

Stellungnahme des Deutschen Verkehrsforums e.V.

zum

**Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2022/2557 und zur
Stärkung der Resilienz von Betreibern kritischer Anlagen**

des Bundesministeriums des Innern und für Heimat

Berlin, 24.01.2024

1. Vorbemerkung

Das Deutsche Verkehrsforum bedankt sich für die Möglichkeit der Stellungnahme zu dem am 22. Dezember 2023 vom Bundesministerium des Innern und für Heimat (BMI) übersandten überarbeiteten Referentenentwurf (RefE) des KRITIS-Dachgesetzes (KRITIS-DachG).

Das KRITIS-DachG soll die Richtlinie (EU) 2022/2557 umsetzen, mit der ein einheitlicher europäischer Rechtsrahmen für die Stärkung der Resilienz kritischer Einrichtungen gegen Gefahren außerhalb des Schutzes der IT-Sicherheit im Binnenmarkt geschaffen wurde. Ziel der Richtlinie ist es, einheitliche Mindestverpflichtungen für kritische Einrichtungen festzulegen und deren Umsetzung durch kohärente, gezielte Unterstützungs- und Aufsichtsmaßnahmen zu garantieren. Die Richtlinie ist bis zum 17. Oktober 2024 in nationales Recht umzusetzen.

2. Allgemeine Bewertung

Das Deutsche Verkehrsforum e.V. begrüßt den vorliegenden, überarbeiteten Entwurf zum KRITIS-DachG grundsätzlich als geeigneten Beitrag zur Stärkung der Resilienz der Kritischen Infrastruktur in Deutschland.

- Im vorliegenden Entwurf sind deutliche Vereinheitlichungen von Begrifflichkeiten und Anpassungen zur Harmonisierung von KRITIS-DachG und NIS2UmsuCG vorgenommen worden. Ferner wurde die Bestimmung der betroffenen Betreiber kritischer Anlagen niedergelegt.
- Eine einheitliche Definition der im KRITIS-DachG und dem NIS2-UmsuCG verwendeten Begrifflichkeiten ist jedoch nicht durchgehend gegeben und es bestehen weiterhin Unklarheiten bzw. Anpassungsbedarf. So sind z.B. die in § 2 RefE des KRITIS-DachG genannten Begrifflichkeiten „kritische Anlage“, „kritische Dienstleistung“ und „Vorfall“ nicht einheitlich definiert. Eine Erläuterung aller

sonstigen im KRITIS-DachG verwendeten Begriffe ist ebenfalls nicht durchgehend gegeben.

- Der Begriff „Beratungsmission“ (u.a. § 7 Abs. 4 RefE) ist erläuterungsbedürftig und fehlt in den Begriffserläuterungen in § 2 RefE. Wünschenswert wäre eine Konkretisierung der in der CER- Richtlinie genannten Beratungsmission.
- Im Anwendungsbereich des KRITIS-DachG fehlt es an einer klaren Benennung aller Regelungen, die von diesem Gesetz unberührt bleiben, inklusive der eindeutigen Bestimmung, welche ggfs. abweichenden Regelungen anzuwenden sind. Die diesbezüglichen Regelungen in § 4 Abs. 7 RefE sind dahingehend nicht aussagekräftig.
- Positiv ist der erklärte Ansatz, eine größtmögliche Kohärenz zwischen IT-Sicherheitsgesetz und KRITIS-DachG zu ermöglichen. Mit dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) liegt bereits eine bewährte Grundlage vor. Bei der Umsetzung der Resilienz-Maßnahmen sollten die Betreiber auf anerkannten Normen und Managementsystemen aufsetzen können.
- Eine einheitliche Definition der unter die jeweiligen Gesetzgebungen fallenden Betreiber, insbesondere eine einheitliche KRITIS-Verordnung, ist geplant. Wir unterstützen dies und betonen die Wichtigkeit dieser beabsichtigten Regelung, die unter Einbeziehung von betroffenen Betreibern und Wirtschaftsverbänden erarbeitet werden sollte.
- Der Entwurf blendet weiterhin Fragen einer Finanzierung aus und sollte dahingehend ergänzt werden.
- Bei der Festlegung der Betreiber kritischer Infrastrukturen im Rahmen des Schwellenwertes sollte weiterhin insbesondere auch durch die Flexibilisierung beachtet werden, dass es u. a. auf regionaler Ebene nicht zu widersprüchlichen Regelungen kommen darf.
- Es bleibt weiter zu beachten, dass bei der Bestimmung kritischer Anlagen sicherzustellen ist, dass nicht unterschiedlich große Adressatenkreise durch BSI und BBK angesprochen werden.
- Die Entwicklung von branchenspezifischen Resilienzstandards ist zu begrüßen (§ 10 Abs. 6 RefE).
- Begrüßt wird ebenfalls, dass zwingende Nachweispflichten nicht mehr vorgesehen sind (§ 11 Abs. 1 RefE).
- Einheitliche Meldefristen sowie Meldewege für Meldungen gemäß KRITIS-DachG und NIS2-UmsuCG, insbesondere inklusive eines einheitlichen Meldeportals sowie einer einheitlichen Meldestelle, sind geplant. Wir regen eine weitestgehende Harmonisierung der beiden Gesetze KRITIS-DachG und NIS2-UmsuCG an.
- Die zeitliche Verschiebung von Umsetzungs- und Nachweispflichten wird grundsätzlich positiv bewertet, reicht jedoch nicht aus.

3. Anmerkungen im Einzelnen

A) Zu den Vorbemerkungen des Referentenentwurfs:

- Zu B: Bis zur Entwicklung und Anerkennung von branchenüblichen Standards werden die Landesbehörden durch Rechtsverordnung zum Erlass von Resilienzmaßnahmen ermächtigt. Damit besteht die Gefahr, dass bei Flächenorganisationen und Verbundunternehmen verschiedene und ggf. widersprüchliche landesspezifische Vorgaben und Anforderungen für Mitbewerber vorliegen werden. Es besteht ein Risiko der Wettbewerbsverzerrung. Es fehlt eine Konkretisierung im Gesetz, wer die Anforderungen der unterschiedlichen Behörden koordiniert, abstimmt und überstimmt, so dass es zu keinen Widersprüchen kommt. Die Aufgabe sollte explizit dem BBK zugeordnet werden.
- Zu E.2 (Erfüllungsaufwand für die Wirtschaft): Für den Bereich der Wirtschaft wird - wie für die Verwaltung - ein „erheblicher“ Erfüllungsaufwand entstehen. Es fehlt hier jedoch an einer realistischen Einschätzung. Die Angabe des Erfüllungsaufwands erhöht die Planungssicherheit und schafft Transparenz hinsichtlich der wirtschaftlichen Belastung durch das Gesetz. So ist unter Bezugnahme auf die erheblichen geschätzten Kosten für den Erfüllungsaufwand davon auszugehen, dass die Produktpreise der betroffenen Unternehmen steigen werden, um einen Teil der Kosten abzudecken. Die erste Erhebung seitens Destatis im Auftrag des BMI geht von einem Erfüllungsaufwand der Wirtschaft im dreistelligen Millionenbereich aus.
- Bei der Infrastruktur müssen Bund und Länder dafür Sorge tragen, dass auch die notwendige Mittelausstattung für die aus KRITIS erwachsenden Zusatzbedarfe berücksichtigt wird.

B) Zum Entwurf des Gesetzestextes:

Zu § 2 - Begriffsbestimmung:

- Der im Entwurf definierte Begriff „Risikoanalyse“ weicht von der Definition von anerkannten Standards wie BSI-200-3 bzw. ISO 31000 / 27005 ab. Dies erschwert die harmonisierte Nachweisbarkeit von KRITIS-DachG und IT-SiG.
- Gleiches gilt für den im Entwurf definierten Begriff „Risikobewertung“, der sowohl von der Definition in der EU-CER-RL als auch von der Definition von anerkannten Standards wie BSI-200-3 bzw. ISO 31000 / 27005 abweicht.

Zu § 3 - Zentrale Anlaufstelle; Zuständigkeiten; behördliche Zusammenarbeit

- Die breit gefächerten Aufsichtsbehörden erschweren die Identifizierung der federführend zuständigen Behörde für die betroffenen Betreiber und erhöhen den Aufwand für den Nachweis- und Vorfallmeldeprozess.
- Abs. 6 – Hier besteht Unklarheit in der Zuordnung kritischer Anlagen in der Bundes- oder Landeszuständigkeit. Es muss definiert werden, für welchen Betreiber von kritischen Anlagen der Bund oder das Land zuständig sind. Die diesbezügliche Regelung ist zumindest in Bezug auf die Länderzuständigkeit nicht aussagekräftig.

- Abs. 7 – Im Zuge der gegenseitigen Übermittlung von Informationen zwischen den Behörden sollten im Rahmen der erforderlichen wechselseitigen Informationen einschränkende Schwellenwerte definiert werden, da sonst eine Vielzahl von Vorfällen gemeldet werden müsste.

Zu § 4 - Anwendungsbereich; kritische Anlagen; Geltungsumfang

- Positiv würden wir feststellen, dass die Systematik zur Bestimmung von KRITIS grundsätzlich beibehalten werden soll und auch im Gesetzentwurf explizit festgehalten wurde (§ 4 Abs. 1).
- Diese Systematik wird jedoch aufgebrochen, wenn Behörden nach entsprechendem Ermessen zukünftig einseitig die Identifizierung als Betreiber kritischer Anlagen vornehmen können (§ 4 Abs. 2). Hierfür maßgebliche Kriterien sind zwar im Entwurf aufgeführt, jedoch erscheinen diese weder als abschließende Aufzählung noch sind sie spezifisch, da beispielsweise sowohl „Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten“ (Ziffer 3.) als auch der „Marktanteil des Betreibers“ (Ziffer 4.) nicht näher eingegrenzt werden. Es steht damit zu befürchten, dass besagte Flexibilisierung zu Lasten eines konsistenten, an klaren Maßstäben ausgerichteten Regelungsrahmens geht.
- Unklar ist die genaue Implikation des Vorrangs, den das Gesetz bereits anzuwendenden Spezialvorschriften beimisst (§ 4 Abs. 7 und 8). Offenbar bleiben die Pflichten zur gesonderten Dokumentation der getroffenen Maßnahmen weiter bestehen (d.h. es reicht nicht der einfache Verweis auf bestehende Auditierung bspw. nach dem LuftSiG), ebenso wie alle sonstigen Vorschriften des KRITIS-DachG.

Zu § 6 - Registrierung der kritischen Anlage und Ansprechpartner; Geltungszeitpunkt

- Die vorgesehenen Fristen sind unklar bzw. unrealistisch. Insbesondere ist die in § 6 Abs. 6 genannte Frist von zehn Monaten zur Umsetzung von Maßnahmen gemäß §§ 10-12 RefE nicht realistisch, dies vor allem dann nicht, wenn die Planung gemäß § 9 RefE nur einen Monat weniger Zeit benötigen soll. Hier sollten längere Zeiträume vorgegeben werden.
- Es sollte klargestellt werden, dass eine zentrale Stelle für einen Unternehmensverbund angegeben werden kann und nicht jeder einzelne KRITIS-Betreiber eine 24/7-Kontaktstelle benennen und vorhalten muss.

Zu § 8 - Nationale Risikoanalysen und Risikobewertungen

- Die nationalen Risikoanalysen sollten durch die Fachbehörden unter Einbeziehung der Wirtschaftsverbände und unter Berücksichtigung von Themenfeldern und gesetzlichen Vorgaben durchgeführt werden. Es ist zu befürworten, dass die Risikoanalysen durch die sektorenzuständigen Behörden erstellt werden. Das BBK muss weiter als zentrale und konsolidierende Funktion bestehen und bei Bedarf auf weitere fachspezifische Behörden zugehen können. Es ist zu beachten, dass eine gesamthafte Risikobetrachtung nicht allein durch den KRITIS-Betreiber geleistet

werden kann, da es sich nicht abschätzen lässt, welchen Einfluss Ausfälle bei Zulieferern haben.

Zu § 10 - Resilienzmaßnahmen der Betreiber kritischer Anlagen; Resilienzplan

- Es ist unklar, in welchen Zyklen die Resilienzpläne überprüft/aktualisiert werden müssen. Die gesetzlichen Vorgaben hierzu müssen in Abstimmung mit den Betreibern von kritischen Anlagen präzisiert werden. Auch der Hinweis auf den Stand der Technik ist zu ungenau und muss in Normen und Vorgaben in Abstimmung mit den Betreibern präzisiert werden.
- Offen bleibt in Abs. 1, in welchen Fällen ein angemessener physischer Schutz der Liegenschaften und kritischen Anlagen vorliegt und welche Maßnahmen hierzu verhältnismäßig sind. Insbesondere wirtschaftliche Aspekte bleiben unberücksichtigt. Klarstellend schlagen wir für § 10 Abs. 1 Satz 2 daher folgende Formulierung vor:
„Bei den von den Betreibern kritischer Anlagen zu treffenden technischen, sicherheitsbezogenen und organisatorischen Maßnahmen ist die Verhältnismäßigkeit zu wahren. Diese ist gewahrt, wenn der Aufwand zur Verhinderung oder Begrenzung eines Ausfalls zum Risiko eines Vorfalls angemessen erscheint. Dabei können auch wirtschaftliche Aspekte berücksichtigt werden.“
- § 10 Abs. 3 Ziffer 5. lit. a) aa) und lit. b) RefE regelt die Gewährleistung eines angemessenen Sicherheitsmanagements hinsichtlich der Mitarbeitenden. Betreiber kritischer Anlagen (Unternehmer) haben bezüglich der Zuverlässigkeitsprüfungen des Personals als Aspekt des Sicherheitsmanagements nur eine geringe Handhabe und können aus Datenschutzgründen i.d.R. selbst keine Zuverlässigkeitsüberprüfungen durchführen, insbesondere nicht bei dem Personal externer Dienstleister. Zur Schaffung eines angemessenen Sicherheitsmanagements könnte sich neben den gesetzlichen Vorgaben (SÜG, SÜFV, AtZÜV) auch an anderen Verfahren (z.B. Background checks/Pre Employment Screenings) orientiert werden. Für die Überprüfung von in kritischen Anlagen eingesetztem Personal wird eine gesetzliche Grundlage benötigt. Grundlagen aus dem SÜG/SÜFV reichen nicht aus. Bei einer gesetzlichen Regelung ist auf eine Widerspruchsfreiheit zwischen gesetzlicher und verordnungsrechtlicher Ebene (bspw. zum NIS2-UmsuCG) zu achten.
- § 10 Abs. 10 RefE: Das BBK kann Betreibern kritischer Anlagen Vorlagen und Muster für einen Resilienzplan zur Verfügung stellen. Im Sinne der Einheitlichkeit und Handhabung sollte dies keine „kann“-Anforderung, sondern eine „muss“-Vorschrift sein.

Zu § 11 - Nachweise; behördliche Anordnungen

- § 11 Abs. 4 RefE: Bei der geplanten Ausgestaltung des Verfahrens der Audits und Erbringung des Nachweises ist darauf zu achten, dass keine mehrfachen Aufwände für die Erbringung des Nachweises gem. IT-SiG und KRITIS-DachG entstehen.
- § 11 Abs. 5 und 6 RefE: In beiden Absätzen werden unbestimmte Rechtsbegriffe verwendet, wie beispielsweise. „erhebliche Zweifel an der Einhaltung von Verpflichtungen“. Diese undefinierten Begriffe lassen erhebliche Spielräume zu. Im Sinne einer Anwendungsklarheit müssen diese spezifiziert werden.

Zu § 12 - Meldewesen für Vorfälle

- Die in diesem Entwurf erfolgte Einschränkung der Meldung von Vorfällen beim Vorliegen einer „Erheblichkeit“ wird begrüßt. Weitere, klare Einschränkungen und Vorgaben der Beurteilung von zu meldenden Vorfällen werden befürwortet, um hier eine Einheitlichkeit zu schaffen. Beispielsweise sollten sogenannte Beinaheunfälle nicht gemeldet werden müssen.
- Bei einem Hybrid-Vorfall, bei dem sowohl die physische Sicherheit als auch die Cyber-Sicherheit betroffen sind, sollte keine doppelte Meldung erfolgen müssen, um Aufwände während der Behandlung von Vorfällen zu minimieren. In diesem Sinne sollte § 12 KRITIS-DachG mit § 32 NIS2UmsuCG harmonisiert werden.

Zu § 14 - Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleiter:innen von Betreibern kritischer Anlagen

- Die im Vergleich zum früheren Entwurf neu eingeführte Verpflichtung von Geschäftsleiter:innen sehen wir kritisch. Eine solche Regelung ist in vielen Fällen nicht zielführend bzw. könnte unbillige Haftungsrisiken (insbesondere) für Leiter:innen nationaler Unternehmensteile von internationalen Konzernunternehmen begründen. In internationalen Konzernen haben nationale Geschäftsleiter:innen oftmals keinen Einfluss auf wesentliche Aspekte des Risikomanagements. Auch bei der Abwehr physischer Gefahren bestehen i.d.R. unternehmensweite Standards oder aber es kommen bereits gesetzliche Vorschriften zu Umsetzung. Gerade im letzteren Fall erübrigt sich, dass Geschäftsleiter:innen Maßnahmen billigen (diese sind vorgeschrieben) oder überwachen (obliegt der Aufsichtsbehörde). Konkret ist keine Veranlassung erkennbar, weshalb ein:e Geschäftsleiter:in zusätzlich zur mit der Umsetzung von „Spezialvorschriften“ betrauten Fachabteilung eine zusätzliche Rolle bzw. Obliegenheit haben sollte. Hier wäre mindestens ein Halbsatz in § 14 zur Klarstellung nützlich („...mit Ausnahme solcher Maßnahmen gemäß § 4 Abs. 7,“).
- Insofern an der Verpflichtung festgehalten wird, sollte daher „der Geschäftsleiter“ mit „die für die Sicherheit und Resilienz zuständige Person“ ersetzt werden, die aufgrund von Verantwortlichkeiten und rechtlichen Konsequenzen eindeutig definiert sein muss.

Zu § 16 - Ermächtigung zum Erlass von Rechtsverordnungen

- Die in Abs. 1 normierte Einbindung von betroffenen Betreibern kritischer Anlagen und weiteren Beteiligten wie Wirtschaftsverbände durch das BMI bei der Bestimmung von kritischen Anlagen qua Rechtsverordnung wird begrüßt. Gemäß § 16 Abs. 2 dürfen einige weitere Bundesministerien, u.a. das BMDV, weitere sektorspezifische Mindestvorgaben für Betreiber kritischer Anlagen bestimmen. Die Sinnhaftigkeit dieser ergänzenden Regelung ist nicht nachvollziehbar. Es sollte kritisch überprüft werden, ob solche ergänzenden Regelungen notwendig sind. Diese stellen ggf. eine deutliche Erhöhung der Komplexität dar und sind ggf. nicht widerspruchsfrei. Die Bestimmung von kritischen Anlagen sollte in einer Hand liegen.

- Soweit an der Einbeziehung weiterer Bundesministerien festgehalten wird, sollten auch die betroffenen Betreiber und Wirtschaftsverbände in die Anlagenbestimmung mit einbezogen werden.

§ 16 Abs. 2 sollte wie folgt formuliert sein (Ergänzungen in blau):

„Das Bundesministerium für Wirtschaft und Klimaschutz, das Bundesministerium für Ernährung und Landwirtschaft, das Bundesministerium für Gesundheit, das Bundesministerium für Digitales und Verkehr und das Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz werden ermächtigt, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber kritischer Anlagen und Einrichtungen der Bundesverwaltung und Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium des Innern und für Heimat, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, im Rahmen ihrer jeweiligen Zuständigkeiten für kritische Dienstleistungen sektorspezifische Mindestvorgaben für Betreiber kritischer Anlagen zu bestimmen, die die Vorgaben des § 10 konkretisieren. Das Bundesministerium des Innern und für Heimat wird ebenfalls ermächtigt, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber kritischer Anlagen und Einrichtungen der Bundesverwaltung und Wirtschaftsverbände, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, im Rahmen seiner Zuständigkeiten für kritische Dienstleistungen sektorspezifische Mindestvorgaben für Betreiber kritischer Anlagen zu bestimmen, die die Vorgaben des § 10 sektorspezifisch konkretisieren.“

Zu § 17 - Ausnahmebescheid

- Bei der Identifizierung von kritischen Anlagen besteht aus unserer Sicht die Notwendigkeit, auch die öffentliche Bundesverwaltung - insbesondere rund um die öffentliche Sicherheit - mit einzubeziehen. Hier sollte der gleiche Maßstab wie bei Betreibern vom KRITIS angesetzt werden, so dass eine Bundesverwaltung mit Zuständigkeit für mehr als 500.000 Bürger unter die Bestimmungen des KRITIS-DachG fallen sollte. Dies ist nur stringent, da Betreiber kritischer Anlagen im Falle einer großflächigen Krise, welche durch das BBK koordiniert werden soll, von dessen Einsatzfähigkeit abhängig sind. Für solche Fälle muss das BBK in die Lage versetzt werden, dieser Verpflichtung nachzukommen und nicht selbst durch sicherheitstechnische Probleme handlungsunfähig sein. Unter diesem Aspekt bewerten wir den Ausnahmebescheid als kritisch.

Zu § 18 - Verarbeitung personenbezogener Daten

- Bei der Verarbeitung von personenbezogenen Daten in § 18 Abs. 2 wären Beispiele hinsichtlich des schutzwürdigen Interesses hilfreich und dienen der Klarheit des personenbezogenen Datenschutzes.