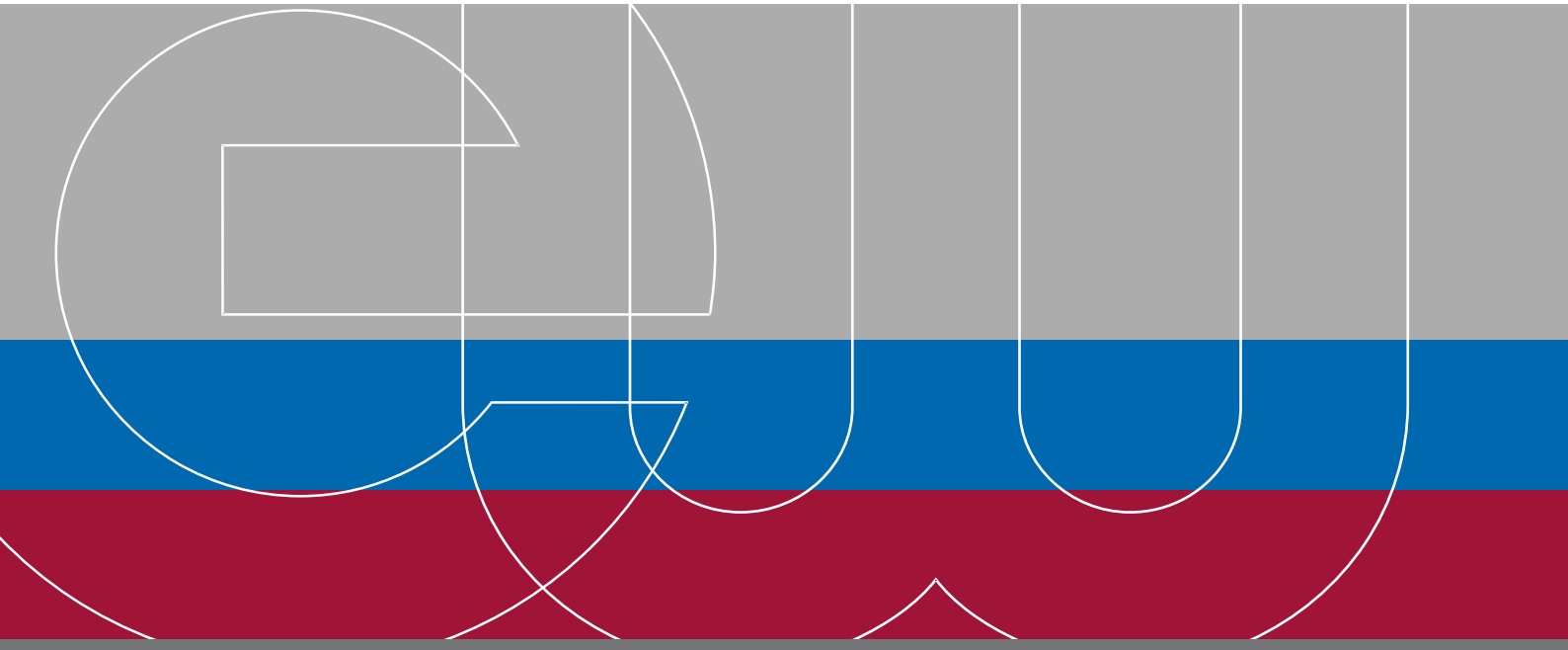
BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.
Reinhardtstraße 32
10117 Berlin

Stellungnahme

Verordnungsvorschlag der EU-Kommission zur ENISA („Cybersecurity Act“)

Vorschlag für eine Verordnung über die „EU-Cybersicherheitsagentur“ (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (2017/0225 (COD))

Berlin, 15. Januar 2018
Transparenz-Register ID: 20457441380-38



Executive Summary

Der Bundesverband der Energie- und Wasserwirtschaft (BDEW) vertritt Betreiber Kritischer Infrastrukturen bzw. Betreiber wesentlicher Dienste im Sinne der Richtlinie (EU) 2016/1148 (NIS-Richtlinie) in den Sektoren Energie und Wasser / Abwasser.

Die Verfügbarkeit von Kritischen Infrastrukturen ist eine zentrale Voraussetzung für das Vertrauen von Bürgern und das Funktionieren von Wirtschaft, Staat und Gesellschaft. Ein effektiver Schutz Kritischer Infrastrukturen kann nur mit einer funktionierenden Partnerschaft zwischen staatlichen Institutionen und mehrheitlich privatwirtschaftlich oder kommunal organisierten Betreibern Kritischer Infrastrukturen gelingen. Dabei müssen Zuständigkeiten sowohl auf europäischer Ebene als auch auf Ebene der Mitgliedsstaaten klar geregelt, und gemeinsame Strategien und Standards abgestimmt sein.

Die Ziele der EU-Kommission, mit dem vorliegenden Verordnungsentwurf die Cyber- und IT-Sicherheit in den Mitgliedsstaaten sowie die Zusammenarbeit in diesem Kontext zu verbessern sind erkennbar. Aus Sicht des BDEW sollten folgende Kernforderungen jedoch noch in den Verordnungsentwurf aufgenommen bzw. im weiteren Gesetzgebungsprozess berücksichtigt werden:

1. Klare Abgrenzung der Kompetenzen zwischen ENISA und nationalen Behörden: Umsetzung der NIS-Richtlinie ist Angelegenheit der Mitgliedsstaaten
2. Offene und transparente Entwicklung des geplanten europäischen Zertifizierungs- und Kennzeichnungsrahmens: Beteiligung der Mitgliedsstaaten sowie der europäischen Normungsorganisationen CEN, CEN ELEC und ETSI
3. Sicherstellung der Kompatibilität zu bestehenden Systemen bei der Vereinheitlichung unterschiedlicher Zertifizierungsschemata
4. Verbesserte Konsistenz und deutlichere Abgrenzung zwischen Legislativvorschlägen zur Cybersicherheit (z.B. NIS-Richtlinie, Cybersecurity Act), Authentifizierung (z.B. eIDAS Verordnung) und Datenschutz (z.B. Datenschutzgrundverordnung, ePrivacy Verordnung)

1 Einleitung

Der Bundesverband der Energie- und Wasserwirtschaft (BDEW) vertritt Betreiber Kritischer Infrastrukturen bzw. Betreiber wesentlicher Dienste im Sinne der NIS-Richtlinie in den Sektoren Energie und Wasser / Abwasser. Insgesamt vertritt der BDEW über 1.800 Unternehmen. Das Spektrum der Mitglieder reicht von lokalen und kommunalen über regionalen bis hin zu überregionalen Unternehmen. Sie repräsentieren rund 90% des Stromabsatzes, gut 60% des Nah- und Fernwärmeabsatzes, 90% des Erdgasabsatzes sowie 80% der Trinkwasser-Förderung und rund ein Drittel der Abwasser-Entsorgung in Deutschland.

Die Europäische Kommission hat am 13. September 2017 ein Maßnahmenpaket zur Cybersicherheit veröffentlicht. Das Paket enthält unter anderem eine neue EU-Cybersicherheitsstrategie, einen Verordnungsvorschlag zur Überprüfung der Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA), und eine Mitteilung zum Umsetzungsstand der NIS-Richtlinie. Der Verordnungsvorschlag wurde am 4. Oktober 2017 korrigiert.

Mit dem nun veröffentlichten Maßnahmenpaket der EU-Kommission soll die Sicherheitsarchitektur für den digitalen Raum in der EU auf einen neuen Stand gebracht werden. Das ist wichtig, denn die Anforderungen an die IT-Sicherheit wachsen mit der zunehmenden Digitalisierung sowie einer immer dezentraler werdenden Energiewende immer weiter. Die Verfügbarkeit von Kritischen Infrastrukturen ist eine zentrale Voraussetzung für das Vertrauen von Bürgern und das Funktionieren von Wirtschaft, Staat und Gesellschaft. Viele Vorteile der Digitalisierung können nur effektiv genutzt werden, wenn ein entsprechendes gemeinsames Sicherheitsniveau sowohl auf Prozessebene als auch bei Produkten und Dienstleistungen und zwischen den EU-Mitgliedsstaaten etabliert sind.

Zudem wird dafür eine funktionierende Partnerschaft zwischen staatlichen Institutionen und mehrheitlich privatwirtschaftlich oder kommunal organisierten Betreibern Kritischer Infrastrukturen benötigt. Dabei müssen Zuständigkeiten sowohl auf europäischer Ebene als auch auf Ebene der Mitgliedsstaaten klar geregelt, und gemeinsame Strategien und Standards abgestimmt sein.

Mit der EU-Richtlinie zur Erhöhung der Netz- und Informationssicherheit ist zwar die Richtung für gemeinsame Standards und eine verstärkte Zusammenarbeit zwischen EU-Ländern vorgegeben, die Umsetzung in den Mitgliedsstaaten ist jedoch aktuell sehr unterschiedlich. Es bleibt daher weiterhin von hoher Priorität, die NIS-Richtlinie in der EU konsistent auszugestalten und dabei sicherzustellen, dass die Mitgliedsstaaten für die jeweilige Umsetzung in nationales Recht zuständig bleiben.

2 Positionen im Einzelnen

Folgende weitergehenden Erläuterungen zu den bereits genannten Kernforderungen sollten aus Sicht des BDEW noch in den Verordnungsentwurf aufgenommen bzw. im weiteren Gesetzgebungsprozess berücksichtigt werden:

2.1 Klare Abgrenzung der Kompetenzen zwischen ENISA und nationalen Behörden: Umsetzung der NIS-Richtlinie ist Angelegenheit der Mitgliedsstaaten

Eine Stärkung des Mandats der ENISA insbesondere im Bereich der Unterstützung von Mitgliedsstaaten bei der Umsetzung der NIS-Richtlinie darf nicht zu einem Kompetenzgerangel zwischen der ENISA und nationalen Behörden oder zu unklaren Ansprechpartnern für Betreiber Kritischer Infrastrukturen führen.

Die Umsetzung der NIS-Richtlinie, insbesondere im Bereich der IT-Sicherheitsmindeststandards sowie der Meldung von Sicherheitsvorfällen nach Artikel 14 der NIS-Richtlinie ist Angelegenheit der Mitgliedsstaaten. Für Betreiber Kritischer Infrastrukturen muss der primäre Ansprechpartner daher die jeweils zuständige nationale Behörde sein und bleiben. Eine verstärkte Zusammenarbeit der Mitgliedsstaaten kann anschließend – unterstützt durch die ENISA – kaskadisch und gesteuert durch die jeweils zuständigen nationalen Behörden erfolgen.

Weiterhin ist aus Sicht des BDEW an geeigneter Stelle festzulegen, wie die ENISA oder das CSIRT-Netzwerk bei einem Informationsaustausch zu Sicherheitsvorfällen mit grenzübergreifenden Auswirkungen die Vertraulichkeit der auszutauschenden sicherheitsrelevanten Daten zu gewährleisten haben.

2.2 Offene und transparente Entwicklung des geplanten europäischen Zertifizierungs- und Kennzeichnungsrahmens: Beteiligung der Mitgliedsstaaten sowie der europäischen Normungsorganisationen CEN, CEN ELEC und ETSI

Ein gemeinsamer europäischer Zertifizierungs- und Kennzeichnungsrahmen für Cybersicherheit kann zum Schutz der Bürger und Unternehmen beitragen. Dies muss jedoch zwingend offen und transparent, und unter Beteiligung der Mitgliedsstaaten sowie der europäischen Normungsorganisationen **CEN, CEN ELEC und ETSI** erfolgen.

Insbesondere kritisiert der BDEW, dass die Entscheidungsbefugnis, welche neuen Schemata erforderlich sind, ausschließlich bei der EU-Kommission liegen soll. Es ist keine Befassung der Mitgliedsstaaten, des Europäischen Rates, des EU Parlaments, nationaler Normenorganisationen, Verbände oder der Industrie geplant. Den Mitgliedsstaaten sowie der neu einzurichtenden „Cybersecurity Certification Group“ soll ferner lediglich ein Vorschlagsrecht zustehen. Der alleinige Hinweis, dass die Schemata zunächst freiwillig angewendet werden sollen, kann diesen Mangel nicht ausgleichen.

Ferner dürfen aus Sicht des BDEW insbesondere für Betreiber essenzieller Dienste keine Zertifizierungsvorgaben oder Vorgaben zur Nutzung zertifizierter Produkte gemacht werden, wenn nicht zuvor die Eignung und Anwendbarkeit qualifiziert geprüft wurden. Dies kann nur unter Einbeziehung der für die jeweiligen Anwendungsfälle zuständigen Standardisierungs-

gremien in den Mitgliedsstaaten sowie in den europäischen Normungsorganisationen CEN, CEN ELEC und ETSI erfolgen.

2.3 Sicherstellung der Kompatibilität zu bestehenden Systemen bei der Vereinheitlichung von unterschiedlichen Zertifizierungsschemata

Das geplante Kennzeichnungs- und Zertifizierungsrahmenwerk sollte ferner bestehende Anforderungen und verbreitete Normen im Bereich der Informationssicherheit berücksichtigen und eine Kompatibilität zu diesen sicherstellen. Dies beinhaltet unter anderem die ISO 2700x Reihe sowie spezifische Standards wie die ISO/IEC 27019 für den Sektor Energie oder die IEC 62443 für industrielle Kommunikationsnetze.

Daneben müssen aus Sicht des BDEW auch in den Mitgliedsstaaten bereits gesetzlich oder regulatorisch vorgegebene Anforderungen betrachtet werden. Im Zuge der Umsetzung des Artikels 14 der NIS-Richtlinie sind in Deutschland beispielsweise mit dem IT-Sicherheitskatalog nach § 11 Abs. 1a EnWG durch die zuständige Regulierungsbehörde bereits verpflichtende Zertifizierungen im Sektor Energie vorgesehen. In einigen anderen Sektoren wie z.B. Wasser/Abwasser existieren bereits branchenspezifische Sicherheitsstandards, die ebenfalls bereits umgesetzt werden und somit beachtet werden sollten.

In Deutschland treibt darüber hinaus beispielsweise das Deutsche Institut für Normung (DIN) über die Projekte „IoT Security“ und „Sichere Identitäten“ die Arbeiten im Industriebereich voran. Sektorspezifische Standardisierung im Bereich IT-Sicherheit wird z.B. auch im DKE (Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE) bereits seit mehreren Jahren erfolgreich vorangetrieben. IT-Sicherheit betrifft nicht ausschließlich den Digitalbinnenmarkt, sondern auch die Mitgliedsstaaten, dies gilt insbesondere bei Fragen von Sicherheitsstandards und Zertifizierungen.

Für eine Analyse auf EU-Ebene, welche Standards bereits bestehen und welche Vorarbeiten bereits geleistet wurden, sollte weiterhin auch das Know-How der Cybersecurity Coordination Group (CSCG) bei CEN/CENELEC eingebunden werden, um mögliche Ineffizienzen und Dopplungen effektiv vermeiden zu können.

2.4 Verbesserte Konsistenz und deutlichere Abgrenzung zwischen Legislativvorschlägen zur Cybersicherheit (z.B. NIS-Richtlinie, Cybersecurity Act), Authentifizierung (z.B. eIDAS Verordnung) und Datenschutz (z.B. Datenschutzgrundverordnung, ePrivacy Verordnung)

Im Zuge zunehmender Digitalisierung in Wirtschaft, Staat und Gesellschaft und der damit einhergehenden technischen Weiterentwicklungen und gesellschaftlichen Realitäten steigen die Anforderungen in den Bereichen Cyber- und IT-Sicherheit, Authentifizierung und Datenschutz rasant an. Auch wenn in diesen Bereichen Schnittmengen und Synergiepotenziale bestehen, ist es aus Sicht des BDEW empfehlenswert, in gemeinsam betroffenen Bereichen konsistentere Anforderungen zu stellen, und an anderer Stelle auf eine deutlichere Abgrenzung zu achten. Hierzu kann auch eine verstärkte Zusammenarbeit und Abstimmung zwischen den beteiligten Generaldirektionen DG CONNECT, DG GROW, DG HOME, DG ENERGY, etc. beitragen.