bdew
Energie. Wasser. Leben.

Die Wasserwirtschaft
im BDEW

Anwendungshilfe Sicherheit und Resilienz in der Wasserwirtschaft

Dr. Jörg Rehberg
Fachgebietsleiter Geschäftsbereich Wasser und Abwasser
BDEW

Lisa Minor M.A.
Referentin der kaufm. Geschäftsführung der Stadtentwässerung Dresden
GELSENWASSER Dresden GmbH

 21.04.2026

Ausgangslage

Hybride Gefährdung kritischer Infrastrukturen nimmt spürbar zu

- Physische Sabotage- und Spionageaktionen bspw. durch Drohnenüberflüge oder mutwillige Zerstörung von Infrastrukturen
- Digitale Bedrohungen und Cyberkriminalität bspw. durch gefälschte E-Mails, Malware, Ransomware etc.
- Kommunikativ bspw. durch Desinformationskampagnen

Fortschreitende Digitalisierung birgt neue Chancen wie auch Risiken, z. B.:

- Datensicherheit durch Cloud-Computing
- Abhängigkeiten von Soft- und Hardware-Anbietern
- Nutzen von KI

Ausgangslage

„Neue“ Gesetzlichkeiten adressieren gesteigerte physische wie digitale Risiken

- **KRITIS-Dachgesetz:** Legt neue Mindestanforderungen und verpflichtendes Risikomanagement für KRITIS-Unternehmen nach dem All-Gefahren-Ansatz fest
  - In Kraft seit dem 16. März 2026
- **NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz:** Weitet das BSI-Gesetz deutlich aus und legt neue Mindestanforderungen und ein verpflichtendes Risikomanagement für IT-Sicherheit für wichtige Wirtschaftssektoren fest, darunter auch die Wasserwirtschaft
  - In Kraft seit dem 6. Dezember 2025
- **KI-Verordnung:** Legt Regeln zur Entwicklung, Einführung und Nutzung von KI für Unternehmen nach risikobasiertem Ansatz fest
  - In Kraft seit dem 12. Juli 2024

Projektgruppe Sicherheit und Resilienz

Teilnehmende Unternehmen:

- EGLV (Emschergenossenschaft und Lippeverband)
- GELSENWASSER AG
- Hessenwasser
- RWW (Rheinisch-Westfälische Wasserwerksgesellschaft mbH)
- Stadtentwässerung Dresden GmbH
- WAZV (Verbandswasserwerk Bad Langensalza/Abwasserzweckverband Mittlere Unstrut)
- Nordwasser
- Wasserwerke Zwickau

Teilnehmende Verbände/Landesgruppen:

- BDEW LG Mitteldeutschland
- BDEW LG NRW
- LDEW (Landesverband der Energie- und Wasserwirtschaft Hessen/Rheinland-Pfalz)
- VBEW (Verband der Bayerischen Energie- und Wasserwirtschaft)
- VDEW (Verband der Elektrizitätswirtschaft)
- VfEW BW (Verband für Energie- und Wasserwirtschaft Baden-Württemberg)

Anwendungshilfe Sicherheit und Resilienz

- Zielgruppe: Obere Managementebene in wasserwirtschaftlichen Versorgungsunternehmen
- Verschafft Überblick über gesetzliche Pflichten und zeigt Wege zur Beantwortung auf
- Bietet praxisrelevante Hinweise und Empfehlungen
- Ersetzt keine zertifizierbaren Managementsysteme oder Standards

Inhaltsverzeichnis

Anwendungshilfe Sicherheit und Resilienz

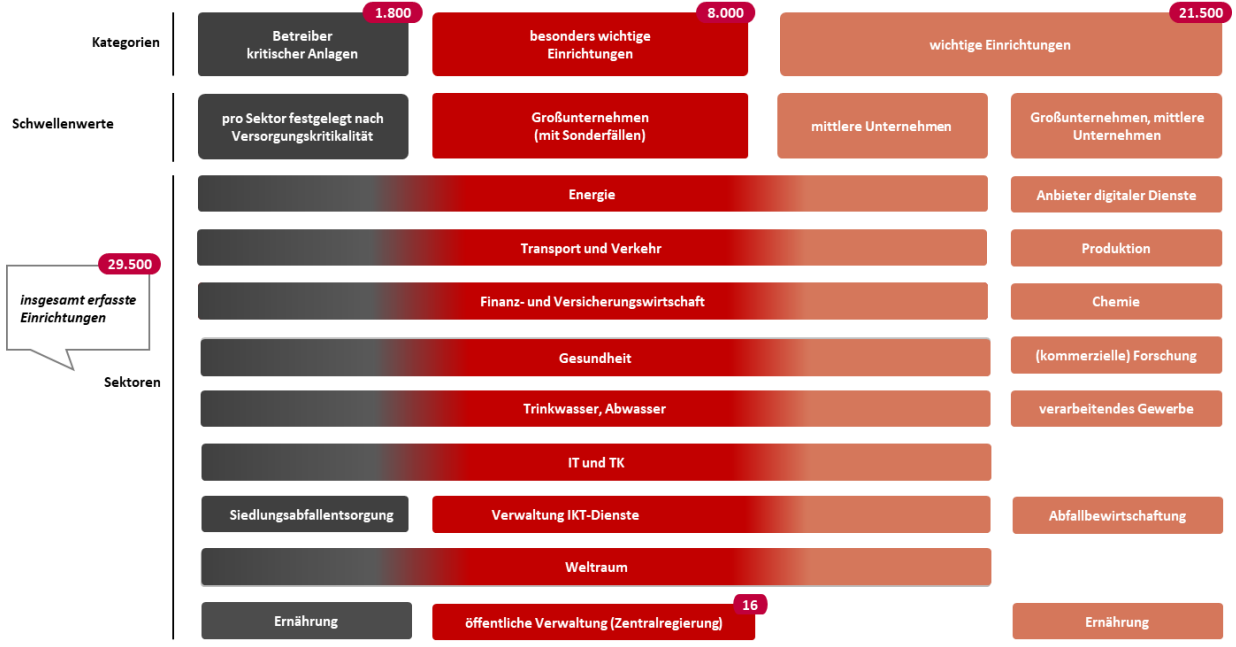
Prüfung der Betroffenheit

- Jedes Unternehmen sollte selbstständig seine Betroffenheit von beiden Gesetzen prüfen
- Eine frühzeitige Absprache mit den wesentlichen Stakeholdern kann hilfreich sein
- Grundsätzlich gilt für Betreiber von Wasserversorgungs- und Abwasserbeseitigungsanlagen:

KRITISDachG	NIS2-UG
• Ab 500.000 zu versorgenden Einwohnern*	• Ab 50 Mitarbeitenden oder Jahresumsatz sowie Jahresbilanzsumme von jeweils mind. 10 Mio. EUR

*Hinweis: Der Schwellenwert nach dem KRITISDachG gilt momentan noch pauschal für alle Sektoren, es sollen per Rechtsverordnung branchenspezifische Werte ergänzt werden

Die Size-Cap-Rule führt grundsätzlich zur Ausweitung von Informations-sicherheitspflichten auf bisher nicht betroffene Unternehmen…



…aber nicht zur Ausweitung der KRITIS-Betroffenheit auf vorher unbetroffener Unternehmen!

Anwendungshilfe Sicherheit und Resilienz

Prüfung der Betroffenheit

Wie definiert sich „Betreiber kritischer Anlagen“ in der Wasserwirtschaft?

- Nach KRITISDachG und NIS2-UG:

  „Betreiber kritischer Anlagen“ [ist] eine natürliche oder juristische Person oder eine rechtlich unselbständige Organisationseinheit einer Gebietskörperschaft, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände **bestimmenden Einfluss auf eine oder mehrere kritische Anlagen** ausübt.

- Prüfung im Einzelfall erforderlich bei verschiedenen Formen der Zusammenarbeit:
  - Konzessionen und Betriebsführungen
  - Beteiligungen und Querverbundunternehmen
  - Interkommunale Zusammenarbeit
  - Mehrere Anlagen desselben Betreibers

Ergänzende Einzelerläuterungen finden sich in der Anwendungshilfe

Empfehlung: Individuelle vertragsrechtliche Prüfung bei Kooperationsformen bzw. vertragliche Anpassung, um festzulegen, wer für Sicherheit & Resilienz zuständig ist

Anwendungshilfe Sicherheit und Resilienz
Pflichten der Geschäftsführung

- Übernimmt Gesamtverantwortung für die Erfüllung der gesetzlichen Pflichten und haftet persönlich für Verstöße
- Teilnahme an Pflicht-Schulungen zum NIS2-Umsetzungsgesetz alle 3 Jahre im Umfang von mind. 4 Stunden, anlassbezogen auch früher (z. B. bei Führungswechsel oder Auffrischungsbedarf)
- Benennung von mind. einer operativ verantwortlichen Person im Unternehmen, die auch als 24/7-Kontaktstelle zum BSI fungiert

Anwendungshilfe Sicherheit und Resilienz

Registrierungspflicht und Schadensmeldung

Registrierungspflicht:

- Bei Betroffenheit durch das KRITISDachG und/oder das NIS2-Umsetzungsgesetz, muss sich das Unternehmen selbstständig auf einem Portal des BSI einmalig registrieren
- Fristen KRITISDachG: 17. Juli 2026
- Fristen NIS2-Umsetzungsgesetz: 05. März 2026
- Voraussetzung: ELSTER-Unternehmenskonto

Schadensmeldung:

- Wird eine kritische Anlage kompromittiert, muss das Unternehmen dies bei einer gemeinsamen Meldestelle zwischen BBK und BSI anzeigen
- Fristen: Erstmeldung innerhalb 24 Std, Nachmeldung nach 72 Std., Abschlussmeldung innerhalb eines Monats
- Schadensmeldung kann auch ohne vorherige Registrierung erfolgen

Anwendungshilfe Sicherheit und Resilienz

Übersicht zentraler Pflichten für Anwender

- Tabellarische Übersicht aller zentraler Pflichten aus beiden Gesetzen
- Dient als Übersicht und Nachschlagewerk
- Zeigt inhaltliche Parallelen/Unterschiede auf
- Gibt Verweise auf die Gesetzes-Passagen wie auch weiterführende Hinweise

Pflicht	KRITISDachG	NIS2-UG[12]
	Betreiber kritischer Anlagen	**Betreiber kritische Anlagen / Besonders wichtige Einrichtungen & wichtige Einrichtungen im Wassersektor**
Betroffenheits-prüfung	§ 4 Abs. 1 Nr. 6 & § 5 Abs. 1 Ab 500.000 zu versorgenden Einwohnern oder durch behördliche Festlegung Hinweis: Spezifischere Festlegungen sind über eine gesonderte Rechtsverordnung zu erwarten	§ 28 Betreiber einer für die Versorgung kritischen Anlage = besonders wichtige Einrichtung: • Trinkwasserversorger ab 22 Mio. m³/Jahr • Abwasserentsorger ab 500.000 EW/Personen Betreiber einer Wasserversorgungs- oder Abwasserbeseitigungsanlage (nach Anlage 1 NIS2-UG): Besonders wichtige Einrichtung: • Ab 250 Mitarbeitende oder Jahresumsatz von mind. 50 Mio. EUR und Jahresbilanzsumme von mind. 43 Mio. EUR Wichtige Einrichtung: • Ab 50 Mitarbeitende oder Jahresumsatz und Jahresbilanzsumme von jeweils über 10 Mio. EUR Tool zur Betroffenheitsprüfung[13] beim BSI nutzbar
Registrierungs-pflicht	§ 8 Abs. 1	§ 33 Registrierung beim BSI-Portal:

Anwendungshilfe Sicherheit und Resilienz
Risikomanagement und Maßnahmenplanung

- Das KRITISDachG verpflichtet u. a. zu:
  - Risikoanalyse und Risikobewertung von naturbedingten, technischen oder menschlich verursachten Risiken
  - Verhinderung von Vorfällen
  - Gewährleistung eines angemessenen Schutzes von Liegenschaften und kritischen Anlagen
  - Abwehr von eingetretenen Vorfällen, Begrenzung negativer Auswirkungen, Wiederherstellung der Dienstleistung

- Das NIS2-UG verpflichtet u. a. zu:
  - Risikoanalyse für die Sicherheit in der Informationstechnik
  - Fähigkeit zur Bewältigung von Sicherheitsvorfällen
  - Aufrechterhaltung des Betriebs, Wiederherstellung nach einem Notfall und Krisenmanagement

Beide Gesetze fordern ein Risikomanagement und darauf aufbauende Maßnahmen zur Verbesserung des Schutzniveaus wie auch reaktiver Maßnahmen im Schadensfall

➢ Entspricht einem BCMS sowie ISMS und B3S

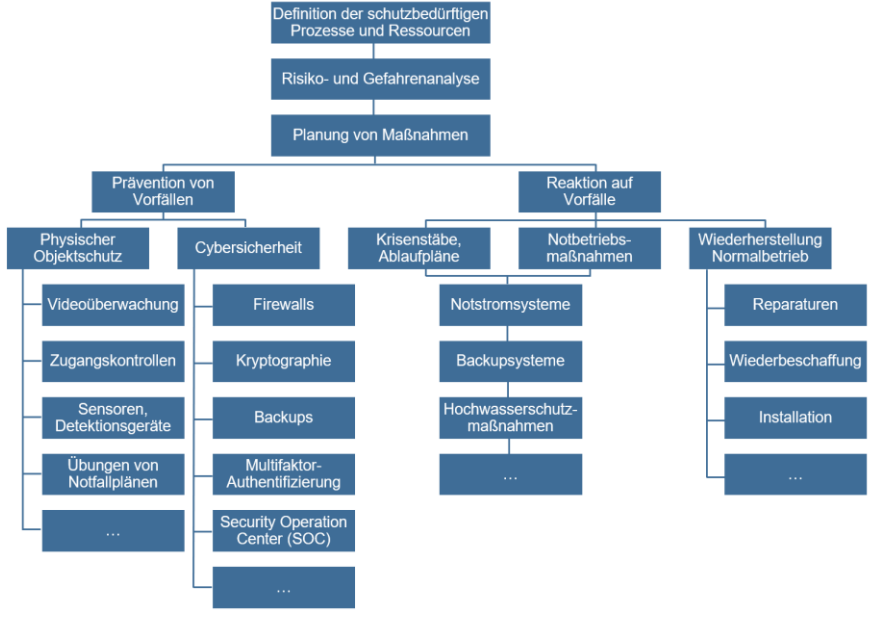
Anwendungshilfe Sicherheit und Resilienz

Aufbau eines Resilienzplanes

Aufbau eines ganzheitlichen Resilienzplanes auf Basis eines Business Continuity Managementsystems (BCMS)

- Beschreibung wesentlicher Schritte eines BCMS wie Business Impact Analyse, Risikoanalyse und Maßnahmenplanung
- Verschafft schnellen Überblick und Verständnis zum BCMS
- Integriert Aspekte der Informationssicherheit

Hinweis: Über das KRITISDachG sind ergänzende methodische Vorgaben zum Aufbau eines Resilienzplanes angekündigt



Anwendungshilfe Sicherheit und Resilienz

Finanzierung von Sicherheits- und Resilienzmaßnahmen

Finanzierungsfähigkeit über Gebühren/Preise für Sicherheits- & Resilienzmaßnahmen ist nicht immer eindeutig gegeben, Gründe sind z. B.:

- Maßnahmen gehen über die Verhältnismäßigkeit hinaus, z. B. bei zusätzlich zum bisherigen Status redundanten Versorgungsstrukturen
- Maßnahmen liegen nicht eindeutig im Aufgabenbereich des Betreibers, z. B. bei Drohnendetektions- und Abwehrsystemen

Empfehlungen: Im Plansatz grundsätzlich einen Anteil des Aufwandes für notwendige Sicherheits- und Resilienzmaßnahmen vorhalten und zusätzlich Förderprogramme des Bundes und der Länder prüfen.

➢ BDEW setzt sich für die Schaffung eines Resilienzfonds aus Mitteln des Verteidigungshaushaltes ein.

Anwendungshilfe Sicherheit und Resilienz
Weiterführende Hinweise aus der Praxis

- Sensibilisierung der Mitarbeitenden
- Angemessene Einbindung der Share- und Stakeholder
- Institutionsübergreifende Katastrophen-, Krisen- und Notfallplanung
- Externe “Auditierung” – Hinweis: Aktuell keine Zertifizierung notwendig, Nachweis bei BSI ausreichend
- Versicherung für Cybersicherheitsschäden

KI-Verordnung - Einordnung Informationssicherheit

- Reguliert einen sicheren Umgang mit KI innerhalb der EU nach einem risikobasierten Ansatz:
  - Verbotene KI-Systeme: Ausbeuterische, manipulative und soziale Kontrollpraktiken
  - Hochriskante KI-Systeme: Z. B. Steuerung von sicherheitsrelevanten Funktionen in kritischen Infrastrukturen
  - KI-Systeme mit geringem Risiko: Keine Gefährdung von Grundrechten oder Unversehrtheit von Personen, aber theoretisch manipulierbar z. B. im Kontext von Fehlinformationen
  - KI-Systeme ohne besonderes Risiko: KI mit limitiertem Regeln z. B. Spam-Filter bei Mailprogrammen
- Sonderfall generative KI (wie ChatGPT, Microsoft Copilot, Claude etc.):
  - Der Einsatzzweck bestimmt die Risikoeinstufung – Hierzu zählt auch der Zugang der KI zu sensiblen Informationen
- Pflichten der Unternehmen, die KI nutzen möchten:
  - Risikomanagement bei hochriskanten KI-Systemen, menschliche Aufsicht, Information an Betriebsrat/Belegschaft, Schulungen der nutzenden Beschäftigten, Transparenzpflicht, etc.

Empfehlung: Risikobewusster Einsatz von KI-Systemen mit Zugang zu sensiblen Unternehmensdaten

Ausblick

- Veröffentlichung Anwendungshilfe „Sicherheit und Resilienz in der Wasserwirtschaft“ voraussichtlich Ende Mai geplant – Information über Newsletter oder Webseite
- Digital für Mitglieder des BDEW abrufbar
- Webinare im Sommer in Planung

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Jörg Rehberg
Fachgebietsleiter Geschäftsbereich
Wasser und Abwasser
BDEW

T +49 30 300199-1211
M +49 173 9619819
joerg.rehberg@bdew.de

Lisa Minor M.A.
Referentin der kaufm. Geschäftsführung
der Stadtentwässerung Dresden
GELSENWASSER Dresden GmbH

T +49 351 822-1937

lisa.minor@se-dresden.de

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

bdew
Energie. Wasser. Leben.

Die Wasserwirtschaft
im BDEW