Was bedeutet das KRITIS-Dachgesetz für Ihre Infrastruktur?

Das KRITIS-Dachgesetz bringt eine entscheidende Neuerung mit sich, um die Widerstandsfähigkeit und Reaktionsfähigkeit kritischer Infrastrukturen zu verbessern.
Es fordert Mindeststandards, die den physischen Schutz und die Cybersicherheit aller für die Versorgungssicherheit relevanten Prozesse kombiniert. Unternehmen und Organisationen im Bereich der kritischen Infrastruktur, aber auch ihre Lieferanten sollten sich schon heute auf die Herausforderungen vorbereiten, die das neue Gesetz mit sich bringt.

Mit dem KRITIS-Dachgesetz ändert sich eine Menge für Sie. Risikobewertungen, Resilienzpläne und Meldungen von Störungen sind nur einige der Themen, die auf Sie zukommen werden. Was gleich bleibt: Mit Siemens können Sie auf einen starken, erfahrenen und zuverlässigen Partner vertrauen, mit dem Sie die gesetzlichen Anforderungen angehen können und der Sie während des gesamten Lebenszyklus Ihrer Infrastruktur unterstützt.

Wer ist betroffen?

Das KRITIS-Dachgesetz ist eine Kombination aus der europäischen NIS2-Richtlinie für Cybersicherheit und der CER-Richtlinie, welche die physische Sicherheit im Fokus hat. Das zukünftige Dachgesetz soll für alle Organisationen und Unternehmen gelten,die laut der CER-Richtlinie zu einem der zwölf Sektoren gehören, sowie für die Unternehmen in deren Lieferketten.

Fünf Schritte bereiten Sie optimal vor

1. Prüfen Sie, ob Ihr Unternehmen in den Anwendungsbereich des KRITIS-Dachgesetzes fällt.
2. Prüfen Sie, was auf Sie zukommen könnte.
3. Wenn Ihr Unternehmen nicht unmittelbar unter das KRITIS-Dachgesetz fällt, prüfen Sie, ob Sie Lieferant oder Dienstleister für ein KRITIS-Unternehmen sind und deshalb den neuen Vorschriften unterliegen.
4. Passen Sie Ihr Sicherheitskonzept basierend auf der vorab erstellten Risikoanalyse gemeinsam mit Ihren Lieferanten und Dienstleistern an, um die Sicherheit der Lieferkette zu gewährleisten.
5. Sprechen Sie mit uns über die beste Umsetzung der Anforderungen aus dem KRITIS-Gesetz – und wie wir diese mit den zusätzlichen branchenspezifischen Anforderungen in einem koordinierten Vorgehen verbinden, um Sie optimal zu unterstützen.

SIEMENS

Regelmäßige Risikoanalysen und -bewertungen
Alle vier Jahre soll durch den Betreiber der Anlage eine Risikoanalyse und -bewertung erfolgen. Daher gilt es im regelmäßigen Turnus den Sicherheitszustand der Gebäudetechnik entsprechend Ihren ggf. veränderten Bedürfnissen aktuell zu halten. Unser Gap Assessment analysiert den Cybersicherheitsstatus Ihrer gebäudetechnischen Anlagen inklusive Prozesse, Organisation und Technik vor Ort.
Mit dem Assessment zeigen wir Ihnen mögliche Sicherheitslücken auf und geben konkrete Handlungsempfehlungen, um diese zu schließen und Cyberrisiken zu senken.

Schutz und Resilienz verbessern
Auf Basis der Risikoanalyse und -bewertung erstellen wir mit Ihnen ein ganzheitliches Schutzkonzept, welches sowohl die Cybersicherheit als auch die physische Sicherheit umfasst. Mit unserem umfangreichen Portfolio an Gebäudesicherheitslösungen und Services, unter anderem für Perimeterschutz, Videosicherheit, Zutrittskontrolle und Einbruchmeldeanlagen für Hochsicherheitsanwendungen, erhöhen wir maßgeblich den physischen Schutz und die Resilienz Ihrer Liegenschaften.

Koordinierte Meldungen für Vorfälle
Störungen sollen künftig innerhalb von 24 Stunden an die gemeinsame Meldestelle des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK) und des Bundesamts für Sicherheit in der Informationstechnik (BSI) gemeldet werden. Unser Managementsystem Siveillance Control fasst einzelne Alarme intelligent und visuell aufbereitet zu einem Ereignis zusammen. Basierend auf vordefinierten Plänen schlägt das System dynamisch Maßnahmen vor und leitet den Bediener kontrolliert durch den Vorfall. Einzelne Maßnahmen werden nacheinander abgearbeitet und dokumentiert.

Diese Dokumentation kann im Building X Security Manager durch weitere Informationen aus der Cloud angereichert und zu einem automatisierten Report zusammengefasst werden. Damit haben Sie schnell alle benötigten Informationen zur Hand, um die zeitlichen Anforderungen zu erfüllen.

Weitere Informationen zum KRITIS-Dachgesetz erhalten Sie unter siemens.de/kritis-dachgesetz

So können wir Sie unterstützen:

- Bei uns erhalten Sie von der Planung bis zur Wartung alles aus einer Hand.
- Wir erstellen maßgeschneiderte Schutzkonzepte für Ihre Liegenschaften – basierend auf Ihren individuellen Sicherheitsanforderungen.
- Wir setzen die definierten Maßnahmen um und prüfen sie auf Wirksamkeit.
- Die Siemens eigene Notruf- und Service Leitstelle (NSL) unterstützt Sie im Gefahrenfall bei der Erhaltung der Geschäftskontinuität und einer schnellen Störungsbehebung.
- Intelligent und disziplinübergreifend vernetzt bieten wir nahtlos integrierte Lösungen in Bezug auf branchenspezifische Anforderungen, die benötigten Technologien und ihre Implementierungsanforderungen.
- Unsere Technologien entsprechen den aktuellen Normen und Richtlinien.
- Mit unserem ganzheitlichen Secure-by-design-Ansatz sorgen wir proaktiv für den modernsten Schutz von Unternehmen und Infrastrukturen – mit Produkten und Lösungen, die über ihre gesamte Nutzungsdauer cybersicher und geschützt sind.
- Die gewonnenen Gebäudedaten lassen sich auch für die Optimierung von Unternehmensprozessen nutzen, wie zum Beispiel zur Vorbeugung von Lebensmittelverschwendung.

Herausgeber
Siemens AG

Smart Infrastructure
Gateway Gardens
De-Saint-Exupéry-Str. 5
60549 Frankfurt am Main
Deutschlannd

Kundenbetreuungs-Center
Tel. 0800 100 76 39
info.de.sbt@siemens.com

Artikel-Nr. E10003-A38-K2
(Stand 05/2024)

SIEMENS