WHITEPAPER

Kritische Infrastrukturen (KRITIS) und NIS-2-Umsetzung

Ein Unternehmen der GU-Gruppe

Zukunftsorientierte Schließsysteme

Die Marke BKS
Sicherheit hat einen Namen, genauer gesagt ist sie eine Marke. Die BKS GmbH – ein Mitglied der Unternehmensgruppe Gretsch-Unitas. Mehr als ein Jahrhundert Erfahrung in der Herstellung von hochwertigen Schließsystemen. Seit der Entwicklung des Rundzylinders im Jahr 1938 ist die BKS GmbH bis heute eines der führenden Unternehmen rund um das Thema Schließtechnologie und Sicherheit.

Öffnen und Schließen
Schließsysteme von BKS bieten individuelle und maßgeschneiderte Lösungen und werden nach höchsten Qualitätsstandards angefertigt. Mit der Wahl einer BKS-Anlage entscheiden Sie sich für höchst moderne Schließsysteme mit unterschiedlichsten Ausstattungen und Funktionalitäten.
Sie eröffnen flexible Gestaltungsmöglichkeiten auch für nachträgliche Erweiterungen.

Vielfältige Lösungen
Schließsysteme von BKS bieten vielfältige Lösungen zur Absicherung einzelner Türen und zur Planung moderner Schließanlagen. Komfort und Sicherheit lassen sich durch die Kombination von mechanischen und elektronischen Schließsystemen individuell gestalten und wirtschaftlich realisieren.

Perfektes Zusammenspiel
Die hohe Qualität der mechanischen, mechatronischen und elektronischen Zylinder wird ergänzt von einem umfassenden Serviceangebot, das Planung, Verwaltung und Nachbestellung von Schlüsseln und Zylindern beinhaltet.

Inhaltsverzeichnis

Herausgeber
Gretsch-Unitas GmbH Baubeschläge I Johann-Maus-Str. 3 I D-71254 Ditzingen
Tel. + 49 (0) 71 56 3 01-0 I Fax + 49 (0) 71 56 3 01-2 93

Foto: Adobe Stock | vegefox.com

Die aktuell beherrschenden Wörter in jeder Branche

Europaweit und global vernetzte Prozesse sowie die zunehmende Digitalisierung aller Lebens- und Wirtschaftsbereiche führen zu einer höheren Anfälligkeit gegenüber externen, oft nicht steuerbaren Faktoren. Diese Entwicklung hat die Cyberbedrohungslage verschärft und neue Herausforderungen geschaffen, die in allen EU-Mitgliedstaaten koordinierte und innovative Reaktionen erfordern.
Die Anzahl, Tragweite, Komplexität, Häufigkeit und Auswirkungen von Vorfällen nehmen zu und stellen eine erhebliche Bedrohung für den störungsfreien Betrieb von Unternehmen und Einrichtungen dar.

Die im Jahr 2023 in Kraft getretene EU NIS-2-Richtlinie (vormals NIS-Richtlinie von 2016) legt in der Europäischen Union die Cybersecurity-Mindeststandards fest.
Zielsetzung ist, die Resilienz und die Cybersicherheitsmaßnahmen in den kritischen Sektoren (KRITIS-Sektoren) zu stärken.

AKTUELL BEHERRSCHENDE WÖRTER

- Kritische Infrastrukturen (KRITIS)
- Umsetzung der EU NIS-2-Richtlinie
- BSI-Kritisverordnung (BSI-KritisV)
- NIS-2-Umsetzungs- und Cybersicherheits-stärkungsgesetz (NIS-2UmsuCG)
- KRITIS-Dachgesetz (KRITIS-DachG)

Resilienz (Widerstandsfähigkeit) bezieht sich im Allgemeinen auf die Fähigkeit, sich vor Störungen, Angriffen oder anderen unerwarteten Ereignissen zu schützen, zu reagieren, sich zu erholen, ohne dass dauerhafte Beeinträchtigungen eintreten, und sich an veränderte Bedingungen anzupassen.

Im Mittelpunkt stehen dabei sowohl die Sicherheitsvorfälle in den Netz- oder Informationssystemen als auch die physische Sicherheit der Infrastruktur dieser Systeme sowie die Personalsicherheit.

Man kann diese in wenigen Punkten zusammenfassen

- Anwendungsbereiche – Definition
- Risikomanagement mit technischen und organisatorischen Sicherheitsmaßnahmen für die Verfügbarkeit von Infrastrukturen
- Sicherheitsvorfall-Management – Erkennung, Überwachung und Reaktion
- Meldepflichten von Sicherheitsvorfällen
- Notfall- und Wiederherstellungsmaßnahmen
- Sicherheitsaudits, Überprüfung der Sicherheitsstandards, Dokumentation
- Schulungen: Sensibilisierung und Förderung einer Sicherheitskultur

Die Umsetzung von NIS-2 wird in Deutschland knapp 30 000 Unternehmen betreffen. Sind Sie als Betreiber, ist Ihr Unternehmen bzw. sind Ihre Einrichtungen davon betroffen?

1.) Anwendungsbereiche – Definition:
Zu den Fragen der Definition der „Anwendungsbereiche“ und „Was sind kritische Infrastrukturen?“ geben Ihnen die Antworten das BSI-Gesetz (BSIG) und die BSI-Kritisverordnung (BSI-KritisV) mit der Festlegung der acht KRITIS-Sektoren. Zudem erfolgt die Definition der Einrichtungen durch das im Jahr 2025 kommende NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS-2UmsuCG).

Damit werden Unternehmen als Betreiber und als Einrichtung(en) in drei Kategorien eingestuft:
- **Betreiber kritischer Anlagen (KRITIS-Betreiber)**
- **Besonders wichtige Einrichtungen**
- **Wichtige Einrichtungen**

Zusätzlich wird das im Jahr 2026 erwartete KRITIS-Dachgesetz (KRITIS-DachG) die Resilienz und vor allem die physische Sicherheit von kritischen Infrastrukturen in Deutschland stärken und regulieren.

Betreiber kritischer Anlagen (KRITIS-Betreiber)

Hierzu zählt Ihr Unternehmen, wenn Sie ein Betreiber einer „kritischen Infrastruktur“ sind, und Einrichtungen, Anlagen oder Teile aus folgenden Sektoren (KRITIS-Sektoren):

- Energie
- Informationstechnik und Telekommunikation
- Transport und Verkehr
- Gesundheit
- Wasser
- Ernährung
- Finanz- und Versicherungswesen
- Siedlungsabfallentsorgung

angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Neben dem Regelschwellenwert von 500 000 zu versorgenden Einwohnern können auch weitere quantitative und qualitative Kriterien einbezogen werden.

Das bedeutet für Ihr Unternehmen: Als Betreiber ergeben sich folgende Sicherheitsmaßnahmen aus dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS-2UmsuCG):

- IT-Sicherheit
- Meldepflicht und
- Systeme zur Angriffserkennung

KRITIS-Dachgesetz (KRITIS-DachG):

Resilienz

Klassifizierungen	Einrichtungen	Schwellwerte
Betreiber kritischer Anlagen (KRITIS-Betreiber)	• Energie • Informationstechnik und Telekommunikation • Transport und Verkehr • Gesundheit • Wasser • Ernährung • Finanz- und Versicherungswesen • Siedlungsabfallentsorgung	Jemand, der kritische Dienstleistungen zur Versorgung der Allgemeinheit erbringt. Zu versorgende Einwohner: ≥ 500 000
Besonders wichtige Einrichtungen (NIS-2-Unternehmen)	• Energie • Transport und Verkehr • Finanzwesen • Gesundheit • Wasser • Digitale Infrastrukturen • Weltraum	Beschäftigte: ≥ 250 oder Umsatz: > 50 Mio. € Bilanz: > 43 Mio. €
	• Öffentlich zugängliche TK-Dienste • Öffentliche TK-Netze	Beschäftigte: ≥ 50 oder Umsatz: > 10 Mio. € Bilanz: > 10 Mio. €
	• Qualifizierte Vertrauensdiensteanbieter • Top Level Domain Name Registries • DNS-Diensteanbieter	Ohne Schwellwerte
Wichtige Einrichtungen (NIS-2-Unternehmen)	• Energie • Transport und Verkehr • Finanzwesen • Gesundheit • Wasser • Digitale Infrastrukturen • Weltraum • Post- und Kurierdienste • Abfallbewirtschaftung • Produktion, Herstellung und Handel mit chemischen Stoffen • Produktion, Verarbeitung und Vertrieb von Lebensmitteln • Verarbeitendes Gewerbe/Herstellung von Waren • Anbieter digitaler Dienste • Forschung	Beschäftigte: ≥ 50 oder Umsatz: > 10 Mio. € Bilanz: > 10 Mio. €
	• Öffentlich zugängliche TK-Dienste • Öffentliche TK-Netze	Beschäftigte: < 50 und Umsatz: ≤ 10 Mio. € Bilanz: ≤ 10 Mio. €
	• Nicht qualifizierte Vertrauensdiensteanbieter	Ohne Schwellwerte

Besonders wichtige Einrichtungen

Zu diesen zählt Ihr Unternehmen bzw. Ihr(e) Einrichtung(en) mit mind. 250 Mitarbeitenden oder einem Jahresumsatz › 50 Mio. € und einer Jahresbilanzsumme › 43 Mio. €, wenn Sie Waren oder Dienstleistungen anbieten und folgenden Sektoren angehören:

- Energie (Stromversorgung, Fernwärmeversorgung oder Fernkälteversorgung, Kraftstoff- und Heizölversorgung, Gasversorgung)
- Transport und Verkehr (Luft-, Schienen-, Straßenverkehr, Schifffahrt)
- Finanzwesen (Bankwesen, Finanzmarktinfrastrukturen)
- Gesundheit (Gesundheitsdienstleister, EU-Referenzlabore, Arzneimittelforschung/-entwicklung, Pharmazeutik, Medizinprodukte)
- Wasser (Trinkwasserversorgung, Abwasserbeseitigung)
- Digitale Infrastrukturen (Internet Exchange Points, Cloud-Computing-Dienste, Rechenzentrumsdienste, Content Delivery Networks, Managed Services Provider, Managed Security Services Provider)
- Weltraum (Bodeninfrastruktur für weltraumgestützte Dienste)

Gleichfalls mit mind. 50 Mitarbeitenden oder einem Jahresumsatz
› 10 Mio. € und einer Jahresbilanzsumme › 10 Mio. €

- öffentlich zugängliche TK-Dienste, öffentliche TK-Netze

Ebenso unabhängig von Mitarbeitenden, Jahresumsatz/ Jahresbilanzsumme:

- qualifizierte Vertrauensdiensteanbieter, Top Level Domain Name Registries oder DNS-Diensteanbieter

Somit ergeben sich für Ihr Unternehmen als Einrichtung folgende Sicherheitsmaßnahmen aus dem:

NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS-2UmsuCG):

- IT-Sicherheit
- Meldepflicht

Wichtige Einrichtungen

Ihr Unternehmen bzw. Ihr(e) Einrichtung(en) mit mind. 50 Mitarbeitenden oder einem Jahresumsatz › 10 Mio. € und einer Jahresbilanzsumme › 10 Mio. € gehört dazu, wenn Sie Waren oder Dienstleistungen anbieten und folgenden Sektoren angehören:

- Energie (Stromversorgung, Fernwärmeversorgung oder Fernkälteversorgung, Kraftstoff- und Heizölversorgung, Gasversorgung)
- Transport und Verkehr (Luft-, Schienen-, Straßenverkehr, Schifffahrt)
- Finanzwesen (Bankwesen, Finanzmarktinfrastrukturen)
- Gesundheit (Gesundheitsdienstleister, EU-Referenzlabore, Arzneimittelforschung und -entwicklung, Pharmazeutik, Medizinprodukte)
- Wasser (Trinkwasserversorgung, Abwasserbeseitigung)
- Digitale Infrastrukturen (Internet Exchange Points, Cloud-Computing-Dienste, Rechenzentrumsdienste, Content Delivery Networks, Managed Services Provider, Managed Security Services Provider)
- Weltraum (Bodeninfrastruktur für weltraumgestützte Dienste)
- Post- und Kurierdienste
- Abfallbewirtschaftung
- Produktion, Herstellung und Handel mit chemischen Stoffen
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln
- Verarbeitendes Gewerbe/Herstellung von Waren (Medizinprodukte, In-vitro-Diagnostika, DV-Geräte, elektronische u. optische Erzeugnisse, elektrisch Ausrüstungen, Maschinenbau, Kraftwagen und Kraftwagenteile, Fahrzeugbau)
- Anbieter digitaler Dienste (Online-Marktplätze, Online-Suchmaschinen, Plattformen für Dienste sozialer Netzwerke)
- Forschung (Forschungseinrichtungen, aber keine Bildungseinrichtungen)

Genauso mit weniger als 50 Mitarbeitenden und einem Jahresumsatz ≤ 10 Mio. € und einer Jahresbilanzsumme ≤ 10 Mio. €

- öffentlich zugängliche TK-Dienste, öffentliche TK-Netze

Ebenso unabhängig von Mitarbeitenden, Jahresumsatz/ Jahresbilanzsumme:

- nicht qualifizierter Vertrauensdiensteanbieter

Das bedeutet für Ihr Unternehmen als Einrichtung(en) ergeben sich folgende Sicherheitsmaßnahmen aus dem:

- NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS-2UmsuCG):
- IT-Sicherheit
- Meldepflicht

Durch die Integration physischer Sicherheitsmaßnahmen in die Cybersicherheitsstrategie im Rahmen der NIS-2-Richtlinie können Unternehmen ihre gesamte Sicherheitslage verbessern und widerstandsfähiger gegen eine Vielzahl von Bedrohungen werden.

> *Die erhöhten Anforderungen aus dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (IT-Sicherheit, Meldepflicht) und aus dem KRITIS-Dachgesetz (Resilienz) haben auch Einfluss auf die Anforderungen zur Sicherheit der physischen Infrastruktur.*

Die Stimme eines Sicherheitsberaters:
„IT-Sicherheit beginnt nicht ab der Tür eines Serverraumes oder ist die Verantwortung des Cloud-Anbieters. Die physische Sicherheit, deren Verfügbarkeit und auch Resilienz beruhen auf den Risikobewertungen, dem Einsatz zukunftsfähiger Lösungen, der Umsetzung, der Einhaltung, der Überprüfung und Anpassung, der Meldepflicht bis zur ständigen Weiterbildung.
Zusätzlich wird in vielen Unternehmen oft unterschätzt, wie schnell ‚interne' Anomalien in einem Gebäude oder einer Liegenschaft durch die Vielzahl der integrierten Systeme zu einer Kette von Ereignissen führen können. Diese Ereignisse können schließlich Sicherheitsvorfälle und Schäden verursachen, die erhebliche zeitliche und wirtschaftliche Beeinträchtigungen sowie Ausfälle zur Folge haben. Der Grund ist simpel: ‚Man hatte es einfach nicht auf dem Schirm!' Ein Beispiel: Der Ausfall der Klimatisierung der USV-Steuerung, die man für nicht so wichtig erachtet, wird somit erst am nächsten Werktag bzw. noch später behoben.
Treten zufälligerweise während dieser Ausfallzeit weitere Probleme (Faktoren) auf wie beispielsweise eine Störung beim lokalen Stromversorgungsunternehmen führt das dazu, dass die Netzersatzanlage (Notstromdiesel) sich aktivieren ‚möchte'. Doch bevor dies geschieht, fällt zuvor die Unterbrechungsfreie Stromversorgung (USV) vollständig aufgrund der überhitzten Steuerung aus. Infolgedessen steht der gesamte Betrieb für eine lange Zeit still."

Risikomanagement mit technischen und organisatorischen Sicherheitsmaßnahmen für die Verfügbarkeit von Infrastrukturen

GEMOS, ein Gebäudemanagement- und Organisationssystem, ist mehr als nur eine technische Maßnahme zum Bündeln von Informationen.
Es organisiert die zentrale Überwachung, Verarbeitung und Visualisierung der umfangreichen Sicherheitsinformationen aus verschiedenen Branchen in ein unabhängiges Risikomanagementsystem.
Durch GEMOS erfolgt die herstellerneutrale Zusammenführung und Integration (Meldungen und Anweisungen) von verschiedenen physischen Sicherheits- und Informationssystemen (GEMOS-Schnittstellen), hier einige Beispiele:

- Brandmelde- und Löschanlagensysteme
- Videomanagementsysteme
- Einbruchmelde- und Überfallsysteme
- Perimetersysteme
- Fluchttürsteuerungssysteme
- Alarmempfangssysteme
- Übertragungssysteme
- Kommunikationssysteme
- Personen-Notsignal-Systeme
- Sprachalarmierungssysteme
- Schlüsselverwaltungssysteme
- Gebäudeautomationssysteme und technische Systeme (z. B. IT-Systeme) über Standard-Protokolle wie BACnet, DALI, EIB/KNX, ESPA, Modbus, OPC, SNMP

Mit einem GEMOS access (Zutrittskontrollsystem) erhalten Sie zusätzlich ein wesentliches Sicherheitssystemelement der NIS-2-Anforderungen, die Ihnen zentral und schnell alle Sicherheitsinformationen zu Ihren Zutrittspunkten (WER-WANN-WO/WOHIN) erlaubt.

› Wir unterstützen Sie bei der Verfügbarkeit von Infrastrukturen mit unseren Produkten:

- GEMOS (Gebäudemanagementsystem)
- GEMOS access (Zutrittskontrollsystem)

Sicherheitsvorfall-Management – Erkennung, Überwachung und Reaktion

Mit einem GEMOS werden sämtliche Sicherheitsinformationen und -ereignisse wie (wie Störungen, Alarme und andere Zustände) aller integrierten physischen Sicherheits- und Informationssysteme (GEMOS-Schnittstellen) überwacht, erkannt und dabei transparent und übersichtlich dargestellt.
Durch die zentrale Verwaltung können Sie mit GEMOS jederzeit auf Sicherheitsvorfälle direkt reagieren. Hier einige Beispiele:

- **Videomanagementsysteme und ihre Kameras:**
Mithilfe der Analysefunktionen dieser Systeme können Sicherheitsvorfälle sofort per Live-Bild erkannt werden. Für eine automatische bzw. manuell durch den Bediener gesteuerte Überwachung kann GEMOS unverzüglich die Pan-Tilt-Zoom-Steuerung (PTZ) der Alarmkameras, das Zuschalten von Live-Bildern der Umfeldkameras, das Starten von Aufzeichnungen und damit das Erstellen von Archiv-Bildern auslösen. In Reaktion auf erkannte Vorfälle können zusätzlich die Interventionskräfte gezielt über die Kommunikationssysteme eingesetzt werden. Darüber hinaus ermöglicht GEMOS die Verknüpfung von Alarmen, Störungen oder Info-Meldungen anderer physischer Sicherheits- und Informationssysteme mit den dazugehörigen Alarmbild-Aufschaltungen.

- **Einbruchmelde- und Perimetersysteme und ihre Sensoren und Detektoren:**
Diese Systeme verhindern unbefugten Zugriff sowie physische Sicherheitsverletzungen und erkennen solche Ereignisse gleichzeitig, wenn sie auftreten. Mit der Verbindung von Videoüberwachungskameras und deren Integration im GEMOS werden die Überwachung und die Reaktionsfähigkeit auf Sicherheitsvorfälle deutlich verbessert. Dazu gehört auch die visuelle Darstellung der Scharf- und Unscharf-Schaltungen von Bereichen und Unterbereichen im Lageplan, insbesondere im Alarmfall. Ebenso wird die dokumentierte Überwachung von Ein- und Abschaltung von Sensoren und Detektoren ermöglicht.

- **Brandmelde- und Löschanlagensysteme und ihre Melder:**
Diese Systeme erkennen Brandschäden frühzeitig, verhindern deren Ausbreitung und minimieren so potenzielle Schäden. Durch die Einbindung im GEMOS werden gezielte Interventionsmaßnahmen, die Alarmierung von Einsatzkräften, die automatische Bereitstellung von Feuerwehrlaufkarten und die eventuelle Ansteuerung von Schlüsselverwaltungssystemen optimal koordiniert, um effizient auf Sicherheitsvorfälle reagieren zu können. Zusätzlich kann die zeitgesteuerte und manuelle Durchführung von Ab- und Einschaltvorgängen ermöglicht werden, einschließlich der Angabe der Notwendigkeit und der Verifikation durch den Bediener.

- **Übertragungssysteme und Alarmempfangssysteme:**
Die Übertragung von Meldungen wie Alarm, Sabotage, Überfall, Störung, Scharf- und Unscharf-Schaltung sowie Wartungs- und Info-Meldungen aus externen Einrichtungen und deren Gefahrenmeldeanlagen über Kommunikationsnetze bildet einen zentralen Punkt für Alarmempfangssysteme. Mit GEMOS können die auslösenden Objekte visuell im Lageplan dargestellt und durch hinterlegte Interventionsmaßnahmen gezielt gesteuert werden. Dabei sind zeitabhängige und kategorienbezogene Maßnahmen möglich, die eine schnelle und effektive Reaktion auf Sicherheitsvorfälle gewährleisten.

- **Personen-Notsignal-Systeme und Überfallmeldesysteme:**
Neben dem physischen Schutz kritischer Infrastrukturen sind der Schutz und die Sicherheit des Personals wesentliche Bestandteile der NIS-2-Richtlinie, insbesondere in Bezug auf physische und sicherheitsbezogene Bedrohungen. Die Überwachung automatischer Notrufauslösungen durch Bewegungs- oder Lagesensoren sowie manueller Notrufauslösungen durch Überfallknöpfe oder mobile Alarmgeräte ermöglicht eine schnelle Erkennung von Sicherheitsvorfällen. In Verbindung mit GEMOS können Lokalisierungsfunktionen zur Darstellung im Lageplan sowie gezielte Reaktionen zur Intervention effektiv umgesetzt werden.

- **Gebäudeautomationssysteme und technische Systeme:**
Die Zustände dieser Systeme und Anlagen wie Temperatur, Druck, Drehzahl, Geschwindigkeit, Füllstand, Zählerstand sowie Klappen- und Ventilstellungen werden im GEMOS überwacht. Diese Informationen können z. B. als Alarm-, Voralarm-, Störungs-, Wartungs- oder Info-Meldungen kategorisiert werden. Mit der Visualisierung als Digital- oder Analogwert im Lageplan, mit der Festlegung von mehreren Schwellwert-Bereichen inklusive deren

Foto: Adobe Stock | JK_kyoto

grafischer Darstellung ermöglicht GEMOS eine präzise Erkennung und Überwachung, sodass rechtzeitig auf kritische Ereignisse reagiert werden kann.

- **Kommunikationssysteme:**
Sie ermöglichen einen nahtlosen Informationsaustausch bei der Erkennung und Überwachung von Vorfällen. In Verbindung mit GEMOS wird auf diese Weise eine effektive, schnelle und koordinierte Reaktion auf Sicherheitsvorfälle gewährleistet. Durch die zusätzliche Integration von Videoüberwachungskameras und anderen physischen Sicherheitssystemen wird eine umfassendere und genauere Lagebilddarstellung erreicht.

- **GEMOS access (Zutrittskontrollsystem):**
Während physische Barrieren wie Zäune, Sperren und Sicherheitsschleusen den unbefugten Zutritt verhindern können, übernimmt ein Zutrittskontrollsystem die Überwachung und Steuerung des Zugangs zu kritischen Infrastrukturen. Dieses System ermöglicht die Beschränkung auf autorisiertes Personal durch die Definition von Bereichs- und Zeitzonen, die Abbildung von Zugangsrechten und den Einsatz von Sicherheitsausweisen (wie RFID-Transpondern und -Karten, NFC-Medien), PIN-Codes und biometrischen Scannern. Mit den „Dynamischen Rechten“ lassen sich weitere typische Funktionen eines Zutrittskontrollsystems umsetzen, darunter Taschenkontrolle, Zutrittswiederholsperre (Anti-Passback), Bereichswechsel-kontrolle, Bilanzierung, Mehrpersonenanwesenheitskontrolle und zeitliche Sperre nach Mehrfachfehlversuchen mit Zwei-Faktor-Authentifizierung. Durch die Integration in GEMOS und die Verknüpfung mit Videoüberwachungskameras sowie die Möglichkeit, Lockdown-Szenarien zu aktivieren, wird die Reaktionsfähigkeit bei Sicherheitsvorfällen erheblich gesteigert. Das ermöglicht eine direkte Steuerung von Sicherheitsschleusen, Personenvereinzelungssystemen, Dreh- und Karusselltüren sowie Zugangstoren.

Meldepflichten von Sicherheitsvorfällen

Wir unterstützen Sie im GEMOS access (Zutrittskontrollsystem) bei der Erfüllung von Meldepflichten zu Sicherheitsvorfällen durch umfassende und detaillierte Aufzeichnungen aller Zutrittsversuche und -ereignisse. Darüber hinaus ermöglicht das System die Protokollierung von Änderungshistorien und Anwesenheitslisten, die für spätere Überprüfungen und Analysen ausgewertet werden können.
Im GEMOS (Gebäudemanagementsystem) werden umfangreiche Meldungs- und Aktionsprotokolle bereitgestellt, um Meldepflichten bei Sicherheitsvorfällen zu erfüllen. Über die GEMOS-Maßnahmenplanverarbeitung können individuelle Überwachungen von integrierten physischen Sicherheits- und Informationssystemen (GEMOS-Schnittstellen) gezielt eingerichtet, konfiguriert und bei Bedarf angepasst werden.

Zusätzlich stehen System- und Sicherheitsüberwachungsprotokolle von GEMOS selbst und den integrierten physischen Sicherheits- und Informationssystemen (GEMOS-Schnittstellen) zur Verfügung. Diese Werkzeuge ermöglichen es, schnell und gezielt auf ungewöhnliche und unerwartete Systemereignisse sowie auf verdächtige Aktivitäten im Bereich der Systemsicherheit zu reagieren.

Dadurch stehen Ihnen, dem autorisierten GEMOS-Bediener, die umfangreichen Instrumente (Berichte) für die Meldepflicht bei Sicherheitsvorfällen zur Verfügung.

Sicherheitsvorfall:

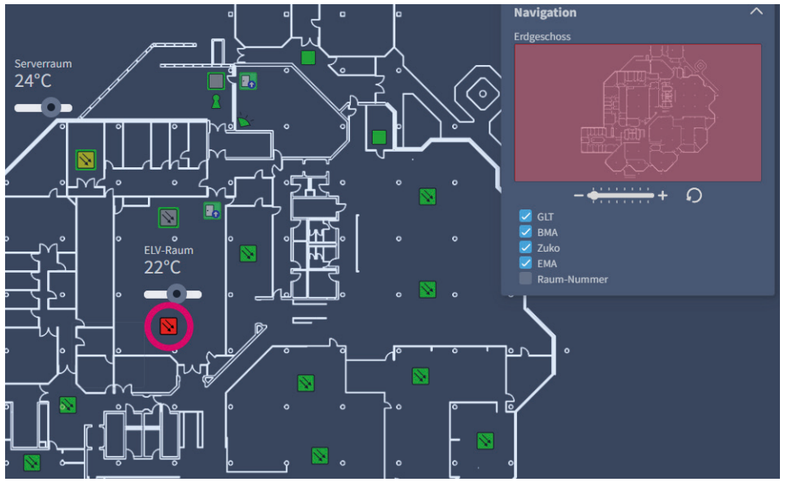
(Auszug aus NIS-2UmsuCG, Begriffsbestimmungen)

Ein „erheblicher Sicherheitsvorfall“ ist ein Sicherheitsvorfall, der
a) schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder
b) andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

GEMOS bietet Ihnen eine ganzheitliche Sicht (WAS-WANN-WO) auf alle Sicherheitsereignisse. Das erhöht die Effizienz bei der Überwachung, Erkennung und Reaktion auf Sicherheitsvorfälle erheblich.

Darüber hinaus bieten Ihnen die zahlreichen GEMOS-Module erweiterte Möglichkeiten, um Ihre individuellen Sicherheitsanforderungen optimal zu erfüllen.

GEMOS ermöglicht ein zentralisiertes Risikomanagementsystem.



Notfall- und Wiederherstellungsmaßnahmen

Neben den normalen Back-up-Möglichkeiten in einem GEMOS-System stehen die Ausfallsicherheit und die umgehende Wiederherstellung im Vordergrund.
GEMOS – ENTERPRISE ONE SERVER dient optional als Grundlage der sicherheitstechnischen Ausfallsicherheit eines GEMOS-Systems, indem es zum Beispiel mit zwei GEMOS-Servern im Hot-Stand-by-Modus betrieben wird. Durch die permanente Überwachung wird der Server-Ausfall bzw. der Ausfall der Netzwerk-Kommunikation zum ersten GEMOS-Server erkannt und es wird automatisch dabei auf den zweiten GEMOS-Server umgeschaltet.
Bei einem Ausfall eines einzelnen Servers kommt es zu keinen Einschränkungen und keinem Meldungsverlust im GEMOS-System. Ebenfalls werden die Wiederherstellung des Normalbetriebs (Datenbankabgleich zwischen den GEMOS-Servern) und die Reaktivierung des ersten GEMOS-Servers unterstützt.

Mit dem GEMOS – ENTERPRISE ONE SERVER werden folgende Grundfunktionen sichergestellt:

Echtzeitdaten-Redundanz:
- Meldungszustände
- Befehle/Anweisungen
- Alarmstapel
- Meldungsprotokoll

Stammdaten-Replikation:
- Datenbanken
- Dateien

Wir empfehlen für den Anspruch der Hochverfügbarkeit eines GEMOS 5 Systems im Sinn der Sicherheitsstufe „Funktion muss jederzeit aufrechterhalten werden, 24/7-Betrieb (24 Stunden, 7 Tage die Woche)“ eine räumliche Trennung der GEMOS-Server.
Das GEMOS-System kann aus physikalischer GEMOS-Server-Hardware und/oder einer virtualisierten GEMOS-Server-Umgebung bestehen.
Notfall- und Wiederherstellungsmaßnahmen sind mehr als nur ein System-Backup, wir bieten und integrieren Lösungen.

Sicherheitsaudits, Überprüfung der Sicherheitsstandards, Dokumentation

GEMOS:
- GEMOS Sicherheit – konfigurierte Kryptologie TLS 1.3 - AES-256 nach BSI
- Plattform-unabhängig (inklusive Verwaltung und Speicherung von importierten oder erzeugten Zertifikaten und den dazugehörigen privaten Schlüsseln) – der Einsatz von Betriebssystemen wie Windows oder Linux auf Servern und Arbeitsplätzen ist möglich.
- Webbasierte Benutzer- und Bedienoberfläche – grundsätzlich sind keine Installationen, Pflege von Client-Software, zusätzlichen Laufzeitumgebungen auf den Arbeitsplätzen notwendig.
- Alle Datenbanken befinden sich und bleiben auf dem GEMOS-Server, es befinden sich keine Datenbanken (bzw. Teile davon) auf den Arbeitsplätzen.

GEMOS – ENTERPRISE ONE SERVER:
- Der Austausch der Echtzeitdaten (Meldungszustände, Befehle/Anweisungen, Alarmstapel, Meldungsprotokoll) zwischen den GEMOS-Servern erfolgt sicher über die konfigurierte Einstellung (BSI-konform) per TLS 1.3 - AES-256 Verschlüsselung.
- Der kontinuierliche, automatische und überwachte Datenabgleich über die Stammdaten-Replikation (Datenbanken und Dateien) zwischen den GEMOS-Servern findet sicher mittels konfigurierter Einstellung (BSI-konform) per TLS 1.3 - AES-256 Verschlüsselung statt.
- Server-Unabhängigkeit – durch die modularen GEMOS-Schnittstellen zu den physischen Sicherheits- und Informationssystemen
- Rechte- u. Rollenkonzept – anhand der granularen GEMOS-Systemarchitektur
- Benutzer-Authentifizierung – umfangreiche Unterstützung von Sicherheitseinstellungen (Passwort-Länge/-Gültigkeit/-Komplexität, Unterstützung für 2-Faktor-Authentifizierung mittels WebAuthn-Standard von FIDO2/U2F, aber auch Unterstützung für Time-based One Time Password und Hash-Based-One-Time-Password)
- Zentrale Steuerung über den GEMOS-Server (Installation, Konfiguration, Update von GEMOS-Schnittstellen und GEMOS-Modulen)

GEMOS access:
- Browserbasiert keine Installation von Software auf den Arbeitsplätzen
- Flexible Konfiguration durch Abstraktion der Zutrittsrechte von der Raumstruktur (Verwaltung von Raumzonen und Lesergruppen)
- Verschlüsselte Datenübertragung (bei entsprechender Leser-Hardware von der Karte/Kartenleser bis zum Datenverkehr der Buskommunikation – Busverschlüsselung)

Schulungen – Sensibilisierung und Förderung einer Sicherheitskultur

	Schulungen für
GEMOS Academy	• Vertrieb/Planer • Technischer Vertrieb/Kundenberater • Errichter • Anwender/Bediener • Individualschulung

So stehen umfassende Seminare und Schulungen nach dem Bedürfnis der Teilnehmer zur Verfügung. Zum Erfolg führen Sie dabei unsere kompetenten Produkttrainer mit jahrelanger Praxiserfahrung. Die Seminare und Schulungen werden in Deutsch oder in Englisch durchgeführt als:
- ortsunabhängige Online-Schulungen
- BKS hauseigene Schulungseinrichtungen in Berlin und Offenbach a. M.
- vor Ort-Schulungen (bestimmte Schulungsinhalte bedürfen einer vorab abgesprochenen und vorhandenen Infrastruktur)

Foto: Adobe Stock | Dinusha

Wir schaffen Lösungen

Die Implementierung eines GEMOS (Gebäudemanagementsystem) und eines GEMOS access (Zutrittskontrollsystem) im Kontext der NIS-2-Richtlinie bietet eine Vielzahl von Vorteilen, insbesondere für Unternehmen, die ihre IT- und physische Sicherheitsinfrastruktur optimieren müssen oder wollen. Die spezifischen Vorteile:

- **Integration von Sicherheitsdaten**
  GEMOS bietet die Möglichkeit, Sicherheitsdaten aus verschiedenen Quellen, sowohl physisch als auch digital, zu integrieren. Dies ermöglicht eine umfassende Sicht auf die gesamte Sicherheitslandschaft eines Unternehmens.

- **Zentralisierte Verwaltung und Kontrolle**
  Mit GEMOS können alle Sicherheitsmaßnahmen zentral verwaltet und überwacht werden. Dieses zentrale Risikomanagement ist entscheidend, um die Koordination bei Sicherheitsvorfällen zu verbessern und eine schnelle sowie effektive Reaktion zu gewährleisten.

- **Automatisierung von Sicherheitsprozessen**
  GEMOS ermöglicht die Automatisierung vieler Sicherheitsprozesse, einschließlich Alarmmanagement und Eskalationen. Dies reduziert die Notwendigkeit manueller Eingriffe und erhöht die Effizienz, was dazu beiträgt, die kontinuierliche Überwachung und Reaktionsfähigkeit zu verbessern.

- **Erhöhte Reaktionsgeschwindigkeit**
  Durch die Integration und Analyse von Sicherheitsdaten kann GEMOS die Reaktionsgeschwindigkeit bei Sicherheitsvorfällen signifikant erhöhen, um die Auswirkungen von Sicherheitsvorfällen zu reduzieren und den Schutz der kritischen Infrastrukturen zu gewährleisten.

- **Umfassende Risikoanalyse und -bewertung**
  GEMOS bietet fortschrittliche Werkzeuge zur Durchführung von Risikoanalysen und Bewertungen. Das hilft Unternehmen, potenzielle Schwachstellen in ihrer Infrastruktur zu identifizieren und geeignete Maßnahmen zur Risikominimierung zu entwickeln.

- **Einhaltung gesetzlicher Anforderungen**
  Durch die Unterstützung bei der Überwachung, Erkennung und Meldung von Sicherheitsvorfällen hilft GEMOS Unternehmen, die Compliance-Anforderungen zu erfüllen. Das beinhaltet die Dokumentation von Vorfällen und die Berichterstattung an die zuständigen Behörden.

GEMOS

Kontakt

GEMOS und GEMOS access Vertriebskontakt
Sie sind auf der Suche nach einem
kompetenten GEMOS-Ansprechpartner?
Schreiben Sie uns – wir helfen gerne weiter.
info@bks.de

https://www.g-u.com/de/DE/kontakt/kontaktformular-gemos.html

Unsere GEMOS-Schnittstellen, schauen Sie vorbei:

https://www.g-u.com/de/DE/produkte/
gebaeudemanagementsysteme/gemos/schnittstellen.html

Quellen:
- EU NIS-2-Richtlinie
- EU RCE Directive bzw. (Critical Entities Resilience Directive) CER-Richtlinie
- BSI-Gesetz (BSIG)
- Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV)
- NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS-2UmsuCG) - (Entwurf für das Bundeskabinett von Juli 2024)
- KRITIS-Dachgesetz (KRITIS-DachG) - kritische Betreiber mit Resilienz (zweiter Referentenentwurf 2023)
- openkritis.de

Gretsch-Unitas GmbH
Baubeschläge
Johann-Maus-Str. 3
D-71254 Ditzingen
Tel. +49 7156 301-0
Fax +49 7156 301-77980

BKS GmbH
Heidestr. 71
D-42549 Velbert
Tel. +49 2051 201-0
Fax +49 2051 201-9733

Gretsch-Unitas AG
Industriestr. 12
CH-3422 Rüdtligen
Tel. +41 34 44845-45
Fax +41 34 44562-49

GU Baubeschläge Austria GmbH
Mayrwiesstr. 8
A-5300 Hallwang
Tel. +43 662 664830
Fax +43 662 664830-301

www.g-u.com

10/2024 Printed in Germany

Vorsprung mit System