SECCOM

Whitepaper

Gebäude- und IT-Schutz im KRITIS-Bereich

Wie Sie Ihre Infrastruktur gegen aktuelle und zukünftige Risiken absichern

Aktualisierte Version

Die Bilder auf dieser Seite wurden mithilfe von künstlicher Intelligenz (KI) generiert.

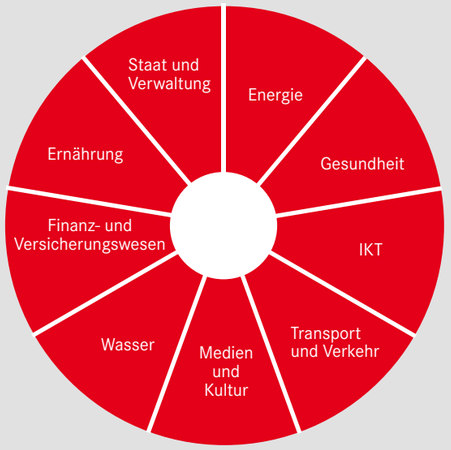
Was ist KRITIS ?

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 robuste 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 sowie regelmäßig überprüft und aktualisiert werden. Ergänzend sind Notfallübungen durchzuführen. Auch muss sichergestellt sein, 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 NIS-2 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 rund 29.500 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 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 weitere „wichtige“ Sektoren. Erfüllt ein Unternehmen die Kriterien der Umsatz- und Unternehmensgröße und ist in den folgenden Sektoren tätig, so unterliegt es der NIS-2.

WESENTLICHE Sektoren	**WICHTIGE Sektoren**
1. Energieversorger	1. Post- und Kurierdienste
2. Transportwesen	2. Abfallwirtschaft
3. Bankwesen	3. Chemikalien
4. Finanzmarktinfrastruktur	4. Lebensmittelproduktion, -verarbeitung und -vertrieb
5. Gesundheit	5. Verarbeitendes Gewerbe bzw. Herstellung von Waren
6. Trinkwasser	6. Digitale Dienste
7. Abwasserwirtschaft	7. Forschungseinrichtungen
8. Digitale Infrastruktur	
9. IKT-Dienstleistungsmanagement	
10. Öffentliche Verwaltungen	
11. Weltraumwirtschaft	

18 KRITIS-Sektoren

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, Link siehe QR Code. Die Prüfung ist als einfache Orientierungshilfe konzipiert und bietet keine tiefen Detailinformationen.

Selbstprüfung unbedingt sorgfältig durchführen

Unternehmen sollten kurzfristig überprüfen, ob sie unter NIS-2 fallen. Das BSI stellt hierfür ein Online-Tool zur Betroffenheitsprüfung bereit, siehe QR-Code auf Seite 5 unten. Das Ergebnis ist nicht rechtsverbindlich, gibt aber eine erste Orientierung.

Was geschieht nach der Selbstprüfung?

Sollte die Selbstprüfung ergeben, dass Ihr Unternehmen unter die NIS-2-Regelung fällt, greifen drei direkte Verpflichtungen:

✓ Registrierungspflicht:

Das Unternehmen muss sich beim Bundesamt für Sicherheit in der Informationstechnik (BSI) bzw. der zuständigen nationalen Behörde registrieren.

✓ Meldepflicht bei Vorfällen:

Erhebliche Sicherheitsvorfälle müssen nach einem gestuften Fristensystem gemeldet werden (Frühwarnung innerhalb von 24 Stunden, vollständige Meldung nach 72 Stunden).

✓ Risikomanagement-Maßnahmen:

Technische und organisatorische Maßnahmen zur IT-Sicherheit müssen nachweisbar etabliert werden.

Unser Tipp:

Betroffene Betriebe sollten frühzeitig Ressourcen in finanzieller, personeller und zeitlicher Hinsicht für die Umsetzung und Erfüllung der NIS-2-Richtlinie einplanen. Ein Information Security Management System (ISMS) nach ISO 27001 deckt rund 70-80 Prozent der NIS-2-Anforderungen ab und bildet damit eine effiziente Grundlage für die Compliance-Umsetzung.

Was ist ein ISMS?

Ein Information Security Management System (ISMS, englisch für „Managementsystem für Informationssicherheit“) ist die Aufstellung von Verfahren und Regeln innerhalb einer Organisation, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

Der Begriff wird im Standard ISO/IEC 27002 definiert. ISO/IEC 27001 definiert ein ISMS. Der deutsche Anteil an dieser Normungsarbeit wird vom DIN NIA-01-27 IT-Sicherheitsverfahren betreut. Je nach Branche und Gesetz muss eine Organisation ein zertifiziertes ISMS betreiben – oft mit einem jährlichen, externen Audit. In anderen Branchen mit weniger strikter Auslegung gilt eine freiwillige Zertifizierung. Sie ist auch ein Wettbewerbsvorteil, um Kunden und Geschäftspartnern gegenüber den Nachweis zu erbringen, ein hohes Maß an IT-Sicherheitsmaßnahmen einzuhalten.

Die Bilder auf dieser Seite wurden mithilfe von künstlicher Intelligenz (KI) generiert.

Technische Vernetzung

So gelingt moderne Gefahrenabwehr

Isolierte Sicherheitssysteme gehören der Vergangenheit an. In modernen Gewerbe- und Verwaltungsimmobilien entfaltet Gebäudesicherheit ihre volle Wirkung erst durch die nahtlose Integration verschiedener technischer Komponenten.

Systeme vernetzen, Sicherheit erhöhen

Wenn Zutrittskontrolle, elektronische Schließsysteme, Einbruch- und Brandmeldeanlagen sowie Videoüberwachung in Echtzeit miteinander kommunizieren, entstehen synergistische Schutzmechanismen. Diese automatisierten Abläufe verkürzen Reaktionszeiten im Notfall entscheidend, leiten Menschen sicher aus Gefahrenzonen und unterstützen Einsatzkräfte präzise. Technische Vernetzung wird so vom passiven Überwachungswerkzeug zum aktiven, lebensrettenden Akteur.
Der Weg von isolierten Sicherheitssystemen hin zu integrierten, miteinander kommunizierenden Komponenten ist deshalb weitaus mehr als bloße Modernisierung.

Klassische Lösungen geraten an Grenzen

Traditionell wurden Sicherheitssysteme in Gebäuden als unabhängige Gewerke geplant und betrieben. Die Brandmeldeanlage schlug Alarm, die Einbruchmeldeanlage überwachte den Perimeterschutz, während die Videoüberwachung und das Zutrittskontrollsystem vollkommen eigenständig agierten. Tritt jedoch ein kritisches Ereignis ein, stößt dieser klassische Ansatz schnell an seine Grenzen, da wertvolle Minuten verstreichen, wenn Informationen manuell zusammengeführt oder Zugänge im Chaos einer Evakuierung händisch freigeschaltet werden müssen. Der Einsatz heutiger Technologie nutzt die Digitalisierung voll aus.

Automatisierung nutzen

Die moderne Gebäudeautomation setzt daher auf offene Schnittstellen wie IP-basierte Protokolle sowie auf übergeordnete Gefahrenmanagementsysteme. Ein solches System führt sämtliche Sensoren und Aktoren auf einer einheitlichen Bedienoberfläche zusammen. Tritt ein Alarm auf, führt die Software die Signale unterschiedlicher Subsysteme zusammen und löst vordefinierte Automatismen aus. Das erhöht nicht nur die Transparenz für Sicherheitsverantwortliche, sondern reduziert auch menschliche Fehlentscheidungen unter extremer Stressbelastung. Gerade in Extremsituationen können uns vernetzte Systeme wertvoll unterstützen.

Szenario A

Dynamischer Amok- und Bedrohungsschutz im Bürogebäude

Wie wirkungsvoll diese Synergien in der Praxis greifen, zeigt das Beispiel eines Verwaltungsgebäudes mit rund 200 Mitarbeitenden. Betritt eine unbefugte, bewaffnete Person das Foyer, wird über eine geschulte Kraft an der Rezeption oder über einen intelligenten Video-Sensor unverzüglich ein stiller Alarm ausgelöst.

Innerhalb von Millisekunden reagieren die vernetzten Systeme vollautomatisch auf diese Bedrohung. Das Zutrittskontrollsystem und die elektronischen Beschläge schalten das Gebäude augenblicklich in einen dynamischen Lockdown-Modus. Außen- und Flurtüren werden für den Zutritt von außen verriegelt, was das weitere Vordringen des Täters effektiv unterbindet, während die Fluchtwege für die Beschäftigten aus der Gegenrichtung weiterhin nutzbar bleiben. Zeitgleich schalten die Kameras im Foyer und in den Fluren auf Höchstauflösung, verfolgen die Zielperson mittels Bewegungs-Tracking und übertragen die Live-Bilder direkt an die Leitstelle der Einsatzkräfte.

Parallel dazu erhalten die Beschäftigten in ihren Büros diskrete Warnmeldungen auf ihre Arbeitsplatz-PCs und Diensthandys mit der konkreten Anweisung, sich einzuschließen und türenferne Bereiche aufzusuchen. Der Aktionsradius des Angreifers wird somit maximal eingeschränkt, während der Polizei bereits bei der Anfahrt ein exaktes Lagebild vorliegt.

Szenario B

Integrierte Gefahrenabwehr im Logistikzentrum

Ein zweites Beispiel verdeutlicht den Nutzen in der Industrie und Logistik. In einer großen Lagerhalle einer Spedition bricht in der Nähe eines Chemikalienlagers ein Brand aus, wodurch durch austretende Substanzen eine akute Explosionsgefahr entsteht. Obwohl hier nur wenige Personen im Schichtbetrieb arbeiten, lagern hohe Sachwerte, und an den Laderampen herrscht reger Lkw-Verkehr.

Sobald ein optischer Rauchmelder anschlägt, setzt das Gefahrenmanagementsystem ohne Zeitverlust eine koordinierte Rettungskette in Gang. Während die Brandmeldeanlage die Entrauchungsanlagen sowie automatische Löscheinrichtungen ansteuert, entriegelt das Zutrittskontrollsystem fluchtplanmäßig alle Notausgänge und Brandschutztüren im betroffenen Sektor. Die Beschäftigten können die Halle dadurch ohne Verzögerung verlassen. Parallel öffnen sich elektronische Schranken automatisch für anrückende Rettungskräfte, während die Videovernetzung an den Zufahrtsrampen ankommende Lkw-Fahrer über digitale Anzeigetafeln warnt und vom Gefahrenbereich wegbeordert.
Über die digitale Erfassung der Transponder am Zutrittssystem lässt sich am Sammelplatz sofort abgleichen, ob sich noch Personen im Gebäude befinden. Ohne manuelles Eingreifen schaffen die vernetzten Komponenten binnen Sekunden optimale Voraussetzungen für die Brandbekämpfung und verhindern eine Katastrophe für Mensch, Material und Umwelt.

Vernetzte Sicherheit greift

Die Zeiten einzelner, isoliert arbeitender Produktlösungen sind vorbei. Wer echte Verbesserungen auf dem Betriebsgelände und bei der Gebäudesicherheit erreichen will, benötigt ein sorgfältig aufeinander abgestimmtes Gesamtsystem. Die eingesetzten Produkte „kennen“ sich und sie kommunizieren miteinander. Wichtige Informationen werden zusammengeführt und ermöglichen eine effiziente Reaktion.

Brandmeldeanlage
Mit einem Handfeuermelder kann ein Alarm im Brandfall manuell ausgelöst werden.

Digitales Schließsystem
Digitales Möbelschloss: Vergabe individueller Schließrechte; passend für jedes Möbelstück, auch für Coworking und Büros auf Zeit

Videoüberwachung
Thermalkamera: Thermalfunktionen wie Branderkennung, Raucherkennung, Temperaturmessung, Erkennung von kalten und heißen Bereichen, Unterscheidung zwischen Personen und Fahrzeugen.

Digitales Schließsystem
Digitaler Beschag: Passend für jede Tür (auch Glastüren), erhältlich in vielen Farben, Formen und Größen

Brandmeldeanlage
Eine moderne BMA dient dem vorbeugenden Brandschutz. Mit den richtigen Detektoren werden alle Erscheinungsformen eines Feuers sofort erfasst.

Videoüberwachung
8MP Bullet Kamera: umfangreiche Funktionen zur Abwehr von Gefahren, Nachtsicht in Farbe, Bewegungserkennung, Wiedergabe von Signaltönen möglich.

Digitales Schließsystem
Digitale Wandleser: Vergabe von individuellen Schließrechten für eine volle Kontrolle über jeden Zugangspunkt; ideal für Eingänge, Tore und Garagen

Digitales Schließsystem
Digitale Wandleser: Vergabe von individuellen Schließrechten für eine volle Kontrolle über jeden Zugangspunkt; ideal für Eingänge, Tore und Garagen

Zutrittskontrolle
Mechanische Zylinder vollständig digitalisiert; individuelle Vergabe von Schließrechten, geegnet für Büro-, Glas- und Eingangstüren

Zufahrtskontrolle
Mithilfe von ANPR Kameras (Kennzeichenerkennung) können anhand von Black- und Whitelisten Tore oder Schranken geöffnet werden.

Einbruchmeldeanlage
Eine EMA erkennt unbefugtes Eindringen in Gebäude in Echtzeit und löst sofort Alarm aus. Alarme können mithilfe von Bewegungs- und Öffnungsmeldern, Außensicherungen und Alarmsirenen und -leuchten ausgelöst werden

Videoüberwachung
PTZ-Kamera: Überwachung des Betriebsgeländes bei Tag und Nacht; Bewegungsverfolgung, gezieltes Zoomen, Fahrzeugerkennung

Unterstützung durch KI und Alarmserver

Technische Infrastruktur bildet das Fundament der Gebäudesicherheit, doch ihre volle Stärke entfaltet sie erst im Zusammenspiel mit klaren organisatorischen Prozessen.

Moderne Bürogebäude stehen vielfältigen Bedrohungen gegenüber: Neben physischem Einbruch und Vandalismus gewinnen Betriebsspionage, Sabotage sowie Elementarschäden wie Feuer oder Wassereinbrüche an Bedeutung. Um diesen Risiken wirksam zu begegnen, müssen betriebliche Sicherheitsrichtlinien dynamisch gelebt werden. Künstliche Intelligenz und dedizierte Alarmserver fungieren hierbei als Bindeglied zwischen technischer Erkennung und menschlicher Handlungsfähigkeit.

Säulen der organisatorischen Gebäuderesilienz

Organisatorische Sicherheit umfasst alle Regeln, Verfahren und Verantwortlichkeiten, die festlegen, wie sich Menschen im Gebäude verhalten und wie im Krisenfall reagiert wird. Dazu gehören unter anderem verbindliche Clear-Desk- und Clear-Screen-Policies zur Unterbindung von Wirtschaftsspionage, strukturierte Besuchermanagement-Prozesse gegen unbefugtes Begleiten sowie detaillierte Notfall- und Wiederanlaufpläne für Elementarereignisse wie Wasserrohrbrüche oder Schwelbrände. Auch regelmäßige Audits und Mitarbeiterschulungen bilden einen unverzichtbaren Bestandteil dieser Schutzstrategie.

Die Praxiserfahrung zeigt allerdings, dass rein organisatorische Vorgaben ohne technologische Unterstützung fehleranfällig bleiben. Menschliche Unachtsamkeit oder Überlastung im Notfall stellen Schwachstellen dar. Hier setzen moderne Softwarelösungen an, indem sie organisatorische Abläufe automatisieren, überwachen und im Ernstfall fehlerfrei durchsteuern.

KI in der Peripherie- und Innenraumüberwachung

Der Einsatz von KI-gestützter Videoanalytik verändert die Überwachung von Bürokomplexen grundlegend. Klassische Bewegungsmelder oder einfache Videokameras lösen bei Witterungseinflüssen, vorbeifahrenden Fahrzeugen oder Lichtreflexen häufig Fehlalarme aus, was zur schnellen Ermüdung des Sicherheitspersonals führt. Auf Deep Learning basierende KI-Modelle sind hingegen in der Lage, präzise zwischen harmlosen Umwelteinflüssen wie einem Eichhörnchen und tatsächlichen Bedrohungen wie einer Drohne zu unterscheiden.

Bei drohendem Einbruch oder Vandalismus erkennt die KI Personen an der Grundstücksgrenze außerhalb der Geschäftszeiten zuverlässig und unterscheidet diese von Tieren oder Passanten. Im Rahmen der Spionageprävention analysieren moderne Kameras an Vereinzelungsschleusen das Durchgangsverhalten und schlagen Alarm, wenn zwei Personen mit nur einem berechtigten Ausweis das Gebäude betreten.

Ebenso identifiziert die Software unbefugtes Verweilen in sensiblen Zonen wie dem Serverraum-Flur. Selbst bei Elementarschäden kann KI deutliche Vorteile bieten, da Spezialkameras Rauch und Flammen optisch erkennen, noch bevor klassische Punktmelder ansprechen, während Thermalkameras Hotspots oder Leckagen frühzeitig identifizieren. Durch diese Vorverarbeitung filtert die KI relevante Ereignisse heraus und entlastet das Leitstandpersonal maßgeblich von der manuellen Sichtung harmloser Zwischenfälle.

Alarmserver als Prozessbeschleuniger

Tritt eine Gefahrensituation ein, reicht die bloße Feststellung des Ereignisses jedoch nicht aus, da der anschließenden Informationsverteilung eine „kriegsentscheidende“ Rolle zukommt. Hier übernimmt der digitale Alarmserver die Funktion einer zentralen Kommunikationsdrehscheibe. Sobald eine Komponente – etwa ein Wassersensor im Rechenzentrum oder ein KI-unterstützter Videokanal – ein kritisches Ereignis meldet, leitet der Server die vordefinierten organisatorischen Maßnahmen ein.

Er kontaktiert die relevanten Personenkreise wie den Sicherheitsdienst, die Gebäudetechnik oder Ersthelfer zeitgleich über verschiedene Kanäle wie Push-Nachrichten, SMS, Sprachanrufe oder Pager. Eine integrierte Quittierungs- und Eskalationslogik stellt sicher, dass keine Zeit verloren geht: Reagiert ein kontaktierter Techniker nicht innerhalb einer festgelegten Frist, leitet der Server die Meldung automatisch an die nächste Vertretungsperson weiter. Zudem erhalten die Empfänger keine kryptischen Fehlercodes, sondern direkt verständliche Klartext-Anweisungen mit genauen Ortsangaben auf ihr Mobilgerät. Diese nahtlose Verbindung aus intelligenter Sensorik und automatisierter Benachrichtigung stellt sicher, dass organisatorische Notfallpläne im Ernstfall innerhalb von Sekunden präzise exekutiert werden.

Fazit: Strategischer Mehrwert durch ganzheitliche Sicherheitskonzepte

Die Modernisierung der Gebäudesicherheit erfordert ein grundlegendes Umdenken in der Unternehmensführung. Sicherheit darf nicht länger als isolierter Kostenfaktor oder reines Pflichtthema der Compliance betrachtet werden. Vielmehr stellt eine integrierte Sicherheitsarchitektur – bestehend aus vernetzter Technik, KI-gestützter Analyse und automatisierten organisatorischen Prozessen – einen strategischen Befähiger für die Resilienz und Zukunftsfähigkeit von Unternehmen dar. Gerade Betriebe, die aufgrund anspruchsvoller regulatorischer Regelungen wie KRITIS und NIS-2 ohnehin zahlreiche Optimierungen vornehmen müssen, ist der Aufbau einer integrierten Sicherheitsarchitektur ein Schritt, der gegangen werden muss.

Für Entscheidungsträger im Management ergeben sich daraus klare Handlungsempfehlungen. Zunächst sollte eine fundierte Bestandsaufnahme der vorhandenen Systeme erfolgen, um bestehende Insellösungen auf ihre Integrationsfähigkeit zu prüfen und bei Neuanschaffungen konsequent auf offene Standards und IP-basierte Schnittstellen zu setzen. Darauf aufbauend gilt es, ganzheitliche Schutzkonzepte zu entwickeln, die physische Sicherheit, Arbeitsschutz und IT-Sicherheit eng miteinander verzahnen. Der Fokussierung auf Automatisierung kommt dabei eine Schlüsselrolle zu: Durch den gezielten Einsatz von KI-Analytik und intelligenten Alarmservern lassen sich Reaktionszeiten minimieren und das eigene Personal spürbar von Routineaufgaben entlasten. Nicht zuletzt müssen die Mitarbeitenden durch kontinuierliche Schulungen eingebunden werden, um eine starke Sicherheitskultur im gesamten Unternehmen zu verankern.

Obwohl die Erstinvestitionen in vernetzte Gefahrenmanagementsysteme, KI-Analytik und moderne Alarminfrastrukturen höher liegen als bei konventionellen Einzellösungen, zahlt sich dieser Ansatz betriebswirtschaftlich rasch aus. Durch extrem kurze Reaktionszeiten bei Bränden, Wassereintritt oder Einbrüchen werden kostspielige Betriebsunterbrechungen vermieden oder drastisch verkürzt, was die Business Continuity sichert. Gleichzeitig sinkt die Zahl teurer Fehlalarme und unnötiger Räumungen. Darüber hinaus honorieren viele Sach- und Betriebsunterbrechungsversicherer nachweisbar integrierte, zertifizierte Sicherheitskonzepte mit Beitragsnachlässen. Hier lohnt es sich nachzufragen. Nicht zuletzt schützt eine zukunftssichere, vernetzte Gebäudeinfrastruktur die Immobilie selbst und steigert deren Marktwert. Investitionen in eine vernetzte und intelligente Gebäudesicherheit schützen somit nicht nur Menschen und Sachwerte, sondern sie sichern direkt auch die Wettbewerbsfähigkeit und Wertschöpfung des gesamten Unternehmens.

Alarmserver-Vorteile

Support im gesamten Ablauf

Organisatorische Prozesse
Regeln, Verantwortlichkeiten, Besucherprozesse und Notfallpläne bilden die Grundlage.

KI-gestützte Erkennung
Empfänger erhalten verständliche Kontext-Hinweise mit Lösungszielen und konkreten Maßnahmen.

Weniger Fehlalarme
KI filtert harmlose Umwelteinflüsse und entlastet das Sicherheitspersonal.

Alarmserver & Eskalation
Meldungen werden automatisch per Push, SMS, Anruf oder Pager verteilt und bei Bedarf eskaliert.

Klare Handlungsanweisungen
Versand von Klartext-Anweisungen mit genauen Ortsangaben auf Mobilgeräte.

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.

Zutrittskontrollen

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

Schließsysteme

- Integration eines digitalen Schließsystems
- Vergeben oder entziehen Sie Schließ-Rechte je nach Person, Uhrzeit oder Tür
- Kopplung des digitalen Systems mit der Alarmanlage 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

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.

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 (z.B. 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

SEC COM

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

www.sec-com.de

Stand: September 2026

2 x in NRW

SEC-COM Sicherheits- und Kommunikationstechnik GmbH

Bochumer Str. 6
45661 Recklinghausen
Fon: 0 23 61 / 93 22-0

Karl-Schurz-Straße 32
33100 Paderborn
Fon: 0 52 51 / 8 74 98-0