21. Wahlperiode

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache 21(4)106
vom 28. November 2025

Schriftliche Stellungnahme

von VATM e.V., Berlin vom 28. November 2025

zu dem

Gesetzentwurf der Bundesregierung

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

BT-Drucksache 21/2510

VATM e. V. ■ Reinhardtstr. 31 • 10117 Berlin

Via Mail an: innenausschuss@bundestag.de

An den amtierenden Vorsitzenden
Herrn Josef Oster MdB
Innenausschuss des Deutschen Bundestages
Platz der Republik 1
11011 Berlin

Ansprechpartner/in	E-Mail	Telefon	Datum
Gerrit Wernke / Solveig Orlowski	gw@vatm.de / so@vatm.de	030 / 506 615 38	28.11.2025

VATM-Stellungnahme zum Regierungsentwurf für ein Gesetz zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz)

Der **Verband der Anbieter im Digital- und Telekommunikationsmarkt e. V. (VATM) nimmt wie folgt zum Entwurf** für ein Gesetz zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen (KRITIS-Dachgesetz) Stellung:

Mit dem KRITIS-Dachgesetz soll die Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022, die sogenannte CER-Richtlinie, in nationales Recht überführt werden. Ziel soll es sein, die Resilienz und Sicherheit kritischer Infrastrukturen zu stärken, indem Betreiber zu wirksamen physischen und organisatorischen Maßnahmen verpflichtet werden. Durch das bereits laufende Vertragsverletzungsverfahren durch die überschrittene Umsetzungsfrist vom 18. Oktober 2024 und die vorgezogenen Neuwahlen, die den vorangegangenen Gesetzgebungsprozess in die Diskontinuität führten, ist eine Umsetzung überfällig.

Die hohe Notwendigkeit eines handlungsfähigen Rechtsrahmens wird nicht zuletzt durch die gegenwärtige Gefahrenlage deutlich: Kritische Infrastrukturen rücken verstärkt in den Fokus internationaler Spionage und Sabotage, sodass aus möglichen Risiken konkrete Bedrohungen werden. Zeitgemäße Schutzmaßnahmen lassen sich im Schulterschluss mit der Wirtschaft entwickeln und weiter vorantreiben. Damit das gelingt, braucht es eindeutige Zuständigkeiten, transparente Vorgaben und einen flexiblen Handlungsspielraum für alle Beteiligten.

Ganz wichtig muss es deswegen sein, dass das KRITIS-DachG Schutzpflichten harmonisiert, die Kooperation zwischen Staat, Wirtschaft und Gesellschaft verbindlich stärkt und wirksame Notfall- und Krisenmechanismen etabliert. Die Orientierung an den Schwellenwerten nach der BSI-KritisVO ist dabei ein wichtiger Anker für eine kohärente Umsetzung.

Der VATM möchte in diesem Zusammenhang zu Beginn die folgenden Punkte hervorheben:

- **Umsetzungsfristen**: Sowohl das Gesetz als auch die Rechtsverordnung, die die Anforderungen konkretisiert, haben sich weiter verzögert. Zugleich hält der (neue) Gesetzentwurf an den ursprünglichen Umsetzungsstichtagen fest. Dadurch verkürzt sich die verbleibende Umsetzungszeit für KRITIS-Betreiber erheblich, was zu einer deutlichen Mehrbelastung führt.

- **Harmonisierung mit der NIS-2-Umsetzung**: Trotz erheblicher Schnittmengen bestehen weiterhin Differenzen zwischen NIS2UmsuCG und KRITIS-DachG, die sich in der Praxis als problematisch erweisen. Abweichende Begrifflichkeiten sowie unterschiedlich ausgestaltete Anforderungen – etwa bei personeller Sicherheit, Sicherheitsüberprüfungen oder alternativen Lieferketten – erschweren eine einheitliche Betroffenheitsprüfung und erhöhen die Komplexität unnötig. Dieser äußerst wichtige Punkt wurde ebenfalls in der Anhörung zum NIS2UmsuCG am 4. Juli 2025 noch einmal seitens des VATM betont.

- **Doppelregulierung**: Doppelte regulatorische Vorgaben sind konsequent auszuschließen. Viele Branchen – insbesondere auch die der Telekommunikation – arbeiten bereits mit etablierten Sicherheitskatalogen oder spezifischen Anforderungen. Zusätzliche Regelungen aus dem KRITIS-DachG sollten diese bestehenden Vorgaben berücksichtigen, statt parallele Pflichten einzuführen.

- **Erfüllungsaufwand**: Die bisherigen Angaben zum Erfüllungsaufwand sind unzureichend. Für die betroffenen Unternehmen ist eine transparente, fortlaufend aktualisierte Aufwandsschätzung erforderlich – insbesondere mit Blick auf die wirtschaftlichen Auswirkungen.

Der Schutz der kritischen Infrastruktur ist eine ganzheitliche Aufgabe, die die Mitgliedsunternehmen des VATM mit aller Verantwortung übernehmen. Die hierfür nötigen gesetzlichen Rahmenbedingungen müssen dieser bedeutenden Aufgabe gerecht werden. Der VATM hofft dabei, dass der nun vorliegende Entwurf im weiteren Gesetzgebungsverfahren nochmals verbessert werden kann.

Im Einzelnen möchten wir gerne auf die folgenden Punkte hinweisen:

Zur Kohärenz zwischen der Umsetzung der NIS-2-Richtlinie und dem KRITIS-DachG

Gesetzliche Vorgaben zur physischen Sicherheit und zur Cybersicherheit müssen passgenau zueinander gestaltet werden. Dies ist eine wesentliche Voraussetzung, um eine einfache und praktikable Rechtsanwendung für alle Unternehmen sicherzustellen. Einheitliche Begriffsdefinitionen sowie überschneidungs- und widerspruchsfreie Vorgaben in beiden Regelungsbereichen sind hierfür zentral. Mit dem neuen Entwurf gibt es in diesem Zusammenhang weiterhin noch offene Fragen zur Kohärenz mit der Umsetzung der NIS-2-Richtlinie.

Verband der Anbieter im Digital- und Telekommunikationsmarkt (VATM) e.V.
Reinhardtstr. 31 • 10117 Berlin • Tel.: 030 50561538 • E-Mail: vatm@vatm.de

Auch vor dem Hintergrund der parallel erfolgten Ausgestaltung des gesetzlichen Rahmens für die Cybersicherheit (NIS2UmsuCG) und die physische Sicherheit kritischer Infrastrukturen (KRITIS-DG) sind weiterhin eindeutige und überschneidungsfreie Regelungen in Bezug auf die behördlichen Zuständigkeiten erforderlich. Diese Regelungen müssen berücksichtigen, dass KRITIS-Unternehmen auch nach den für sie geltenden spezialgesetzlichen Regelungen (z. B. dem TKG) einer aufsichtsbehördlichen Kontrolle (z. B. durch die BNetzA) unterliegen. In diesem Zusammenhang bleibt es sinnvoll, für Unternehmen einen Single-Point-of-Contact (SPOC) unter den Behörden einzurichten, damit Informationen bzw. Meldungen „in“ und „aus“ den Unternehmen ohne Zeitverlust und möglichst wirksam und zielgerichtet verarbeitet werden können.

Gemäß den unionsrechtlichen Vorgaben nach § 4 Absatz 2 sind für bestimmte Sektoren – darunter Informationstechnik und Telekommunikation – Ausnahmen vorgesehen. In der aktuellen Entwurfsfassung verbleibt jedoch die Registrierungspflicht nach § 8, die bereits in der NIS-2 sowie im entsprechenden Umsetzungsgesetz geregelt ist. Die nur teilweise Herausnahme dieser Sektoren aus dem Anwendungsbereich des KRITIS-DachG führt zu vermeidbaren Rechtsunsicherheiten. Vor diesem Hintergrund empfiehlt der VATM, die Sektoren Informationstechnik und Telekommunikation vollständig aus dem Anwendungsbereich des KRITIS-DachG herauszunehmen.

Zu den betroffenen Sektoren und deren Definition

Das KRITIS-DachG enthält keine sektor- oder gar branchenspezifischen Detailregelungen, sondern legt abstrakt fest, dass in allen KRITIS-Sektoren geeignete und verhältnismäßige Maßnahmen zum physischen Schutz kritischer Anlagen zu treffen sind. Angesichts des Umsetzungsaufwands bis 2026 sind eine praxisnahe Unterstützung der Betreiber und eine möglichst schnelle Arbeits- und Lieferfähigkeit des BBK, insbesondere bei Vorgaben zur Risikobewertung und zu Resilienzplänen, erfolgsentscheidend. Der Entwurf bleibt hier insgesamt zu unkonkret. Unklar ist, ob die vom BBK vorgesehenen Vorlagen, Muster und Leitlinien für Unternehmen verbindlich sein sollen; falls nicht, könnte im Sinne der Ressourcenschonung darauf verzichtet werden.

Zur Vereinheitlichung und Konkretisierung der Anforderungen ist die Beibehaltung und teilweise Neuentwicklung branchenspezifischer Standards, ergänzend zu horizontal wirkenden Standards, für die Umsetzung innerhalb und zwischen den Sektoren wichtig. Positiv hervorzuheben ist, dass die branchenspezifischen Resilienzstandards künftig öffentlich beim BBK abrufbar sein werden.

Verband der Anbieter im Digital- und Telekommunikationsmarkt (VATM) e.V.
Reinhardtstr. 31 • 10117 Berlin • Tel.: 030 50561538 • E-Mail: vatm@vatm.de

Zur Feststellung der Erheblichkeit einer Anlage

Die in § 5 Absatz 3 vorgesehene Möglichkeit, dass das Bundesministerium des Innern im Einzelfall die Erheblichkeit einer Anlage für die Erbringung einer kritischen Dienstleistung feststellen kann – selbst, wenn die Voraussetzungen der Rechtsverordnung nach Absatz 1 Satz 1 nicht erfüllt sind – ist kritisch zu bewerten. Die Formulierung erlaubt eine einseitige Feststellung der Kritikalität durch das BMI und führt zu rechtlicher Unsicherheit sowie Planungsproblemen für Unternehmen. Zudem erschwert sie eine nachvollziehbare und einheitliche Risiko- und Sicherheitsbewertung auf Unternehmensseite und kann durch mögliche Einzelentscheidungen zu unnötigen Belastungen führen.

Zu den Erfüllungsaufwänden

In den ausgewiesenen Erfüllungsaufwänden fehlt eine Darstellung der Aufwände für die Wirtschaft. Es gilt, die finanziellen Auswirkungen auf betroffene Unternehmen zu quantifizieren, um die Effizienz des Gesetzes bewerten zu können. Als Kompromiss sprechen wir uns dafür aus, weitgehend auf die Verlagerung von Regelungen in Rechtsverordnungen zu verzichten und diese unmittelbar im Gesetz zu verankern. So ließe sich der Erfüllungsaufwand seriös und belastbar abschätzen.

In diesem Kontext fordern wir zudem eine Anpassung des Punktes F „Weitere Kosten“. Investitionen und Aufwendungen der Wirtschaft zur Erhöhung von Resilienz und Sicherheit sollten auf die Produkte und Dienstleistungen der betroffenen Unternehmen umlegbar sein. Die bisherige Formulierung legt hingegen nahe, dass eine Steigerung von Resilienz und Sicherheit keine Kosten verursache.

Zur KRITIS-Resilienzstrategie

Der VATM begrüßt die Vorlage einer nationalen KRITIS-Resilienzstrategie. Diese sollte jedoch vor der Festlegung regulatorischer Pflichten für KRITIS-Betreiber vorliegen. Um frühzeitig Klarheit und Planungssicherheit für die betroffenen Unternehmen zu gewährleisten, sollte zudem weitgehend auf Rechtsverordnungen verzichtet und die zentralen Regelungen sollten direkt im Gesetz verankert werden.

Zum Registrierungs- und Meldewesen inkl. Registrierung kritischer Anlagen

Im Ernstfall sollten Meldungen betroffener Unternehmen ausschließlich an eine zentrale Stelle – oder zumindest an wenige klar definierte Stellen – gehen und einheitlichen Kriterien folgen. Parallelstrukturen zwischen BBK und BSI, etwa durch getrennte Registrierungs- oder Meldeportale, sind zu vermeiden. Ebenso darf es nicht dazu kommen, dass bundesweit tätige Unternehmen mit unterschiedlichen länderspezifischen Auslegungen einer Bundesregelung konfrontiert werden. Um einer Zersplitterung zwischen Bundes- und Länderzuständigkeiten vorzubeugen, sollte daher eine zentrale Stelle eingerichtet werden, die die Harmonisierung und Koordinierung der den Ländern zugewiesenen Regelungsbereiche übernimmt.

Verband der Anbieter im Digital- und Telekommunikationsmarkt (VATM) e.V.
Reinhardtstr. 31 • 10117 Berlin • Tel.: 030 50561538 • E-Mail: vatm@vatm.de

Hinzu kommt die derzeitige Unklarheit zu konkreten Mindestmaßnahmen. Zwar ist vorgesehen, branchenspezifische Resilienzstandards zu erarbeiten und freizugeben, diese liegen bislang jedoch nicht vor. In der Zwischenzeit könnten BMI, Bundesressorts oder Landesregierungen eigene Mindestvorgaben festlegen, mit der Folge zusätzlicher Fragmentierung.

Von zentraler Bedeutung ist darüber hinaus ein medienbruchfreies Registrierungs- und Meldeportal. Meldungen müssen digital eingereicht werden können; eine automatische Weiterleitung und Bearbeitung durch die zuständige Behörde sind sicherzustellen – ohne weiteren Aufwand für die Unternehmen. Auch hier gilt eine bestmögliche Harmonisierung mit der NIS-2-Umsetzung.

In § 8 sollte weiterhin sichergestellt werden, dass Unternehmen, die ihre Anlagen bereits beim BSI gemeldet haben, kein erneutes Registrierungsverfahren durchlaufen müssen. Eine Übernahme der bestehenden Daten mit der Möglichkeit zur bedarfsweisen Aktualisierung wäre sachgerecht und würde unnötige Mehrbelastungen vermeiden.

Ferner werfen einzelne Anforderungen in § 8 Absatz 1 Fragen auf. Die unter Nummer 4 genannten öffentlichen IP-Adressbereiche sind nicht hinreichend nachvollziehbar und bedürfen einer Konkretisierung. Ebenso sollte klargestellt werden, dass die in Nummer 6 geforderte Kontaktstelle ausschließlich die Erreichbarkeit über Leitstellen sicherstellt. Eine Pflicht, jederzeit unmittelbare fachliche Expertise zum Objektschutz vorzuhalten, wäre unverhältnismäßig und führte zu zusätzlichen Aufwänden für die Unternehmen.

Zu den Nachweispflichten

Um den Prüf- und Auditaufwand der betroffenen Unternehmen zu reduzieren, sollten entsprechende vorhandene Nachweise anerkannt werden. Resilienzmaßnahmen können nach verschiedenen ISO-Standards (z. B. ISO 22316, 22320, 22301, 31000 u. a.) zertifiziert und auditiert werden; diese Standards eignen sich als Belege für umgesetzte Maßnahmen.

Ferner muss grundsätzlich gewährleistet sein, dass Nachweise aus anderen Zertifizierungen und Genehmigungen auch im Rechtskontext des KRITIS-DG anerkannt und verwendet werden können. Es sollte sichergestellt werden, dass BBK und/oder BSI auf etablierte Normen und Standards Bezug nehmen. Dies ist eine zentrale Voraussetzung dafür, die Sicherheit zu erhöhen und eine europaweite Vergleichbarkeit herzustellen. Es hilft außerdem, die Kosten für Antragsteller und Behörden in einem angemessenen Rahmen zu halten und die Prozesse beherrschbar, wiederholbar und planbar zu gestalten.

Verband der Anbieter im Digital- und Telekommunikationsmarkt (VATM) e.V.
Reinhardtstr. 31 • 10117 Berlin • Tel.: 030 50561538 • E-Mail: vatm@vatm.de

Zu der weiteren Kommunikation der Behörden

Unabdingbar ist eine zügige und klar geregelte Abstimmung zwischen den Behörden, damit Betreiber kritischer Anlagen größtmögliche Rechtssicherheit über ihre Pflichten erhalten und auf ein einheitliches Vorgehen vertrauen können. Dazu gehört auch, dass in den Behörden ein mit den betroffenen Unternehmen vergleichbares Schutz- und Resilienz-Niveau gewährleistet wird, um nach der Übermittlung vertraulicher Daten und Geschäftsgeheimnisse deren Vertraulichkeit nicht zu gefährden.

Der Regierungsentwurf des KRITIS-DachG sieht an mehreren Stellen vor, dass das BBK Vorlagen, Muster oder sonstige Vorgaben veröffentlicht, an denen sich betroffene Unternehmen orientieren können. Es ist sicherzustellen, dass diese Unterlagen möglichst frühzeitig vor Inkrafttreten der gesetzlichen Pflichten bereitgestellt werden. So bleibt ausreichend Zeit für Vorbereitung und Implementierung – insbesondere mit Blick auf klare Kriterien, wann eine Meldung nach dem KRITIS-DachG zu erfolgen hat.

In diesem Zusammenhang sollte auch die Bereitstellung eines Sicherheitslageberichts für den Geltungsbereich des KRITIS-DachG geprüft werden. Der IT-Sicherheitslagebericht des BSI wird KRITIS-Betreibern, die unter das IT-Sicherheitsgesetz und die KRITIS-Verordnung fallen, bereits täglich zur Verfügung gestellt.

Verband der Anbieter im Digital- und Telekommunikationsmarkt (VATM) e.V.
Reinhardtstr. 31 • 10117 Berlin • Tel.: 030 50561538 • E-Mail: vatm@vatm.de