innovativer und zeitgemäßer Lösungen deutlich erschwert. Durch die Konsolidierung der eingesetzten Lösungen, können einzelne Schwachstellen auf ganze Sektoren oder sogar Sektorübergreifend wirken. Produktzertifizierungen beziehen sich auf klar definierte Konfigurationen und Produktversionen, was allerdings nicht praxisgerecht erscheint, weil IKT-Produkte und Dienste regelmäßig aktualisiert werden müssen.

Weiterhin unterscheiden sich die realen Konfigurationen der Produkte bei den betroffenen Einrichtungen stark: die wesentlichen Geschäftsprozesse der Einrichtungen werden häufig von Eigenentwicklungen oder sehr spezifisch konfigurierten Standard-Anwendungen abgebildet. Eine vergleichbare Zertifizierung dieser Adaptionen ist schwer bis unmöglich nachweisbar.

Weiterhin ist zu verhindern, dass durch nationale Verordnungen sich Wettbewerbsnachteile ergeben, wenn andere Mitgliedsstaaten diese Zertifizierung nicht fordern. Die potenzielle Monopolisierung schwächt die Verhandlungsposition der Einrichtungen und führt zu überhöhten Kosten bei der Beschaffung und dem Betrieb.