

Das KRITIS-Dachgesetz

Ganzheitlicher Schutz von Anlagen und Betrieb kritischer Infrastrukturen

Um die Anforderungen des KRITIS-Dachgesetzes sicher zu erfüllen, müssen Betreiber kritischer Infrastrukturen jetzt tätig werden. Und auch ihre Dienstleister und Zulieferer entlang der Lieferkette sind aufgrund des erweiterten Geltungsbereichs gefordert: Um die Sicherheit und Resilienz des Betriebs zu jeder Zeit zu gewährleisten, müssen Verantwortliche einen 360-Grad-Schutz vor sämtlichen Gefahren aufbauen.



Abbildungen und Fotos: Siemens AG

Zeitliche Abfolge der juristischen Maßnahmen: Betreiber kritischer Infrastrukturen müssen jetzt tätig werden, um die Anforderungen des KRITIS-Dachgesetzes zu erfüllen.

Kritische Infrastrukturen (kurz KRITIS) sind unverzichtbar für das Funktionieren der Gesellschaft und des täglichen Lebens. Entsprechend wichtig ist es, ihre Sicherheit und Integrität zu schützen. Drei Gefährdungsarten stehen dabei heute im Fokus: Physische Bedrohungen, Cyberkriminalität und geopolitische Beeinträchtigungen. Mit der NIS-2-Richtlinie hat die Europäische Union bereits eine Gesetzgebung zur Cybersicherheit in Kraft gesetzt. Die CER-Richtlinie zielt ergänzend auf die physische Widerstandsfähigkeit kritischer Infrastrukturen ab. Das KRITIS-Dachgesetz (KRITIS-DachG) stellt die deutsche Umsetzung beider Richtlinien in nationales Recht dar: Unter einem Dach adressiert das

Gesetz den Schutz der kritischen Infrastrukturen vor Bedrohungen aller Art. Für Staat und Bevölkerung bedeutet das mehr Sicherheit – für Betreiber jedoch zunächst viel Arbeit. Zwar wurde das Gesetz bereits im November 2024 beschlossen, aber es wird wohl erst im Laufe dieses Jahres in Kraft treten. Nach einer nationalen Risikobewertung soll eine verpflichtende Umsetzung in Resilienzmaßnahmen bis zum November 2026 erfolgen. Alle vier Jahre ist dann durch die Betreiber eine Neubewertung durchzuführen.

Darüber hinaus erweitert sich der Geltungsbereich. Denn mit dem Dachgesetz erkennt der Gesetzgeber an, dass für den Betrieb sicherer Infrastrukturen nicht nur die Anlagen selbst ge-

schützt werden müssen, sondern auch deren gesamte Lieferkette. Die Folge ist dann einerseits, dass für wesentliche Betriebsmittel eine zweite oder gar dritte Lieferkette aufgebaut werden muss – beispielsweise für Gas als Energieträger.

Abseits der eigentlichen Anlagen der kritischen Infrastrukturen definiert das KRITIS-Dachgesetz zudem „Unternehmen von besonderem Interesse“. Ist etwa für die Aufrechterhaltung der Prozesse einer Anlage ein Dienstleister verantwortlich, kann dieser automatisch zu einem Unternehmen von besonderem Interesse werden.

Diese Neuerung des Gesetzes erweitert den Kreis der betroffenen Akteure erheblich: Während in Deutschland die



Mit den geeigneten Maßnahmen sichern Betreiber ihre Anlage ganzheitlich gegen Bedrohungen.

kritischen Infrastrukturen im engeren Sinne schätzungsweise 5.000 Betriebe umfassen, wird davon ausgegangen, dass die gesamten Lieferketten bundesweit aus bis zu 30.000 weiteren Unternehmen bestehen.

Gesetzes-Anforderungen

Das KRITIS-Dachgesetz soll kritische Infrastrukturen schützen, indem es Betreiber zu technischen, sicherheitsbezogenen und organisatorischen Maßnahmen für die Stärkung der physischen Sicherheit und Resilienz ihrer Anlagen verpflichtet. Dabei wird zwischen verschiedenen Pflichten unterschieden:

- **Prävention:** Vorbeugende Maßnahmen, die Risiken reduzieren und Anlagen gegen künftige Bedrohungen schützen. Dazu zählt das Gesetz auch Aspekte des Klimawandels wie Sturmschäden oder Überflutungen.
- **Physischer Schutz:** Mit Zäunen und Sperren, Videosicherheit, Detektionseinrichtungen und Zutrittskontrollen müssen Anlagen gegen den unbefugten Zutritt von Angreifern geschützt werden.
- **Reaktion:** Betreiber müssen Risiko- und Krisenmanagementverfahren etablieren, Protokolle führen und Krisenreaktionspläne erstellen.
- **Wiederherstellung:** Im Falle eines Angriffs soll die Aufrechterhaltung des Betriebs sichergestellt werden

(etwa durch Notstromaggregate) bzw. die schnellstmögliche Wiederaufnahme gewährleistet sein. Dabei müssen Betreiber auch ihre Lieferketten berücksichtigen.

- **Personalsicherheit:** Das Gesetz verpflichtet Betreiber, Personen mit kritischen Funktionen zu definieren, individuelle Zutrittskontrollen zu etablieren und eine Rechte- und Rollenprüfung zu gewährleisten. Außerdem müssen sie Schulungsanforderungen berücksichtigen und alle relevanten Qualifikationen der Mitarbeitenden sicherstellen.

- **Sensibilisierung:** Mit Pflichtveranstaltungen (wie Webinare oder Schulungen) und Übungen zum Notfallmanagement müssen Betreiber die Aufrechterhaltung aller relevanten Tätigkeiten zu jeder Zeit sicherstellen.
- **Stand der Technik:** Verantwortliche haben die Pflicht, ihre Anlage auf dem Stand der Technik gemäß europäischen Richtlinien zu halten. Dabei müssen sie Normen und Standards, Zertifizierungen, Best Practices und aktuelle Softwareversionen berücksichtigen.



Mit einem Videomanagementsystem können Betreiber ihre Anlage kontinuierlich überwachen und die Umgebung analysieren. Die Lösung ermöglicht auch das Aufdecken von Anomalien oder kriminellen Handlungsabsichten.



In Hochsicherheitsanwendungen werden Zutrittskontrollsysteme mit einem Berechtigungsmanagement verknüpft, um so die Zuweisung von Zugriffsrechten basierend auf Rollen, Aufgaben und Verantwortlichkeiten effektiv und sicher verwalten zu können.

Besonders der erweiterte physische Schutz und die Betrachtung der gesamten Lieferkette stellen Betreiber vor neue Herausforderungen. Nicht zuletzt aufgrund der erwartungsgemäß hohen Strafen bei Nichtbeachtung sollten Verantwortliche hier unverzüglich aktiv werden: Das Gesetz nennt den Betreiber einer kritischen Anlage als Verantwortlichen für die Umsetzung der Maßnahmen. Der Geschäftsführer haftet dafür auch persönlich.

Außerdem müssen Betreiber umfangreiche Meldepflichten bei Störungen beachten, die das KRITIS-Dachgesetz vorgibt: Sie besagen, dass Meldungen innerhalb von 24 Stunden nach Bekanntwerden an das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) gemeldet werden müssen. Anschließend bleibt dem Betreiber ein Monat Zeit für einen zusätzlich einzureichenden ausführlichen Bericht.

Alle Lösungen unter einem Dach

Ob Einbruchschutz, Zutrittskontrolle oder Cybersicherheit: Für jeden Baustein der Maßnahmen des KRITIS-Dachgesetzes gibt es zahlreiche Dienstleister, die Betreiber unterstützen. Wer für jeden Bereich einen individuellen Anbieter wählt, steht jedoch schnell vor einem Flickenteppich an Maßnahmen, Produkten und Dienstleistungen. Betreiber sind deshalb gut beraten, sich an einen Komplettanbieter zu wenden. Siemens bietet einen 360-Grad-

Ansatz, der wie das KRITIS-Gesetz alle Schutzmaßnahmen unter einem Dach vereint. Das ganzheitliche Angebot umfasst alle vom Gesetz geforderten Aspekte:

- Zutrittskontrolle
- Perimeterschutz
- Einbruchschutz
- Physical Security as a Service
- Digitale Services
- Videosicherheit
- Gefahrenmanagement
- Cybersecurity Services
- Sichere Cloud- und Hybrid-Lösungen
- Modernisierungskonzepte



Ein Perimeterschutzsystem teilt das Gelände in verschiedene Sektoren mit eigenen Schutzgraden ein, um Anlagen bedarfsgerecht zu schützen.

Basierend auf den Erfahrungen zahlreicher abgeschlossener Projekte startet Siemens den Umsetzungsprozess mit einem Gap Assessment, das eine systematische und umfassende Beurteilung des Cybersicherheitsstatus der Anlage ermöglicht. Darauf aufbauend werden konkrete Handlungsempfehlungen erstellt. Diese umfassen individuelle Schutzkonzepte, die auf den betreiberspezifischen Sicherheitsanforderungen basieren. Ein Schutzkonzept besteht aus physischen und Cyber-Sicherheitsmaßnahmen, um einen ganzheitlichen Schutz der Anlagen zu gewährleisten. Nach der Umsetzung erfolgt eine Wirksamkeitsprüfung. Über eine Siemens-eigene Notruf- und Serviceleitstelle (NSL) wird zu jedem Zeitpunkt die Aufrechterhaltung der Geschäftskontinuität und eine schnelle Störungsbehebung gewährleistet.

Sicherheit für alle Bereiche

Kritische Infrastrukturen decken alle Bereiche des Lebens ab und halten zahlreiche branchenspezifische Besonderheiten bereit. Sicherheit muss für alle Bereiche der kritischen Infrastrukturen gegeben sein. Staat und Gesellschaft verlassen sich im Alltag auf die Leistungen der kritischen Infrastrukturen.

*Jürgen Rumenev, Senior Consultant
Security Lifecycle, Siemens AG, Siemens
Smart Infrastructure, Deutschland*

FACILITY MANAGEMENT

Integration | Planung | Gebäudemanagement

Zukunftsweisende Themen für die Facility ManagerInnen

Jetzt **2** Ausgaben lesen

und über **40%** sparen*



Jetzt zugreifen!



facility-management.de/vorteilspaket

*Ich erhalte die FACILITY MANAGEMENT gedruckt 2 Ausgaben lang zum Preis von nur 36,00 € (inkl. gesetzl. MwSt.) und spare im Vergleich zum Einzelheftkauf über 40% pro Ausgabe. Außerdem erhalte ich als Dankeschön ein Geschenk meiner Wahl gratis dazu. Das Abonnement verlängert sich um 1 Jahr zum regulären Preis, wenn es nicht schriftlich, spätestens 2 Wochen nach Erhalt der letzten Ausgabe, gekündigt wird. Ihnen steht ein gesetzliches Widerrufsrecht zu. Alle Informationen über dieses Recht und die Widerrufsbelehrung finden Sie unter www.bauverlag-shop.de/widerrufsbelehrung – Bauverlag BV GmbH, Friedrich-Ebert-Straße 62, 33330 Gütersloh

Mini-Abo