Energie. Wasser. Leben.

Berlin, 12. Mai 2026

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

Stellungnahme

Cybersecurity Act (CSA) 2

Versionsnummer: final

Inhalt

1 Kernaussagen des BDEW 3

2 ENISA stärken und Meldewege vereinheitlichen 3

3 ICT-Lieferkettensicherheit risikobasiert und resilienzorientiert ausgestalten 3

5 Bestehende EU-Cyberregulierung besser aufeinander abstimmen 6

6 Mögliche sektorbezogene Vollharmonisierung durch EU-Durchführungsrechtsakte 7

7 Fazit 8

1 Kernaussagen des BDEW

Der Bundesverband der Energie- und Wasserwirtschaft (BDEW) unterstützt die Überarbeitung des Cybersecurity Acts (CSA) im Rahmen des Legislativvorschlags für den CSA 2 vom 20. Januar 2026. Ziel der EU-Kommission ist es, die Cybersicherheitskapazitäten und die Widerstandsfähigkeit zu stärken und eine Fragmentierung des digitalen Binnenmarktes der EU zu verhindern.

Entscheidend ist ein kohärenter, risikobasierter und praxistauglicher europäischer Rahmen, der Resilienz stärkt, neue operative Risiken, Doppelregulierung und unnötige Bürokratie vermeidet und die betrieblichen Realitäten kritischer Infrastrukturen berücksichtigt. Entscheidend ist, dass CSA 2 die Resilienz tatsächlich erhöht, ohne durch zusätzliche Komplexität oder praxisferne Anforderungen neue Belastungen zu erzeugen.

2 ENISA stärken und Meldewege vereinheitlichen

Position: Angesichts der verschärften Cyberbedrohungslage braucht Europa eine leistungsfähige Agentur, die grenzüberschreitende Lagebilder erstellt, Risiken frühzeitig erkennt und relevante Informationen schnell an betroffene Einrichtungen weitergibt.

Der BDEW fordert:

- Keine zusätzlichen Mehraufwände oder Parallelstrukturen bei Meldewegen zu schaffen.
- Sichere Übertragungswege und eine verlässliche Datenverwahrung sicherzustellen.
- Aus Meldungen und Lagebildern einen konkreten operativen Mehrwert für Unternehmen abzuleiten.

Einordnung: Belastbare Lagebilder mit operationalisierbaren Informationen für Betreiber (z. B. *Indicators of Compromise* oder Handlungsempfehlungen), klare Schwellenwerte und funktionierende Rückkanäle sind für Unternehmen der Energie- und Wasserwirtschaft zentral. Ein einheitlicher europäischer Meldeansatz kann Resilienz stärken und Bürokratie abbauen, sofern der Informationsfluss bidirektional ausgestaltet wird.

3 ICT-Lieferkettensicherheit risikobasiert und resilienzorientiert ausgestalten

Position: Der BDEW unterstützt das Ziel, die Sicherheit europäischer ICT-Lieferketten zu erhöhen. In der Energie- und Wasserwirtschaft sind Integrität, Verfügbarkeit und Beherrschbarkeit

eingesetzter Komponenten und Systeme von zentraler Bedeutung. Mit dem „ICT Supply Chain Framework“ im Rahmen des CSA 2 ergeben sich für die Beschaffung von Komponenten in der Energiewirtschaft als Teil der kritischen NIS-2-Sektoren jedoch teilweise tiefgreifende Veränderungen, im Wesentlichen durch die Verschiebung von kostengetrieben zu sicherheits- und geopolitikgetrieben. Zusätzlich gibt es im Rahmen nationaler Gesetzgebung schon weitreichende Regelungen für den Einsatz von kritischen Komponenten, insbesondere im Energiewirtschaftsgesetz (EnWG) in Verbindung mit dem BSI-Gesetz. Hier muss eine Dopplung unbedingt vermieden werden.

Der BDEW fordert:

- Regulatorische Anforderungen so auszugestalten, dass sie Resilienz stärken und nicht durch abrupte Austauschpflichten, überkomplexe Verfahren oder realitätsferne Fristen neue Risiken erzeugen.
- Falls ein Verbot für bereits verbaute Technik ergeht, die von ihrem Lebenszyklus her noch nicht ersetzt werden müsste, bedarf es einer Entschädigung für frustrierte Investitionen.
- Mögliche Verbote wirken sich auch massiv auf Verhandlungspositionen gegenüber anderen Ausrüstern aus. Wenn der Gesetzgeber – aus öffentlichen Sicherheitsinteressen – bestimmte Komponenten/Ausrüster verbietet, muss er gleichzeitig auch Möglichkeiten für die heimische Wirtschaft unterstützen, Komponenten mit vergleichbarer Leistungsfähigkeit (und zu vergleichbaren Preisen) innerhalb der EU herstellen zu können.
- Gerade in langzyklischen OT-Infrastrukturen ausreichende Planbarkeit, realistische Übergangszeiträume und betriebliche Kontinuität sicherzustellen. Rückwirkende Forderungen schaden der Planungssicherheit.
- Risiken sind differenziert zu betrachten und nicht allein auf Herstellerebene zu verengen, sondern Hersteller-, Produkt- und Systemrisiken jeweils eigenständig zu bewerten; dabei müssen auch Wechselwirkungen in der Integration, die technische Beherrschbarkeit im Betrieb sowie die Auswirkungen auf Stabilität und Sicherheit bestehender Infrastrukturen berücksichtigt werden. Dabei sollten auch die Auswirkungen von Datenflüssen und Cloud-Lösungen Berücksichtigung finden.
- Resilienzanforderungen so auszugestalten, dass realistische Transformationspfade und die tatsächliche Umsetzbarkeit in komplexen Bestandsumgebungen mitgedacht werden.
- Kohärenz mit anderer sektoraler Regulierung mit ähnlicher Zielsetzung, insbesondere dem Industrial Accelerator Act (IAA) und hierin enthaltene Änderungsvorschläge am Net Zero Industry Act (NZIA), dem Critical Raw Materials Act (CRMA), dem AI Act

(insbesondere bezüglich „Toxic AI“) sowie den nationalen Vorgaben an kritische Komponenten gemäß Energiewirtschaftsgesetz in Verbindung mit BSI-Gesetz herzustellen.

Einordnung: Gerade in komplexen Migrationsumgebungen können kurzfristige regulatorische Eingriffe erhebliche betriebliche Risiken auslösen. Die Regulierung sollte deshalb Versorgungssicherheit und technische Umsetzbarkeit von Beginn an mitdenken.

4 Zertifizierungsrahmen beschleunigen und praxistauglich gestalten

Position: Der europäische Zertifizierungsrahmen sollte Sicherheitsanforderungen transparent machen, Vertrauen stärken und regulatorische Nachweispflichten effizienter erfüllen. Voraussetzung ist jedoch, dass (Sicherheits-)Zertifizierung in der Praxis anwendbar, wirtschaftlich und zuverlässig sind. Aus Sicht der Unternehmen ist entscheidend, dass Zertifizierungsanforderungen mit bestehenden Betriebs- und Instandhaltungsprozessen kompatibel ausgestaltet werden. Eine mangelnde Abstimmung mit etablierten Update- und Wartungszyklen führt insbesondere bei Altsystemen sowie in Märkten mit geringer Anbieterdiversität zu erheblichen Umsetzungsrisiken. Zertifizierungsvorgaben sollten daher die tatsächlichen technischen, wirtschaftlichen und marktstrukturellen Rahmenbedingungen stärker berücksichtigen.

Der BDEW fordert:

- Zertifizierungsschemata transparenter und stärker an internationalen Standards ausrichten.
- Zertifikate unionsweit als belastbaren Nachweis anzuerkennen, um Mehrfachprüfungen zu vermeiden und Marktabschottung durch nationale Sicherheitsanforderungen und Zertifizierungsverfahren zu unterbinden.
- Kosten und Dokumentationsaufwand auf ein wirtschaftliches und verhältnismäßiges Maß zu begrenzen.
- Rezertifizierungs- und Updateprozesse innovationsfreundlich auszugestalten.
- Bedachte Änderungen und kontinuierliche Verbesserung an Zertifizierungsanforderungen mit ausreichender Planbarkeit und angemessenen Übergangsfristen so auszugestalten, dass sie in bestehende Betriebs-, Update- integriert werden können (da jede Änderung Aufwand und Anpassung im Sicherheitsmodel bedeute) und größeren Änderungen an den Rezertifizierungszyklen orientieren.

Einordnung: Die Erfahrungen aus dem Smart-Meter-Umfeld in Deutschland zeigen, dass langwierige und komplexe Zertifizierungsprozesse Innovation und Umsetzung erheblich bremsen können. Zugleich sollten Zertifizierungsvorgaben ausreichend risikoorientiert und praxisnah bleiben; übermäßig detaillierte Verfahrensvorgaben schränken betriebliche Flexibilität ein und erhöhen den Aufwand. Ein einheitlicherer europäischer Rahmen sollte zudem die gegenseitige

Anerkennung von Sicherheitsnachweisen stärken und damit Nachweisverfahren über Ländergrenzen hinaus vereinfachen.

5 Bestehende EU-Cyberregulierung besser aufeinander abstimmen

Position: Der CSA 2 sollte eng mit der NIS2-Richtlinie, der DORA-Verordnung (Digital Operational Resilience Act), dem Cyber Resilience Act (CRA) und weiteren sektorspezifischen Vorgaben abgestimmt werden. Für Unternehmen der Energie- und Wasserwirtschaft ist ein kohärenter und widerspruchsfreier Rechtsrahmen von zentraler Bedeutung.

Der BDEW fordert:

- Europäische Cybervorgaben konsequent aufeinander abzustimmen und bewährte nationale sowie sektorale Umsetzungswege nur dann zu verändern, wenn hierdurch ein klarer Mehrwert für Cybersicherheit, Resilienz und Rechtsklarheit erreicht wird.
- Doppelregulierungen und Mehrfachnachweise zu vermeiden.
- Sektorspezifische Besonderheiten und die Realität von Mehrspartenunternehmen angemessen zu berücksichtigen, zu vereinheitlichen und zu harmonisieren.
- Für Mehrspartenunternehmen auf europäischer Ebene praktikable Sonderregelungen oder geeignete Öffnungsklauseln vorzusehen.
- Zusätzliche nationale Verschärfungen möglichst zu vermeiden oder zumindest eine nationale Anerkennung durch einheitliche Standardvorgaben zu erwirken.
- Risikobasierte und sektorspezifisch anschlussfähige Anforderungen zu fördern, die bestehende Schutzgüter und Betriebsrealitäten kritischer Infrastrukturen angemessen berücksichtigen.

Besonderer Handlungsbedarf bei Mehrspartenunternehmen

Die geplante Anpassung der NIS2-Anlagen im Bereich der Stromerzeugung kann erhebliche Folgen für Unternehmen haben, die nur in untergeordnetem Umfang Energie erzeugen, deren Haupttätigkeit aber in einem anderen Bereich liegt. Konkret schlägt die EU-Kommission in ihrem Legislativvorschlag für eine Richtlinie zur Anpassung der NIS2-Richtlinie und zur Anpassung an den CSA 2 (COM (2026) 13 final) im Annex 1 vor, dass Erzeuger mit einer Erzeugungsmenge kleiner/gleich 1MW vom Anwendungsbereich der NIS2 ausgenommen sein sollen. Dies steht allerdings im Widerspruch zu bisherigen Ausnahmen im Rahmen der deutschen Umsetzung der NIS2 Richtlinie (siehe § 28 Abs. 3 und Abs. 4 BSIG). Werden europäische Sonderregelungen enger gefasst, drohen neue Rechtsunsicherheiten und zusätzlicher Regulierungsaufwand. Bewährte nationale Abgrenzungen für Nebentätigkeiten und

vernachlässigbare Tätigkeiten sollten daher nicht ohne erkennbaren Sicherheitsmehrwert verloren gehen.

Einordnung: In regulierten Infrastruktursektoren bestehen bereits differenzierte Nachweis-, Prüf- und Sicherheitsstrukturen, die an die jeweiligen Betriebsrealitäten angepasst sind. Neue europäische Vorgaben sollten diese Strukturen aufgreifen und anschlussfähig ausgestalten, statt zusätzliche Parallelregime oder unnötige Umstellungsaufwände zu erzeugen.

6 Mögliche sektorbezogene Vollharmonisierung durch EU-Durchführungsrechtsakte

Position: Mit dem vorgeschlagenen neuen Artikel 5 NIS2 in Verbindung mit Artikel 21 Absatz 5 erhält die Kommission die Möglichkeit, technische, methodische und sektorspezifische Cybersicherheitsanforderungen künftig unionsweit per Durchführungsrechtsakt zu harmonisieren. Für die Energie- und Wasserwirtschaft ist dies von erheblicher Bedeutung.

Der BDEW fordert:

- Etwaige sektorspezifische Durchführungsrechtsakte nur unter enger Einbindung der betroffenen Sektoren zu erlassen.
- Praxistaugliche Übergangsfristen und die Berücksichtigung bestehender sektoraler Besonderheiten, insbesondere langzyklischer OT-Infrastrukturen und hoher Resilienzerfordernisse, sicherzustellen.
- Bei vollharmonisierender Wirkung Umstellungsaufwände, Migrationsrisiken und Wechselwirkungen mit bestehenden nationalen Regelungen frühzeitig zu berücksichtigen und neue europäische Vorgaben nur bei erkennbarem Mehrwert in bestehende Sicherheitsregime eingreifen zu lassen.

Einordnung: Der Vorschlag enthält noch keine sektorspezifischen Vorgaben für den Energiesektor, eröffnet der Kommission aber ausdrücklich die Möglichkeit, solche Vorgaben künftig zu erlassen. Aufgrund der grenzüberschreitenden Relevanz des Energiesektors ist eine spätere unionsweite Konkretisierung der NIS2-Risikomanagementmaßnahmen nicht ausgeschlossen.

7 Fazit

Der CSA 2 bietet die Chance, den europäischen Cyberrahmen wirksamer, kohärenter und praxistauglicher auszugestalten. Aus Sicht des BDEW kommt es darauf an, die Resilienz kritischer Infrastrukturen gezielt zu stärken, ohne neue operative Risiken oder unnötige Bürokratie zu erzeugen. Entscheidend ist dabei ein klarer Mehrwert für die betroffenen Unternehmen, eine risikobasierte Regulierung und ein Rahmen, der technische Realität, Versorgungssicherheit und betriebliche Umsetzbarkeit angemessen berücksichtigt.