Schutz von kritischen Infrastrukturen

Hinweise zur Stärkung von Sicherheit und Resilienz

Sicherheitsrisiken haben Auswirkungen auf den Schutz der kritischen Infrastrukturen (KRITIS).

Physische Sicherheitsrisiken, z. B.:

- Unbefugter Zugang zu kritischen Infrastrukturen
- Sabotage und Wirtschaftskriminalität

Cybersicherheitsrisiken, z. B.:

- Cyberangriffe, einschließlich Malware und Ransomware
- Datenverlust oder –manipulation

Organisatorische Schwachstellen, z. B:

- Fehlen eines ganzheitlichen Sicherheitsrisiko-Managements
- Mangelndes Sicherheitsbewusstsein

Was besagt das KRITIS-Dachgesetz?

Das KRITIS-Dachgesetz (KRITIS-DachG) in Deutschland zielt darauf ab, die physische Resilienz und Sicherheit von kritischer Infrastrukturen durch strenge Sicherheitsanforderungen, Risikomanagement und Meldepflichten für Betreiber zu stärken.

Tritt in Kraft:	Geplant: Oktober 2024
Umzusetzen bis:	Bis Juli 2026
Minimale Versorgungseinheit, ab der das KRITIS-DachG gilt:	500.000 betroffene Personen

Energie	Entsorgung	Ernährung	Finanzen und Versicherung	Gesundheit
IT und Tele-kommunikation	Transport und Verkehr		Wasser	Weltraum

pwc

Was fordert das KRITIS-DachG?

Was sind die prioritären Anforderungen des KRITIS-DachG?

§7 – Registrierung als Betreiber
- Spätestens 1 Arbeitstag nach Inbetriebnahme als kritisches System
- Bereitstellung eines Ansprechpartners
- Registrierung kann auch von Behörden vorgegeben werden

§9 Risikoanalyse und Bewertung
- Erstmalig 9 Monate nach der Registrierung
- Regelmäßig alle 4 Jahre
- Grundlage: Risikoanalyse der Bundesministerien
- Bewertung von Risiken wie Naturgefahren, hybride Bedrohungen, Spionage, Terrorismus und Abhängigkeit von anderen Stellen

§10 Festlegung von Maßnahmen und Plänen zur Resilienz
- Maßnahmen zur Prävention und angemessenen Reaktion auf kritische Zwischenfälle
- Implementierung von physischen Sicherheitsmaßnahmen
- Dokumentation in einem Resilienzplan

§12 Berichtswesen bei Vorfällen
- Störungen müssen den zuständigen Behörden gemeldet werden
- Zu meldende Daten:
    - Anzahl der betroffenen Nutzer
    - Voraussichtliche Dauer der Unterbrechung
    - Betroffenes geografisches Gebiet

Wie können Unternehmen jetzt auf diese Anforderungen reagieren?

Prüfung etwaiger regulatorischer Anforderungen
- Durchführung einer Betroffenheitsanalyse hinsichtlich des KRITIS-DachG

Erfassung und Bewertung von Sicherheitsrisiken
- Risikoanalyse inkl. Identifizierung und Bewertung von Assets, Gefährdungen, Schwachstellen und Auswirkungen
- Ableitung von Schutzmaßnahmen

Entwicklung eines Standortsicherheitskonzepts
- Konzeptionierung von standortspezifischen Schutzmaßnahmen auf Grundlage der Sicherheitsrisiken

Implementierung physischer Schutzmaßnahmen
- Videoüberwachung, Zutrittskontrolle, Einbruchdetektion, Perimeterschutz, Bewachungsdienste
- Schulung von Mitarbeitern

Etablierung einer Steuerungs- und Analyseplattform
- Einheitliche Steuerung und Auswertung von Daten und Systemen

Wie unterstützt PwC bei der Umsetzung der KRITIS-DachG-Anforderungen?

Wir unterstützen unsere Mandanten in vier Fachdisziplinen, um sie auf die Anforderungen des KRITIS-DachG vorzubereiten.

1 Schutz von physischer Infrastruktur und Gebäuden

- Identifikation von möglichen Risiken
- Erstellung eines risikobasierten Standortsicherheitskonzepts
- Definition von Schutzmaßnahmen, um Risiken zu begegnen (Videoüberwachung, Perimeterschutz, Einbruchserkennung, Zutritts-kontrolle, Wachpersonal)
- Prävention des Schwunds von Unternehmenswerten
- Integration von Leading Practices und Benchmarks

2 Sicherheit im ganzheitlich-strategischen Ansatz

- Durchführung einer ganzheitlichen Risikoanalyse und Bewertung potenzieller Bedrohungen
- Entwicklung und Implementierung einer Sicherheitsstrategie
- Analyse und Anpassung der Sicherheitsmaßnahmen
- Integration von Sicherheitsmanagement und sicherheitsrelevanten Erkenntnissen in die Unternehmensführung und Entscheidungsfindung

3 Schutz von Mitarbeitenden und Gästen

- Durchführung von regelmäßigen Sicherheitsunterweisungen
- Förderung einer Sicherheitskultur durch Schulungen und Sensibilisierungsprogramme
- Schaffung von Maßnahmen zum Schutz besonders gefährdeter Personen
- Zusätzlich auch: Implementierung von Maßnahmen zur Resilienz von Reisenden und Expatriates

4 Konvergenz der Sicherheit (Cyber und Physisch)

- Schaffung einer gemeinsamen Sicherheitsinfrastruktur
- Durchführung regelmäßiger Koordinationstreffen
- Implementierung von integrierten Detektionssystemen
- Entwicklung von gemeinsamen Resilienzplänen und Reaktionsstrategien
- Nutzung von Technologien zur Echtzeit-Detektion und Analyse von Sicherheitsdaten aus beiden Bereichen

Sie haben Fragen?
Kontaktieren Sie unsere Experten.

Andre Glenzer
Partner
Risk & Regulatory
+49 160 94470376
andre.glenzer@pwc.com

Jens Greiner
Director
Risk & Regulatory
+49 175 353 2089
jens.greiner@pwc.com

Über uns

Unsere Mandanten stehen tagtäglich vor vielfältigen Aufgaben, möchten neue Ideen umsetzen und suchen Rat. Sie erwarten, dass wir sie ganzheitlich betreuen und praxisorientierte Lösungen mit größtmöglichem Nutzen entwickeln. Deshalb setzen wir für jeden Mandanten, ob Global Player, Familienunternehmen oder kommunaler Träger, unser gesamtes Potenzial ein: Erfahrung, Branchenkenntnis, Fachwissen, Qualitätsanspruch, Innovationskraft und die Ressourcen unseres Expertennetzwerks in 155 Ländern. Besonders wichtig ist uns die vertrauensvolle Zusammenarbeit mit unseren Mandanten, denn je besser wir sie kennen und verstehen, umso gezielter können wir sie unterstützen.

PwC Deutschland. Rund 12.000 engagierte Menschen an 21 Standorten. 2,3 Mrd. Euro Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland.