KRITIS-Dachgesetz: Was auf Betreiber kritischer Infrastrukturen jetzt zukommt

15.04.2025, 14:32 Uhr
Kommentare: 0
Sicher arbeiten



Betreiber kritischer Infrastrukturen müssen sich auf Krisenszenarien vorbereiten. (Bildquelle: kobpr2/iStock/Getty Images Plus) © kobpr2/iStock/Getty Images Plus

Die Sicherheit kritischer Infrastrukturen steht in Deutschland zunehmend im Fokus. Das KRITIS-Dachgesetz spielt eine Schlüsselrolle bei der Transformation hin zu einer resilienten Gesellschaft. Damit soll der physische Schutz der kritischen Infrastrukturen verbessert und die Versorgungssicherheit in Deutschland gestärkt werden. Dafür müssen KRITIS-Betreiber Maßnahmen treffen, um sich gegen alle denkbaren Risiken zu schützen.

Was ist das KRITIS-Dachgesetz?

Der Entwurf zum KRITIS-Dachgesetz (Gesetz zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen) wurde am 06. November 2024 beschlossen und ins parlamentarische Verfahren eingebracht. Es wird voraussichtlich im Laufe des Jahres 2025 in Kraft treten. Ein genaues Datum steht noch nicht fest, da das Gesetzgebungsverfahren durch politische Verzögerungen ins Stocken geraten ist.

Dieses geplante deutsche Gesetz soll die physische Sicherheit und Widerstandsfähigkeit kritischer Infrastrukturen stärken. Es setzt die EU-CER-Richtlinie um und ergänzt bestehende Cybersicherheitsregelungen, damit die Cybersicherheit kritischer Infrastrukturen weiterhin gewährleistet werden kann. Ziel ist es, Betreiber von Einrichtungen wie Energieversorgern, Krankenhäusern oder Wasserversorgungsunternehmen dazu zu verpflichten, umfassende Sicherheitsmaßnahmen gegen Naturkatastrophen, Sabotage und andere Bedrohungen zu implementieren. Das Gesetz sieht unter anderem Risikoanalysen, Resilienzpläne und Meldepflichten vor.

Was ist das Ziel des Gesetzes?

Das KRITIS-Dachgesetz verfolgt das Ziel, die Funktionsfähigkeit kritischer Infrastrukturen auch unter extremen Bedingungen sicherzustellen. Es soll:

- Präventive Maßnahmen gegen Ausfälle fördern,
- eine schnelle Reaktion auf Störungen ermöglichen,
- negative Auswirkungen minimieren und
- die Wiederherstellung der Infrastruktur beschleunigen.

Dabei helfen kann auch die NIS2 (“Network and Information Systems Directive 2”), die das Ziel hat, umfassende Risiko- und Vorfallmanagementsysteme zu etablieren.

Darüber hinaus sollen durch Harmonisierung sektorenübergreifender Standards sowie institutionelle Zusammenarbeit zwischen Behörden und Betreibern die Sicherheitsvorkehrungen effizienter gestaltet werden.

Downloadtipps der Redaktion

E-Book: Industrie 4.0 in der Anwendung

Hier gelangen Sie zum Download.

E-Book: Photovoltaikanlagen normkonform errichten

Hier gelangen Sie zum Download.

Checkliste: Funktionale Aspekte - Energieeffizienz

Hier gelangen Sie zum Download.

E-Book: Elektrosicherheit in der Elektromobilität

Hier gelangen Sie zum Download.

Was sind kritische Infrastrukturen?

Kritische Infrastrukturen umfassen Einrichtungen und Organisationen, deren Ausfall schwere Folgen für die Gesellschaft hätte. Dazu zählen:

- Energieversorgung,
- Gesundheitswesen,
- Transport und Verkehr,
- Wasserwirtschaft und
- Lebensmittelversorgung.

Unter einer kritischen Infrastruktur versteht man eine Einrichtung, die die folgenden Kriterien erfüllt: Sie ist unentbehrlich für die Gesamtversorgung und versorgt mehr als 500.000 Personen. Sie ist also essenziell für die öffentliche Sicherheit sowie die wirtschaftliche Stabilität und steht daher im Fokus besonderer Schutzmaßnahmen.

Welche Risiken gibt es?

Die Risiken entstehen durch Naturereignisse, technisches oder menschliches Versagen, Kriege oder vorsätzliche Handlungen mit terroristischem oder sonstigem kriminellem

Hintergrund.

Für Betreiber kritischer Infrastrukturen ist es essenziell, sich proaktiv auf potenzielle Krisenszenarien vorzubereiten. Dabei spielen fundierte Annahmen über Eintrittswahrscheinlichkeit und Plausibilität möglicher Ereignisse ebenso eine Rolle wie die Bewertung der eigenen Verwundbarkeit, der Kritikalität betroffener Prozesse und der potenziellen Schadensfolgen. Auf dieser Grundlage lassen sich geeignete Strategien zur Risikobehandlung ableiten:

- Lassen sich Risiken vermeiden oder zumindest wirksam reduzieren?
- Ist eine Übertragung an Dritte – etwa durch Versicherungen oder vertragliche Regelungen – möglich?
- Oder entscheidet man sich bewusst dafür, ein Risiko zu akzeptieren und die Verantwortung selbst zu tragen?

Tipp der Redaktion



Das Nachschlagewerk für die Elektrofachkraft

Organisation, Durchführung und Dokumentation elektrotechnischer Prüfungen – „Elektrosicherheit in der Praxis“ unterstützt Sie bei der Umsetzung der Elektrosicherheit in Ihrem Unternehmen.

Jetzt testen!

Was kommt mit dem KRITIS-Dachgesetz auf Betreiber zu?

Das KRITIS-Dachgesetz enthält folgende zentrale Regelungen:

1. Resilienzpläne: Betreiber müssen branchenspezifische Schutzmaßnahmen entwickeln, darunter physische Sicherheitsvorkehrungen wie Zugangskontrollen.
2. Risikobewertungen: Regelmäßige Analysen zur Identifikation potenzieller Gefahren
3. Meldepflichten: Sicherheitsvorfälle müssen unverzüglich gemeldet werden.
4. Personalsicherheit: Schulungen und Sicherheitsüberprüfungen für Schlüsselpersonal
5. Sanktionen: Bußgelder bei Verstößen gegen die Vorschriften

Die Betreiber kritischer Infrastrukturen sollten sich jetzt schon mit den Anforderungen des KRITIS-Dachgesetzes auseinandersetzen und diese in ihren Unternehmen etabliert haben.

Quellen:

https://www.openkritis.de/

https://nis2-umsetzung.com/dachg-kritis/

https://kommunikation.assaabloy.de/blog/kritis-dachgesetz

https://www.bmi.bund.de/SharedDocs/faqs/DE/themen/bevoelkerungsschutz/kritis-dach/kritis-dach.html

https://mittlerer-niederrhein.ihk.de/de/digitalisierung-internet/datenschutz-und-it-sicherheit/kritis-dachgesetz-zum-schutz-kritischer-infrastrukturen.html

https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html

Risikomanagement KRITIS - Risikomanagement in Kritischen Infrastrukturen - BBK

https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2024/11/kabinett-kritis.html

Weitere Beiträge zum Thema

Industrie 4.0 und der Einfluss auf die (Elektro-)Berufe

Industrie 4.0 - Digitalisierung und Vernetzung

Künstliche Intelligenz (KI)

Machine to Machine Communication (M2M)