KRITIS-Dachgesetz: Physische Resilienz, Meldepflichten und Geschäftsleiterhaftung – was in 2026 auf Sie zukommt

Die **jüngsten Angriffe auf Teile der Energieinfrastruktur in Berlin** haben eindrücklich gezeigt, wie zentral eine robuste Absicherung kritischer Infrastrukturen ist und wie aufmerksam Aufsichtsbehörden, Politik und Öffentlichkeit Sicherheits- und Compliance-Themen künftig verfolgen werden. Vor diesem Hintergrund **markiert das KRITIS-Dachgesetz einen Paradigmenwechsel**: Erstmals rückt die **physische Resilienz** (Schutz von Anlagen, Personal und Lieferketten) gleichberechtigt **neben die IT-Sicherheit**. Für viele Unternehmen bedeutet das bereits vor dem erwarteten Inkrafttreten im Sommer 2026 **akuten Handlungsbedarf**, neue Pflichten mit kurzen Umsetzungsfristen und einen deutlich geschärften Blick auf **Haftungsrisiken der Geschäftsleitung.**

1. Kurze Einordnung & Geltungsbereich

Was ist das KRITIS-DachG?

- Neues Stammgesetz zur Stärkung der **Resilienz** und **physischen Sicherheit** Kritischer Infrastrukturen (KRITIS) in Deutschland
- Setzt die EU-CER-Richtlinie (EU 2022/2557) um und ergänzt die NIS2-Umsetzung (Cybersecurity)
- Regierungsentwurf vom September 2025; **Inkrafttreten wird im Laufe des Jahres 2026 erwartet**

Wer ist betroffen?

Betroffen sind **Betreiber kritischer Anlagen**, die mit ihren kritischen Dienstleistungen regelmäßig mindestens **500.000 Personen** in Deutschland versorgen (Fortführung der bisherigen KRITIS-Logik).

Wichtig: *Ob eine Anlage konkret als „kritische Anlage“ gilt, wird noch durch **separate Rechtsverordnungen** (Kategorien, Schwellenwerte, versorgte Einwohner, Stichtage) konkretisiert.*

Betroffene Sektoren:


Energie


Transport & Verkehr


Finanzwesen


Sozialversicherung & Grundsicherung


Gesundheitswesen


Wasser


Ernährung


IT & TK


Weltraum


Entsorgung


Bundesverwaltung

2. Zentrale Pflichten für Betreiber

a) Registrierungspflicht

– *Pflicht zu Selbstidentifikation und Registrierung innerhalb von **drei Monaten** nach Identifikation*

b) Risikoanalysen

– *Grds. mindestens **alle vier Jahre** Pflicht zu Risikoanalyse und –bewertung*
– *Erstmalige Risikoanalyse **innerhalb von 9 Monaten nach Registrierung***

c) Resilienzmaßnahmen & Resilienzplan

– *Bspw. Notfallvorsorge, physischer Schutz, Sicherheitsmanagement Personal, Schulungen etc.*
– *Resilienzmaßnahmen und –plan sind **spätesten 10 Monate nach Registrierung** umzusetzen*

d) Meldewesen

– *Meldepflicht für Störungen innerhalb von 24h / Ausführlicher Bericht innerhalb eines Monats*

e) Nachweise & Prüfungen

– *Auf Anforderung der BBK erforderlich*

3. Rolle der Geschäftsleitung

- Geschäftsleiter sind ausdrücklich **verpflichtet**, die **Resilienzmaßnahmen umzusetzen** und **durch geeignete Organisationsmaßnahmen zu sichern**
- **Geschäftsleitungen haften** gegenüber ihrer Einrichtung bei Pflichtverletzungen

Konsequenz: ***Persönliche Verantwortung auf C-Level****; mangelnde Umsetzung von Resilienzpflichten kann zu **Haftungsrisiken** für Geschäftsleiter führen*

4. Sanktionen & Fristen

Fristen nach Registrierung

Mit der Registrierung beginnt ein sehr knappes Umsetzungsfenster für zentrale Pflichten:

- **Risikoanalyse:** spätestens innerhalb von **9 Monaten**
- **Resilienzmaßnahmen & Resilienzplan:** spätestens innerhalb von **10 Monaten**
- **Meldewesen** (inkl. interner Prozesse für 24h-Meldungen): spätestens innerhalb von **10 Monaten**

Angesichts dieser Fristen ist eine **Vorbereitung bereits vor Inkrafttreten und vor der eigentlichen Registrierung faktisch erforderlich**, um keine aufsichtsrechtlichen Maßnahmen und empfindliche Bußgelder zu riskieren.

Bußgelder

Verstöße gegen zentrale Pflichten (z.B. Registrierung, Vorlage von Risikoanalyse oder Resilienzplan, Meldungen) können mit **Bußgeldern von bis zu 500.000 EUR** geahndet werden.

5. Typische Problemfelder & Fallstricke

Wer ist „Betreiber kritischer Anlage“?

- Eigentümer vs. Betriebsführer
- Konzerninterne Betreibermodelle
- Betreiberkonsortien, Joint Ventures
- Auslagerungen / Outsourcing

Welche Anlagen / Dienstleistungen sind konkret kritisch?

- Einordnung vor dem Hintergrund der noch ausstehenden Rechts-verordnungen
- Abgrenzung zu anderen regulierten Bereichen (z.B. DORA, EnWG, NIS2)

Wie weit reicht der Geltungsbereich der Pflichten?

- Strikter Anlagenbezug?
- oder weitreichender bspw. alle IT-Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit und Absicherung maßgeblich sind?

Welche bestehenden Standards können angerechnet werden / sind ggf. relevant?

- ISO 27001/22301, BCM-Konzepte, bestehende Sicherheitskonzepte, B3S etc.
- Umgang mit Doppelregulierung (z.B. EnWG, NIS2, DORA)

Sonderfall: Einsatz intelligenter Überwachungs- und Sicherheitssysteme

- Nutzung KI-gestützter CCTV, Zutrittskontrollen, Anomalieerkennung etc.
- Schnittstellen zu weiteren Regimen wie dem AI Act (Hochrisiko-KI, Transparenzpflichten, Daten- und Governance-Anforderungen)

Gerne prüfen wir mit Ihnen in einem kurzen Erstgespräch, ob und in welchem Umfang Handlungsbedarf für Ihr Unternehmen besteht und wie wir Sie bei der Umsetzung unterstützen können.

Ansprechpartner

Dr. Nicolas Sonder (Partner Tax & Legal)
Tel +49 151 525 16789 / E-Mail: nicolas.sonder@pwc.com

Dr. Friedrich Kneuper (Senior Manager Tax & Legal)
Tel +49 160 5363848 / E-Mail: friedrich.kneuper@pwc.com