KRITIS im Ernstfall

Physische Resilienz, KI-Bedrohungen und Haftung als neue Realität für Infrastrukturbetreiber

Kritische Infrastrukturen stehen unter wachsendem Druck – durch hybride Bedrohungen, geopolitische Spannungen, Naturkatastrophen und zunehmend auch durch KI-gestützte Cyberangriffe. Der Schutz dieser Anlagen ist längst keine rein technische Frage mehr, sondern eine rechtliche, organisatorische und strategische Gesamtaufgabe. Der Gesetzgeber hat darauf reagiert: Mit dem KRITIS-Dachgesetz (KRITIS-DachG), das am 29. Januar 2026 vom Deutschen Bundestag verabschiedet wurde, wird erstmals auch die physische Resilienz zur verbindlichen Betreiberpflicht. Das Gesetz setzt die europäische Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie, RL (EU) 2022/2557) um und ergänzt die bisher geltenden Regelungen aus dem Bereich der IT-Sicherheit, insbesondere die NIS2-Richtlinie (in Deutschland umgesetzt durch das BSI-Gesetz). Damit entsteht erstmals ein übergreifender Rahmen, der IT-Sicherheit, physischen Schutz von Anlagen, Personal und Lieferketten sowie den Umgang mit neuen Technologien wie KI zusammendenkt.

Mit dem KRITIS-DachG reagiert der Gesetzgeber auf eine sich deutlich verschärfende Bedrohungslage. Aktuelle Themen wie Drohnensichtungen über Flughäfen, der Anschlag auf das Berliner Stromnetz und die wachsende Bedrohung durch KI-gestützte Cyberangriffe machen deutlich: Die Risiken für kritische Infrastrukturen sind vielfältiger und komplexer geworden. Der Schutz kritischer Infrastrukturen erfordert daher heute ein abgestimmtes regulatorisches Zusammenspiel: Das KRITIS-DachG adressiert die physische Resilienz, das BSI-Gesetz (als deutsche Umsetzung der NIS2-Richtlinie) die Cybersicherheit, und der EU AI Act schafft den Rahmen für den verantwortungsvollen Einsatz Künstlicher Intelligenz – auch und gerade in sicherheitskritischen Umgebungen. Dieser Dreiklang prägt die neue Realität für Betreiber kritischer Infrastrukturen.

All-Gefahren-Ansatz: Jedes Risiko zählt

Die Grundlage der Neuregelung bildet die seit dem 16. Januar 2023 für alle EU-Mitgliedstaaten verbindliche CER-Richtlinie. Diese schuf erstmals einen einheitlichen europäischen Rechtsrahmen zur Stärkung der Resilienz kritischer Anlagen in verschiedenen Sektoren. Dies markierte einen Paradigmenwechsel, denn die CER-Richtlinie geht ausdrücklich über den bisherigen Fokus der IT-Sicherheit hinaus und nimmt auch physische und personelle Schutzaspekte in den Blick.

Das KRITIS-DachG sieht vor, die Resilienz kritischer Anlagen nach dem sogenannten „All-Gefahren-Ansatz" zu stärken.

Dabei muss jedes denkbare Risiko berücksichtigt werden. Das bedeutet: Die Betreiber müssen nicht nur technische IT-Sicherheitsmaßnahmen implementieren, sondern auch gegenüber menschengemachten und natürlichen Bedrohungen wie Naturkatastrophen, Terroranschlägen und Sabotage gewappnet sein. Dazu verpflichtet das Gesetz die Betreiber kritischer Anlagen verschiedener Sektoren, geeignete physische Schutzmaßnahmen umzusetzen und damit Ausfälle oder Beeinträchtigungen möglichst frühzeitig zu verhindern oder zumindest deren Auswirkungen zu minimieren.

Flankiert wird dieser Ansatz durch die Cybersicherheitsanforderungen des BSI-Gesetzes (NIS2) sowie – wenn KI-Systeme eingesetzt werden – durch den EU AI Act. Erst im Zusammenspiel dieser drei Regelwerke entsteht ein umfassender Schutzrahmen für kritische Infrastrukturen.

Wer ist betroffen? Schwellenwerte und Länderermächtigung

Betroffen sind vor allem Betreiber von Anlagen, die eine hohe Bedeutung für das Gemeinwesen haben, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder eine Gefährdung für die öffentliche Sicherheit drohen. Diese Voraussetzung sieht der Gesetzgeber bei Anlagen der kritischen Infrastruktur als gegeben, wenn dadurch regelmäßig mindestens 500.000 Personen versorgt werden. Dieser Schwellenwert, der bereits im früheren Entwurf enthalten war und stark umstritten ist, bleibt unverändert bestehen. Als kritische Infrastruktur gelten etwa große Energie- oder Wasserversorgungsunternehmen sowie weitere Schlüsselbereiche.

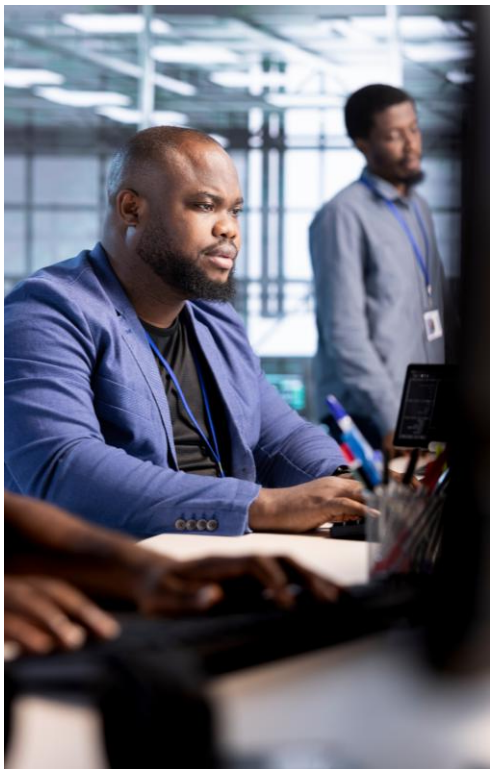
Konkretisiert wird der Anwendungsbereich durch die neue KRITIS-Verordnung, zu der seit 26. Mai 2026 ein erster Referentenentwurf zirkuliert. Die Verordnung soll die erfassten kritischen Dienstleistungen, Anlagenkategorien und anlagebezogenen Schwellenwerte im Einzelnen festlegen. Dabei werden zahlreiche Begriffe und Konzepte – etwa zur Bestimmung des Versorgungsgrades – klarer definiert als bisher. Der Regelschwellenwert von 500.000 Personen soll als Berechnungsbasis für die anlagebezogenen Schwellenwerte jedoch erhalten bleiben. Unternehmen, die bislang noch nicht abschließend einschätzen konnten, ob sie vom KRITIS-DachG erfasst sind, sollten die weitere Entwicklung aufmerksam verfolgen und ihre Betroffenheit frühzeitig konkret überprüfen.

Ergänzend sieht das Gesetz in § 5 Abs. 7 KRITIS-DachG eine neue Ermächtigung der Länder vor, die es ihnen ermöglicht, durch Rechtsverordnungen weitere kritische Anlagen zu identifizieren, die ausschließlich in ihre Zuständigkeit fallen. Die Bundesländer können hier also zusätzliche Schutzbereiche innerhalb ihrer Zuständigkeit definieren. Das Bundesministerium des Inneren (BMI) wiederum ist ermächtigt, die relevanten Kriterien und Verfahren durch Verordnung festzulegen. Hierfür ist die Zustimmung des Bundesrats erforderlich.

Präventions-Compliance: Fristen, Risikoanalyse und Resilienzplan

Die zentralen Betreiberpflichten sind in der neuen Regelung im Grundsatz klar formuliert und mit zeitlichen Fristen unterlegt. Betreiber müssen sich innerhalb von drei Monaten, nachdem sie als kritische Infrastruktur klassifiziert wurden, selbst registrieren. Unmittelbar darauf ist eine erste Risikoanalyse vorzunehmen, die spätestens neun Monate nach der Registrierung abgeschlossen sein muss. Diese Risikoanalyse ist als dauerhafter Prozess alle vier Jahre zu wiederholen. Parallel dazu müssen die Betreiber geeignete Resilienzmaßnahmen umsetzen und einen Resilienzplan erstellen, der unter anderem Notfallvorsorge, physische und personelle Sicherheit sowie regelmäßige Schulungen umfasst. Diese Maßnahmen müssen innerhalb von zehn Monaten nach der Registrierung erfolgen.

Die Lieferkette ist dabei ausdrücklich Teil der Betrachtung: Betreiber müssen auch Abhängigkeiten von Zulieferern und Dienstleistern in ihre Risikoanalyse einbeziehen und entsprechende Vorkehrungen treffen. Dies kann Anpassungen bestehender Betriebsführungsverträge ebenso erfordern wie die Berücksichtigung entsprechender Anforderungen in künftigen Ausschreibungsunterlagen.



Wichtig dabei:

KRITIS-Betreiber werden gemäß § 28 Abs. 1 Nr. 1 BSIG automatisch als besonders wichtige Einrichtungen eingestuft und haben damit

zusätzlich die entsprechenden Pflichten nach dem BSI-Gesetz zu erfüllen – von verschärften Anforderungen an das Risikomanagement über Registrierungs- und Nachweispflichten bis hin zu den Meldepflichten nach NIS2. Beide Pflichtenprogramme müssen von Anfang an integriert gedacht und in einer gemeinsamen Compliance-Struktur zusammengeführt werden.

Incident Response: Meldepflichten und das 24-Stunden-Fenster

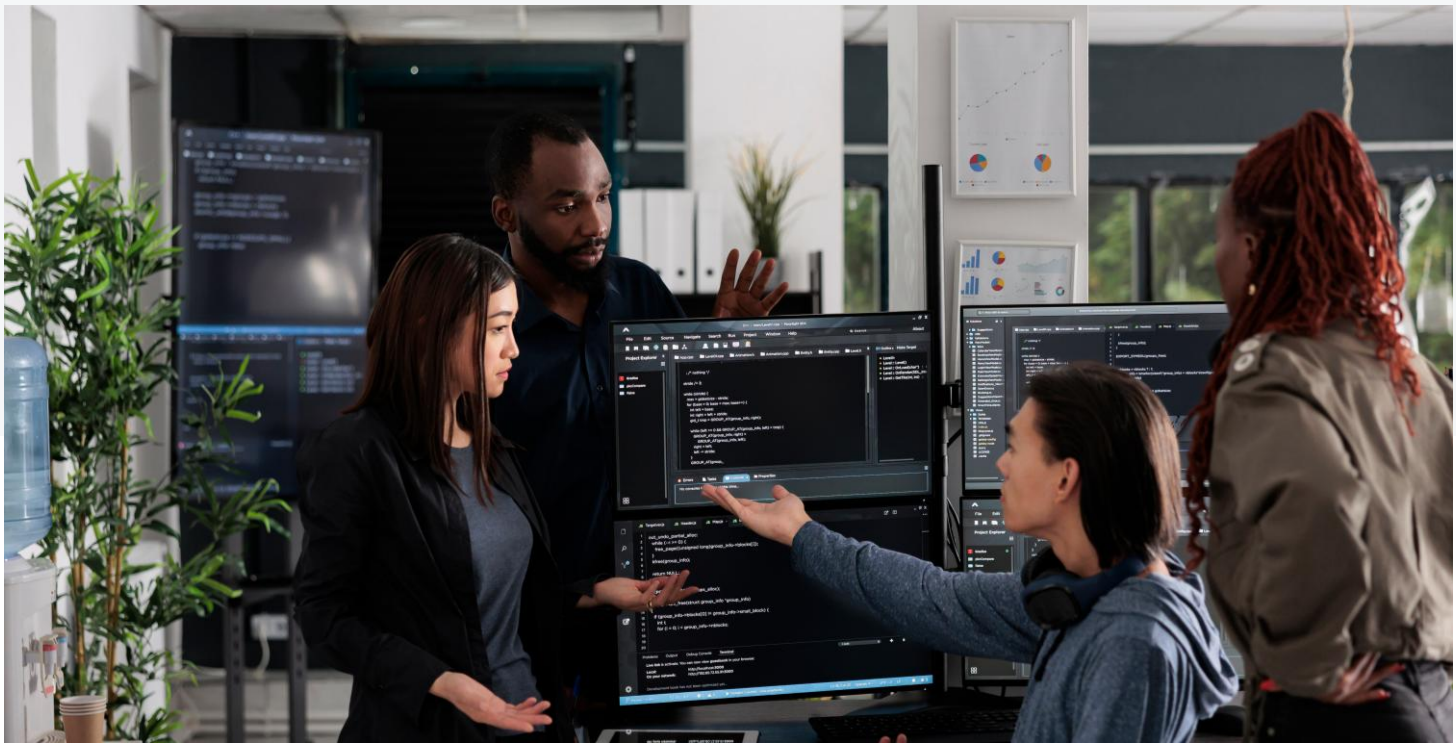
Ein besonders wichtiger Bestandteil ist nach § 18 KRITIS-DachG die Ausweitung und Präzisierung der Meldepflichten bei sicherheitsrelevanten Vorfällen. Sicherheitsstörungen oder Beeinträchtigungen sind unverzüglich, in der Regel spätestens binnen 24 Stunden ab Kenntnis, an das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) zu melden. Innerhalb eines Monats muss der Betreiber einen detaillierten Bericht mit weiterführenden Informationen vorlegen. Dabei unterstützt das BBK die Betreiber mit Folgeinformationen, um eine wirksame Reaktion auf den Vorfall zu ermöglichen. Diese detaillierte Meldepflicht wird vor dem Hintergrund des Anschlags in Berlin als notwendig erachtet, um schnelle und koordinierte Schutzmaßnahmen zu gewährleisten.

Mit dem Aufkommen KI-gestützter Angriffe und im Kontext des BSIG wird die zeitgerechte Einhaltung der Meldepflichten schwieriger. KI-Modelle sind in der Lage, Schwachstellen in IT-Infrastrukturen schneller und systematischer auszunutzen, als klassische Meldeprozesse mit manueller Erfassung, interner Eskalation und Freigabeschleifen überhaupt greifen können. Für KRITIS-Betreiber wächst damit das Bedürfnis, regulatorische Meldeprozesse nicht mehr nur organisatorisch, sondern auch technisch in die Sicherheitsarchitektur einzubetten – als eine Art Echtzeit-Compliance-Reaktion.

Spezialfall KI: Bedrohung und Schutzinstrument zugleich

KI verändert die Bedrohungslage für kritische Infrastrukturen grundlegend – in beide Richtungen. Auf der einen Seite beschleunigen KI-gestützte Angriffswerkzeuge die Ausnutzung von Sicherheitslücken erheblich: Modelle, die eigenständig Schwachstellen in Software und IT-Infrastrukturen identifizieren und binnen kürzester Zeit funktionsfähige Angriffsprogramme erstellen können, sind keine Zukunftsmusik mehr. Für KRITIS-Betreiber, deren Systeme häufig eng mit physischer Infrastruktur verknüpft sind, hat eine erfolgreiche Cyberattacke potenziell auch unmittelbare physische Konsequenzen. Genau das soll durch den All-Gefahren-Ansatz adressiert werden.

Auf der anderen Seite bietet KI erhebliches Potenzial zur Verteidigung: KI-gestützte Überwachungssysteme können Anomalien in Echtzeit erkennen, Angriffsmuster frühzeitig identifizieren und damit den Zeitraum bis zur Meldung und Reaktion deutlich verkürzen. Der verantwortungsvolle Einsatz solcher Werkzeuge wirft jedoch anspruchsvolle Fragen auf – von der Risikoklassifizierung nach dem EU AI Act über Beschaffungs- und Governance-Anforderungen bis hin zur Frage, welche Pflichten aus dem Zusammenspiel von AI Act, BSIG und KRITIS-DachG entstehen. EU AI Act, BSIG und KRITIS-DachG bilden dabei kein isoliertes Nebeneinander, sondern ein zusammenhängendes Anforderungsgeflecht, das Betreiber integriert im Blick behalten sollten.



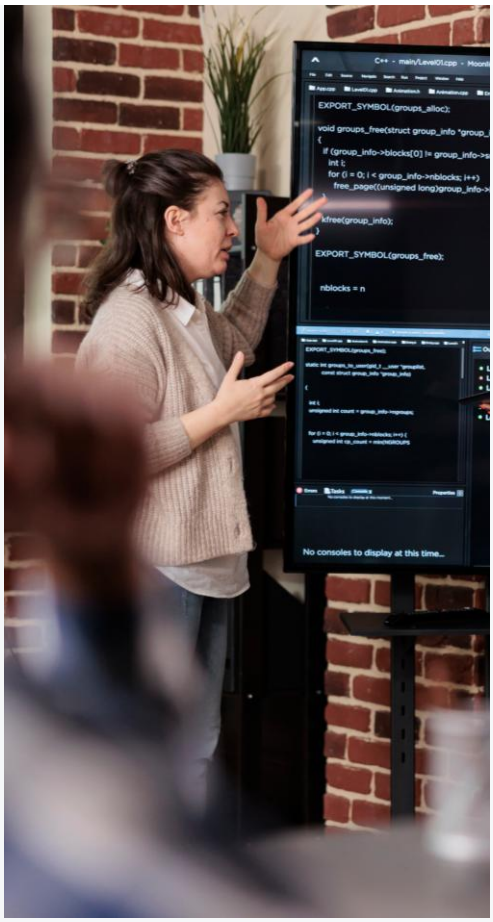
Haftung und Sanktionen: Kumuliertes Risiko aus zwei Regelwerken

Die Dokumentationspflichten des KRITIS-DachG sorgen dafür, dass die Betreiber ihre getroffenen Maßnahmen nachvollziehbar nachweisen müssen und sich regelmäßig Prüfungen durch das BBK unterziehen müssen. Damit soll die Umsetzung der Sicherheitsverpflichtungen sichergestellt und eine lückenlose Kontrolle durch die zuständigen Behörden ermöglicht werden.

Eine weitere wichtige Neuerung sind die deutlich verschärften Sanktionen bei Verstößen gegen die gesetzlichen Pflichten. Nach § 24 KRITIS-DachG gelten insbesondere bei Verstößen gegen die Meldepflicht Bußgelder zwischen 100.000 und 500.000 Euro.

Da KRITIS-Betreiber gemäß § 28 Abs. 1 Nr. 1 BSIG stets als besonders wichtige Einrichtungen eingestuft werden, drohen parallel auch die Sanktionen des BSI-Gesetzes: Für besonders wichtige Einrichtungen sieht das BSIG Bußgelder von bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes vor – in vielen Fällen damit das deutlich schärfere Sanktionsinstrument. KRITIS-Betreiber stehen damit vor einem kumulierten Haftungsrisiko aus beiden Regelwerken, dass eine integrierte Compliance-Strategie nicht nur sinnvoll, sondern unabdingbar macht.

Für Unternehmen, die als Betreiber kritischer Infrastrukturen in den gesetzlich geregelten Bereich fallen, bedeutet das Zusammenspiel von KRITIS-DachG und BSIG insbesondere eines: Physische Resilienz und Cybersicherheit werden gleichermaßen zur verbindlichen Betreiberpflicht – und damit zu einem verbindlichen Bestandteil der Unternehmensverantwortung, der nicht länger in das Ermessen des Betreibers gestellt ist. Betroffene Unternehmen müssen ihre Sicherheits- und Krisenmanagementstrukturen daher dringend überprüfen, überarbeiten und auf die Anforderungen beider Regelwerke ausrichten.



Engere Zusammenarbeit im Unternehmen notwendig

Das erfordert eine verbesserte Verzahnung der verschiedenen Fachbereiche im Unternehmen. Technik, IT, Betrieb, Personalmanagement, Sicherheit und Compliance sind aufgefordert, künftig noch enger zusammenzuarbeiten. Prozesse wie Risikoanalyse, Meldewege und Krisenkommunikation müssen formalisiert und standardisiert sowie Verantwortlichkeiten klar verankert werden. Zudem sind regelmäßige Schulungen und Übungen notwendig, um die Reaktionsfähigkeit bei sicherheitsrelevanten Vorfällen sicherzustellen.

Gerade die neu definierten Meldepflichten stellen einen zentralen operativen Faktor dar. Verzögerungen oder Versäumnisse beim Melden von Störungen ziehen empfindliche Bußgelder nach sich. Unternehmen müssen daher ihre Meldeprozesse optimieren und sicherstellen, dass sie Vorfälle rechtzeitig, vollständig und korrekt an das BBK oder/und das BSI melden.

Gleichzeitig unterstützt das BBK die Betreiber mit Folgeinformationen, was eine effektive Reaktion auf sicherheitsrelevante Ereignisse ermöglicht und damit zum Schutz der gesamten kritischen Infrastruktur beiträgt.

KRITIS-DachG, BSI-Gesetz und EU AI Act bilden gemeinsam die neue regulatorische Grundlage für den Schutz kritischer Infrastrukturen. Unternehmen sollten daher frühzeitig prüfen, von welchen dieser Regelwerke sie erfasst sind und wie sich die jeweiligen Anforderungen sinnvoll harmonisieren und in eine gemeinsame Compliance-Struktur integrieren lassen. Eine isolierte Betrachtung einzelner Regelwerke greift zu kurz – gefragt ist eine übergreifende Sicherheitsarchitektur, die IT-Sicherheit, physischen Schutz und den verantwortungsvollen KI-Einsatz zusammendenkt.

Das KRITIS-DachG markiert einen Meilenstein im Schutz kritischer Infrastruktur in Deutschland. Es rückt physische Schutzaspekte, die bisher neben der IT-Sicherheit weitgehend zurückstanden, in den Mittelpunkt. Hinzu tritt mit der KI eine neue Bedrohungsdimension, die zugleich Risiko und Chance ist: Sie erhöht den Angriffsdruck auf kritische Anlagen, bietet aber auch neue Möglichkeiten zur Absicherung – wenn sie verantwortungsvoll und regulatorisch eingebettet eingesetzt wird. Die neuen Betreiberpflichten sind mit strengen Fristen und erheblichen Sanktionen versehen. Unternehmen sind daher gut beraten, die neuen gesetzlichen Vorgaben frühzeitig zu prüfen und ihre Sicherheits- und Krisenmanagementprozesse zügig anzupassen. Dies leistet nicht nur einen wichtigen Beitrag zur Sicherstellung der Versorgungssicherheit, sondern mindert auch Haftungsrisiken und schützt vor hohen Bußgeldern.

PwC Legal begleitet Unternehmen, öffentliche Einrichtungen und KRITIS-Betreiber bei allen Fragen rund um die Umsetzung des KRITIS-DachG und des BSI-Gesetzes – von der Betroffenheitsanalyse über die Entwicklung integrierter Compliance- und Krisenmanagementstrukturen bis hin zur vertraglichen Absicherung in Liefer- und Betriebsführungsbeziehungen. Darüber hinaus beraten wir an der Schnittstelle von KRITIS-Regulierung und KI – von der Risikoklassifizierung nach dem EU AI Act bis zur Governance beim Einsatz von KI-Sicherheitslösungen. Sprechen Sie uns gerne an.