By PwC Deutschland | 10. Dezember 2025

Geplantes KRITIS-Dachgesetz: Pflichten, Risiken und praktische Schritte für die Unternehmensleitung

Mit dem geplanten KRITIS?Dachgesetz, dessen Gesetzesentwurf am 10. September 2025 vom Bundeskabinett beschlossen wurde, wird ein rechtlicher Rahmen geschaffen, um wichtige Anlagen und Dienstleistungen besser vor physischen Gefahren zu schützen, also vor allem vor Ausfällen durch Sabotage, Naturereignisse oder andere Störungen. Das Gesetz setzt die EU?Vorgaben zur Resilienz kritischer Einrichtungen (CER) um und ergänzt die bereits laufende NIS?2?Umsetzung zur Cybersicherheit.

Content

Autoren dieses Beitrags sind David Santa, Robert Schiller und Jens Greiner.

Für betroffene Unternehmen bedeutet das: Mehr klare Pflichten beim Risiko? und Krisenmanagement sowie beim Melden von Vorfällen. Dies hat unmittelbare Folgen für den Aufgabenkreis der Geschäftsleitung und mögliche persönliche Haftungsrisiken nach dem GmbHG und dem AktG.

Ziel und Zeitplan - worum es geht

Das Gesetz soll den physischen Schutz von Anlagen sichern, deren Ausfall das tägliche Leben der Bürger empfindlich treffen würde. Dies betrifft insbesondere die Sektoren Strom, Wasser und Verkehr sowie Gesundheit und Finanzen. Der Ansatz des KRITIS-Dachgesetzes ist, dass alle relevanten Gefahren betrachtet und verbindliche Mindeststandards festgelegt werden, die je nach Branche weiter konkretisiert werden können. Zuständig werden vor allem zwei Behörden sein. Zum einen ist dies das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe („**BBK**") für den physischen Schutz der Anlagen und das Bundesamt für Sicherheit in der Informationstechnik („**BSI**") für IT?Sicherheit. Beide Behörden werden eine gemeinsame Stelle für die Registrierung und Meldungen einrichten.

Eckdaten

Eine nationale KRITIS?Resilienzstrategie soll bis zum 17. Januar 2026 stehen. Zentrale Pflichten, wie Risikoanalysen, Schutzmaßnahmen, Nachweise und Meldungen, greifen voraussichtlich ab dem 17. Juli 2026. Unternehmen sollten deshalb jetzt organisatorisch und finanziell planen.

Wer betroffen ist

Betroffen sind Betreiber von Anlagen, die „kritische Dienstleistungen" erbringen, also Leistungen, deren Ausfall zu Versorgungsengpässen oder Risiken für Wirtschaft, Sicherheit, Gesundheit oder Umwelt führen

kann. Dazu zählen u. a. folgende Sektoren:

- Energie, Verkehr, Finanz? und Versicherungswesen, Gesundheit, Trink? und Abwasser, Ernährung, IT und Telekommunikation, Weltraum sowie Abfallentsorgung.

Die Schwellen, ab wann ein Unternehmen vom Anwendungsbereich erfasst ist, orientieren sich an bekannten Maßstäben aus der BSI?KritisV. Häufig gilt: Wer für etwa 500.000 Menschen Leistungen erbringt, fällt in den Fokus, gemessen z.B. an Energie?Mengen, Transaktionen oder versorgten Personen. Zusätzlich können nationale Risikoanalysen im Einzelfall weitere Betreiber einbeziehen, etwa wegen besonderer Lieferketten oder regionaler Besonderheiten.

Zuständigkeiten

Erste Anlaufstelle für Fragen zum physischen Schutz ist das BBK. Die jeweiligen Branchenaufsichten bleiben zuständig (zum Beispiel BaFin, BNetzA), das BSI kümmert sich um Cyberthemen. Vorgesehen ist eine enge Zusammenarbeit der Behörden, auch mit Blick auf die EU. Die Länder benennen zentrale Ansprechpartner; für bestimmte kritische Dienstleistungen wird die Bundeszuständigkeit hervorgehoben (unter anderem Strom, Verkehr, Zahlungsverkehr, Weltrauminfrastruktur, Bundesverwaltung).

Pflichten für Betreiber

Der Entwurf bündelt Pflichten entlang eines klaren Prozesses. Wichtig sind eine frühzeitige Registrierung und ein wirksames System für Resilienz und Krisenmanagement.

- **Registrierung**: Spätestens drei Monate nach Eintritt der Kriterien muss die Anlage über die gemeinsame BBK/BSI?Stelle registriert werden, inklusive einer ständig erreichbaren Kontaktstelle. Registriert der Betreiber nicht, kann das BBK die Eintragung selbst vornehmen.
- **Risikoanalysen**: Spätestens neun Monate nach Registrierung müssen Betreiber ihre Risiken

erheben und danach mindestens alle vier Jahre überprüfen – orientiert an nationalen Risikoanalysen. Betrachtet werden alle relevanten Gefahren, Abhängigkeiten (einschließlich Lieferketten) und Standortfaktoren.

- **Resilienzmaßnahmen und Plan**: Spätestens zehn Monate nach Registrierung sind passende technische, organisatorische und sicherheitsbezogene Maßnahmen umzusetzen. Ziel ist Vorbeugung, Schutz, schnelle Reaktion, Begrenzung von Schäden und zügige Wiederherstellung. Beispiele sind Notfallvorsorge, Objektschutz, Zugangskontrollen, Alarmabläufe, alternative Lieferketten, Notstrom und personelle Maßnahmen. Mindestanforderungen legt das BBK fest; Branchenregeln können ergänzt werden. Alles wird in einem Resilienzplan dokumentiert.
- **Meldewesen**: Erhebliche Störungen oder drohende Störungen sind unverzüglich zu melden. Zunächst ist eine Kurzmeldung binnen 24 Stunden erforderlich, dann ein ausführlicher Bericht binnen eines Monats. Die gemeinsame Meldestelle von BBK und BSI bündelt Informationen; grenzüberschreitende Fälle werden EU?weit koordiniert. Bei erheblichem öffentlichen Interesse kann das BBK informieren oder eine öffentliche Unterrichtung verlangen.
- **Nachweise und Prüfungen**: Betreiber müssen belegen, welche Maßnahmen sie umgesetzt haben; dazu kann es Audits und Pläne zur Mängelbeseitigung geben. Behörden dürfen bei Zweifeln prüfen. In besonderen Fällen sind Ausnahmen möglich, wenn gleichwertige Sicherheitsniveaus nachgewiesen werden.

Verstöße gegen die Meldepflichten und Einrichtungspflichten sind bußgeldbewährt.

Pflichten und Haftung

Die Geschäftsleitung steht ausdrücklich in der Verantwortung. Sie muss Schutzmaßnahmen genehmigen, deren Umsetzung überwachen und sich regelmäßig fortbilden, um Risiken und Gegenmaßnahmen beurteilen zu können. Zudem soll auf Ersatzansprüche wegen Pflichtverletzungen grundsätzlich nicht wirksam verzichtet werden können. Die Haftung orientiert sich an der NIS?2?Logik zu Leitungspflichten und persönlicher Verantwortung.

Für die Organhaftung heißt das konkret:

- **Legalität und Organisation**: Die Geschäftsleitung muss für eine gesetzeskonforme Organisation Sorgen, was auch ein funktionierendes Resilienz? und Krisenmanagement umfasst.

- **Regress und D&O**: Wenn auf Ersatzansprüche kaum verzichtet werden kann, steigt der Druck auf interne Inanspruchnahmen. D&O?Policen sollten auf Deckungslücken geprüft werden, etwa bei wissentlichen Pflichtverstößen oder fehlenden Schulungen. In diesem Zusammenhang gilt es die jüngsten Entwicklungen in Zusammenhang mit der Verletzung von Kardinalpflichten der Geschäftsleitung und damit einhergehender Leistungsfreiheit der D&O Versicherer zu berücksichtigen (OLG Frankfurt am Main, Urteil vom 5. März 2025, Az. 7 U 134/23).

Folgen für die Corporate Governance

Für die Praxis ergeben sich insbesondere:

- **Verankerung in der Governance**: Aufsichtsrat bzw. Beirat sollten die KRITIS?Themen aktiv überwachen. In Vorstand/Geschäftsführung braucht es klare Zuständigkeiten und Eskalationsregeln.
- **Information und Dokumentation**: Entscheidungen zu Maßnahmen, Prioritäten und Budgets sollten nachvollziehbar dokumentiert werden. Regelmäßige Risiko? und Resilienzberichte gehören in die Organberichterstattung; der Resilienzplan ist laufend zu pflegen.
- **Physisch trifft digital**: NIS?2/BSIG und KRITIS?DachG sollten dahingehend organisatorisch verzahnt werden, dass ein einheitlicher Meldeweg existiert.
- **Lieferkette und Verträge**: In M&A?Prozessen werden KRITIS/NIS?2 zu festen Due?Diligence?Bausteinen; Garantien und Freistellungen sollten Registrierungs?, Melde? und Maßnahmenpflichten abdecken. Post?Closing?Pläne müssen die Umsetzung zeitnah sicherstellen.
- **Anreize**: Variable Vergütung kann an Resilienz?Ziele (KPIs) gekoppelt werden, um Fokus und Umsetzung zu stärken.

Ausblick

Das KRITIS?Dachgesetz verbindet physischen Schutz und IT?Sicherheit und nimmt die Unternehmensspitze deutlich in die Pflicht. Konkret heißt das: Ein wirksames Resilienz?Management mit klaren Genehmigungsprozessen, effektiver Überwachung, regelmäßiger Schulung und sauberer Dokumentation wird zur Kernaufgabe der Geschäftsleitung und zum Gegenstand der Überwachung seitens des Aufsichtsrats. Wer frühzeitig Strukturen, Budgets und Prozesse anpasst, senkt Bußgeld?, Betriebsunterbrechungs? und persönliche Haftungsrisiken.

Wir stehen mit unseren Kolleginnen und Kollegen von PwC Risk & Regulatory gerne für einen Austausch dazu, was die Neuerungen für Ihr Unternehmen bedeuten zur Verfügung.

Kontaktieren Sie uns

David Santa

Senior Manager Mannheim
Tel.: +49 621 40069-320
E-Mail:**david.a.santa@pwc.com**

Dr. Robert Schiller

Senior Manager Mannheim
Tel.: +49 151 52157484
E-Mail:**robert.schiller@pwc.com**

Schlagwörter

EU-Recht, Gesetzgebung