bitkom

Stellungnahme

September 2025

KRITIS-Dachgesetz Referentenentwurf

Zusammenfassung

Mit dem KRITIS-Dachgesetz soll die Richtlinie (EU) 2022/2557, die sogenannte CER-Richtlinie, in deutsches Recht überführt werden. Ziel ist es, die Resilienz und Sicherheit kritischer Infrastrukturen zu stärken, indem Betreiber zu wirksamen physischen und organisatorischen Maßnahmen verpflichtet werden. Die Umsetzung ist bereits überfällig. Die nationale Frist vom 18. Oktober 2024 wurde überschritten, die Europäische Kommission hat inzwischen ein Vertragsverletzungsverfahren eingeleitet.

Die Dringlichkeit eines handlungsfähigen Rechtsrahmens zeigt sich auch an der aktuellen Bedrohungslage. Kritische Infrastrukturen geraten zunehmend ins Visier internationaler Spionage und Sabotage, sodass aus potenziellen Risiken reale Gefahren werden. Moderne Schutzmaßnahmen, etwa Technologien zur Drohnendetektion, könnten gemeinsam mit der Wirtschaft entwickelt und weiter ausgebaut werden. Damit dies gelingt, braucht es jedoch klare Zuständigkeiten, transparente Vorgaben und einen flexiblen Handlungsspielraum für alle Beteiligten.

Das KRITIS-DachG sollte daher Schutzpflichten harmonisieren, Kooperation zwischen Staat, Wirtschaft und Gesellschaft verbindlich stärken und wirksame Notfall- und Krisenmechanismen etablieren. Die Orientierung an den Schwellenwerten nach der BSI-KritisVO ist dabei eine wichtige Stütze für eine kohärente Umsetzung. Insgesamt bleibt der aktuelle Entwurf jedoch hinter den Erwartungen zurück. Der Bitkom plädiert deshalb für einen Ansatz, der die Vorschläge dieser Anhörung berücksichtigt und im Dialog mit der Wirtschaft umsetzt. Besonders hervorzuheben sind folgende Punkte:

- **Zu geringe Harmonisierung mit der NIS2-Umsetzung**: Trotz weitgehender Überschneidungen bestehen weiterhin Unterschiede zwischen der NIS-2-Umsetzung und KRITIS-DachG, die in der Praxis problematisch sind. Abweichende Begriffsverwendungen sowie unterschiedlich ausgestaltete Anforderungen, beispielsweise im Bereich personeller Sicherheit, Sicherheitsüberprüfungen oder alternativer Lieferketten, erschweren eine einheitliche Betroffenheitsprüfung und erhöhen die Komplexität unnötig.

- **Doppelregulierung vermeiden**: Doppelte regulatorische Vorgaben gilt es konsequent auszuschließen. Viele Branchen unterliegen bereits etablierten Sicherheitskatalogen oder spezifischen Anforderungen. Zusätzliche Regelungen aus dem KRITIS-DachG sollten diese bestehenden Vorgaben berücksichtigen und anstatt parallele Pflichten einzuführen.
- **Zu knappe Fristen**: Das Gesetz und die dahinter liegende Rechtsverordnung, welche Anforderungen konkretisiert, haben sich nun weiter verzögert. Zeitgleich bleiben die Fristen für Betreiber kritischer Anlagen im (neuen) Gesetzesentwurf auf Juli 2026 bestehen. Damit verkürzt sich die Registrierungsfrist für KRITIS-Betreiber signifikant.
- **Keine Ausnahmen für die Verwaltung**: Ein erheblicher Teil der Bundesverwaltung vom Gesetz ausgenommen und die Landesverwaltungen nicht erst adressiert. Diese Infrastrukturen im KRITIS Sektor "Staat und Verwaltung" sollten Resilienzmaßnahmen ebenso erfüllen wie private Anlagen, ansonsten sind sie weiterhin physischen Risiken ausgesetzt.
- **Angemessenen Erfüllungsaufwand angeben**: Die Angaben zum Erfüllungsaufwand sind bislang unzureichend. Im Entwurf heißt es, dieser könne „in seiner Gesamtheit zum jetzigen Zeitpunkt noch nicht geschätzt werden“. Für die betroffenen Unternehmen ist jedoch eine transparente und fortlaufend aktualisierte Aufwandsschätzung erforderlich, insbesondere im Hinblick auf die wirtschaftlichen Auswirkungen. Zudem bleibt bislang offen, wie die Finanzierung der vorgesehenen Maßnahmen sichergestellt werden soll.
- **Erforderliche Einbindung von Wirtschaftsverbänden**: Für eine praxistaugliche und wirksame Ausgestaltung des Gesetzes ist die frühzeitige und kontinuierliche Einbindung von Wirtschaftsverbänden unverzichtbar. Nur durch die enge Zusammenarbeit mit den betroffenen Akteuren kann ein umsetzbarer Rechtsrahmen geschaffen werden, der Sicherheit erhöht, ohne unnötige Belastungen zu erzeugen.

Notwendige Klarheit und Kohärenz

Harmonisierung KRITIS-DachG und NIS-2

Auch im neuen Entwurf gibt es Fragen zur Kohärenz, die eine sorgfältige Prüfung und mögliche Anpassung, auch im Zusammenspiel mit der Umsetzung der NIS-2-Richtlinie, erfordern. Die Überschneidungen beider Regulierungen müssen konsequent aneinander angeglichen werden.

Entsprechend den EU-rechtlichen Vorgaben gemäß § 4 Absatz 2 sind für bestimmte Sektoren, darunter Informationstechnik und Telekommunikation, Ausnahmen vorgesehen. Übrig bleibt in der aktuellen Fassung des Entwurfs die Registrierungspflicht nach § 8, die jedoch bereits in der NIS-2 sowie im entsprechenden Umsetzungsgesetz geregelt ist. Die teilweise Herausnahme dieser Sektoren aus dem Anwendungsbereich des KRITIS-Dachgesetzes führt zu rechtlichen Unklarheiten, die

vermieden werden sollten. Vor diesem Hintergrund regen wir an, die Sektoren Informationstechnik und Telekommunikation vollständig aus dem Anwendungsbereich des KRITIS-Dachgesetzes herauszunehmen.

Umsetzung in der Praxis

Betroffene Sektoren

Das KRITIS-DachG wird keine sektoren- oder gar branchenspezifischen Regelungen treffen, sondern abstrakt vorgeben, dass in allen KRITIS-Sektoren geeignete und verhältnismäßige Maßnahmen zum physischen Schutz kritischer Anlagen zu treffen sind. Die umsetzungsorientierte Unterstützung der Betreiber ist mit Blick auf den Umsetzungsaufwand bis 2026 hierbei erfolgsentscheidend, ebenso wie eine schnellstmögliche Arbeits- und Lieferfähigkeit des BBKs (insb. bei Vorgaben der Risikobewertung und Resilienzpläne). Hier bleibt der Entwurf insgesamt zu vage. Es ist unklar, ob die bereitgestellten Vorlagen, Muster und Leitlinien durch das BBK für die Unternehmen verbindlich sind. Sollte das Gegenteil der Fall sein, kann hierauf im Sinne der Ressourcenschonung verzichtet werden.

Zur Vereinheitlichung und Spezifizierung der Anforderungen ist die Beibehaltung und teilweise Neuentwicklung von branchenspezifischen Standards (neben den horizontal wirkenden Standards) für die Umsetzung innerhalb und zwischen den Sektoren wichtig. Es ist positiv hervorzuheben, dass die branchenspezifischen Resilienzstandards öffentlich beim BBK abrufbar sein werden.

Obwohl der Begriff „Digitalsektor“ in der Gesetzesbegründung mehrfach aufgegriffen und betont wird, findet er im eigentlichen Normtext, insbesondere in § 4 Absatz 1, keine Erwähnung. Eine ausdrückliche Nennung würde die besondere Bedeutung des Sektors verdeutlichen und zugleich für mehr Klarheit und Rechtssicherheit bei der praktischen Anwendung sorgen.

Staat und Verwaltung umfassend einbeziehen

Die Regelungen in § 5 betreffen ausschließlich Bundesministerien und das Kanzleramt, schließen jedoch nachgeordnete Behörden sowie Landes- und Kommunalverwaltungen aus. Damit bleiben zentrale Teile des KRITIS-Sektors Staat und Verwaltung ungeregelt, obwohl gerade viele Kommunen nicht über ausreichende Ressourcen für eine durchgehende Überwachung ihrer Sicherheitsinfrastrukturen verfügen. Angesichts zahlreicher Angriffe auf die öffentliche Hand ist es notwendig, Verwaltungseinrichtungen aller Ebenen systematisch im KRITIS-Dachgesetz zu berücksichtigen.

In § 7 verschärft die restriktive Definition der „Einrichtungen der Bundesverwaltung“ das Problem zusätzlich. Die Möglichkeit, Maßnahmen durch Verweigerung des Einvernehmens zu blockieren, schwächt die Umsetzung, während Ausnahmen für einzelne Ressorts wie das Auswärtige Amt oder das Verteidigungsministerium die

Kohärenz der Regelung weiter unterlaufen. Um Resilienz verbindlich zu stärken, sollte der Geltungsbereich klar und umfassend gefasst werden.

Erheblichkeit einer Anlage

Die Regelung in § 5 Absatz 3, nach der das Bundesministerium des Innern im Einzelfall feststellen kann, ob eine Anlage für die Erbringung einer kritischen Dienstleistung erheblich ist, auch wenn die Voraussetzungen der Rechtsverordnung des Absatzes 1 Satz 1 nicht erfüllt werden, ist kritisch zu bewerten. Durch diese Formulierung kann die Kritikalität einseitig vom BMI bestimmt werden, was zu rechtlicher Unsicherheit und Planungsproblemen für Unternehmen führen kann. Dies erschwert zudem eine nachvollziehbare und einheitliche Risiko- und Sicherheitsbewertung auf Unternehmensseite und kann zu unnötiger Belastung durch mögliche Einzelentscheidungen führen.

Risikobewertungen

Die in § 12 eingeführten „*vertrauenswürdigen Informationsquellen*“ sind zu unbestimmt. Wir schlagen vor, diese durch „*…und andere, von ihnen als vertrauenswürdig eingeschätzte Informationsquellen*“ zu ersetzen.

Die Bewertungen sollen sich auf Risiken konzentrieren, die von den Anlagenbetreibern bewältigt werden können. Es bestehen Bedenken hinsichtlich der Einbeziehung von hybriden oder feindlichen Bedrohungen, da der Schutz vor solchen Risiken primär in den Verantwortungsbereich staatlicher Gewalt fällt. Die Forderung nach einer klaren Definition von »*hybriden Bedrohungen oder anderen feindlichen Bedrohungen*« (§ 11) wird erhoben, um Rechtsklarheit zu schaffen und Unsicherheiten zu beseitigen. Um nicht nur theoretische Bedrohungen und Maßnahmen zu berücksichtigen, ist eine Mitarbeit der Wirtschaft bei der nationalen Risikoanalyse wünschenswert.

Resilienzpflichten

Der Entwurf des KRITIS-DachG enthält nur wenige Vorgaben dazu, welche konkreten Maßnahmen umzusetzen sind. Stattdessen legt er im Wesentlichen fest, welche Stellen Rechtsverordnungen erlassen müssen, aus denen sich die Pflichten der Unternehmen erst später ergeben. Damit wird der Beginn wirksamer Maßnahmen auf einen unbestimmten Zeitpunkt in der Zukunft verschoben. Ob die vorgesehenen Mindestverpflichtungen tatsächlich zu einer höheren Resilienz kritischer Anlagen und Systeme beitragen, lässt sich auf Grundlage des Referentenentwurfs nicht beurteilen. Für Betreiber entsteht so keine verlässliche Rechtssicherheit.

In Deutschland wurden wiederholt Drohnen über kritischen Infrastrukturen und Bundeswehrliegenschaften registriert. Darin spiegelt sich auch die Taktik des russischen Angriffskriegs gegen die Ukraine mit einer erheblichen Zahl sicherheitsrelevanter Drohnenvorfälle. Der aktuelle Entwurf enthält jedoch keine Vorgaben zur Abwehr solcher Bedrohungen. Hier besteht eine sicherheitspolitische Lücke, da Drohnenangriffe mit vergleichsweise geringem Aufwand erhebliche Schäden verursachen können. Es sollte daher geprüft werden, ob § 13 ohne klare

Anforderungen an den Schutz vor unbemannten Luftfahrtsystemen den heutigen Bedrohungen angemessen Rechnung trägt.

Erfüllungsaufwände

In den aufgeführten Erfüllungsaufwänden fehlt eine Angabe von Aufwänden für die Wirtschaft. Es gilt hier, die finanziellen Auswirkungen auf betroffene Unternehmen abzuschätzen und so das Gesetz auf seine Effizienz zu überprüfen. Als Kompromiss sprechen wir uns dafür aus, möglichst auf die Verlagerung von kostenrelevanten Regelungen in Rechtsverordnungen zu verzichten. Diese sollten stattdessen direkt im Gesetz verankert werden. Damit wäre eine Abschätzung der Erfüllungsaufwände seriös darstellbar, ohne zusätzliche Ungewissheit zu verursachen.

In diesem Kontext fordern wir auch eine Anpassung des Punktes F „Weitere Kosten“. Investitionen und Kosten der Wirtschaft für eine Erhöhung der Resilienz und Sicherheit sollten umlagefähig auf die Produkte und Dienstleistungen der betroffenen Unternehmen sein. Die bisherige Formulierung suggeriert, dass eine Erhöhung der Resilienz und Sicherheit keine Kosten verursacht.

Die derzeitige Formulierung stellt die Umsetzung des KRITIS-Dachgesetzes unter Haushaltsvorbehalt. In der Praxis bedeutet dies, dass Maßnahmen von nachgelagerten Finanzierungsentscheidungen der Ministerien abhängig sind. Damit besteht das Risiko, dass Resilienz nicht als verbindliche Aufgabe verstanden wird, sondern lediglich als Option. Dies steht im Widerspruch zum Ziel, kritische Infrastrukturen systematisch und verbindlich zu stärken.

KRITIS-Resilienzstrategie

Die Vorlage einer Nationalen KRITIS-Resilienzstrategie sollte vor Festlegung von Regulatorischen Verpflichtungen für KRITIS Betreiber vorliegen. Um möglichst frühzeitig Klarheit und Planungssicherheit für die betroffenen Unternehmen zu schaffen, sollte außerdem auf Rechtsverordnungen weitestgehend verzichtet und die zentralen Regelungen bereits im Gesetz verankert werden.

Registrierungs- und Meldewesen

Zuständigkeiten

Im Ernstfall sollten Meldungen betroffener Unternehmen ausschließlich an eine zentrale Stelle oder zumindest an wenige definierte Stellen erfolgen und einheitlichen Kriterien folgen. Wir begrüßen daher, dass §8 Abs. 1 eine „gemeinsam vom Bundesamt für Sicherheit in der Informationstechnik und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete Registrierungsmöglichkeit“ vorsieht, wie in früheren Stellungnahmen vorgeschlagen.

Es darf nicht geschehen, dass bundesweit tätige Unternehmen mit unterschiedlichen länderspezifischen Interpretationen einer Bundesregelung konfrontiert werden. Um

einer Zersplitterung zwischen Bundes- und Länderzuständigkeiten entgegenzuwirken, sollte daher eine zentrale Stelle eingerichtet werden, die die Harmonisierung und Koordinierung der den Ländern zustehenden Regelungsbereiche übernimmt.

Hinzu kommt die derzeitige Unklarheit bezüglich konkreter Mindestmaßnahmen: Zwar ist die Möglichkeit vorgesehen, branchenspezifische Standards zur Resilienz zu erarbeiten und freigeben zu lassen, diese liegen jedoch bislang nicht vor. In der Zwischenzeit könnten BMI, Bundesressorts oder Landesregierungen eigene Mindeststandards festlegen, was zu zusätzlichen Fragmentierungen führen würde.

Von zentraler Bedeutung ist darüber hinaus die Umsetzung eines medienbruchfreien Registrierungs- und Meldeportals. Dies setzt voraus, dass Meldungen digital eingereicht werden können und eine automatische Weiterleitung sowie Bearbeitung durch die zuständige Behörde ohne weiteren Aufwand für die Unternehmen gewährleistet ist.

Registrierung kritischer Anlagen

In § 8 wird die Registrierungsfrist für Betreiber kritischer Anlagen weiterhin auf den 17. Juli 2026 festgelegt. Aufgrund der zwischenzeitlichen Verzögerungen beim Gesetzgebungsverfahren und der zugrunde liegenden Rechtsverordnung verkürzt diese Frist jedoch die zur Umsetzung erforderliche Zeit erheblich. Die Frist sollte angepasst werden, um den Verzögerungen Rechnung zu tragen und eine ausreichende Umsetzungszeit für Betreiber kritischer Anlagen sicherzustellen.

Es sollte sichergestellt werden, dass Unternehmen, die ihre Anlagen bereits beim BSI gemeldet haben, nicht erneut ein Registrierungsverfahren durchlaufen müssen. Eine Übernahme der bestehenden Daten und die Möglichkeit, diese bei Bedarf zu aktualisieren, wäre zweckmäßig und würde unnötige Mehrbelastungen vermeiden.

Darüber hinaus ergeben sich bei einzelnen Anforderungen in § 8 Absatz 1 offene Fragen. Die in Nummer 4 genannten öffentlichen IP-Adressbereiche sind nicht nachvollziehbar und bedürfen einer Konkretisierung. Ebenso sollte klargestellt werden, dass die in Nummer 6 geforderte Kontaktstelle ausschließlich die Erreichbarkeit über Leitstellen sicherstellt. Eine Verpflichtung, jederzeit unmittelbare fachliche Expertise zum Objektschutz bereitzuhalten, würde zu unverhältnismäßigen Zusatzaufwänden führen.

Meldepflichten

Es ist zu begrüßen, dass basierend auf der 1:1-Umsetzung und Erwägungsgrund 33 der CER-Richtlinie: „[...] In einer solchen Meldung sollte, *soweit möglich*, die *mutmaßliche* Ursache des Sicherheitsvorfalls angegeben werden.“ die 24-Stunden-Meldepflicht entschärft wird.

Die Formulierung in § 18, Abs. 1 und 2., dass Vorfälle gemeldet werden müssen, die „erheblich stören könnten“ kann in der praktischen Abgrenzung erhebliche Probleme bereiten. Für Vorfälle, die stören können, es aber letztendlich nicht tun, stellt sich die Frage, ob mit der Meldung solcher Vorfälle betroffene Unternehmen, Behörden und Meldewege nicht überfordert werden. Wir empfehlen daher, diesen Passus zu

streichen oder zu präzisieren. Bei Präzisierung könnte auf Erwägungsgrund 33 der CER-Richtlinie aufbauen und spezifizieren. Der Erwägungsgrund sieht vor , dass durch die Übermittlung „die *Ressourcen* der kritischen Einrichtung für Tätigkeiten im Zusammenhang mit der Bewältigung von Sicherheitsvorfällen, die Vorrang haben sollten, *nicht beeinträchtigt werden*."

Nachweise

Um den Prüf- und Auditierungsaufwand betroffener Unternehmen zu minimieren, sollten entsprechende Nachweise Anerkennung finden. Resilienzmaßnahmen lassen sich nach verschiedenen ISO-Standards (ISO 22316, 22320, 22301, 31000 und andere) zertifizieren und auditieren. Diese Standards eignen sich hierbei als Nachweise über ergriffene Maßnahmen. Es ist sicherzustellen, dass die in § 13 Abs. 3 genannten Maßnahmen lediglich beispielhaft zu verstehen sind, und eine auf die im betroffenen Unternehmen bzw. in der betroffenen Anlage vorliegende konkrete Situation abgestimmte Maßnahme der Auflistung in § 13 Abs. 3 in jedem Fall vorgeht.

Weiterhin muss generell sichergestellt werden, dass Nachweise im Rahmen anderer Zertifizierungen und Genehmigungen auch im Rechtskontext des KRITIS-DG anerkannt/verwendet werden können und das BBK und/oder das BSI sich auf etablierte Normen und Standards referenziert. Dies ist eine elementare Voraussetzung dafür, dass die Sicherheit erhöht, eine europäische Vergleichbarkeit hergestellt und die Kosten für die Antragsteller und Behörden in einem angemessenen Rahmen gehalten werden sowie Prozesse beherrschbar, wiederholbar und voraussagbar bleiben.

Kommunikation der Behörden

Es ist unabdingbar, dass die Abstimmung unter den Behörden zügig und nach klaren Regeln erfolgt, damit Betreiber kritischer Anlagen größtmögliche Sicherheit über ihre Pflichten erlangen und auf ein einheitliches Vorgehen vertrauen können. Dies schließt auch ein, dass in Behörden ein vergleichbares Schutz- und Resilienzniveau wie in den betroffenen Unternehmen sichergestellt wird, um vertrauliche Daten und Unternehmensgeheimnisse nach Übermittlung an die zuständigen Behörden nicht zu kompromittieren.

Der Referentenentwurf des KRITIS-DachG sieht an mehreren Stellen die Möglichkeit vor, dass das BBK Vorlagen, Muster oder anderweitige Vorgaben veröffentlicht, an denen sich betroffene Unternehmen orientieren können. Es ist sicherzustellen, dass diese Unterlagen möglichst frühzeitig vor Inkrafttreten der gesetzlichen Pflichten für die betroffenen Unternehmen veröffentlicht werden, um diesen eine ausreichende Zeit zur Vorbereitung und Implementierung zu ermöglichen. Dies gilt insbesondere für klare Kriterien, in welchen Fällen eine Meldung nach KRITIS-DachG zu erfolgen hat.

In diesem Kontext sollte auch die Bereitstellung eines Sicherheitslageberichts für den Geltungsbereich des KRITIS-DachG bedacht werden. Bisher wird der IT-Sicherheitslagebericht des BSI KRITIS-Betreibern, die unter das IT-Sicherheitsgesetz und KRITIS-Verordnung fallen, täglich bereitgestellt. Hier ist uns aktuell keine Entwicklung bzw. Diskussion zum Bereich der physischen Sicherheit bekannt.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Felix Kuhlenkamp | Bereichsleiter Sicherheitspolitik
T 030 27576-279 | f.kuhlenkamp@bitkom.org

Verantwortliches Bitkom-Gremium

AK Sicherheitspolitik

Copyright

Bitkom 2025

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung im Bitkom zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim Bitkom oder den jeweiligen Rechteinhabern.