Berlin, 19. März 2021

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

www.bdew.de

Stellungnahme

zum Kommissionsvorschlag für die Überarbeitung der „NIS-Richtlinie“ (EU) 2016/1148 (Gewährleistung einer EU-weit hohen Netz- und Informationssicherheit)

Stellungnahme der Energie- und Wasserwirtschaft

Transparenz-Register-ID: 20457441380-38

Die Europäische Kommission hat am 16. Dezember 2021 den Legislativvorschlag für die NIS-Richtlinie 2.0 vorgelegt. Mit der Neufassung der aus dem Jahr 2016 stammenden Richtlinie verfolgt die Europäische Kommission das Ziel, den Rechtsrahmen mittels neuer einheitlicher EU-Cybersicherheitsstandards an die Weiterentwicklung der Technologie- und Bedrohungslandschaft anzupassen. Der BDEW begrüßt die Überarbeitung der NIS-Richtlinie, denn aus Sicht der deutschen Energie- und Wasserwirtschaft muss der jeweils gültige Rechtsrahmen im Einklang mit der sich dynamisch entwickelnden Risikolandschaft stehen.

Für den weiteren legislativen Prozess hat der BDEW konkrete Forderungen verfasst, die darauf abzielen, eindeutige und erreichbare Ziele in den Vordergrund zu stellen, welche die Netz- und Informationssicherheit in der EU weiter auf kosteneffiziente Art und Weise stärken und dabei die notwendige Rechtssicherheit und angemessene Umsetzungsspielräume für die Mitgliedstaaten sicherstellen.

Kernpunkte aus Sicht des BDEW:

1. **Anwendungsbereich der Richtlinie (Artikel 2 + Anhang):** Die vorgeschlagene Ausweitung des Anwendungsbereichs sollte nur die Unternehmen von systemischer Relevanz umfassen. Ausnahmemöglichkeiten für Kleinst-, kleine und mittlere Unternehmen der Energie- und Wasserwirtschaft sollten auch zukünftig möglich sein (keine Anwendung der EU-KMU-Definition). Die Einführung des Abwasser- und Telekommunikationssektors in den Geltungsbereich der NIS-Richtlinie steht im Einklang mit der nationalen Regelung.
2. **Anbieter digitaler Dienste und Hersteller/Lösungsanbieter (Anhang):** Der BDEW begrüßt die Gleichstellung zwischen den Unternehmen der Energie- und Wasserwirtschaft und den Anbietern digitaler Infrastruktur als wesentliche Einrichtungen. Wir fordern zudem, dass Hersteller und Lösungsanbieter von IKT-Produkten, -Dienstleistungen und -Prozessen zukünftig einen verstärkten Beitrag zum Schutz kritischer Infrastrukturen leisten sollen. Hierzu sollten die Produkthaftungsregelungen um Aspekte der IT-Sicherheit erweitert werden.
3. **Einführung von Schemata für die Cybersicherheitszertifizierung (Art. 21):** Auf die gesetzliche Grundlage zur Einführung einer verpflichtenden Nutzung von IKT-Produkten, –Dienstleistungen und -Prozessen, die nach einem e europäischen Schema für die Cybersicherheitszertifizierung geprüft wurden, sollte verzichtet werden. Der bestehende, risikobasierte Regulierungsansatz der NIS-Richtlinie erfüllt den Anspruch, ein hohes Schutzniveau zu erreichen, ohne die negativen Folgen von verpflichtenden Cybersicherheitszertifizierungen mit sich zu bringen.

4. **Aufsicht und Durchsetzung der rechtlichen Anforderungen (Art. 28-34):** Der BDEW begrüßt die Bestrebungen der Kommission, einheitliche Wettbewerbsbedingungen und Rechtssicherheit durch die Festsetzung von Höchstbeträgen sicherzustellen. Der Höchstbetrag sollte jedoch bei 2 Mio. € liegen und nicht in Relation zum Jahresumsatz stehen. Das vorübergehende persönliche Verbot der Ausübung von Leitungsaufgaben durch verantwortliches Personal bei Nichteinhaltung der Richtlinie geht dagegen verschärfend über derzeitige Regelungen hinaus, ohne verhältnismäßig und zielführend zu sein.
5. **Informationsaustausch und Meldepflichten zur Cybersicherheit (Artikel 20):** Der BDEW unterstützt grundsätzlich die Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle. Meldepflichten sollten sich aber auch weiterhin auf erhebliche IT-Sicherheitsvorfälle mit überregionaler, nationaler oder europäischer Bedeutung beschränkt bleiben. Mehrfache und konkurrierende Meldepflichten und Zuständigkeiten sind zwingend zu vermeiden.
6. **Stärkung der operativen Kapazitäten der MS (Artikel 7, 8, 9, 11, 13, 14, 19):** Kernelement einer nachhaltigen Netz- und Informationssicherheit ist die vertrauensvolle Zusammenarbeit zwischen den zuständigen nationalen und europäischen Behörden und den Betreibern wesentlicher Dienste. Der BDEW spricht sich deshalb für umfangreiche Informations- und Meldepflichten der nationalen Behörden gegenüber den betroffenen Unternehmen der Energie- und Wasserwirtschaft aus.
7. **Rechtsinstrument und Rechtswirkung (Artikel 1):** Das Rechtsinstrument in Form einer Richtlinie ist zu begrüßen, da es verhältnismäßig und angemessen ist.

Vorbemerkungen

Aus Sicht des BDEW ist die Gewährleistung der Netz- und Informationssicherheit durch Betreiber wesentlicher Dienste eine Daueraufgabe höchster Priorität.

Mit der Einführung der NIS-Richtlinie wurde 2016 ein einheitlicher Rechtsrahmen für den EU-weiten Aufbau nationaler Kapazitäten für die Cybersicherheit, die Cyberabwehrfähigkeit, die verstärkte zwischenstaatliche Zusammenarbeit und den Informationsaustausch sowie Mindestsicherheitsanforderungen und Meldepflichten für Betreiber Kritischer Infrastrukturen geschaffen.

Die bisherige Richtlinie hat sich aus Sicht des BDEW grundsätzlich bewährt und ihre Umsetzung hat in Deutschland zu einem sehr guten Niveau der Netz- und Informationssicherheit in der Energie- und Wasserwirtschaft geführt.

Vor diesem Hintergrund sollte sich die Europäische Kommission auf die effektive Umsetzung konzentrieren, um ein harmonisiertes Sicherheitsniveau in allen Mitgliedstaaten zu erreichen. Die Richtlinie wurde bisher nicht vollumfänglich von allen Mitgliedstaaten umgesetzt. Ein weiteres Ziel der Überarbeitung sollte die kontinuierliche Verbesserung des Ordnungsrahmens sein. Dieser evidenzbasierte, strukturierte Ansatz sollte die regelmäßige Überprüfung der Vorgaben und den kontinuierlichen Austausch zwischen den Mitgliedsstaaten berücksichtigen.

Die Überarbeitung der Richtlinie sollte vor diesem Hintergrund die weitere Entwicklung eines kohärenten und gestrafften Rechtsrahmens für die Sicherheit von Netz- und Informationssystemen ermöglichen, ohne jedoch der Wirtschaft überhöhte Aufwände aufzuerlegen. Gleichzeitig sollten Doppelregulierungen und Inkonsistenzen mit bereits bestehenden sektoralen und digitalen Richtlinien vermieden werden.

Die Überarbeitung der Richtlinie sollte auch zu einer weiteren Stärkung des Präventionsansatzes führen. Dazu zählen entscheidend die Aspekte Aufdeckung und Wiederherstellung durch Bereitstellung von mehr und detaillierteren Informationen über Risiken und Vorfälle in den Mitgliedstaaten, von den nationalen zuständigen Behörden bis hin zu den Betreibern wesentlicher Dienste.

Des Weiteren sollte die Überarbeitung zu einem verstärkten strategischen Dialog auf EU-Ebene über Cyber-Risiken und -Bedrohungen führen (insbesondere auch über staatlich finanzierte/unterstützte Akteure, Advanced Persistent Threats). Darin würde ein wesentlicher Mehrwert der EU-Ebene liegen.

Im Detail zum Richtlinienvorschlag der Kommission (KOM 2020/823)

1 Anwendungsbereich der Richtlinie (Artikel 2 + Anhang)

Mit ihrem Richtlinienvorschlag schlägt die Kommission vor, die Definitionen und Kriterien zur Ermittlung des Adressatenkreises der Richtlinie auszuweiten, um eine umfassende Abdeckung der Sektoren und Dienste zu gewährleisten, die im Binnenmarkt für grundlegende gesellschaftliche und wirtschaftliche Tätigkeiten von entscheidender Bedeutung sind.

Einrichtungen werden nun in wesentliche (10 Sektoren) und wichtige (6 Sektoren) Einrichtungen eingeteilt. Wesentliche wie auch wichtige Einrichtungen unterliegen denselben Anforderungen an das Risikomanagement und den Meldepflichten. Die Aufsichts- und Sanktionsregelungen zwischen diesen beiden Kategorien von Unternehmen sind jedoch unterschiedlich (siehe Artikel 29 und 30). Davon ausgenommen werden sollen nur Kleinst- und Kleinunternehmen gemäß der Empfehlung 2003/361/EG (EU-KMU Definition).

1.1 Ausnahmen für Kleinst- und kleine Unternehmen

Im Sinne eines ganzheitlichen Sicherheitsniveaus sind alle Unternehmen aufgefordert, ihren möglichen Beitrag zur Zielerreichung in den Mitgliedstaaten zu leisten. Der BDEW erachtet die Ausnahme für Kleinst- und Kleinunternehmen dabei grundsätzlich als sinnvoll, sofern diese **unabhängig von ihrer Eigentümerschaft** betrachtet werden. Ferner sollte die Ausnahme **auf mittlere Unternehmen erweitert** werden. Nur so würde dem Grundsatz der Verhältnismäßigkeit Rechnung getragen werden. Der Verweis auf die Empfehlung 2003/361/EG der Kommission in Artikel 16 Ziffer 11 der NIS-Richtlinie würde dagegen dazu führen, dass die angedachte Ausnahme für zahlreiche kommunale Unternehmen nicht anwendbar wäre und daher der Zweck der Ausnahme für Kleinstunternehmen und kleine Unternehmen im Kontext der Energie- und Wasserwirtschaft verfehlt würde.

Die KMU-Definition der Kommission zählt Unternehmen, deren Anteile zu mindestens 25 % von einer staatlichen Stelle oder Körperschaft des öffentlichen Rechts kontrolliert werden, grundsätzlich nicht zu den KMU. Damit sind beispielsweise Kleinstunternehmen und kleine Unternehmen, die zu einem überwiegenden Teil kommunale Anteilseigner haben, automatisch ausgeschlossen.

Der Verweis auf die EU-KMU-Definition (2003/361/EG) sollte folglich gestrichen werden und die Ausnahmeregelung unabhängig der Eigentümerschaft eines Unternehmens ausgerichtet sein. Alternativ könnte eine Festlegung auch auf Ausnahmeregelungen in der nationalen Gesetzeslage (wie bspw. basierend auf der BSI-Verordnung zur Bestimmung kritischer Infrastrukturen in Deutschland) basiert werden. Die systemische Relevanz wesentlicher Einrichtungen muss der Leitgedanke sein.Im deutschen Ordnungsrahmen wird zur Bestimmung von Betreibern wesentlicher Dienste die sogenannte **Versorgungskritikalität einer Einrichtung** zugrunde gelegt, die sowohl sektorspezifische Gegebenheiten als auch die systemische Relevanz einer Einrichtung berücksichtigt. Der BDEW bewertet diesen Bestimmungsansatz als sachgemäß und zielführend, um den Adressatenkreis der NIS-Richtlinie bestimmungsgemäß einzugrenzen.

Der BDEW fordert nachdrücklich, dass auch weiterhin ein derartiges Kriterium im **Energie- und Wassersektor** angelegt werden sollte, um Überregulierung und unnötige organisatorische und finanzielle Aufwendungen auf Seiten der Wirtschaft und insbesondere Kleinst-, kleinen und mittleren Unternehmen vorzubeugen.

Gleichzeitig sollten Kleinstunternehmen, kleinen und mittleren Unternehmen Angebote im Bereich der Weiterbildung zu IT-Sicherheitsfragen offenstehen und Möglichkeiten zur fachgerechten Beratung eröffnet werden, z.B. in Form einer auf diese Kategorie spezialisierte Ansprechstelle. Die zuständigen nationalen Behörden könnten hier verstärkt sowohl Sensibilisierungsmaßnahmen als auch Workshops und Trainings zu spezifischen IT-Sicherheitsfragen durchführen. Daher begrüßt der BDEW die vorgeschlagenen Unterstützungsmaßnahmen für KMUs in Art.5.2(h).

1.2 Aufnahme der Energienetze und der Energieerzeugung

Durch die vorgeschlagene Ausweitung des Anwendungsbereichs würde im deutschen Energiesystem der **Großteil der Anlagen und Betriebseinrichtungen in den Bereichen der Verteilung und Übertragung sowie Erzeugung erfasst** werden, unabhängig ob diese eine kritische Funktion für die gesellschaftliche und wirtschaftliche Tätigkeit in Deutschland erbringen. Durch den Verweis auf die unvollständige EU-KMU-Definition (siehe oben) prognostiziert der BDEW, dass zukünftig mehr als 2.000 Unternehmen allein im Sektor Energie (Strom, Gas, Wasserstoff) über die Wertschöpfungsstufen Erzeugung, Verteilung und Übertragung hinweg betroffen wären.

Die **finanziellen und organisatorischen Auswirkungen** auf diese Unternehmen wären enorm, da die Umsetzung der Vorgaben des Legislativvorschlags erhebliche Kosten in mindestens niedriger sechststelliger Höhe je Einrichtung nach sich ziehen würden. Es ist daher zu erwarten, dass eine derart umfassende Ausweitung des Anwendungsbereichs die Wirtschaftlichkeit insbesondere von bestehenden und in der Planung befindlichen Erneuerbaren Energie-Anlagen nachhaltig gefährden würde, wodurch letztendlich die Erreichung der Erhöhung der Emissionsminderungsziele bis 2030 nachteilig betroffen werden könnte. Die **Verhältnismäßigkeit** der Ausweitung auf beinahe alle Unternehmen des Sektors Energie ist aus Sicht des BDEW nicht gewahrt, da diese aufgrund ihrer bloßen sektoriellen Zugehörigkeit als wesentliche Einrichtung und nicht etwa aufgrund ihrer Relevanz für den sicheren Betrieb des Energiesystems adressiert würden.

1.3 Aufnahme der Abwasserwirtschaft

Die Einführung des Abwassersektors in den Geltungsbereich der NIS-Richtlinie steht aus unserer Sicht im Einklang mit der nationalen Regelung. Die BSI-Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV) subsumiert bereits heute unter dem Sektor sowohl die Trinkwasserversorgung als auch Abwasserbeseitigung. Im Sektor Wasser/Abwasser ist darüber hinaus sicherzustellen, dass ein Eingriff in die kommunale Entscheidungshoheit der Wasserwirtschaft und insbesondere im hoheitlichen Sektor Abwasser ausgeschlossen wird. Denn diese kommunale Entscheidungshoheit ist verfassungsrechtlich geschützt.

1.4 Aufnahme öffentlicher elektronischer Kommunikationsnetze

Wir begrüßen ebenfalls die Aufnahme von Betreibern öffentlicher elektronischer Kommunikationsnetze in den Anwendungsbereich der NIS-Richtlinie 2.0. Flächendeckend verfügbare und leistungsfähige Telekommunikations- und Breitbandinfrastrukturen stellen eine Grundvoraussetzung für den Einsatz digitaler Technologien und digitaler Anwendungsfälle in Gesellschaft, Staat und Wirtschaft dar. Der Vorschlag steht zudem im Einklang mit der nationalen Regelung.

1.5 Aufnahme der öffentlichen Verwaltung

Der BDEW begrüßt die vorgeschlagene Aufnahme der öffentlichen Verwaltung in den Anwendungsbereich der Richtlinie. Zum einen haben die Erfahrungen aus dem Krisenmanagement zur COVID19-Pandemie gezeigt, dass in einem Krisenfall die Reaktionsfähigkeit des Staates von erheblicher Bedeutung für die Organisation des gesellschaftlichen Umgangs mit einer Krise ist. Zum anderen werden bei einigen dieser Institutionen (z.B. national zuständige Behörden wie das deutsche Bundesamt für Sicherheit in der Informationstechnik) sensible Informationen von Betreibern wesentlicher Dienste geführt. Diese sind als kritisch einzustufen und müssen entsprechend geschützt werden.

1.6 Kohärenz zu sektorspezifischen Anforderungen (Artikel 2 (6))

Sofern sektorspezifische EU-Vorschriften ein vergleichbares oder darüberhinausgehendes Mindestmaß an die Netz- und Informationssicherheit der Sektoren der NIS-Richtlinie 2.0 formulieren, haben diese Rechtsakte einschließlich der Bestimmungen über die gerichtliche Zuständigkeit Vorrang. Aus Sicht der deutschen Energie- und Wasserwirtschaft ist ein derartiger Vorrang der Lex-specialis-Bestimmungen im Kern sinnvoll. Dies sollte in der Richtlinie auch explizit festgehalten werden, u.a. mit erklärendem Verweis auf parallele Arbeiten an sektorieller Gesetzgebung (z.B. Netzkodex zu Cybersicherheit im Energiesektor) oder sektorielle verpflichtende Sicherheitsstandards (z.B. den Branchensicherheitsstandards von DVGW und DWA).

Es muss im Zuge der Ausarbeitung sektorspezifischer Rechtsakte jedoch sichergestellt werden, dass es für die betroffenen Betreiber weder zu Doppelregulierungen noch zu Rechtsunsicherheiten in der Auslegung kommen kann, die aufgrund eines unklaren und unscharfen Rechtsrahmens entstehen könnten.

2 Anbieter digitaler Dienste und Hersteller/Lösungsanbieter

Der BDEW begrüßt die Unterteilung der digitalen Dienste in Digitale Infrastruktur als wesentliche Einrichtungen und Digitale Anbieter als wichtige Einrichtungen. Die damit verbundene **Gleichstellung zwischen den Betreibern wesentlicher Dienste und denen digitaler Infrastruktur als zukünftig wesentliche Einrichtungen** ist angesichts ihrer Bedeutung beispielsweise für die sichere Energie- oder Wasserversorgung als echter Mehrwert anzusehen, da sie einen direkten Beitrag zur verlässlichen Erbringung von kritischen Dienstleistungen haben.

Die Pflicht zur Umsetzung von Risikomanagementmaßnahmen durch Anbieter Digitaler Infrastruktur wird dazu beitragen, die Netz- und Informationssicherheit zielgerichtet und effizient zu erhöhen. Der BDEW befürwortet ausdrücklich diesen Schritt, da auf diesem Weg die Verlässlichkeit, Integrität und Verfügbarkeit von digitalen Dienstleistungen erhöht werden. Sie sind für das reibungslose Funktionieren vieler wesentlicher Einrichtungen, die solche Dienstleistungen täglich nutzen, von herausragender Bedeutung. Eine Störung eines solchen digitalen Dienstes könnte die Bereitstellung anderer, von ihnen abhängiger Dienste verhindern und somit wesentliche wirtschaftliche und gesellschaftliche Tätigkeiten in der Union beeinträchtigen.

Die Neuaufnahme im Bereich der Digitalen Infrastruktur für Anbieter von Cloud-Diensten, Datenzentren, „Content Delivery“, Network-Anbieter, Vertrauensdienste, Anbieter öffentlicher elektronischer Kommunikationsnetze sowie die Ergänzung der digitalen Dienste um Anbieter einer Plattform für soziale Netzwerkdienste sind gleichermaßen zu begrüßen.

Zusätzlich sollten zudem weitere Anbieter digitaler Dienste um Service-Hosting-Provider und Anbieter von Navigationsdienstleistungen aufgenommen werden, da eine Vielzahl von energie- und wasserwirtschaftlichen informationstechnischen Anwendungen auf verlässliche und konsistente digitale Dienstleistungen dieser Art aufsetzen.

Der BDEW bittet darüber hinaus um eine Klarstellung, dass mit „**Online-Marktplätzen**“ gemäß Artikel 4 Ziffer 17 des Kommissionsvorschlags, Plattformen zum Abschließen von Kauf- oder Dienstleistungsverträgen mit anderen juristischen oder natürlichen Personen als dem Eigentümer oder Betreiber der Webseite oder des Dienstes selbst gemeint sind. „Online-Marktplätze“[1] wären demnach Webseiten, bei denen der Betreiber nicht selbst Vertragspartner wird, sondern als Vermittler zwischen zwei Vertragsparteien auftritt. Somit wären beispielsweise Web-Dienste zum Vertragsschluss sowie Online-Shops für Waren und Dienstleistungen von Unternehmen der Energie- und Wasserwirtschaft auf deren eigenen Webseiten ausgeschlossen.

[1] Der Legislativvorschlag der Kommission verweist in Artikel 4 Punkt 17 auf eine Definition von Online-Marktplätzen gemäß 2005/29/EC Art.2 Ziffer n. Nach einer Überprüfung der RL 2005/29/EC, möchte der BDEW die Kommission darauf aufmerksam machen, dass Ziffer n nicht Teil der Richtlinie ist. **Dieser Verweis sollte korrigiert werden**.

2.1 Sicherheit von IKT-Produkten und -Diensten durch Einbindung von Herstellern und Lösungsanbietern

Verfehlt ist aus Sicht des BDEW, dass **Soft- und Hardwarehersteller im Kommissionsvorschlag nicht ausreichend erfasst** werden. Hersteller von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen sollen zukünftig als wichtige Einrichtungen zwar Anforderungen an die Sicherheit ihrer eigenen informationstechnischen Systeme genügen müssen. Dies adressiert jedoch nicht einmal grundlegene Sicherheitseigenschaften von IKT-Produkten und -Dienstleistungen, die von ebendiesen hergestellt und vertrieben werden.

Die deutsche Energie- und Wasserwirtschaft fordert die Kommission, das Europäische Parlament und den Rat der EU daher auf, Hersteller und Lösungsanbieter von IKT-Produkten, -Dienstleistungen und -Prozessen im Rahmen der NIS-Richtlinie 2.0 **zu einem risikoorientierten und adäquaten Umgang mit Grundprinzipien der IT-Sicherheit zu verpflichten**. Dies umfasst beispielsweise den „Security by Design"-Gedanken, also das Entwickeln von Soft- und Hardware unter Berücksichtigung elementarer Sicherheitsanforderungen oder das Behandeln von Schwachstellen über den gesamten Lebenszyklus ihrer am Markt vertriebenen Produkte durch einen Update-Zwang. Denn nach Bekanntwerden von Schwachstellen können nur Hersteller und Dienstleister ihre Produkte und Systeme zeitnah absichern und ihren Kunden, den Betreibern wesentlicher Dienste, möglichst umgehend Sicherheitsupdates zur Verfügung stellen. Durch eine derartige Verpflichtung von Herstellern und Dienstleistern kann die Kommission die Erhöhung der Netz- und Informationssicherheit schneller und effizienter erreichen, ohne die Betreiber wesentlicher Dienste zusätzlich zu belasten.

Dieses Ziel sollte aus Sicht des BDEW über eine **Erweiterung der Produkthaftung** gemäß Richtlinie 85/374/EWG **um Aspekte der IT-Sicherheit** verfolgt werden, um Kausalitätsketten zu schließen und Hersteller und Lösungsanbieter zu einer gewissenhaften Pflege der IT-Sicherheit ihrer Produkte und Dienstleistungen zu bewegen.

2.2 Risikomanagement- und -bewertungsmaßnahmen kritischer Lieferketten (Artikel 18, 19)

Die deutsche Energie- und Wasserwirtschaft stimmt der Beobachtung der Kommission zu, dass in Zeiten global vernetzter Produktionsweisen und internationaler Lieferketten zunehmend **Cybersicherheitsrisiken** für die informationstechnischen Systeme von wesentlichen Einrichtungen entlang **kritischer Lieferketten** aufkommen. Der Fall SolarWinds verdeutlicht die besorgniserregende Bedrohung durch Angriffe über Lieferketten hinweg.

Der derzeitige Ordnungsrahmen weist diesbezüglich Regelungslücken auf, um die Zusammenführung der Erkenntnisse nationaler zuständiger Behörden zur weiteren Analyse von Cyber-Bedrohungsszenarien aus strategischer und europäischer Perspektive sicherzustellen. Der BDEW regt daher an, die **Vorgabe bindend zu formulieren** („soll" statt „kann", Artikel 19 (1)) und festzuschreiben, dass die gewonnen Erkenntnisse z.B. über Angriffsstrategien, statistischen Informationen und weiteren Quellen und Informationsarten den Betreibern wesentlicher und wichtiger Dienste zeitnah, aktuell und **regelmäßig zur Verfügung gestellt** werden. Darauf aufbauend sollte ein strukturierter Dialog zur Behandlung potenzieller, identifizierter Risiken entlang von kritischen

Lieferketten mit allen relevanten Interessensträgern geführt werden, um die **technologische Souveränität der EU langfristig stärken** zu können.

Vor diesem Hintergrund begrüßt der BDEW den Kommissionsvorschlag, wonach die NIS-Koordinationsgruppe gemäß Artikel 19 beauftragt werden soll, strukturiert und koordiniert Risikobewertungen von Lieferketten durchzuführen, um für jeden Sektor die kritischen IKT-Dienste, -Systeme oder -Produkte sowie relevante Bedrohungen und Schwachstellen zu ermitteln.

Darüber hinaus schlägt die Kommission zwei weitere Ansatzpunkte vor, um Cybersicherheitsrisiken entlang von Lieferketten zu adressieren:

- Mitgliedsstaaten sollen im Rahmen der nationalen Cybersicherheitsstrategie ein Konzept für die Cybersicherheit in der Lieferkette für IKT-Produkte und -Dienste vorlegen, die von wesentlichen und wichtigen Einrichtungen für die Erbringung ihrer Dienste genutzt werden.
- Im Zuge der Risikomanagementmaßnahmen sollen Betreiber gemäß Artikel 18 (2) d) verpflichtet werden, Maßnahmen für die Sicherheit von Lieferketten einschließlich sicherheitsbezogener Aspekte der Beziehungen mit den Anbietern oder Diensteanbietern von bspw. Datenspeicher- und Datenverarbeitungsdiensten oder verwalteten Sicherheitsdiensten (MSS) umzusetzen.

Der BDEW gibt zu bedenken, dass dies nicht in neuerliche Mehraufwände bürokratischer Natur für Betreiber münden sollte, da die Unternehmen der Energie- und Wasserwirtschaft bereits etablierte, branchenspezifische Verfahren und Empfehlungen umsetzen, wie beispielsweise das BDEW / OE Whitepaper zu Anforderungen an sichere Steuerungs- und Telekommunikationssysteme[2]. Ein erhöhtes Maß der IT-Sicherheit von Produkten, Dienstleistungen und Prozessen im EU-Binnenmarkt sollte stattdessen über die Weiterentwicklung der Produkthaftungsregelungen gemäß Richtlinie 85/374/EWG erwirkt werden (siehe Kapitel 2.1).

Der **Einsatz von starken und verlässlichen Verfahren der Kryptografie** ist elementar für die Netz- und Informationssicherheit von Gesellschaft, Wirtschaft und Staat. Der Gesetzgeber sollte im Sinne von Erwägungsgrund 54 und Artikel 18 Ziffer 5 jedwede potenzielle technische Maßnahme zur systematischen Schwächung von kryptografischen Verfahren gesetzlich ausschließen, da er sonst die Vertrauenswürdigkeit, Verlässlichkeit und Integrität informationstechnischer Systeme in ihrer Allgemeinheit aktiv gefährdet. Der BDEW fordert den Gesetzgeber daher auf, die Schutzziele der Netz- und Informationssicherheit uneingeschränkt zu respektieren und deren breite Umsetzung zu fördern.

[2] BDEW/OE Whitepaper (2018): Anforderungen an sichere Steuerungs- und Telekommunikationssysteme: https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems-engl.pdf

3 Einführung von Schemata für die Cybersicherheitszertifizierung (Artikel 21)

Die Kommission sieht die Möglichkeit vor, dass Mitgliedstaaten von wesentlichen und wichtigen Einrichtungen verpflichtet werden können, nur noch bestimmte IKT-Produkte, -Dienstleistungen und -Prozesse einsetzen zu dürfen, die zuvor im Rahmen spezifischer europäischer Systeme für die Cybersicherheitszertifizierung zertifiziert worden sind. Des Weiteren hat die Kommission das Recht, delegierte Rechtsakte zur Festlegung der betroffenen Kategorien von wichtigen Einrichtungen zu erlassen. Damit soll in der Richtlinie die Grundlage dafür geschaffen werden, dass der EU Cybersecurity Act von seiner freiwilligen Natur entledigt und in eine **verpflichtende Vorgabe zum Einsatz zertifizierter IKT-Produkte, -Dienstleistungen und -Prozesse** durch Betreiber wesentlicher und wichtiger Einrichtungen gewandelt werden.

Der BDEW lehnt eine derartige verpflichtende Einführung von Cybersicherheitszertifizierungen ab, die entgegen der Bestimmungen des EU Cybersecurity Acts durch eine parallele Gesetzgebung eingeführt werden sollen. Dies gilt insbesondere für Standard-Software, wie bspw. Firewalls, Betriebssysteme, etc. Wir sprechen uns dagegen aus, dass die Kommission Rechtsakte zur Festlegung der betroffenen Kategorien erlassen kann. Grundsätzlich sollte die Europäische Kommission die Marktstellung auf der Anbieterseite im Hinblick auf die Anbietervielfalt beobachten.

Eine Zertifizierungspflicht von IKT-Produkten, -Dienstleistungen und -Prozessen im energie- und wasserwirtschaftlichen Umfeld ist eine hochsensible Angelegenheit, deren Auswirkungen im vorherrschenden Einsatzumfeld vielfältig und nur schwer endgültig zu bemessen sind.

Der BDEW weist daraufhin, dass der Markt für Hersteller und Lösungsanbieter von wesentlichen Komponenten der Prozess- und Automatisierungstechnik, die in der Energie- und Wasserwirtschaft zum Einsatz kommen, überschaubar ist. **Eine Zertifizierungspflicht hätte aller Voraussicht zur Folge, dass die Anbietervielfalt auf dem Markt möglicherweise auf wenige Hersteller weltweit eingeschränkt werden könnte**. Vor dem Hintergrund der Bestrebungen um technologische Souveränität in der Europäischen Union muss anhand der politischen und regulatorischen Rahmenbedingungen sichergestellt werden, dass jederzeit eine ausreichende Anzahl an vertrauenswürdigen europäischen Herstellern von relevanten Produkten, Dienstleistungen und Prozessen garantiert ist. Eine sektorspezifische Zertifizierungspflicht darf nicht in eine **Abhängigkeit von Herstellern aus Nicht-EU-Staaten** münden. Zudem ist davon auszugehen, dass eine derartige Zertifizierungspflicht steigende Preise für betroffene Komponenten zur Folge haben würde, was wiederum Kosteneffekte in der Versorgung mit Energie und Trinkwasser sowie der Entsorgung von Abwasser haben könnte.

Die Energie- und Wasserwirtschaft gibt darüber hinaus zu bedenken, dass eine alleinige Zertifizierungspflicht von einzelnen Komponenten nicht das Schutzniveau einer Anlage als Ganzes steigert. Die Anlagensicherheit wird durch das schwächste Glied in der Kette definiert und ist immer im spezifischen, eingesetzten Kontext zu bewerten. Nur durch das Zusammenspiel aller Komponenten, Anlagenteile und Ressourcen (Personal, Infrastrukturen, Prozesse, Verfahren und deren regelmäßige Pflege und Ineinanderwirken) kann ein hohes Schutzniveau erreicht werden. Der bestehende, risikobasierte Regulierungsansatz der aktuellen NIS-Richtlinie erfüllt diesen Anspruch.

Eine Zertifizierungspflicht, die einen Mehrwert für den Schutz wesentlicher und wichtiger Einrichtungen bewirkt, muss aus Sicht des BDEW Hersteller eindeutig in die Pflicht nehmen. Hierzu sollten die Produkthaftungsregelungen der Richtlinie 85/374/EWG um Aspekte der IT-Sicherheit erweitert werden. So sollten ausschließlich Minimalanforderungen an die Sicherheit von IKT-Produkten, -Dienstleistungen und -Prozesse gestellt werden. Dies könnte beispielsweise den Nachweis einer sicheren Produktentwicklung, Nachweis über positive Schwachstellenprüfung, Vorlage eines Sicherheitskonzepts und Empfehlungen für den sicheren Betrieb, Nachweis über den umgesetzten Stand der Technik (z.B. von Verschlüsselungsmechanismen), Nachweis über sichere Voreinstellungen, Betriebsgarantien wie Wartung, Patches, Updates, etc. umfassen.

Eine Fortschreibung des Ordnungsrahmens, der die vorgenannten Aspekte berücksichtigt, könnte einen positiven Effekt auf den Schutz wesentlicher und wichtiger Einrichtungen entfalten. Jedoch ist davon auszugehen, dass dieser Effekt umgehend verpuffen würde, wenn statt der Hersteller die Betreiber in die Pflicht genommen würden. Zur Herstellung und Aufrechterhaltung eines sicheren Einsatzes von IKT-Produkten, -Dienstleistungen und -Prozessen ist ein stärkerer Beitrag von Herstellern und Lösungsanbietern elementar. Dabei muss der Fortbetrieb von bereits im Einsatz befindlichen Produkten, Dienstleistungen und Prozessen gewährleistet werden.

4 Aufsicht und Durchsetzung der rechtlichen Anforderungen (Art. 28-34)

Die Kommission legt mit dem vorliegenden Vorschlag einen stringenten Rahmen dar für die Aufsicht und Durchsetzung der rechtlichen Anforderungen an Betreiber wesentlicher und wichtiger Dienste. Der BDEW begrüßt dies grundsätzlich, da auf diesem Weg Transparenz und Rechtssicherheit hinsichtlich möglicher Mitwirkungspflichten und Sanktionstatbeständen erwirkt werden können. Klare Vorgaben und die Pflicht der zuständigen Behörden zur ausführlichen Begründung ihrer Durchsetzungsentscheidungen sind die Voraussetzungen für eine zielführende und effiziente Erhöhung des Cybersicherheitsniveaus in der Union.

4.1 Überwachung und Durchsetzung der rechtlichen Anforderungen an wesentliche Einrichtungen

Die zuständigen Behörden sollen gemäß Artikel 29 Ziffer 4 Buchstabe e) zukünftig befugt werden, Betreiber wesentlicher Einrichtungen dazu zu verpflichten, die Empfänger ihrer Dienste, die potenziell von einer Cyberbedrohung betroffen sind, über mögliche Abwehr- oder Abhilfemaßnahmen zu unterrichten. Während eine derartige Information für Empfänger digitaler Dienste oder Infrastrukturdienstleistungen hilfreich ist, entspringt aus dieser potenziellen Unterrichtungspflicht **kein ersichtlicher Mehrwert im Kontext der Energie- und Wasserversorgung**. Die Intention dieser Vorgabe und der Nutzen, wenn Betreiber aus sämtlichen wesentlichen Sektoren ihre Kunden über Vorfälle informieren sollen, bleibt in der vorliegenden Fassung vage. Der BDEW empfiehlt daher, diese Befugnis seitens der zuständigen Behörden auf Anbieter digitaler Infrastruktur oder Dienste zu begrenzen.

Weitere zu hinterfragende Befugnisse werden in Ziffer 4 Buchstaben h) und i) formuliert. Zum einen sollen Einrichtungen angewiesen werden können, Aspekte der Nichteinhaltung der Richtlinie zu veröffentlichen. Zum anderen soll diese Bekanntmachungspflicht auch die Angabe, der für einen Verstoß der Verpflichtungen der Richtlinie verantwortlichen juristischen oder natürlichen Person umfassen. Beide Befugnisse gehen weit über die heutigen Durchsetzungsmaßnahmen hinaus und lassen keinen direkten Bezug zur Stärkung der Netz- und Informationssicherheit einer Einrichtung erkennen. Die Veröffentlichung von Abweichungen gegenüber den Vorgaben der Richtlinie erscheinen im Gegenteil kontraproduktiv für die Gewährleistung der IT-Sicherheit. Der BDEW lehnt darüber hinaus eine mögliche Pflicht, einzelne Angestellte persönlich in der Öffentlichkeit kritisch hervorzuheben, als unsachgemäß ab. Die Androhung von finanziellen Sanktionen gegen Betreiber wesentlicher Einrichtungen stellt erfahrungsgemäß einen ausreichenden Anreiz zur Erfüllung der gesetzlichen Pflichten dar.

Bei Verstoß gegen die Vorgaben der Richtlinie schlägt die Kommission gemäß Ziffer (5) a) nichtfinanzielle Sanktionen vor, in deren Folge nationale Behörden künftig die Autorisierung oder Zulassung für einen Teil oder die Gesamtheit der von einer wesentlichen Einrichtung erbrachten Dienstleistungen oder Tätigkeiten ausgesetzt werden müsste. Bei einer solchen Regelung wäre das Ausmaß der Betroffenheit auf Seiten der Wirtschaft enorm. Eine derartige Sanktionsmaßnahme geht verschärfend über den heutigen Rahmen hinaus und stellt einen **Eingriff in den operativen Betrieb einer wesentlichen Einrichtung** dar. Der BDEW fordert, diesen Passus ersatzlos zu streichen, da dies eine **negative Auswirkung auf das Regelungsziel der Richtline** darstellt.

4.2 Verhängung von Geldbußen (Artikel 31, 33)

Die europäische Gesetzgebung sollte die Kohärenz der Sanktionen in allen Mitgliedstaaten sicherstellen. Insbesondere sollte sie dafür Sorge tragen, dass Betreiber wesentlicher Dienste im europäischen Binnenmarkt vergleichbare Wettbewerbsbedingungen vorfinden. Wir begrüßen daher den Vorschlag der Kommission zu diesem Zweck einen Höchstbetrag gemäß Artikel 31 festzulegen, um übermäßige Strafen zu verhindern und Rechtssicherheit zu gewährleisten.

Ein Höchstmaß von mindestens 10 Mio. € zollt jedoch den erheblichen Bemühungen von Betreibern wesentlicher Einrichtungen, die Netz- und Informationssicherheit zu gewährleisten, nicht Rechnung. Ein derart enormes Sanktionsmaß wäre einer guten und vertrauensvollen Zusammenarbeit zwischen Betreibern und den zuständigen Behörden tendenziell abträglich. In den letzten Jahren wurde ein gutes, sachdienliches Vertrauensverhältnis erarbeitet. Es ist anzuzweifeln, ob gewünschte Investitionen in die Informationssicherheit gefördert würden, wenn stattdessen für unverhältnismäßige Sanktionsrisiken umfangreiche Rückstellungen gebildet werden müssten.

Wir plädieren für eine maximale Bußgeldhöhe von zwei Millionen Euro, um das Prinzip der Verhältnismäßigkeit zu würdigen. Der Bezug zu dem Jahresumsatz sollte gestrichen werden.

5 Informationsaustausch und Meldepflichten zur Cybersicherheit

Der BDEW unterstützt grundsätzlich die Pflicht zur Meldung erheblicher sowie potenzieller zukünftiger IT-Sicherheitsvorfälle. Meldepflichten sollten jedoch auch weiterhin maximal **auf potenziell erhebliche IT-Sicherheitsvorfälle mit überregionaler, nationaler oder europäischer Bedeutung beschränkt** bleiben. Aus Sicht der Energie- und Wasserwirtschaft ist es unabdinglich, dass der Ordnungsrahmen folgende unionsweite Vorgaben enthält:

- Schlanke und einfache Meldewege, die auf etablierte Strukturen und Verfahren aufsetzen,
- standardisierte Meldeformulare, sowie
- die Ermöglichung eines vertrauensvollen und vertraulichen Informationsaustauschs zwischen der zuständigen Behörde und den Betreibern, indem Geschäftsgeheimnisse durch die Behörden geschützt werden.

Erweiterte Berichtspflichten in Form von mehrfachen und konkurrierenden Meldepflichten und Zuständigkeiten, die über den derzeitigen Rechtsrahmen hinausgehen, würden nur zu einem hohen Aufwand an Bürokratie und Kosten auf Seiten der Wirtschaft führen. Sie sind aus Sicht des BDEW daher zwingend zu vermeiden.

Der Kommissionsvorschlag enthält eine hinreichend **klare Definition von erheblichen Sicherheitsvorfällen** (Artikel 20 Ziffer 3). Neu ist die **Aufnahme potenzieller Unterbrechungen** des von der wesentlichen Einrichtung erbrachten Dienstes, die Auswirkungen auf die öffentliche Sicherheit, die öffentliche Ordnung, oder die öffentliche Gesundheit haben oder zu systemischen Risiken führen könnten. Eine solche Erweiterung der Meldepflicht um potenzielle Unterbrechungen ist analog zur derzeitigen rechtlichen Lage in Deutschland. Die Erfahrungen hierzulande zeigen, dass durch ein erhöhtes Meldeaufkommen die zuständige Behörde in die Lage versetzt wird, ein differenzierteres und umfassenderes Bild über die Bedrohungen aus dem digitalen Raum zu erfassen. Dabei darf der **Informationsfluss jedoch nicht einseitig** sein. Es ist daher zu begrüßen, dass die zuständigen Behörden gemäß Artikel 20 Ziffer 5 verpflichtet werden sollen, den meldenden Betreibern eine qualifizierte Rückmeldung zu geben.

Die Kommission sieht zudem strikte Zeiträume für die Abgabe von verpflichtenden (Teil-)Meldungen durch Betreiber wesentlicher und wichtiger Dienste an die zuständigen Behörden vor (Artikel 20 Ziffer 4). Darüber hinaus wird ein ausreichender Spielraum eröffnet, um im begründeten Einzelfall von diesen Vorgaben abzuweichen. Sowohl der Umfang als auch der Turnus der (Teil-)Meldungen stehen im Einklang mit der gelebten Praxis in Deutschland. Der BDEW gibt zu bedenken, dass Abschlussmeldungen erst mit in dem nötigen Detail- und Evidenzgrad erbracht werden können, nachdem Betreiber die IT-forensischen Analysen und potenzielle Gegenmaßnahmen vollends durchgeführt haben, die zur Gewährleistung der Betriebskontinuität erforderlich sind. Vor diesem Hintergrund ist es zu erwarten, dass eine Abschlussmeldung in aller Regelmäßigkeit erst nach mehr als einem Monat vollumfänglich vorgenommen werden kann.

Der BDEW begrüßt den Vorschlag der Kommission, dass im Sinne der koordinierten Offenlegung von Schwachstellen die national benannten **„Cyber Security Incident Response Teams“ (CSIRT)**

als vertrauenswürdige Vermittler zwischen einer meldenden Einrichtung und betroffenen Herstellern oder Anbietern von IKT-Produkten und -Diensten agieren sollen (Artikel 6). Relevante Informationen über auf diesem Weg gemeldete Schwachstellen sollen von ENISA in einem europäischen Register gesammelt und gepflegt werden. Der BDEW gibt zu bedenken, dass es für die Wirksamkeit einer solchen Praxis entscheidend ist, dass hinreichende Kapazitäten zur Einrichtung, Kuration von spezifischen technischen Mitigationsmaßnahmen und zur Pflege des Registers zur Verfügung stehen. Darüber hinaus sollte in der Richtlinie geklärt werden, welche Kreise Einsicht in das Register erhalten sollen. **Geschäftsgeheimnisse** von meldenden Einrichtungen müssen jederzeit geschützt werden, um die Akzeptanz eines europäischen Registers auf Seiten der Wirtschaft zu wahren.

Ferner zielt die Kommission gemäß Artikel 26 darauf ab, dass **wesentliche und wichtige Einrichtungen untereinander relevante Cybersicherheitsinformationen austauschen** können. Der BDEW begrüßt das Vorhaben, den Informationsfluss innerhalb der EU zur Stärkung der Cybersicherheit anzureizen.

Die Neufassung der Richtlinie sieht vor, dass – sofern der Verstoß einer wesentlichen oder wichtigen Einrichtung gegen die festgelegten Verpflichtungen zu den Risikomanagement- und Meldepflichten (Artikel 18 und 20) eine Verletzung des Schutzes personenbezogener Daten zur Folge hat, die gemäß der DSGVO-Verordnung meldepflichtig ist – die zuständigen Aufsichtsbehörden innerhalb einer angemessenen Frist informiert werden müssen.

Aus Sicht des BDEW ist es positiv zu bewerten, dass die zuständigen Behörden für denselben Verstoß keine Geldbuße nach DSGVO und zusätzlich gemäß Artikel 31 der vorliegenden Richtlinie verhängen können. Eine doppelte Sanktion wäre nicht zielführend und würde keinen zusätzlichen Beitrag zum erhöhten Cybersicherheitsschutz gewährleisten.

6 Stärkung der operativen Kapazitäten der Mitgliedsstaaten (Artikel 7, 8, 9, 11, 13, 14, 19)

Der BDEW begrüßt, dass die Kommission die Mitgliedsstaaten zur Stärkung ihrer operativen Kapazitäten im Bereich der Cybersicherheit und zur Bewältigung grenzüberschreitender Krisenlagen verpflichten will. Das Kernelement einer nachhaltigen Netz- und Informationssicherheit ist die vertrauensvolle Zusammenarbeit einerseits zwischen den zuständigen staatlichen Behörden untereinander und andererseits mit den Betreibern wesentlicher und wichtiger Dienste. Die staatlichen Aktivitäten sollten dabei passgenau und effizient entlang der Bedarfe der Betreiber ausgestaltet werden. Zu diesem Zweck merkt der BDEW im Detail an:

Die Kommission legt in Artikel 7 die Anforderungen an den nationalen Rahmen für das **Cybersicherheitskrisenmanagement** dar. Das nationale Krisenmanagement muss auf den Aufbau und die Koordination der Reaktionsfähigkeit der einzelnen Mitgliedsstaaten konzentriert sein. Betreiber wesentlicher und wichtiger Dienste sollten jedoch als interessierte Parteien in die Ausarbeitung staatlicher Reaktionspläne beteiligt werden. Jedoch ist ein Eingriff in das betriebliche Krisenmanagement der Betreiber hierbei nicht zielführend und sollte demnach unterbleiben.

Es muss klar geregelt werden, dass auch die zuständigen nationalen Behörden gegenüber den betroffenen Unternehmen **umfangreiche Informations- und Meldepflichten** haben damit ein verlässlicher Informationsaustausch zur IT-Sicherheitslage möglich ist. Laufende Frühwarnungen und koordinierte Reaktionen gegenüber den betroffenen Unternehmen sind essenziell. Damit kann ergänzend zur Veröffentlichung gegenüber der Allgemeinheit das besondere Informationsinteresse der Betreiber wesentlicher Dienste sichergestellt und ihre eigenverantwortliche Bewertung von relevanten Informationen (auch von anderen Branchen) gestärkt werden.

Die zuständigen nationalen Behörden sollten eine koordinierende Funktion einnehmen, um **aggregierte und anonymisierte Meldungen** an die zuständigen Behörden anderer Mitgliedstaaten weiterzuleiten und die Benachrichtigung in der gesamten EU zeitnah zu gewährleisten. Darüber hinaus sollten die nationalen IT-Lagezentren einen besseren Informationsaustausch über Vorfälle und bewährte Praktiken koordinieren. Der BDEW spricht sich aus diesen Gründen für umfangreiche **Informations- und Meldepflichten der nationalen Behörden** gegenüber den betroffenen Unternehmen aus.

Ergänzend schlägt die Kommission vor, ein europäisches Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe) einzurichten, um die Mitgliedsstaaten im **koordinierten Management massiver Cybersicherheitsvorfälle und -krisen** zu unterstützen sowie um einen regelmäßigen Informationsaustausch zwischen den Mitgliedsstaaten und den Einrichtungen der Union zu gewährleisten. Der BDEW begrüßt dieses Vorhaben, da im Falle groß angelegter, grenzüberschreitender Cybersicherheitsvorfälle eine zeitnahe und effektive Koordination zwischen Mitgliedsstaaten und den Einrichtungen der Union sichergestellt sein muss.

Der BDEW begrüßt ausdrücklich, dass die Mitgliedsstaaten angehalten werden sollen, die nationalen Fähigkeiten zur **operativen Behebung von IT-Sicherheitsvorfällen** weiter zu stärken (Artikel 9 und 13). Diesbezüglich konkretisiert die Kommission die Anforderungen an den Aufbau, die Ausstattung, die Aufgaben und die zugrundeliegenden Verfahren von nationalen Reaktionsteams für IT-Sicherheitsvorfälle, um ein einheitlicheres Niveau in der Union sicherzustellen.

Es ist folgerichtig, dass die Handlungsfähigkeit und Zuverlässigkeit der nationalen CSIRTs weiter gestärkt werden sollen, um auf diesem Weg die operative Zusammenarbeit zwischen den einzelnen Mitgliedstaaten zu vertiefen.

Aus unserer Sicht könnten folgende Maßnahmen einen wesentlichen Beitrag leisten:

- Die Einführung von nationalen und europäischen Bildungs- und Weiterbildungsprogrammen für IT-Sicherheitsexperten, um Fachkräfte im Einsatz bei Betreibern wesentlicher Dienste angemessen auszubilden.
- Die Cyberabwehrfähigkeiten der CSIRTs gegen sogenannte fortgeschrittene, andauernde Sicherheitsbedrohungen (Advanced Persistent Threats) aufgrund komplexer, zielgerichteter und effektiver Angriffe auf kritische IT-Infrastrukturen und vertrauliche Daten von Behörden, Groß- und Mittelstandsunternehmen zu erhöhen.
- Die Verbesserung der Informationsweitergabe aus den anderen Mitgliedstaten an die Betreiber wesentlicher Dienste im eigenen Land. Die Betreiber wesentlicher Dienste erhalten

zurzeit kaum bis keine Informationen von den nationalen Sicherheitsbehörden über Vorfälle aus anderen europäischen Ländern. Es wäre begrüßenswert, wenn das CSIRT das gesammelte Knowhow aus der Praxis schnell, kompakt und einfach an das CERT und damit auch an andere Bedarfsträger weiterreichen könnte.

7 Rechtsinstrument und Rechtswirkung (Artikel 1)

Wir befürworten allgemeine EU-weite Sicherheitsanforderungen, die den Mitgliedstaaten und den Betreibern Kritischer Infrastrukturen Spielräume ermöglichen, um Sicherheitsmaßnahmen gemäß dem Ansatz der Subsidiarität und der Verhältnismäßigkeit umzusetzen. Aus diesem Grund begrüßen wir die Entscheidung der Kommission, ihren Vorschlag in Form einer Richtlinie vorzulegen.

Dies sollte vom Europäischen Parlament und Rat der EU unterstützt werden. Zur Rechtswirkung vertritt der BDEW die Ansicht, dass die Kommission mit dem vorliegenden Vorschlag die Pflichten von Unternehmen weiter anpasst und innerhalb der Union stärker harmonisiert. Zugleich soll der Vorschlag den Mitgliedstaaten die erforderliche Flexibilität einräumen, besondere nationale und sektorspezifische Gegebenheiten zu berücksichtigen, indem er z. B. die Möglichkeit vorsieht, über den im Rechtsakt festgelegten Ausgangswert hinaus zusätzliche wesentliche oder wichtige Einrichtungen zu ermitteln. Dies ist zu begrüßen. Aus Sicht der Energie- und Wasserwirtschaft wird dieses sinnvolle Maß an Flexibilität jedoch gleichzeitig durch eine sehr umfassende Ausweitung des Anwendungsbereichs konterkariert, indem der Großteil der Unternehmen eines jeweiligen Sektors erfasst werden soll, unabhängig von deren Bedeutung für die Versorgung der Allgemeinheit.

Ansprechpartner

Christina Christopoulou
Brüsseler EU-Vertretung
Telefon: +32 2 774 5119
christina.christopoulou@bdew.de

Yassin Bendjebbour
Berliner Hauptgeschäftsstelle
Telefon: +49 30 300199-1526
yassin.bendjebbour@bdew.de

Johannes Imminger
Brüsseler EU-Vertretung
Telefon: +32 2 774 5114
johannes.imminger@bdew.de