VERBAND DER INTERNETWIRTSCHAFT E.V.

STELLUNGNAHME

zum Referentenentwurf für ein Gesetz zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz – KRITIS-DachG)

Berlin, 4. September 2025

Mit dem KRITIS-Dachgesetz (KRITIS-DachG) werden in Deutschland erstmals bundesweit einheitliche Vorgaben zum physischen Schutz kritischer Anlagen geschaffen. Gleichzeitig soll mit dem Gesetz auch die europäische „Richtlinie über die Resilienz kritischer Einrichtungen und zur Aufhebung der Richtlinie 2008/114/EG des Rates“ (CER-Richtlinie) in deutsches Recht überführt werden. Das KRITIS-DachG ist aus komplementär mit dem im parlamentarischen Verfahren befindlichen „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS2UmsuCG)“ zu sehen. Hier sind die Regeln und Vorgaben für digitale Unternehmen zentral geregelt. Aus Sicht der Internetwirtschaft und im Sinne einer stringenten und nachvollziehbaren Gesetzgebung ist es daher sinnvoll, die Vorgaben für IT-Unternehmen im NIS2UmsuCG zu bündeln. Die Vorgaben aus dem KRITIS-DachG sollten dementsprechend für die Internetwirtschaft nicht in größerem Umfang relevant sein. Auch sollte bei der Gesetzgebung darauf geachtet werden, dass durch die beiden Gesetze keine Unklarheiten oder Doppelregulierung geschaffen wird.

eco – Verband der Internetwirtschaft e.V. nimmt zu dem vorliegenden Entwurf des KRITIS-Dachgesetzes (KRITIS-DachG-E) wie folgt Stellung.

▪ Erfüllungsaufwand

Der aktuelle Referentenentwurf enthält keine belastbare Schätzung des Erfüllungsaufwands für die Wirtschaft, da sowohl die konkretisierende Rechtsverordnung als auch wesentliche Risikoanalysen noch ausstehen (vgl. E.2). Mit der ersatzlosen Streichung des zuvor vorgesehenen Belastungsrichtwerts fehlt den betroffenen Betreibern jedoch jegliche Orientierung über die voraussichtliche finanzielle Größenordnung der neuen Anforderungen. Ohne einen solchen Orientierungsrahmen ist es den Unternehmen nicht möglich, Rückstellungen und Investitionen planungssicher vorzubereiten. Dies führt zu erheblicher Rechts- und Investitionsunsicherheit und konterkariert das Ziel, Resilienzmaßnahmen in effizienter und wirtschaftlich tragfähiger Weise umzusetzen. Es ist daher zwingend erforderlich, dass zeitnah eine belastbare Kostenabschätzung vorgelegt und damit eine Grundlage für verlässliche Finanz- und Investitionsentscheidungen geschaffen wird.

- **Resilienz- und Nachweispflichten**

Die vorgesehenen Resilienz- und Nachweispflichten, darunter Risikoanalysen und -bewertungen (§ 12 KRITIS-DachG-E), die Erstellung von Resilienzplänen (§ 13 Abs. 4), Nachweisdokumentationen (§ 16) sowie Berichtspflichten gegenüber nationalen Behörden und der Europäischen Kommission (§ 21), verfolgen grundsätzlich das richtige Ziel, die Widerstandsfähigkeit kritischer Anlagen gegenüber vielfältigen Gefahren zu erhöhen.

In ihrer aktuellen Ausgestaltung droht jedoch eine Überregulierung. Betreiber müssen künftig parallel bestehende IT-Sicherheitskonzepte nach BSIG/NIS2 und Resilienzpläne nach KRITIS-DachG vorhalten. Dies führt zu erheblichem Mehraufwand, Doppelprüfungen verbunden mit hohen zusätzlichen Kosten. Insbesondere, da Risikoanalysen standortbezogen durchzuführen sind und häufig externe Expertise sowie neue Tools erforderlich machen. Für kleine und mittlere Betreiber, die nur knapp über den Schwellenwert fallen, stellt dies eine unverhältnismäßige Belastung dar.

Zwar enthält der Entwurf in § 17 eine Öffnungsklausel, wonach gleichwertige Nachweise aus anderen Gesetzen anerkannt werden können. Diese Regelung bleibt jedoch zu unbestimmt und bietet den Betreibern keine Planungssicherheit. Positiv hervorzuheben ist, dass branchenspezifische Standards nach dem BSI-Gesetz grundsätzlich als Grundlage für Resilienzstandards nach dem KRITIS-DachG dienen können. Dieser Ansatz sollte verbindlicher ausgestaltet werden, um Doppelstrukturen zu vermeiden und die Praxistauglichkeit der Nachweise zu erhöhen. Um unnötige Bürokratie und Doppelarbeit zu vermeiden, ist eine weitergehende Harmonisierung mit den bestehenden IT-Sicherheitsgesetzen erforderlich. Dazu gehören klare und verbindliche Regelungen zur gegenseitigen Anerkennung von Nachweisen sowie abgestimmte Prüfverfahren. Nur so kann gewährleistet werden, dass Resilienzpflichten wirksam, verhältnismäßig und zugleich wirtschaftlich tragfähig umgesetzt werden.

- **Fehlende Konkretisierung durch Rechtsverordnung**

Ein zentrales Problem des Referentenentwurfs besteht darin, dass die für die Umsetzung wesentliche Rechtsverordnung zur Bestimmung der kritischen Dienstleistungen und Anlagen bislang nicht vorliegt. Nach §§ 4 Abs. 3 und 5 Abs. 1 KRITIS-DachG-E ist das BMI ermächtigt, in einer gesonderten Verordnung sowohl die kritischen Dienstleistungen als auch die maßgeblichen Anlagenkategorien und Schwellenwerte zum Versorgungsgrad festzulegen. Erst durch diese Konkretisierung wird für die Betreiber verbindlich klar, ob sie in den Anwendungsbereich des Gesetzes fallen und welche Pflichten damit verbunden sind.

Solange diese Rechtsverordnung aussteht, entsteht für Unternehmen erhebliche Rechtsunsicherheit. Sie können weder den Umfang ihrer künftigen Pflichten abschätzen noch notwendige Investitionen und organisatorische Anpassungen rechtzeitig planen. Auch belastbare Aussagen zum finanziellen und administrativen Aufwand sind ohne Kenntnis der konkreten Anlagen- und

Dienstleistungsdefinitionen nicht möglich. Dies widerspricht dem Ziel der Planbarkeit und Verlässlichkeit, das für Unternehmen mit hohen Investitions- und Sicherheitsverpflichtungen unabdingbar ist.

Eine zeitnahe Vorlage der konkretisierenden Rechtsverordnung ist daher zwingend erforderlich. Zudem sollte das Gesetz sicherstellen, dass deren Erarbeitung in einem transparenten Verfahren erfolgt und die betroffenen Branchen frühzeitig einbezogen werden, um Rechtssicherheit und eine angemessene Legitimation zu gewährleisten. Vor allem die Schwellenwerte sollten einer kritischen Prüfung unterzogen werden, um sicherzustellen, dass sie risikoadäquat und sektorspezifisch ausgestaltet sind.

- **Zuständigkeits- und Abgrenzungsfragen**

Die vorgesehene Aufgabenverteilung zwischen Bund, Ländern sowie den zuständigen Bundesbehörden (insbesondere BBK und BSI) bleibt im Entwurf unklar. Während das BBK als zentrale Anlaufstelle vorgesehen ist, behalten die Länder zugleich ihre Regelungskompetenzen außerhalb des KRITIS-DachG. Dies birgt die Gefahr von Doppelzuständigkeiten, unklaren Schnittstellen und administrativen Redundanzen. Auch das Verhältnis zwischen BBK und BSI ist nicht hinreichend konkretisiert. Es bleibt offen, wie sich die beiden Behörden sinnvoll ergänzen sollen, ohne für Betreiber zusätzliche Belastungen durch parallele Anforderungen oder Prüfverfahren zu erzeugen.

Besonders deutlich wird dies im Hinblick auf den Sektor Informationstechnik und Telekommunikation (§ 4 Abs. 2 Nr. 2). Zwar sind bestimmte Pflichten des KRITIS-DachG hier ausgenommen, dennoch verbleibt ein Nebeneinander von Verpflichtungen aus BSIG/NIS2 und dem neuen Dachgesetz. Dies widerspricht dem Grundsatz einer kohärenten Regulierung und führt zu doppeltem Aufwand für die betroffenen Betreiber.

Es ist daher erforderlich, klare Abgrenzungen zwischen den Kompetenzen von Bund, Ländern, BBK und BSI zu schaffen und die Schnittstellen verbindlich zu regeln. Zudem sollte die IT-/TK-Branche vollständig aus dem Anwendungsbereich des KRITIS-DachG ausgenommen werden, da für diesen Sektor bereits ein eigenständiger, umfassender Regulierungsrahmen durch BSIG und NIS2 besteht. Nur so lassen sich Doppelregulierungen und unverhältnismäßige Belastungen für die betroffenen Unternehmen vermeiden.

- **Zu § 4: Sektoren; Geltungsbereich; Verordnungsermächtigung**

§ 4 Abs. 5 KRITIS-DachG-E sieht ausdrücklich vor, dass ein Zugang zu den Akten, die die Erstellung oder Änderung von Rechtsverordnungen betreffen, nicht gewährt wird. Dies bedeutet, dass das BMI weitreichende Änderungen etwa zu Geltungsbereichen oder Schwellenwerten ohne Bundesratszustimmung und ohne Transparenz hinsichtlich der Entscheidungsgrundlagen vornehmen kann. Gerade bei Regelungen, die erhebliche neue Betreiberpflichten begründen oder bestehende Verpflichtungen erweitern, sind jedoch Nachvollziehbarkeit und demokratische Legitimation unerlässlich. Die vollständige Ausschlussregelung steht

im Spannungsverhältnis zu Grundsätzen von Transparenz und parlamentarischer Kontrolle und birgt das Risiko, das Vertrauen in die Rechtssetzung zu schwächen. Aus Sicht der Internetwirtschaft ist daher eine Korrektur geboten. Die Ausschlussklausel sollte entweder gestrichen oder zumindest eingeschränkt werden.

- **Zu § 12: Risikoanalyse und Risikobewertung des Betreibers kritischer Anlagen; Verordnungsermächtigung**

Mit § 12 KRITIS-DachG-E wird für Betreiber kritischer Anlagen die Pflicht eingeführt, mindestens alle vier Jahre eine Risikoanalyse und -bewertung auf Grundlage staatlicher sowie weiterer vertrauenswürdiger Informationsquellen durchzuführen. Dabei sind sowohl naturbedingte, klimatische und vom Menschen verursachte Risiken (§ 11 Abs. 2 Nr. 1) als auch Abhängigkeiten von und zwischen kritischen Dienstleistungen (§ 12 Abs. 1 Nr. 2) zu berücksichtigen. Für die Betreiber bleibt jedoch unklar, wie diese Anforderungen von den bereits nach dem NIS2UmsuCG in dreijährigem Turnus zu erbringenden Nachweisen zur Erfüllung der gesetzlichen Cybersicherheitsanforderungen abzugrenzen sind. Eine kohärente Abstimmung der Vorgaben zwischen dem KRITIS-Dachgesetz und dem NIS2UmsuCG, wie sie seitens der Wirtschaft und auch von eco bereits in den Anhörungen der vergangenen Legislaturperiode eingefordert wurde, ist erneut ausgeblieben. Damit besteht weiterhin das Risiko einer Doppelbelastung durch parallele Berichtspflichten sowie rechtlicher und praktischer Unsicherheiten für die Betreiber.

- **Zu § 16: Nachweise und behördliche Anordnungen zu Resilienzpflichten**

Der Referentenentwurf enthält keine hinreichend klaren Regelungen zu den Rechtsfolgen im Falle einer nicht bestandenen Prüfung von Nachweisen und Resilienzpflichten. Zwar sieht § 16 Abs. 5 KRITIS-DachG-E vor, dass Behörden die Vorlage eines Mängelbeseitigungsplans innerhalb einer „angemessenen Frist“ anordnen können. Die Ausgestaltung bleibt jedoch unbestimmt und eröffnet einen weiten Ermessensspielraum. In der Folge besteht für Betreiber das Risiko, unmittelbar mit Bußgeldern (§ 24 KRITIS-DachG-E), Zwangsmaßnahmen oder im Extremfall Betriebseinschränkungen konfrontiert zu werden, ohne dass zuvor ein verbindliches, gestuftes Verfahren zur Nachbesserung durchlaufen wurde.

Dies schafft erhebliche Rechtsunsicherheit und könnte in der Praxis unverhältnismäßige Belastungen zur Folge haben. Hinzu kommt, dass mangels klarer Abgrenzung zwischen KRITIS-DachG und BSIG/NIS2 parallele Verfahren drohen. Betreiber könnten somit für denselben Mangel doppelt sanktioniert werden.

Um Rechtssicherheit und Verhältnismäßigkeit zu gewährleisten, sollte der Gesetzgeber ein transparentes Stufenmodell verankern: Zunächst die Feststellung des Mangels und eine verbindliche Nachbesserungsfrist, sodann eine erneute Prüfung und erst bei fortgesetzter Nichterfüllung die Verhängung von Sanktionen

(Bußgeld, Zwangsmaßnahmen o.ä.). Dies würde sowohl die Effektivität der Aufsicht als auch die Planbarkeit für die Betreiber deutlich verbessern.

- **Zu § 18: Meldewesen für Vorfälle**

§ 18 KRITIS-DachG-E sieht die Schaffung einer zentralen Meldestelle beim BBK in Kooperation mit dem BSI vor, an die Betreiber kritischer Anlagen relevante Vorfälle innerhalb von 24 Stunden zu melden haben. Der Ansatz, die Informationsflüsse an einer Stelle zu bündeln, ist grundsätzlich zu begrüßen. Allerdings sieht der Entwurf keine Fallback-Regelungen für den Fall vor, dass das Meldeportal durch technische Störungen, Cyberangriffe oder Überlastung selbst nicht verfügbar ist. Für Betreiber besteht damit das Risiko, ihrer gesetzlichen Meldepflicht im Ernstfall nicht nachkommen zu können und formell in eine Pflichtverletzung zu geraten, obwohl die Ursache in einer behördlichen Infrastrukturschwäche läge. Dies ist für die Wirtschaft unzumutbar und widerspricht dem Grundgedanken eines verlässlichen Meldewesens. Aus Sicht der Betreiber ist daher eine klare gesetzliche Regelung erforderlich, die alternative Meldewege (z. B. E-Mail, Telefon o.ä.) vorsieht und sicherstellt, dass bei nachweislich unternommenen Meldeversuchen keine nachteiligen Rechtsfolgen entstehen.

Fazit

Der Referentenentwurf zum KRITIS-DachG setzt ein wichtiges Signal für die Stärkung der Resilienz kritischer Anlagen. In der aktuellen Form bestehen jedoch noch einige Unsicherheiten. Die ausstehende Rechtsverordnung zu kritischen Dienstleistungen und Anlagen verhindert verlässliche Planungen, die vorgesehenen Nachweis- und Prüfpflichten drohen Doppelregulierungen mit bestehenden IT-Sicherheitsgesetzen zu schaffen und die unklare Rollenverteilung zwischen Bund, Ländern sowie BBK und BSI führt zu Schnittstellenproblemen. Zudem fehlen klare Nachbesserungsfristen, wodurch das Risiko unverhältnismäßiger Sanktionen steigt.

Hervorzuheben ist, dass der Entwurf immerhin mit dem Allgefahrenansatz einen umfassenden Rahmen vorsieht, der klassische Bedrohungen ebenso berücksichtigt wie neuartige Risiken (Spionage, Sabotage, Ausspähen und Gefährdung durch Drohnen). Die Möglichkeiten müssen nun vom Gesetzgeber nachhaltig genutzt werden, um behördliche Strukturen und wirtschaftliche Akteure stärker zu verzahnen und gemeinsam innovative Lösungen für den Schutz kritischer Infrastrukturen zu entwickeln. Wird dieser Ansatz durch ein nachvollziehbares Verfahren mit klar geregelten Zuständigkeiten und einer engeren Beteiligung der betroffenen Branchen unterlegt, kann er sich zu einem wirksamen und praxistauglichen Instrument für die langfristige Stärkung der Resilienz entwickeln.

Über eco: Mit rund 1.000 Mitgliedsunternehmen ist eco (www.eco.de) der führende Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, schafft Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. eco hat Standorte in Köln, Berlin und Brüssel. eco setzt sich in seiner Arbeit vorrangig für ein leistungsfähiges, zuverlässiges und vertrauenswürdiges Ökosystem digitaler Infrastrukturen und Dienste ein.