M Security Consulting H R

Planungs- & Sachverständigenbüro für Sicherheitstechnik
* Sicherheitsberatung * Sicherheitsplanung * Sicherheitskonzepte
* Physical Security Management * Technischer Risikomanager *
Corporate Security * Notfall- Krisenmanagement * Risiko-
Gefährdungsanalysen * Projektmanagement *

Dachgesetz zur Stärkung kritischer Anlagen (KRITIS-Dachgesetz)

Übersicht

Am 16.01.2023 trat die Richtlinie (EU) 2022/2557 (CER-Richtlinie) in den EU-Mitgliedstaaten in Kraft. Betreiber systemrelevanter / kritischer Infrastrukturen (KRITIS) sehen sich in der aktuellen geopolitischen Lage realen Bedrohungsszenarien ausgesetzt. Die Betreiber kritischer Infrastrukturen werden mit dem NIS2 und KRITIS-Dachgesetz sektorübergreifende Anforderungen bezüglich der IT-Sicherung und dem physischen Schutzes auferlegt. NIS2 und das KRITIS-Dachgesetz beinhalten auch regelmäßige, wiederkehrende Risikobewertungen und ein zentrales Störungs-Monitoring, welches gegenüber Behörden (BSI und BKK) nachzuweisen ist.

Bildnachweis: www.bmi.bund.de

Die nationale Verabschiedung der Resilienzstrategie der Bundesregierung soll bis **17. Januar 2026** erfolgen. Betreiber kritischer Infrastrukturen haben bis einschließlich **17. Juli 2026** Zeit, um eine Registrierung beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) vorzunehmen.

Gefahrenansatz / Schutzniveau / Schutzmaßnahmen

M Security Consulting H R

Planungs- & Sachverständigenbüro für Sicherheitstechnik * Sicherheitsberatung * Sicherheitsplanung * Sicherheitskonzepte * Physical Security Management * Technischer Risikomanager * Corporate Security * Notfall- Krisenmanagement * Risiko-Gefährdungsanalysen * Projektmanagement *

Grundsätzlich ist nach dem All-Gefahren-Ansatz sich zu orientieren, bei dem alle denkbaren Risiken wie:

- Naturereignisse (Erdbeben; Hochwasser; Schlagregen; Sturm….)
- Sabotage, Vandalismus, Einbruch, Diebstahl, Feuer;
- Pandemie;
- Spionage;
- Anschlag, Bombendrohung, Terror;
- menschliches Versagen,
- Cyberattacken….

berücksichtigt werden müssen.

Um das Schutzniveau verbindlich zu erhöhen, müssen Betreiber umsetzen:

- Resilienzpläne erstellen,
- betriebliches Risiko- und Krisenmanagement einrichten,
- angemessenes Sicherheitsmanagement gewährleisten,
- geeignete technische Schutzmaßnahmen.

Geeignete technische Schutzmaßnahmen sind:

Zutrittskontrolle, Gefahrenmeldeanlage, Videoüberwachung, Perimeterschutz, IT-Grundschutz.

Gesetzesvorgaben / Resilienzplan

M Security Consulting H R

Planungs- & Sachverständigenbüro für Sicherheitstechnik * Sicherheitsberatung * Sicherheitsplanung * Sicherheitskonzepte * Physical Security Management * Technischer Risikomanager * Corporate Security * Notfall- Krisenmanagement * Risiko-Gefährdungsanalysen * Projektmanagement *

Nachfolgende Paragraphen sollen erst am 1. Januar 2026 in Kraft treten:
– § 6 (Anforderungen an Betreiber Kritischer Infrastrukturen)
– § 7 (Kritische Anlagen von besonderer Bedeutung für Europa)
– § 8 (Registrierung der kritischen Anlage)
– § 10 (Risikoanalysen und Risikobewertungen der Betreiber kritischer Anlagen)
– § 11 (Resilienzmaßnahmen der Betreiber kritischer Anlagen)
– § 12 (Meldewesen für Störungen)

Folgender Paragraph soll erst am 1. Januar 2027 in Kraft treten.

– § 19 (Bußgeldvorschriften)

Was ist ein Resilienzplan und was beinhaltet dieser?

- Risikobewertung: Bewertung der Risiken, denen die Organisation ausgesetzt ist, einschließlich potenzieller Cyber-Bedrohungen und Schwachstellen;
- Entwicklung von Reaktionsstrategien: Festlegung von Verfahren und Maßnahmen zur Reaktion auf Sicherheitsvorfälle und zur Minderung ihrer Auswirkungen;
- Business Continuity Management: Sicherstellen, dass kritische Geschäftsprozesse auch bei Störungen aufrechterhalten oder schnell wiederhergestellt werden können;
- Redundanz- und Ausfallsicherungsmechanismen: Implementierung von Systemen und Prozessen, die bei einem Ausfall als Backup dienen;
- Regelmäßige Tests und Übungen: Durchführung von Tests und Übungen zur Überprüfung und Verbesserung der Resilienz- und Wiederherstellungsstrategien;
- Mitarbeiterschulung und Sensibilisierung: Sensibilisierung und Vorbereitung des Personals auf potenzielle Bedrohungen (Cyber und physisch) und deren Auswirkungen;

Wichtige Eckpunkte aus dem KRITIS-Dachgesetz

M Security Consulting H R

Planungs- & Sachverständigenbüro für Sicherheitstechnik
* Sicherheitsberatung * Sicherheitsplanung * Sicherheitskonzepte
* Physical Security Management * Technischer Risikomanager *
Corporate Security * Notfall- Krisenmanagement * Risiko-
Gefährdungsanalysen * Projektmanagement *

Die wichtigsten Eckpunkte aus dem KRITIS-Dachgesetz zusammengefasst:
Physische Sicherheit ist verpflichtend,

- Verpflichtende Umsetzung einheitlicher technischer Mindeststandartschutz u.a. mit Detektionssystemen und Systemen zur Überwachung der Umgebung, → nach Stand der Technik (z.B. durch Videoüberwachung,...)
- klare, einheitliche „Wer gehört zu KRITIS“-Definitionen nach qualitativen und quantitativen Kriterien,
- Meldepflicht von Störfällen innerhalb 24 Stunden
- Nachweispflicht der Resilienzen;

Bei kritischen IT-Komponenten:

- BSI-Gesetz (§ 9b Abs. 3 BSIG) fordert Garantieerklärungen über Vertrauenswürdigkeit des Herstellers.

Bei anderen kritischen NICHT-IT-Komponenten:

- Für einen umfassenden Schutz werden Regelungen geprüft, um KRITIS insgesamt vor Einflüssen und Abhängigkeiten von bedenklichen Herstellern aus dem Ausland zu schützen.

Ziel: Ganzheitliche Resilienz:

- Physische Sicherheit und Cybersicherheit gemeinsam und übergreifend „denken“, monitoren und prüfen („Security Convergence“),
- Steigerung der „geopolitischen“ Resilienz,
- Prüfung auf Verbau / Anwendung bedenklicher Hersteller (z. Bsp. Hard- und Software in IT) aus dem Ausland.

Abstimmung beim Cyberschutz und beim physischen Schutz, durch enge Zusammenarbeit zweier Aufsichtsbehörden mit Meldepflicht bei Vorkommnissen:

- **IT- und Cyberschutz:** Bundesamt für Sicherheit in der Informationstechnik (**BSI**)
- **Physischer Schutz (neu):** Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (**BBK**)

Unsere Dienstleistungen

M Security Consulting H R

Planungs- & Sachverständigenbüro für Sicherheitstechnik * Sicherheitsberatung * Sicherheitsplanung * Sicherheitskonzepte * Physical Security Management * Technischer Risikomanager * Corporate Security * Notfall- Krisenmanagement * Risiko-Gefährdungsanalysen * Projektmanagement *

- Ganzheitliche Bestandsaufnahme (Ist-Situation) anhand einer Vorortbegehung (Perimeter, Zuko,-systeme, VSS, IT- und Technikräume, Entwicklung- / Versuchsräume ….)
- Abgleich Bestandsaufnahmen mit evtl. bestehenden Konzepten / Unternehmensvorgabe…
- Abgleich gesetzlicher Rahmen (BSI; BKK; BMI; KRITIS-Dachgesetz; DSGVO)
- Bedrohungs- / Risikoanalyse
- Ermitteln von Schwachstellen
- Erstellen von Empfehlung für ein nachhaltiges Basisschutzkonzept unter Berücksichtigung aktueller politischer Lage und gesetzl. Vorgaben, Schließung von ermittelten Sicherheitslücken. (Empfehlung für jeden Standort separat, da evtl. abweichende Risiken oder Sicherheitslücken bestehen)
- Anfertigung von Entwurfsplänen (z. B.: Perimeterschutz in 2 D / 3 D),
- Konzepterstellung von Notfall- und Krisenmanagementunterlagen,
- Erarbeitung von Sicherheitsrichtlinien,
- Wiederkehrende Audits zur Erfüllung der Nachweispflicht und Resilienzpflichten (alle vier Jahre);

Alle Leistungen werden schriftlich erbracht und werden Ihnen nach einer Abschlusspräsentation übergeben. Die Unterlagen können auch zum Nachweis gegenüber den Behörden vorgelegt werden.

Optionale Leistungen

M Security Consulting H R

Planungs- & Sachverständigenbüro für Sicherheitstechnik
* Sicherheitsberatung * Sicherheitsplanung * Sicherheitskonzepte
* Physical Security Management * Technischer Risikomanager *
Corporate Security * Notfall- Krisenmanagement * Risiko-
Gefährdungsanalysen * Projektmanagement *

- Erstellen von Ausschreibungsunterlagen nach Thematik (z. Bsp.: Perimeter; Zuko; Sicherung IT- / Technikräume; Werkschutz; Sicherungszentrale; …… incl. Grobkostenschätzung)
- Mitwirkung / Unterstützung Einkauf bei Ausschreibung / Auswertung Bieterangebote / Empfehlung Bieter ….
- Koordinierung / Beaufsichtigung / Abnahme / Inbetriebnahme von Ausführungen der Gewerke

Let‘s keep in touch – Unsere Kontaktdaten

Planungs- und Sachverständigenbüro Mohr
- Sicherheitsexperten für physische Sicherheit -
Luckenstraße 43
D – 70794 Filderstadt
Tel.: 0711 / 773020

E-Mail: info@fachplaner-mohr.de

Web: www.fachplaner-mohr.de