

Das KRITIS-Dachgesetz

Was Bauherren und Betreiber jetzt wissen müssen



Das KRITIS-Dachgesetz und was man dazu wissen sollte

Mit dem KRITIS-Dachgesetz will die Bundesregierung die Widerstandsfähigkeit kritischer Infrastruktur gegen Gefahren aller Art stärken. Es wurde am 29. Januar 2026 vom Bundestag beschlossen. Wie geht es nun weiter? 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-Richtlinie zur Cybersicherheit NIS2 und deren Umsetzung in nationales Recht NIS2UmsuCG ergänzt.

Hintergrund und aktueller Stand

Das KRITIS-DachG setzt die EU-Richtlinie 2022/2557 über die Resilienz kritischer Einrichtungen, die sogenannte CER-Richtlinie, in deutsches Recht um (CER = Critical Entities Resilience). 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.

Am 29. Januar 2026 hat der Bundestag den Entwurf des KRITIS-DachG angenommen. Die beschlossene Version weist gegenüber dem Entwurf der Bundesregierung sowie früheren Versionen einige Änderungen auf. Alle Änderungen sind im vorliegenden White Paper berücksichtigt.

Kernelemente des Kritis-DachG

Das KRITIS-DachG definiert die betroffenen Sektoren wie beispielsweise Energie, Gesundheitswesen und Transport. 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
- 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. Betroffen sind sowohl Betreiber kritischer Anlagen wie auch Erbringer von Dienstleistungen zur Versorgung („kritische Dienstleistungen“).

Hierzu wurden im §4 des Gesetzes 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 Schwellenwerte nicht erfüllen. Solche Betreiber können sowohl vom Bund als auch von den Ländern bestimmt werden. Die Details regelt eine noch zu erlassende Rechtsverordnung.

Nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik waren Ende 2025 in Deutschland 2136 Anlagen von 1179 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. In der politischen Diskussion ist zudem eine Ausweitung der Sektoren sowie die Senkung des Schwellenwerts auf 150.000 Einwohner. Sollten diese Änderungen Einzug in die nachfolgenden Rechtsverordnungen halten, dürfte sich die Zahl der Betroffenen noch einmal erheblich vergrößern.

Player und Zuständigkeiten

Die Federführung für das KRITIS-DachG sowie die zentrale politische Steuerung liegen beim Bundesinnenministerium. Als Koordinationsstelle für Risikoanalysen und Resilienzprüfungen fungiert das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, welches 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 arbeitet in verschiedenen Gremien der Branche an einem 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

Dazu müssen Betreiber verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen treffen, basierend auf nationalen Risikobewertungen und Analysen. Dabei soll der „Stand der Technik“ eingehalten werden. Zu dessen

Bestimmung sind einschlägige Normen und Standards heranzuziehen, aber auch Vorgehensweisen und Konstruktionen, die praktisch bewährt und allgemein anerkannt sind, jedoch noch keinen Einzug in die Normung gehalten haben.

Zu den technischen Maßnahmen zählen u.a. bauliche und technische Sicherungen wie z.B. hemmende Fassadenelemente, Detektionsgeräte und Zugangskontrollen.

Die Maßnahmen müssen in einem Resilienzplan dargestellt und dieser muss angewendet werden.

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?

Jeder Betreiber ist nach Inkrafttreten des Gesetzes im ersten Schritt dazu verpflichtet, seine Anlagen nach den benannten Kriterien zu überprüfen. Wird eine Anlage als kritische Infrastruktur identifiziert bzw. kann dies zumindest nicht ausgeschlossen werden, muss sich der Betreiber nach spätestens drei Monaten beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe BBK registrieren lassen. Nach der Registrierung ist eine Frist von neun Monaten zur Umsetzung von Risikoanalyse und Risikobewertung vorgesehen.

Zusammenfassung und Ausblick

Mit der Verabschiedung des KRITIS-DachG am 29. Januar 2026 hat der Bundestag den rechtlichen Rahmen für den Schutz kritischer Infrastruktur in Deutschland geschaffen. Gegenüber vorherigen Versionen wurden einige Änderungen eingebracht, der Kern des Gesetzes jedoch im Wesentlichen beibehalten. So wurden beispielsweise Nachweis- und Meldepflichten angepasst und mögliche Geldbußen auf bis zu eine Million Euro erhöht.

Das KRITIS-DachG muss nun durch eine oder mehrere Verordnungen konkretisiert werden. Dies betrifft u.a. die Schwellenwerte für kritische Dienstleistungen und Anlagen, die unabhängig von Schwellenwerten als kritisch eingestuft werden. Ein Entwurf dieser Rechtsverordnung(en) ist noch nicht verfügbar.

„Sicherheit wächst nicht allein anhand der Vorschriften im Bundesgesetzblatt“, sagte der Parlamentarier Sebastian Schmidt (CDU) anlässlich der Verabschiedung des KRITIS-DachG. In diesem Sinne sollten Betreiber von kritischen Infrastrukturen und potenziell betroffene Unternehmen sich frühzeitig mit der Thematik 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; Fassung 21/2510, 21/3855 sowie 21/3906, Stand 29. Januar 2026

Abkürzungen

BSI	Bundesamt für Sicherheit in der Informationstechnik
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
CER	EU-Richtlinie über die Resilienz kritischer Einrichtungen
KRITIS-DachG	KRITIS-Dachgesetz, regelt den Schutz kritischer Infrastrukturen
NIS2	EU-Richtlinie zur Cybersicherheit systemrelevanter Einrichtungen
NIS2UmsuCG	Nationale Umsetzung der EU-Richtlinie 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