SÄLZER

Das KRITIS-Dachgesetz

Was Bauherren und Betreiber jetzt wissen müssen

White Paper

Stand: 4.8..2025

Das KRITIS-Dachgesetz und was man dazu wissen sollte

Mit einem neuen Gesetz will die Bundesregierung die Widerstandsfähigkeit kritischer Infrastruktur gegen Gefahren aller Art stärken. Sälzer beantwortet die wichtigsten Fragen rund um das aktuelle Thema.

Um was geht es?

Das KRITIS-Dachgesetz („Kritis-DachG“) ist ein zentrales Gesetzesvorhaben der Bundesregierung zur Verbesserung der Resilienz Kritischer Infrastrukturen. Das Ziel: systemrelevante Einrichtungen besser vor Ausfällen, Angriffen und Katastrophen schützen – unabhängig davon, ob diese durch Naturereignisse, technische Störungen oder gezielte Angriffe entstehen.

Bisherige Regelungen auf Bundesebene betrafen lediglich die IT-Sicherheit kritischer Infrastrukturen. Das Kritis-DachG soll diese nun ergänzen und um den physischen und organisatorischen Schutz vor Gefahren erweitern. Das Gesetz verfolgt einen sektorenübergreifenden Ansatz, der bereits bestehende Regelungen wie die EU-Richtline zur Cybersicherheit NIS2 und deren Umsetzung in nationales Recht NIS2UmsuCG ergänzt.

Hintergrund und aktueller Stand

Am 6. November 2024 wurde der Regierungsentwurf des Kritis-DachG verabschiedet.

Der Entwurf basiert auf der EU-Richtlinie über die Resilienz kritischer Einrichtungen (Critical Entities Resilience – CER-Richtlinie 2022/2557 oder auch RCE). Diese verpflichtet die Mitgliedstaaten, Maßnahmen zur Verbesserung der Resilienz kritischer Einrichtungen zu ergreifen, die grenzüberschreitend relevant sind. Die EU verfolgt damit das Ziel, auf europäischer Ebene ein hohes einheitliches Schutzniveau gegen physische Risiken für kritische Einrichtungen sicherzustellen.

Die Parlamentarische Beratung des Gesetzes findet voraussichtlich im Sommer 2025 statt, die Verabschiedung ist für das vierte Quartal geplant. Inkrafttreten könnte es dann im Jahr 2026.

Kernelemente des Kritis-DachG

Das Kritis-DachG definiert die betroffenen Sektoren wie Energie, Gesundheitswesen, Transport usw. Es regelt die Anforderungen an die Betreiber, die erforderlichen Maßnahmen, Berichtspflichten und das Meldewesen. Wesentliche Elemente sind:

- Einführung einer zentralen Registrierungspflicht für kritische Einrichtungen
- Verpflichtung zur Erstellung eines Resilienzplans alle vier Jahre
- Meldepflicht bei erheblichen Störungen

- Etablierung eines Risiko- und Bedrohungsmonitorings durch den Staat
- Erweiterte Prüf- und Anordnungsbefugnisse für zuständige Behörden
- Aufbau eines Zentralregisters beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe BBK

Ein zentrales Prinzip ist dabei der sog. *All-Gefahren-Ansatz*. Dabei geht es um die Betrachtung aller potenziellen Gefahrenquellen, seien es Extremwetter, Pandemien, terroristische Anschläge, Stromausfälle oder Lieferengpässe.

Wer ist vom Kritis-DachG betroffen?

Was zählt überhaupt zur kritischen Infrastruktur? Es geht um Unternehmen und Einrichtungen, die von entscheidender Bedeutung für das Funktionieren unseres Gemeinwesens sind. Ein Ausfall oder eine Beeinträchtigung hätte gravierende Folgen für die öffentliche Sicherheit und die Versorgung im Land. Hierzu wurden im §4 des Gesetzentwurfes folgende Sektoren identifiziert:

- Energie
- Transport & Verkehr
- Finanzwesen
- Leistung der Sozialversicherung und Grundsicherung für Arbeitssuchende
- Gesundheitswesen
- Wasser
- Ernährung
- Informationstechnik und Telekommunikation
- Weltraum
- Abfallentsorgung

Ob ein Unternehmen aus diesem Sektor zur kritischen Infrastruktur zählt, wird unter anderem anhand von *Schwellenwerten* definiert. Betroffen sind demnach überwiegend Betriebe und Institutionen, die mehr als 500.000 Einwohner versorgen. Es gibt jedoch auch Einrichtungen, die für das öffentliche Leben essenziell sind, auch wenn sie die klassischen Schwellenwerte nicht erfüllen. Die Details regelt die Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz, kurz KritisV.

Nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik waren 2024 in Deutschland 2095 Anlagen von 1132 Betreibern als kritische Infrastruktur registriert. Es muss jedoch davon ausgegangen werden, dass die Zahl mit in Kraft treten des Kritis-DachG deutlich steigt. Schätzungen gehen von bis zu 30.000 betroffenen Betreibern aus.

Player und Zuständigkeiten

Die Federführung für das Kritis-DachG sowie zentrale politische Steuerung liegt beim Bundesinnenministerium. Als Koordinationsstelle für Risikoanalysen und Resilienzprüfungen

fungiert das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, das auch das Kritis-Register betreibt. Die Schnittstelle zum NIS2UmsuCG übernimmt das Bundesamt für Sicherheit in der Informationstechnik (BSI). Es ist die zuständige Stelle für Cybersicherheit in kritischen Infrastrukturen. Den Länderbehörden obliegt die Umsetzung, Kontrolle und gegebenenfalls Anordnung konkreter Maßnahmen in ihrem Zuständigkeitsbereich.

Was müssen Betroffene tun?

Einrichtungen, die dem Kritis-DachG unterliegen, haben folgende Pflichten:

- Registrierung beim BBK
- Durchführen einer Risikoanalyse und -bewertung
- Erstellen und Anwenden eines Resilienzplans
- Meldung von Störungen

Die Registrierung beim BBK (§8)

Unternehmen müssen sich selbst als Betreiber kritischer Anlagen identifizieren und beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe registrieren. Dies geschieht durch Übermitteln des Namens, der Rechtsform, ggf. der Handelsregisternummer, der Anschrift und den Kontaktdaten, des Sektors und der Kategorie, einer Liste der EU-Länder für die oder in denen der Betreiber tätig ist sowie dem Benennen einer Kontaktstelle.

Durchführen einer Risikoanalyse und -bewertung (§12)

Auf Grundlage der nationalen Risikoanalyse und -bewertung (§11) hat der Betreiber eine Risikoanalyse und -bewertung vorzunehmen. „Im Bedarfsfall, mindestens jedoch alle vier Jahre“ heißt es dazu im Kritis-DachG. Inhaltliche und methodische Vorgaben einschließlich Muster und Vorlagen kann das BBK bestimmen.

Eine Risikoanalyse und -bewertung umfasst typischerweise naturbedingte, technische oder menschlich verursachte Risiken, darunter extreme Wetterereignisse und hybride Bedrohungen wie Terroranschläge. Außerdem beleuchtet sie die Abhängigkeit von Leistungen anderer Betreiber und Sektoren, auch aus dem Ausland.

Hinweis: Sälzer entwickelt derzeit einen Leitfaden zur Vorgehensweise. Der Leitfaden bietet betroffenen Unternehmen konkrete Unterstützung bei Risikoanalyse, Risikobewertung und Resilienzplan.

Erstellen und Anwenden eines Resilienzplans (§13)

Ein wesentliches Element des Kritis-DachG ist der *Resilienzplan*. Auf Grundlage der Risikoanalyse und -bewertung sind Betreiber kritischer Anlagen verpflichtet, Maßnahmen zu treffen, um …

- das Auftreten von Vorfällen zu verhindern
- physischen Schutz der Anlage zu gewährleisten
- auf Vorfälle zu reagieren, sie abzuwehren und die negativen Auswirkungen zu begrenzen
- nach Vorfällen die zügige Wiederherstellung zu gewährleisten

Diese Maßnahmen müssen in einem Resilienzplan dargestellt und dieser muss angewendet werden. Zu den Maßnahmen können u.a. zählen: Bauliche und technische Sicherungen wie z.B. hemmende Fassadenelemente, Detektionsgeräte und Zugangskontrollen.

Dabei heißt es im Wortlaut: Es sind „verhältnismäßige, technische, sicherheitsbezogene und organisatorische Maßnahmen zu treffen. Der Stand der Technik soll eingehalten werden“. Der Gesetzesentwurf definiert jedoch nicht explizit, was mit „Stand der Technik“ gemeint ist. Aus Sicht von Sälzer sind dies zum einen die geltenden Normen und Regelwerke im Bereich der physischen und elektronischen Sicherheit. Zum anderen umfasst dies auch Vorgehensweisen und Konstruktionen, die praktisch bewährt und allgemein anerkannt sind, jedoch noch keinen Einzug in die Normung gehalten haben.

Meldung von Störungen (§18)

Der Betreiber kritischer Anlagen ist verpflichtet, Vorfälle spätestens nach 24 Stunden der vom BBK eingerichteten Meldestelle zu melden. Spätestens einen Monat danach ist ein ausführlicher Bericht zu übermitteln.

Wie ist Zeitplan für Betroffene?

Zur Registrierung heißt es im aktuellen Entwurf des Kritis DachG wörtlich: „Spätestens drei Monate nachdem eine Anlage als kritische Anlage gilt, frühestens jedoch bis 17. Juli 2026“. Diese unklare Formulierung interpretiert Sälzer dahingehend, dass Betreiber sich frühestens im Juli 2026 registrieren können. Nach der Registrierung sind dann Fristen von neun bis zehn Monaten zur Umsetzung von Risikoanalyse, Resilienzplan usw. vorgesehen. Das BBK stellt bis 17. Januar 2026 Vorlagen für die Erstellung von Resilienzplänen bereit.

Betreiber von kritischen Infrastrukturen und potenziell betroffene Unternehmen sollten sich frühzeitig mit dem Kritis-Dach-Gesetz auseinandersetzen. Sälzer als Spezialist für physische Hochsicherheit, steht mit langjähriger Expertise für alle Fragen rund um das Thema ganzheitlicher Schutz kritischer Infrastrukturen zur Verfügung. Weiterführende Infos unter www.saelzer-security.com

Quellen: Kritis-DachG-Entwurf vom 6.11.24, BSI-KritisV mit letzter Änderung vom 29.11.23, www.openkritis.de

Abkürzungen

BSI	Bundesamt für Sicherheit in der Informationstechnik
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BMI	Bundesministerium des Inneren
BSIG	BSI-Gesetz, regelt die Aufgaben und Zuständigkeiten des BSI
ECR/CER	EU-Richtlinie über die Resilienz kritischer Einrichtungen
Kritis-DachG	regelt den physischen Schutz kritischer Infrastrukturen in Deutschland
KritisV	regelt die Bestimmung kritischer Infrastrukturen in Deutschland (=BSI-KritisV)
NIS2	EU-Richtlinie: Regelt die Cybersicherheit in systemrelevanten Einrichtungen
NIS2UmsuCG	Nationale Umsetzung der NIS2 in deutsches Recht

Weitere Informationen

SÄLZER GmbH

Zentrale Deutschland

Dietrich-Bonhoeffer-Str. 1-3

35037 Marburg

Telefon: +49 6421 938 100

info@saelzer-security.com

www.saelzer-security.com