KRITIS-Dachgesetz und NIS 2: was bei Notstrom und Zutrittsschutz bereits gilt – und was noch kommt

09.10.2026, 13:15 Uhr
Kommentare: 0
Sicher arbeiten



NIS 2 und KRITIS-Dachgesetz: Was Betreiber jetzt umsetzen müssen © kobpr2/iStock/Getty Images Plus

Das Gesetz zur Umsetzung der europäischen NIS-2-Richtlinie und das KRITIS-Dachgesetz verschärfen die Anforderungen an die Sicherheit kritischer Anlagen in Deutschland. NIS 2 adressiert die Cybersicherheit, das KRITIS-Dachgesetz die physische Widerstandsfähigkeit. Für Betreiber und Elektrofachkräfte geht es damit konkret um Netzersatzanlagen, Zutrittskontrollen, Meldeanlagen und vernetzte Leittechnik. Während ein Teil der Pflichten bereits gilt, hängt ein weiterer Teil noch von einer ausstehenden Rechtsverordnung ab.

Zwei Gesetze mit zwei Aufsichtsbehörden

Das Gesetz zur Umsetzung der NIS-2-Richtlinie wurde im Bundesgesetzblatt 2025 I Nr. 301 vom 05.12.2025 (www.recht.bund.de) verkündet. Am Tag nach der Verkündung ist es in Kraft getreten. Nach der Pressemitteilung des Bundesamts für Sicherheit in der Informationstechnik (BSI) vom 05.12.2025 erweitert es den Kreis der beaufsichtigten Einrichtungen von rund 4.500 auf rund 29.500. Betreiber kritischer Infrastrukturen gelten automatisch als „besonders wichtige Einrichtungen“ (www.bsi.bund.de).

Das KRITIS-Dachgesetz (KRITISDachG) wurde am 16.03.2026 im Bundesgesetzblatt 2026 I Nr. 66 verkündet (www.recht.bund.de). Am Tag darauf ist es in Kraft getreten. Als Ziel beschreibt das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) bundesweit einheitliche Mindestanforderungen an die physische Resilienz kritischer Anlagen (www.bbk.bund.de).

NIS-2-Schwellen, Mindestmaßnahmen und Meldefristen

Nach § 28 des BSI-Gesetzes (BSIG) gilt ein Unternehmen aus den in den Anlagen 1 und 2 des BSIG genannten Sektoren als wichtige Einrichtung, wenn es

- mindestens 50 Mitarbeiter beschäftigt oder
- sowohl einen Jahresumsatz als auch eine Jahresbilanzsumme von jeweils mehr als zehn Millionen Euro erreicht (www.gesetze-im-internet.de).

§ 30 Abs. 2 BSIG nennt zehn Mindestmaßnahmen. Drei davon sind für die Elektrotechnik besonders relevant:

- Nr. 3 betrifft die Aufrechterhaltung des Betriebs und die Wiederherstellung nach einem Notfall,
- Nr. 4 die Sicherheit der Lieferkette und
- Nr. 9 Konzepte für die Zugriffskontrolle.

Nach § 30 Abs. 1 BSIG muss die Einrichtung die Umsetzung dokumentieren (www.gesetze-im-internet.de).

§ 32 BSIG regelt ein dreistufiges Meldeverfahren für erhebliche Sicherheitsvorfälle. Die frühe Erstmeldung muss unverzüglich, spätestens jedoch 24 Stunden nach Kenntnis, an die gemeinsame Meldestelle von BSI und BBK gehen. Spätestens nach 72 Stunden hat eine Meldung mit erster Bewertung zu erfolgen, die Abschlussmeldung ist spätestens einen Monat danach fällig (www.gesetze-im-internet.de). Betreiber kritischer Anlagen nutzen laut BSI vorübergehend ihre bisherigen Meldewege (www.bsi.bund.de).

Downloadtipps der Redaktion

E-Book: Industrie 4.0 in der Anwendung

Hier gelangen Sie zum Download.

E-Book: Elektrosicherheit in der Elektromobilität

Hier gelangen Sie zum Download.

Unterweisung: Elektrofachkraft/verantwortliche Elektrofachkraft

Hier gelangen Sie zum Download.

Checkliste: Energiemanagementsystem nach DIN VDE 0100-801

Hier gelangen Sie zum Download.

Angriffserkennung für maßgebliche Leittechnik

§ 31 Abs. 2 BSIG verpflichtet Betreiber kritischer Anlagen zu Systemen zur Angriffserkennung für alle informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der Anlage maßgeblich sind. Die Systeme erfassen Parameter aus dem laufenden Betrieb kontinuierlich und automatisch und werten sie aus. Der Stand der Technik soll eingehalten werden (www.gesetze-im-internet.de).

Das Gesetz knüpft die Pflicht an die Frage, ob ein informationstechnisches System, eine Komponente oder ein Prozess für die Funktionsfähigkeit der Anlage maßgeblich ist;

einzelne Gewerke nennt es nicht. Nach Einschätzung des Autors können Fernwirk-, Leit- und Gebäudeautomationstechnik dieses Kriterium erfüllen, wenn die Anlage ohne sie nicht funktionsfähig ist. In diesem Fall sind auch ihre Netzwerkanschlüsse in die Angriffserkennung einzubeziehen. Entsprechendes gilt nach dieser Einschätzung für vernetzte Zutrittskontrollen, die zugleich eine physische Schutzmaßnahme nach dem KRITIS-Dachgesetz darstellen. Jede neue Vernetzung einer Steuerung, eines Zählers, einer Schaltanlage oder einer Zutrittskontrolle sollte daher mit dem IT-Verantwortlichen des Betreibers abgestimmt werden.

KRITIS-Dachgesetz nennt die Notstromversorgung ausdrücklich

§ 13 Abs. 1 KRITISDachG verpflichtet Betreiber zu Maßnahmen, die Vorfälle verhindern, Liegenschaften physisch schützen, Vorfälle abwehren und die kritische Dienstleistung nach einem Vorfall zügig wiederherstellen. Soweit keine spezialgesetzlichen Regelungen der jeweiligen Branche vorgehen, nennt § 13 Abs. 3 KRITISDachG unter anderem Objektschutz, Instrumente zur Überwachung der Umgebung, Detektionsgeräte und Zugangskontrollen als mögliche Maßnahmen. § 13 Abs. 3 Nr. 4 Buchst. a KRITISDachG führt außerdem Maßnahmen zur Aufrechterhaltung des Betriebs auf und nennt dabei ausdrücklich die Notstromversorgung (www.gesetze-im-internet.de).

§ 13 Abs. 2 KRITISDachG verlangt verhältnismäßige Maßnahmen nach dem Stand der Technik, § 13 Abs. 4 KRITISDachG einen Resilienzplan, der die Maßnahmen und die zugrunde liegenden Erwägungen darstellt. Nach Einschätzung des Autors gehören damit Netzersatzanlage, unterbrechungsfreie Stromversorgung, Einbruchmeldetechnik, Videoüberwachung und elektronische Schließsysteme in diesen Plan. Eine DIN-VDE-Norm oder eine technische Regel nennt § 13 KRITISDachG nicht. Verbindliche Mindestanforderungen kann nach § 14 Abs. 1 KRITISDachG erst eine Rechtsverordnung des Bundesinnenministeriums mit Zustimmung des Bundesrates festlegen. Nach § 14 Abs. 2 KRITISDachG dürfen Betreiber oder Branchenverbände branchenspezifische Resilienzstandards vorschlagen, deren Eignung das BBK feststellt (www.gesetze-im-internet.de).

Welche Norm den Stand der Technik für die Notstromversorgung beschreibt, richtet sich nach dem Zweck der Stromquelle. Nach Einschätzung des Autors zielt § 13 KRITISDachG auf eine Ersatzstromversorgung, die den Betrieb der kritischen Dienstleistung aufrechterhält. Für ihre Errichtung gilt DIN VDE 0100-551 in der Ausgabe Februar 2017 (www.dke.de); als Nachfolger dieses Normteils steht DIN VDE 0100-751 im Arbeitsprogramm der DKE. Versorgt dasselbe Aggregat zusätzlich Sicherheitsbeleuchtung oder Brandschutzeinrichtungen, ist außerdem DIN VDE 0100-560 in der Ausgabe Oktober 2022 zu berücksichtigen. Sie lässt RCDs und AFDDs in Sicherheitsstromkreisen nicht zu (www.dke.de/de).

Aggregate in Krankenhäusern und baulichen Anlagen für Menschenansammlungen fallen unter DIN 6280-13. Die gültige Ausgabe stammt von Dezember 1994 (www.dinmedia.de).

Für Zutrittskontrollen legt DIN EN 60839-11-1 (VDE 0830-8-11-1) in der Ausgabe Dezember 2013 Sicherheitsgrade, Mindestfunktionen und Prüfverfahren fest (www.dke.de).

Einbruch- und Überfallmeldeanlagen fallen unter DIN VDE 0833-1 in der Ausgabe Oktober 2014 (www.dke.de); seit Februar 2025 liegt dazu der Entwurf einer Neufassung vor.

Nach Einschätzung des Autors können Prüfprotokolle nach diesen Normen im Resilienzplan

als Nachweise dafür dienen, dass die jeweiligen Anlagen fachgerecht geprüft wurden und der Stand der Technik berücksichtigt wurde.

Tipp der Redaktion



Sie wollen mehr Infos zu diesem und weiteren Themen?

Dann empfehlen wir Ihnen **elektrofachkraft.de** – Das Magazin:

- spannende Expertenbeiträge zu aktuellen Themen
- Download-Flat mit Prüflisten, Checklisten, Arbeits- und Betriebsanweisungen.

Erste Ausgabe gratis!

Auch als Onlineversion erhältlich. Machen Sie mit beim Papiersparen.

Registrierung wartet auf die Rechtsverordnung

§ 8 Abs. 1 KRITISDachG verlangt die Registrierung spätestens drei Monate nach Einstufung einer Anlage als kritische Anlage. Nach Abs. 7 gilt die Pflicht zur Risikoanalyse nach § 12 KRITISDachG neun Monate nach der Registrierung. Die Pflichten nach §§ 13, 18 und 20 KRITISDachG gelten nach zehn Monaten. § 18 KRITISDachG verlangt dann die Meldung von Vorfällen unverzüglich, spätestens 24 Stunden nach Kenntnis. Ein ausführlicher Bericht folgt spätestens nach einem Monat (www.gesetze-im-internet.de). Für die 24-Stunden-Frist braucht der Betreiber nach Einschätzung des Autors eine sofortige Nachricht der Elektrofachkraft, sobald eine Netzersatzanlage ausfällt.

Ob eine Anlage als kritische Anlage gilt, bestimmt eine Rechtsverordnung nach § 4 Abs. 3 und § 5 Abs. 1 KRITISDachG. Ende September 2026 befand sich diese Verordnung laut FAQ des BBK noch in Erarbeitung und Abstimmung. Deshalb besteht derzeit noch keine Registrierungspflicht. Auch die Muster für Resilienzpläne sind nach derselben Seite noch in Erstellung (www.bbk.bund.de). Nach § 13 Abs. 5 KRITISDachG muss das BBK die Muster spätestens acht Monate nach Inkrafttreten der Verordnung bereitstellen (www.gesetze-im-internet.de).

Externe Elektrobetriebe im Sicherheitsmanagement des Betreibers

§ 13 Abs. 3 Nr. 5 KRITISDachG nennt als mögliche Maßnahme ein Sicherheitsmanagement für die Mitarbeiter, das auch das Personal externer Dienstleister einbezieht; Nr. 6 führt

Schulungen und Übungen auf. Adressat der gesetzlichen Pflichten ist der Betreiber der kritischen Anlage. Für einen externen Elektrobetrieb werden die Anforderungen daher erst durch die vertragliche Einbindung verbindlich. § 16 KRITISDachG regelt den Nachweis: Nach Abs. 3 kann der Betreiber die Einhaltung seiner Pflichten durch Audits belegen, wobei die Behörde die zugrunde liegende Dokumentation anfordern darf. Nach Abs. 4 müssen ausgewählte Betreiber den Prüfern Zutritt zu Betriebsräumen und Anlagen gewähren (www.gesetze-im-internet.de).

Die Vorbereitung lohnt sich nach Einschätzung des Autors bereits vor Erlass der Rechtsverordnung. Betreiber und beauftragte Elektrobetriebe sollten

- Netzersatzanlagen,
- unterbrechungsfreie Stromversorgungen,
- Zutrittskontrollen und
- Meldeanlagen

mit Prüfprotokollen, Wartungsstand und vernetzten Komponenten erfassen. Diese Übersicht liefert eine Grundlage für die Risikoanalyse nach § 12 und für Audits nach § 16 KRITISDachG. Zusätzlich sollte ein verbindlicher Meldeweg für den Ausfall einer Netzersatzanlage vereinbart werden. Auch das BBK empfiehlt Betreibern in seinen FAQ, sich schon jetzt mit der Steigerung der Resilienz zu befassen (www.bbk.bund.de).

Fazit

NIS 2 und das KRITIS-Dachgesetz greifen ineinander, setzen aber unterschiedliche Schwerpunkte: Das BSIG regelt bereits heute die Cybersicherheit und Angriffserkennung, während die konkrete Einstufung kritischer Anlagen nach dem KRITIS-Dachgesetz noch von der ausstehenden Rechtsverordnung abhängt. Betreiber und Elektrobetriebe sollten diese Wartezeit nutzen, um relevante Anlagen, Nachweise, Zuständigkeiten und interne Meldewege strukturiert vorzubereiten.

Kurz & knapp

- NIS 2: Cybersicherheit und Meldepflichten für kritische Anlagen
- KRITIS-Dachgesetz: Anforderungen an die physische Resilienz
- Fokus auf Notstromversorgung, Zutrittskontrollen und vernetzte Leittechnik
- Angriffserkennung für maßgebliche IT- und OT-Systeme erforderlich
- Registrierungspflichten nach KRITIS-Dachgesetz noch von Rechtsverordnung abhängig
- Anlagen, Nachweise und Meldewege bereits jetzt vorbereiten und dokumentieren

Weitere Beiträge zum Thema

KRITIS-Dachgesetz: Was auf Betreiber kritischer Infrastrukturen jetzt zukommt

Cybersicherheit: Herausforderung für kritische Infrastrukturen

Basiswissen Cybersecurity – die Bandbreite der Bedrohungen

Smart Grids in kritischen Infrastrukturen – Netzstabilität im Zeitalter von Extremwetter und Cybergefahren

KI-basiertes Lastmanagement für USV-Systeme in Rechenzentren und Industrieanlagen (Teil 1)

KI-basiertes Lastmanagement für USV-Systeme in Rechenzentren und Industrieanlagen (Teil 2)

KI-basiertes Lastmanagement für USV-Systeme in Rechenzentren und Industrieanlagen (Teil 3)

Autor:

Thomas Joos

freiberuflicher Publizist



Thomas Joos ist freiberuflicher Publizist und veröffentlicht neben seinen Büchern auch Artikel für verschiedene Medien wie dpa, Computerwoche und C’t.

Seit seinem Studium der medizinischen Informatik berät er auch Unternehmen im Bereich IT, Security und Absicherung von Rechenzentren.