Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall e. V.
German Association for Water, Wastewater and Waste

01.04.2026

Stellungnahme

zum

Referentenentwurf eines Gesetzes zur Durchführung der Verordnung (EU) 2024/2847 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen (Cyberresilienz-Verordnung)
(Stand: 12.03.2026**)**

Das Bundesministerium des Innern hat einen Referentenentwurf für ein Gesetz zur Durchführung der Verordnung, (EU) 2024/2847, über horizontale Cybersicherheits-anforderungen für Produkte mit digitalen Elementen (Cyberresilienz-Verordnung) vorgelegt. Mit dem Entwurf werden drei verschiedene Gesetze und Verordnungen u.a. BSI-Gesetz (BSIG), Telekommunikationsgesetz, Energiewirtschaftsgesetz novelliert.

Zusammenfassende Bewertung:

Die DWA begrüßt es, dass besonders wichtige Unternehmen und wichtige Unternehmen nicht das gleiche Schutzniveau wie Betreiber Kritischer Anlagen in deren Anlagen-Scope einhalten sollen. Diese Abstufung des Sicherheitsniveaus wurde schon im Branchenstandard Wasser/Abwasser vorgesehen. Hierdurch können, dem jeweiligen Risiko entsprechend, angemessene Sicherheitsmaßnahmen implementieren werden.

Die DWA ist kein Branchenverband im klassischen Sinne, sieht sich aber nach dem Sinn und Zweck des Gesetzentwurfes als Branchenverband nach dem NIS2UmsuCG. Einige Kommentare und Verbesserungsvorschläge möchten wir mit den nachfolgenden Kernforderungen geben.

Kernpunkte:

Zu Teil 8 § 65, § 66 sowie Teil 2 § 5 Absatz 3 Satz 5 (Rolle des BSI):

Die vorgesehene Bündelung der Aufgaben der Marktüberwachung, der notifizierenden und akkreditierenden Stelle sowie der CSIRT Funktion beim BSI ist grundsätzlich sachgerecht und stärkt die zentrale Steuerung der Cybersicherheit. Voraussetzung für eine wirksame und rechtssichere Umsetzung ist jedoch eine klare organisatorische und funktionale Trennung der einzelnen Rollen sowie eine angemessene personelle und fachliche Ausstattung, um Interessenkonflikte, Vollzugsdefizite und Verzögerungen zu vermeiden.

Zur praktischen Umsetzbarkeit für KRITIS Betreiber:

Die Ausgestaltung der Informations- und Meldeprozesse muss sich an der operativen Realität von KRITIS Betreibern orientieren. Insbesondere ist sicherzustellen, dass Informationen zu relevanten Schwachstellen priorisiert, zielgerichtet und zeitnah

bereitgestellt werden und keine unverhältnismäßige Mehrbelastung durch eine Vielzahl paralleler oder wenig relevanter Meldungen entsteht.

Zur Abgrenzung gegenüber bestehenden Regelwerken (u. a. NIS2, BSIG):

Zur Vermeidung von Doppelmeldungen und redundanten Verfahren ist eine klare Abgrenzung sowie eine kohärente Verzahnung der Pflichten nach CRA mit bestehenden Melde- und Nachweispflichten nach NIS2 und dem BSIG erforderlich. Ziel muss ein möglichst einheitlicher, konsolidierter Meldeweg sein.

Zu Beschaffung, Bestandsanlagen und Lieferketten (§ 65 Abs. 1 BSIG-E):

Der CRA sollte konkrete und praxistaugliche Vorgaben für die Beschaffung sicherer Produkte, den Umgang mit bestehenden Legacy und OT Systemen sowie für die Bewertung und Steuerung komplexer Lieferketten enthalten, um Planungssicherheit und Umsetzbarkeit insbesondere in kritischen Infrastrukturen zu gewährleisten.

OT-spezifische Einsatzbedingungen in der Marktüberwachung berücksichtigen (Produktlebenszyklen von 15 bis 25 Jahren, Echtzeit-Anforderungen, proprietäre Protokolle und Feldbus-Systeme, usw.). Insbesondere sollte die Bewertung der Konformität die tatsächlichen Einsatzbedingungen in der Prozessautomatisierung einbeziehen und nicht ausschließlich auf IT-typische Maßstäbe abstellen.

Zum Schutz sensibler KRITIS-Informationen:

Im Rahmen von Meldungen, Marktüberwachungsmaßnahmen und der behördlichen Informationsweitergabe ist dem besonderen Schutz sensibler KRITIS-Informationen Rechnung zu tragen. Dies erfordert klare Vorgaben zur Vertraulichkeit, Zweckbindung und Zugriffsbeschränkung, um zusätzliche Sicherheitsrisiken durch Offenlegung zu vermeiden.

Unterstützungsmaßnahmen und Reallabor (§ 67 BSIG-E)

Die Verankerung konkreter Unterstützungsmaßnahmen für betroffene Wirtschaftsakteure, insbesondere KMU, wird begrüßt. Die Wasserwirtschaft ist in hohem Maße von spezialisierten, oft mittelständischen Herstellern abhängig (z. B. im Bereich Mess-, Steuerungs- und Regelungstechnik, Fernwirktechnik, Prozessanalytik).

Das vorgesehene Reallabor für Cyberresilienz bietet die Möglichkeit, neue Produkte vor Inverkehrbringen in einer Prüfumgebung zu testen. Die Wasserwirtschaft verfügt über eine spezifische Systemlandschaft mit typischen Architekturmustern (ISA-95/Purdue-Modell, Feldbus-Ebene bis MES/SCADA-Ebene), die sich von anderen KRITIS-Sektoren unterscheidet.

Sektorspezifische Testszenarien für OT-Produkte der Wasserwirtschaft vorsehen z.B.:

- Prüfung der CRA-Konformität von OT-Komponenten im Zusammenspiel mit gängigen Prozessleitsystemen der Wasserwirtschaft (z. B. Siemens PCS 7/WinCC, ABB Ability Symphony Plus, Schneider Electric, usw.)
- Bewertung der Interoperabilität von Sicherheitsmechanismen über verschiedene Kommunikationsprotokolle hinweg (OPC UA, Modbus TCP, PROFINET, HART-IP)
- Validierung der „Secure-by-Default“-Konfiguration in typischen Anlagentopologien der Wasser-/Abwasserwirtschaft

Diese Hersteller stehen vor der Herausforderung, die CRA-Anforderungen in bestehende Produktentwicklungsprozesse zu integrieren. Gezielte Schulungs- und Sensibilisierungsmaßnahmen durch das BSI können dazu beitragen, die

Umsetzungsqualität zu erhöhen und Marktverzerrungen zulasten kleinerer Hersteller zu vermeiden.

Die DWA bittet um Einbindung bei der weiteren Ausgestaltung des Rechtsrahmens, insbesondere durch konkretisierende Verordnungen und bietet ihre Unterstützung an.

Hennef, den 01.04.2026

DWA
Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall e. V.
Theodor-Heuss-Allee 17
53773 Hennef
www.dwa.de

EU-Transparenzregister: 227557032517-09
Lobbyregister: R001008