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

23.08.2023

Stellungnahme

zum

Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen

(KRITIS-Dachgesetz – KRITIS-DachG)
(Stand: 17.07.2023**)**

Das Bundesministeriums des Innern und für Heimat hat einen Referentenentwurf für ein Gesetz zur Umsetzung der europäischen CER-Richtlinie, (EU) 2022/2557, und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz – KRITIS-DachG) vorgelegt. Der Entwurf sieht weitreichende Regelungen für Einrichtungen oder sog. „kritische Anlagen“ und deren Betreiber u.a. in den Sektoren Energie, Gesundheitswesen, Trinkwasser und Abwasser sowie Siedlungsabfallentsorgung vor, die durch eine noch zu erlassende Rechtsverordnung konkretisiert werden. Die neuen Regelungen legen z.B. Verpflichtungen für Betreiber fest, die eine Aufgabenerfüllung auch unter dem Eindruck von Unfällen, Naturkatastrophen, gesundheitlichen Notlagen, hybriden oder feindlichen Bedrohungen oder Terrorismus gewährleisten sollen.

Zusammenfassende Bewertung:

Der russische Angriffskrieg gegen die Ukraine mitten in Europa und die geopolitischen Entwicklungen führen zu einer Neubewertung der Sicherheitslage für die kritischen Infrastrukturen und beeinflussen in erheblicher Weise die europäischen und globalen Märkte. Gleichzeitig nehmen im Zuge des Klimawandels Extremwetterereignisse mit teilweise katastrophalen Folgen zu. Ein sektoren- und gefahrenübergreifender Schutz physischer Kritischer Infrastrukturen (KRITIS) ist für ein funktionierendes gesellschaftliches Zusammenleben unerlässlich. Die DWA unterstützt daher die Festlegung eines Kernbestands zu schützender Sektoren einschließlich der konkret zugehörigen Anlagen (besser „Infrastrukturen“), zu denen insbesondere auch die Bereiche Wasser und Energie gehören. Es gilt die Resilienz für diese Sektoren zu erhöhen und im Hinblick auf potentielle Gefahren einen ganzheitlichen Ansatz zu verfolgen. Mit der CER-Richtlinie und deren Umsetzung wird hier ein richtiger Weg verfolgt. **Den Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-DachG) vom 17. Juli 2023 begrüßt die DWA daher grundsätzlich**.

Kernforderungen:

1. Ein sachgerechter Schutz und eine hohe Resilienz der kritischen Infrastruktur lässt sich nur unter Einbindung aller wesentlichen Akteure erreichen. Dazu gehören neben Bund, Ländern und Kommunen die Betreiber kritischer Anlagen und die Branchenverbände der relevanten Sektoren. Aus Sicht der DWA ist dies

ein zentraler Punkt, insbesondere die im Entwurf vorgesehene Möglichkeit, branchenspezifische Resilienzstandards vorzuschlagen (vgl. § 11 Abs. 5 KRITIS-DachG-E), wird von der DWA nachdrücklich begrüßt. **Bei der Stärkung der Resilienz kritischer Anlagen sollten die bewährten Strukturen und Mechanismen der technischen Selbstverwaltung zum Einsatz kommen.** Dies hat sich z.B. im Bereich der IT-Sicherheit mit dem B3S und dem DWA-M 1060 bereits etabliert. Gerade im Bereich der Technischen Sicherheit verfügt die DWA über viel Erfahrung. Sie bietet hier in enger Abstimmung mit anderen technischen Regelsetzern für die kritischen Infrastrukturen wie Strom (VDE-FNN), Wasser (DVGW) und Fernwärme (AGFW) neben dem Regelwerk bereits mit dem Technischen Sicherheitsmanagement (TSM) Hilfestellungen an, die wichtige Beiträge zur Resilienzerhöhung in den Bereichen leisten.

2. Bei den Vorgaben zur Sicherung von kritischen Infrastrukturen durch die Betreiber vor entsprechenden Gefahren muss eine **Abwägung einerseits zwischen Schadenseintrittswahrscheinlichkeit und Schadenintensität (Risiko) sowie andererseits der Wirtschaftlichkeit und Angemessenheit von Resilienzmaßnahmen** erfolgen. Der Aufbau von **Bürokratie ist auf das notwendige Maß** zu **beschränken**, z.B. indem -wo möglich- die regulären Aufsichtsbehörden einbezogen werden.

3. Es sollte sichergestellt werden, dass auch **mittlere und kleine Betriebe** ihre Resilienz gegen sich wandelnde Bedrohungslagen erhöhen können. Dafür braucht es sachgerechte **Hilfestellungen**, wobei der technischen Regelsetzung eine besondere Bedeutung zukommt. Zudem bedarf es finanzieller Förderung bzw. einer Klärung, inwieweit freiwillige Maßnahmen in Gebühren und Entgelte rechtskonform integriert werden können (Kommunales Abgabenrecht, Kartellrecht).

4. Es muss eine **sachgerechte Harmonisierung zwischen dem KRITIS-Dachgesetz** zur Umsetzung der CER-Richtlinie **und dem NIS-2-Umsetzungsgesetz** zur Umsetzung der Richtlinie (EU) 2022/2555 erfolgen, die sich auch in den noch auf dieser Grundlage zu erlassenden Rechtsverordnungen fortsetzt. Es ist nicht klar erkennbar, wie ein Koordinierung mit den landesrechtlichen Kompetenzen (Gefahrenabwehrrecht, Baurecht) erfolgen soll. Das betrifft auch die praktische Umsetzung von Informations- und Meldeketten, z.B. der geforderten Resilienzpläne, Maßnahmenpläne oder Störungsmeldungen. Hier drohen durch Splittung oder Dopplung von Zuständigkeiten vermeidbare Unklarheiten. Zudem sieht die DWA **bei den Begriffsdefinitionen** dringenden **Nachbesserungsbedarf.**

5. **Der Schutz von sensiblen Informationen ist sicherzustellen.** Dies dient dem Schutz vor Bedrohungen und entspricht dem Sinn und Zweck des KRITIS-DachG. Der Austausch aller verpflichtenden und sehr sensiblen Informationen zwischen den Behörden und den Betreibern kritischer Anlagen, sollte verschlüsselt oder auf sicherem digitalem Weg erfolgen. Darunter fallen auch bestimmte Inhalte der Risikoanalysen und Resilienzpläne.

Im Einzelnen:

Im § 2 Absatz 2 Satz 1muss es heißen:
„Kritische Infrastrukturen“ Organisationen oder Einrichtungen mit ~~wichtiger~~ **hoher** *Bedeutung [...]*.

§ 2 Nr. 7 „Risiko“:
Es wird der Begriff „Risiko“ verwendet. Dabei handelt es sich um das Produkt aus (Schadenseintritts-)Wahrscheinlichkeit und Konsequenzen (z. B. Schaden in €/a), vgl. auch Art 2 (6) der CER-Richtlinie. Die im Entwurf des KRITISDachG verwendete Definition ist unscharf oder unvollständig und sollte geändert werden.

§ 2 Nummern 11 und 12:
Die Unterscheidung in „besonders wichtige Einrichtungen“ und „wichtige Einrichtungen“ lässt sich nicht aus der CER-Richtlinie herleiten. Diese kennt „wesentliche Dienste“ (Artikel 2 Nummer 5), „kritische Einrichtungen“ (Artikel 2 Nummer 1) und „kritische Infrastrukturen“ (Artikel 2 Nummer 4), sowie „Einrichtungen der öffentlichen Verwaltung“ (Artikel 2 Nummer 10).
Was „kritische Einrichtung“ ist, bestimmt sich nach dem Anhang, explizit über die Auflistungen der Kategorien von Einrichtungen (Spalte 3 der Tabelle).
Diese Tabelle im Anhang der CER-Richtlinie ist weitgehend inhaltsgleich mit der Tabelle im Anhang I der NIS 2-Richtlinie.
Unterschiede:

- Im Anhang der CER-Richtlinie wird im Sektor „1. Energie“ der erste Teilsektor mit „a) Strom“ bezeichnet, während er im Anhang I der NIS 2-Richtlinie mit „a) Elektrizität“ geführt wird. Tatsächlich findet sich in den englischen Fassungen in beiden Fällen der Ausdruck „a) Electricity“. Kann man grds. als synonym betrachten.
- Die CER-Richtlinie weist für den Sektor „2. Verkehr“ einen Teilsektor „e) Öffentlicher Verkehr“ aus, der nicht in der Tabelle der NIS 2-Richtlinie steht
- Die Spaltenbezeichnungen der beiden Tabellen unterscheiden sich: CER-Richtlinie: Sektoren | Teilsektoren | Kategorien von Einrichtungen NIS 2-Richtlinie: Sektor | Teilsektor | Art der Einrichtung
  Das kann ebenfalls als synonym betrachtet werden.

Insgesamt können die Tabelle im Anhang der CER-Richtlinie und im Anhang I der NIS 2-Richtlinie als inhaltsgleich angesehen werden, mit den marginalen, aufgeführten Unterschieden.

In den Begründungen, zu finden unter „Begründung B. Besonderer Teil“ (hier: Seite 32) wird zu § 2 Nummer 11, in den Begründungen fälschlich als „Zu Nr. 10 (besonders wichtige Einrichtungen)“ angegeben, und § 2 Nummer 12, in den Begründungen fälschlich als „Zu Nr. 11 (wichtige Einrichtungen)“ angegeben, erläutert, dass die Einführung der „besonders wichtigen Einrichtungen“ und der „wichtigen Einrichtungen“ im KRITIS-Dachgesetz ausschließlich erfolgt, um eine gemeinsame Rechtsverordnung mit den Schwellenwerten erlassen zu können. Das ist nicht notwendig. Aufgrund der Tatsache, dass der Anhang der CER-Richtlinie und der Anhang I der NIS 2-Richtlinie quasi identisch sind (siehe oben) und sich auf dieselben Einrichtungen vergleichbarer Kritikalität beziehen, sollte es problemlos möglich sein, eine entsprechende Rechtsverordnung zu erlassen, in der für die

Einrichtungen entsprechend Anhang II der NIS-Richtlinie weitere Festsetzungen angeführt werden, die ausschließlich die Cyber-Sicherheit betreffen.

Eine Verkomplizierung im nationalen Recht im Zusammenhang mit dem NIS2UmsuCG in Bezug auf die Unterscheidung „kritische“, „besonders wichtige“ und „wichtige“ Einrichtung, sollte nicht stattfinden.

Die Harmonisierung zwischen dieser und der Umsetzung der NIS 2-Richtlinie sollte sich vor allem auf die formalen Verfahren wie Meldeverfahren, Nachweisverfahren etc. beziehen.

§ 4 und § 6 tauschen (Kritische Anlage/ kritische Infrastruktur):
Nach der Definition der CER-Richtlinie (Art. 2 Nr. 4) umfasst der Begriff der kritischen Infrastruktur u.a. auch „Anlagen“ und ist damit weiter gefasst. Aus systematischen Gründen sollten die Vorschriften des § 4 „Kritische Anlagen“ und § 6 „Anforderungen an Betreiber Kritischer Infrastrukturen“ getauscht werden.
Zudem: Der Begriff „Anlage“ genauer: „kritische Anlage“ sowie „Betreiber kritischer Anlagen“ wird an keiner Stelle in der CER-Richtlinie verwendet. Es ist ausschließlich die Rede von „kritischer Einrichtung“ oder „kritischer Infrastruktur“, was grundsätzlich ausreichend ist. Nach der Begriffsdefinition der „kritischen Infrastruktur“ (Artikel 2 Nummer 4) ist eine Anlage ein mögliches Objekt der Infrastruktur. „Infrastruktur“ ist im Sinne der CER-Richtlinie ein umfassender Begriff, der den Begriff „Anlage“ einschließt. Die Verwendung des Begriffs „Anlage“ im KRITIS-Dachgesetz an Stellen, wo in der CER-Richtlinie von „Infrastruktur“ die Rede ist, greift somit zu kurz und gibt nicht den Inhalt der CER-Richtlinie wieder.
Hier ist nicht zu erkennen, warum das KRITIS-Dachgesetz anderslautende Begriffe verwendet, die teilweise nicht den Regelungsinhalt der CER-Richtlinie widerspiegeln

Wie auch immer der Gesetzgeber sich entscheidet, mindestens sollten die Begriffsdefinitionen konsistent sein. Dies ist bislang nicht der Fall.

In § 6 Absatz 1 muss es heißen:

(1) Resilienzmaßnahmen nach § 11 Absatz 1 Satz 1 und § 11 Absatz 1 Satz 3 können, soweit geeignet und verhältnismäßig, auch von Betreibern Kritischer ~~Infrastrukturen~~ **Anlagen** *in den nach § 4 Absatz 1 festgelegten Sektoren, die die Schwellenwerte der Rechtsverordnung nach § ~~155~~* **15** *nicht erreichen, zur Steigerung ihrer Resilienz ergriffen werden. Soweit an der Verwendung bzw. Einführung des Begriffs der kritischen Anlage festgehalten wird, ist mit Rücksicht auf den Verweis auf § 4 Abs. 1 wie vor zu formulieren.*

In § 6 Absatz 1sollte es heißen:

(1) Resilienzmaßnahmen nach § 11 Absatz 1 Satz 1 und § 11 Absatz 1 Satz 3 können, soweit geeignet und verhältnismäßig, auch von Betreibern **in den nach § 4 Absatz 1 festgelegten Sektoren, deren Anlagen** *~~Kritischer Infrastrukturen~~* **Anlagen** *~~in den nach § 4 Absatz 1 festgelegten Sektoren, die~~ die Schwellenwerte der Rechtsverordnung nach ~~§ 155~~* **15** *nicht erreichen, zur Steigerung ihrer Resilienz ergriffen werden.*
Begründung: Betreiber, deren Anlagen nicht die Schwellenwerte erreichen oder über diesen liegen, sind nach diesem Gesetz keine Betreiber Kritischer Anlagen.

In § 6 Absatz 2 Satz 1 muss es heißen:
Die Betreiber Kritischer Infrastrukturen nach [...] nach § 11 Absatz 5 zu entwickelnden branchenspezifischen Resilienzstandards ~~berücksichtigen~~ **anwenden***.*

§ 7: Der Titel muss gemäß Artikel 17 der CER-Richtlinie lauten:
„*Kritische ~~Anlagen~~* **Einrichtungen** *von besonderer Bedeutung für Europa*“

Wortlaut in der CER-Richtlinie:

„KAPITEL IV KRITISCHE EINRICHTUNGEN, DIE VON BESONDERER BEDEUTUNG FÜR EUROPA SIND“

„*Artikel 17* Ermittlung kritischer Einrichtungen, die von besonderer Bedeutung für Europa sind“

§ 7 Absatz 4:
Die Formulierung „***oder in Bezug stehen***“ lässt offen, in welcher Hinsicht hier ein Bezug bestehen muss. Beispiel: Der „Bezug“ kann sich z. B. auf einen geregelten Erfahrungsaustausch oder gegenseitigen Hospitationen von Personal bestehen. Das Ganze kann sehr wohl vertraglich abgesichert sein.

§ 8 Absatz 3 und 4: 24/7 Bereitschaft im ISMS/IT/OT Umfeld ?
Die Betreiber haben sicherzustellen, dass sie über die benannte Kontaktstelle (Person mit vergleichbarer Aufgabenstellung als Ansprechpartner) jederzeit (24/7) erreichbar sind. Insbesondere ist nicht geklärt, über welche Fähigkeit die Kontaktstelle verfügen muss. Nach derzeitiger Lesart bedeutet das eine zusätzliche ISMS/IT/OT Bereitschaft.

§ 10 Absatz 1:
Die DWA versteht die §§ 9, 10 und 11 als aufeinander aufbauend. Dies ist auch notwendig. § 10 Abs. 1 setzt voraus, dass bei Registrierung die staatlichen Risikoanalysen und -bewertungen nach § 9 tatsächlich vorliegen. Gemäß § 10 Abs. 1 führen wir eine Risikoanalyse und Risikobewertung erstmals neun Monate nach der Registrierung als kritische Anlage durch. Die Analyse und Bewertung erfolgt auf der Grundlage der staatlichen Risikoanalyse und -bewertung nach § 9. Für diese ist aber keine Frist bestimmt. Es ist also unklar, ob diese bis zu dem verpflichtenden Termin überhaupt erstellt ist und mit ausreichendem zeitlichem Vorlauf vorliegt. Das ist zu korrigieren. Liegt keine nationale Bewertung vor, können auch Betreiber ihrerseits keine sachgerechten Risikoanalysen und –bewertungen durchführen. Daher sollte in diesem Fall dann auch keine Frist beginnen. Die Neun-Monate-Frist sollte frühestens ab Veröffentlichung der staatlichen Risikoanalysen und –bewertungen zu laufen beginnen oder ab Registrierung als kritische Anlage, wenn dies zeitlich später erfolgt.

Gemäß § 10 Abs. 1 Nr. 2 sollen Risiken bewertet werden, die sich aus dem Ausmaß der Abhängigkeit anderer Sektoren von der kritischen Dienstleistung ergeben. Das ist nicht zu leisten. Über das Ausmaß solcher Abhängigkeiten haben wasserwirtschaftliche Betreiber i.d.R. keine Informationen und könnten nur spekulieren. Die Bestimmung entspricht § 9 Abs.1 Nr. 2 zur NATIONALEN Risikoanalyse und Risikobewertung. Dort – und nur dort – ist sie richtig verortet.

§ 10 Abs. 1 Nr. 1 „hybride Bedrohungen“:
Der Begriff wird unterschiedlich gedeutet und in der Fachöffentlichkeit unterschiedlich interpretiert. Wird er nicht im KRITIS-DachG definiert, sollte die nationale Risikoanalyse und Risikobewertung unbedingt eine praxistaugliche Konkretisierung enthalten.

§ 11 Resilienzmaßnahmen der Betreiber kritischer Anlagen:
Sinnvoll ist eine Anerkennung von branchenspezifischen Sicherheitsstandards (vgl. § 5 KRITIS-DachG) der Technischen Regelsetzung als wesentliches Instrument zur Umsetzung des KRITIS-DachG durch Aufnahme einer Vermutungsregelung, dass mindestens die allgemein anerkannten Regeln der Technik einzuhalten sind.

§ 11 Absatz 5
Ob die Feststellung im Benehmen mit dem BSI **oder** im Einvernehmen mit einer zuständigen Aufsichtsbehörde des Bundes erfolgt, lässt Spekulationen zu, wie denn dieses „oder“ zu verstehen ist. Stellt es eine ausschließliche Alternative dar, entscheidet es sich aufgrund der Branche? Was ist wirklich gemeint? Im geltenden BSIG und im Entwurf zum NIS2UmsuCG steht statt des „oder“ ein Komma. Hier ist eine Klarstellung erforderlich.

§ 11 Absatz 7:
Nachweise zur Einhaltung bereits etablierter Risiko- und Sicherheitsmanagementsysteme (z. B. Technisches Sicherheitsmanagement der DWA, TSM) der mindestens einzuhaltenden anerkannten Regeln der Technik sollten nach § 11 KRITIS-DachG anerkannt werden, um keinen zusätzlichen Aufwand zu erzeugen. Es sollten bereits bestehende Systeme, Strukturen und Dienstleistungen im Bereich der Nachweisführung genutzt und ggf. ausgebaut werden.

§ 11 Absätze 6 und 8:
Hier ist ein Mindestzeitraum festzulegen. Auf jeden Fall muss sichergestellt werden, dass der Zeitraum mindestens zwei Jahre beträgt, wie dann zukünftig ohnehin. Deutlich besser wäre eine Konkretisierung und Festlegung z. B. auf 3 Jahre. Den Zeitraum auf 3 Jahre festzulegen würde der Qualität der operativen Umsetzung dienen.

§ 11 Absatz 8 Zeile 15 sollte es heißen:
[..] die prüfende Stelle nach Anhörung von Vertretern der betroffenen Betreiber und Einrichtungen und der betroffenen ~~Wirtschaftsverbände~~ **Branchenverbände** *festlegen. Die Festlegung nach Satz 1 erfolgt [..].*
Begründung: „Branchenverbände“ wird auch, korrekt, im § 11 Absatz 5 verwendet.

§ 11 Absatz 13:
Die Formulierung „Frühestens nach Ablauf von zehn Monaten“ ist unklar. Wer legt fest was „spätestens“ bedeutet? Hier entsteht der Eindruck von Beliebigkeit, ohne dass erkennbar wird, wer denn die Grenzen setzt und wann das geschieht.
In § 11 Abs. 13 muss ergänzt werden, dass die Verpflichtungen frühestens nach Ablauf von 10 Monaten nach der Registrierung UND DER VERÖFFENTLICHUNG DER ANFORDERUNGEN NACH § 11 Abs. 8 gelten. Sonst gibt es im Nachweisverfahren vermeidbare Diskussionen über die Verwendbarkeit der Nachweise. Das BBK sollte die

Anforderungen auch nicht definieren KÖNNEN, sondern MÜSSEN (wie bislang auch das BSI).

§ 12 Absatz 6 Meldewesen:
Das Meldewesen sollte nicht nur einseitig ausgestaltet werden. Es ist sicherzustellen, dass die zuständigen Behörden „den ~~betroffenen~~ Betreibern…“ kritischer Infrastrukturen Informationen über potentielle Störungen und Sicherheitsvorfälle sowie etwaige hilfreiche Erfahrungen mit deren Behebung oder Beseitigung mitteilt, jeweils unter Wahrung der schutzwürdigen Interessen der von den Störfällen oder Sicherheitsvorfällen betroffenen Betreibern.

§ 13:
Ein Text fehlt ohne weiteren Hinweis. Auch in den Begründungen gibt es keinen Hinweis.

§ 15 Nummer 1 sollte lauten:
1. *~~unter Festlegung der in den jeweiligen~~* **welche Anlagen der Einrichtungen in den** *Sektoren Energie, Transport und Verkehr, Bankwesen, [..] anzusehenden Versorgungsgrads, ~~welche Anlagen davon~~ als kritische Anlagen im Sinne dieses Gesetzes gelten,*
Begründung: Verständlichere Formulierung.

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

Hennef, den 23.08.2023

DWA
Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall e. V.
Theodor-Heuss-Allee 17, 53773 Hennef
Tel.: + 49 2242 872-110
Fax: + 49 2242 872-8250
E-Mail: info@dwa.de
www.dwa.de

EU-Transparenzregister: 227557032517-09