Whitepaper

Gebäude- und IT-Schutz im KRITIS-Bereich

Wie Sie Ihre Infrastruktur gegen aktuelle und zukünftige Risiken absichern

Foto: istock - CHUNYIP WONG

Foto: istock - SasinParaksa

Foto: istock - anandaBGD

Was ist KRITIS ?

Kritische Infrastrukturen (KRITIS) sind Einrichtungen oder Organisationen, die für das staatliche Gemeinwesen von großer Bedeutung sind. Ihr Ausfall oder ihre Beeinträchtigung kann zu Versorgungsengpässen, Störungen der öffentlichen Sicherheit und anderen dramatischen Folgen führen. Zu den Sektoren kritischer Infrastrukturen gehören Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Medien und Kultur, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung.

Regulierte Sektoren

Die Identifikation und Bewertung von kritischen Infrastrukturen erfolgt in Deutschland durch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK). In umfangreichen Verfahren werden die relevanten Einrichtungen, Anlagen oder Teile davon identifiziert, die für das Funktionieren des Gemeinwesens von hoher Bedeutung sind. Erreicht oder überschreitet eine Einrichtung bestimmte Schwellenwerte, wird sie als kritische Infrastruktur eingestuft. Hierüber wird die Organisation aktiv informiert. Als KRITIS-Betrieb eingestuft, müssen gesetzliche Melde- und Nachweispflichten gemäß dem Bundesamt für Sicherheit in der Informationstechnik (BSI) erfüllt werden.

KRITIS-Sektoren

Erforderliche Schutzmaßnahmen

Um Ausfälle und Beeinträchtigungen von kritischen Infrastrukturen zu verhindern, sind Schutzmaßnahmen erforderlich. Hierzu zählen präventive Maßnahmen wie das Risikomanagement. Durch eine systematische Analyse und Bewertung können mögliche Schwachstellen identifiziert und entsprechende Gegenmaßnahmen ergriffen werden.

Eine weitere wichtige Komponente des Schutzes kritischer Infrastrukturen ist die Stärkung der Cybersicherheit. In Zeiten zunehmender digitaler Angriffe ist es unerlässlich, geeignete Maßnahmen zum Schutz vor Cyberbedrohungen zu ergreifen. Sofern noch nicht vorhanden, müssen robusten Sicherheitslösungen implementiert werden. Es muss außerdem eine regelmäßige Aktualisierung und ein Patch- Management erfolgen. Das in einem KRITIS-Betrieb arbeitende Personal muss im Umgang mit Cybersicherheit geschult werden. Angemessene Sicherheitsrichtlinien und Verfahren müssen aufgestellt und eingehalten werden.

Zusätzlich ist eine umfassende Notfallplanung und -vorbereitung erforderlich, um auf mögliche Ausfälle vorbereitet zu sein. Notfallpläne müssen ausgearbeitet werden, die regelmäßig überprüft und aktualisiert werden. Regelmäßig müssen Notfallübungen durchgeführt werden. Sichergestellt werden muss auch, wie im Fall einer Krise miteinander kommuniziert wird.

Nicht zuletzt sind KRITIS-Organisationen aufgefordert, Widerstandsfähigkeit aufzubauen und Sicherheitslücken zu schließen. Dies beinhaltet die regelmäßige Überprüfung und Aktualisierung von bestehenden Sicherheitsmaßnahmen, die Durchführung von Sicherheitstests und Audits sowie die Implementierung von geeigneten Schutzmechanismen und -verfahren.

So handeln Sie richtig

Wurde ihr Betrieb vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) erstmals als KRITIS-Betrieb identifiziert? Hier erhalten Sie erste Tipps zum weiteren Vorgehen.

- ✔ Intern Verantwortlichkeiten klären und zuordnen
- ✔ Bestandsaufnahme machen indem die vorhandene Infrastruktur und Sicherheitslage als Basis für die Risikoanalyse erfasst wird
- ✔ Risikoanalyse selbst durchführen oder durchführen lassen um Schwachstellen und Bedrohungen auf Basis der Bestandsaufnahme zu identifizieren
- ✔ Team benennen, das die Einhaltung aller gesetzlichen Anforderungen während der gesamten Umsetzung sicherstellt
- ✔ Sicherheitskonzept erstellen, das alle identifizierten Risiken adressiert.
- ✔ Etablierung eines Krisen- und Sicherheitsmanagements
- ✔ Planung für effizientes Notfall- und Krisenmanagement beginnen um im Ernstfall schnell reagieren zu können.
- ✔ Einführung der im Sicherheitskonzept festgelegten Maßnahmen
- ✔ Unter allen Mitarbeitern Bewusstsein schaffen, was KRITIS bedeutet und die implementierten Maßnahmen verstehen.
- ✔ Fortlaufende Information und Sensibilisierung für alle Mitarbeitenden, um das Sicherheitsbewusstsein kontinuierlich zu stärken.

Was ist NIS-2?

Die EU-Richtlinie NIS-2 ist eine überarbeitete Version der NIS-1-Richtlinie aus dem Jahr 2016. Sie soll einheitliche Standards für Cybersicherheit schaffen, die europaweit gelten. Die NIS2 besagt, dass betroffene Unternehmen bestimmte Informationssicherheitsstandards einhalten müssen – ihre IT-Infrastruktur darf nicht „einfach“ angreifbar sein.

Welche Betriebe sind betroffen?

In Deutschland sind von der NIS-2-Richtlinie laut Schätzungen zwischen 29.000 bis 40.000 Unternehmen betroffen. Es unterliegen deutlich mehr Unternehmen der NIS-2-Richtlinie als der NIS-1, da die Schwellenwerte aktualisiert wurden. Grundsätzlich adressiert NIS-2 Unternehmen mit mindestens 50 Mitarbeitenden und 10 Millionen Euro Umsatz in bestimmten Sektoren. Die betroffenen Unternehmen werden NICHT aktiv informiert, sondern sie sind aufgefordert, selbst zu überprüfen, ob sie unter NIS-2 fallen.

Die festgelegten Sektoren machen schlagartig eine ganze Reihe von Unternehmen verantwortlich, die bisher kaum Vorschriften zu ihrer Informationssicherheit beachten mussten. Wer die NIS-2-Richtlinie nicht beachtet, muss mit Sanktionen und Strafen rechnen. Diese können bis zu zehn Millionen Euro oder zwei Prozent des gesamten weltweiten Jahresumsatzes betragen. Auch Geschäftsführer oder andere Verantwortliche können persönlich belangt werden, selbst dann, wenn es andere, vertragliche Vereinbarungen gibt.

Erforderliche Schutzmaßnahmen

Was müssen Unternehmen tun, damit sie nicht gegen die NIS-2-Richtlinie verstoßen? Sie müssen verschiedene Cybersecurity-Maßnahmen umsetzen.
Hierzu zählen:
- Richtlinien für Risiken und Informationssicherheit erstellen und umsetzen
- Prävention, Detektion und Bewältigung von Cybersecurity-Vorfällen (Sicherheitspannen)
- Betrieb eines Business Continuity Managements (BCM) inkl. Backup- bzw. Krisen-Management
- Gewährleistung der Sicherheit bei der Beschaffung von IT- und Netzwerk-Systemen
- Beachtung von Vorgaben für Kryptographie oder Verschlüsselung
- Umsetzung angemessener Maßnahmen zur Zugangskontrolle
- Einsatz sicherer Sprach-, Video- und Text-Kommunikation
- Einsatz gesicherter Notfall-Kommunikations-Systeme
- Überprüfung der Sicherheit in der gesamten Lieferkette
- Schulung und Sensibilisierung von Beschäftigten

WICHTIG

Unternehmen sollten kurzfristig überprüfen, ob sie unter NIS-2 fallen.
Betroffene Betriebe sollten frühzeitig Ressourcen in
finanzieller, personeller und zeitlicher Hinsicht einplanen.

Welche Sektoren gibt es?

In der NIS-2 gibt es elf „wesentliche“ und sieben „wichtige“ Sektoren. Erfüllt ein Unternehmen die Kriterien der Umsatz- und Unternehmensgröße und ist in den folgenden Sektoren tätig, so unterliegt es der NIS-2.

18 KRITIS-Sektoren

WESENTLICHE Sektoren	WICHTIGE Sektoren
1. Energieversorger	1. Post- und Kurierdienste
2. Transportwesen	2. Abfallwirtschaft
3. Bankwesen	3. Chemikalien
4. Finanzmarktinfrastruktur	4. Lebensmittel
5. Gesundheit	5. Industrie
6. Trinkwasser	6. Digitale Dienste
7. Abwasserwirtschaft	7. Forschungseinrichtungen
8. Digitale Infrastruktur	
9. IKT-Dienstleistungsmanagement	
10. Öffentliche Verwaltungen	
11. Weltraumwirtschaft	

Beachten Sie, dass Ihr Unternehmen von keiner Behörde wegen der NIS-2-Richtlinie angeschrieben und zum Handeln aufgefordert wird. Jeder Betrieb muss selbst prüfen, ob die Regelung auf ihn zutrifft. Das zuständige Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet online eine Betroffenheitsprüfung > an. Die Prüfung ist als einfache Orientierungshilfe konzipiert und bietet keine tiefen Detailinformationen.

So unterstützt SEC-COM bei KRITIS-Anforderungen

Wir bieten unseren von KRITIS betroffenen Kunden genau passende Cyber-Sicherheitslösungen an, mit denen Sie alle gesetzlichen Anforderungen erfüllen können. Mit Unterstützung von SEC-COM können Sie ein zuverlässiges Risikomanagement einführen. Selbstverständlich unterstützen wir auch bei der Notfallplanung und -wiederherstellung. Unser Team kann die Mitarbeitenden in KRITIS-Betrieben in Sachen Cybersicherheit schulen und sensibilisieren.
Außerdem kümmern sich die Experten von SEC-COM auch um das Thema Gebäudesicherheit. Dort, wo wir Sicherheitsmängel feststellen, können wir beispielsweise durch eine engmaschige Zutrittskontrolle, durch Lösungen für die Videoüberwachung, durch einen modernen Einbruchschutz und die Einrichtung eines passenden Alarmservers für höchste physische Sicherheit in ihren Gebäuden oder auf dem umliegenden Gelände sorgen.

So unterstützt SEC-COM bei NIS-2-Anforderungen

Mit der NIS-2-Richtlinie gelten ab Oktober 2024 für viele Unternehmen und Organisationen in 18 kritischen Sektoren verpflichtende Sicherheitsmaßnahmen und Meldepflichten – auch für viele Betriebe, die bisher nicht betroffen waren. Zum Teil können auch Lieferanten von NIS-2-Betrieben indirekt betroffen sein. Unternehmen und Organisationen, die unter die NIS-2-Richtlinie fallen, müssen fast immer ihre IT-Sicherheit stärken, aber auch die physische Umwelt muss vorschriftsgemäß abgesichert sein („All-Gefahren-Ansatz“).
SEC-COM unterstützt Sie hier in allen Belangen. Wir nehmen ihre vorhandene Technik genau unter die Lupe und erarbeiten in Abstimmung mit ihnen eine Strategie, mit der sie alle NIS-2-Anforderungen zuverlässig erfüllen. Kommt es zu einem Ereignisfall, können Sie auf unsere Unterstützung zu jeder Stunde an jedem Tag im Jahr vertrauen. Besser ist es jedoch, mit nachhaltiger Beratung und innovativer Technologie präventiv zu handeln.

Zutrittskontrollen

- Integration einer digitalen Zutrittskontrolle
- Protokollieren Sie jederzeit und automatisiert, wer wann in Ihrem Gebäude ein- und ausgeht

Schließsysteme

- Integration eines digitalen Schließsystems
- Vergeben Sie oder entziehen Schließ-Rechte je nach Person, Uhrzeit oder Tür
- Kopplung des digitalen Systems mit der Alarm anlage oder anderen Sicherungssystemen
- Einfaches Ersetzen oder Sperren verlorener Schlüssel

Brandmeldetechnik

- Integration einer modernen Brandmeldeanlage
- Vernetzung mit Leitstellen oder der Feuerwehr
- Automatisierte Alarmierung zur Räumung des Objektes
- Ansteuerung von Rauchableitungen von Aufzugbetrieb und Löschanlagen

Videoüberwachung

- Integration von leistungsstarken Kamerasystemen für alle Anforderungen
  Behalten Sie Gebäude innen und außen im Blick
- Überwachung des Betriebsgeländes auch bei völliger Dunkelheit
- Videoüberwachung auch in Bereichen mit großer Hitze, Kälte, Feuchtigkeit
- Beratung zur Einhaltung des Datenschutzes

Einbruchmeldeanlagen

- Beratung und fachmännische Installation von Alarmanlagen (verdrahtet oder als Funk-Version) mit unterschiedlicher VdS-Klassifizierung
- Integration streng gemäß den üblichen Normen, Bestimmungen und Richtlinien
- Wartung aller technischen Komponenten in regelmäßigen Abständen
- Regelmäßige Tests aller Systeme

IT-Sicherheitslösungen

- Erarbeitung einer maßgeschneiderten IT-Sicherheitslösung, die Ihre Firmen-IT und Ihre Daten auf allen Ebenen schützt
- Berücksichtigung mobiler Geräte
- Lösungen zur SSL-Verschlüsselung

Firewalls

- Zuverlässige Abwehr von Cybersicherheitsbedrohungen
- Anti-Spy-Filter

Alarmserver

- Erarbeitung einer passenden Lösung für technische Störfälle, Überfall und Einbruch, Feuer und Terroralarm
- Sofortige Warnung bei allen Ereignisfällen
- Effiziente und zuverlässige Kommunikation bei Notfällen
- Schnelle Evakuierung von Gebäuden
- sofortige Alarmierung von Sicherheitskräften
- exakte Gebäudeplanung in Zusammenarbeit mit der Polizei, der Feuerwehr oder anderen Organisationen
- Nutzung standardisierter Schnittstellen – dadurch Integration vorhandener Systeme
- Verknüpfung mit anderen Sicherheitstechniken (zB. Brandmeldeanlage)

Sie haben Fragen zu unseren Produkten oder Dienstleistungen?
Dann rufen Sie uns einfach an unter der Telefonnummer +49 2361 9322445
oder senden uns eine E-Mail an sicherheit@sec-com.de

Unternehmensgruppe

SEC COM

Ihr **Systemhaus** für Kommunikation, Sicherheit und IT

www.sec-com.de

Stand: August 2024

2 x in NRW

SEC-COM Sicherheits- und Kommunikationstechnik GmbH

Bochumer Str. 6
45661 Recklinghausen
Telefon: 0 23 61 / 93 22-0
info@sec-com.de

SEC-COM Sicherheits- und Kommunikationstechnik Ostwestfalen GmbH
Karl-Schurz-Straße 32
33100 Paderborn
Telefon: 0 52 51 / 8 74 98-0
info@sec-com.de

Zertifiziert gemäß DIN EN ISO 9001

qualityaustria
SYSTEMZERTIFIZIERT
ISO 9001:2015 NR.21628/399