Das KRITIS-Dachgesetz und seine Umsetzung

Höchste Sicherheit für kritische Infrastrukturen

Kritische Infrastrukturen (KRITIS) stellen die Versorgung der Bevölkerung sicher. Sabotage ihrer Einrichtungen oder Anschläge darauf können weitreichende Folgen haben und wegen der Verzahnung verschiedener Sektoren fatale Kettenreaktionen in Gang setzen. Zudem nehmen weltweit die Naturereignisse mit katastrophaler Wirkung zu – und die Rolle Deutschlands als Unterstützer von Sanktionen in Konfliktfällen hat die Gefährdungslage noch einmal gesteigert.

Bislang gab es für kritische Infrastrukturen auf Bundesebene lediglich Regelungen zu ihrer IT (Informationstechnologie)-Sicherheit. Das KRITIS-Dachgesetz soll die Cybersicherheit nun ergänzen und ihre physische Widerstandskraft, ihre Resilienz, stärken.

Hinweis: Dieses Whitepaper basiert auf dem Gesetzentwurf für das KRITIS-Dachgesetz vom 21. Dezember 2023.

Das KRITIS-Dachgesetz

Das Gesetzeswerk wird „Dachgesetz“ genannt, weil es sich künftig wie ein schützendes Dach über die Sektoren mit kritischen Infrastrukturen legen soll.

Der Anlass

Die am 13. Januar 2023 in Kraft getretene CER-Richtlinie des Europäischen Parlaments schafft einen Rahmen, den alle Mitgliedsstaaten in nationales Recht umsetzen müssen. CER steht für Critical Entities Resilience, also die Widerstandsfähigkeit kritischer Einrichtungen.

Das Ziel

Mit dem KRITIS-Dachgesetz soll ein kohärentes System zur Stärkung der Resilienz kritischer Anlagen entstehen, mit klar definierten Verantwortlichkeiten und Zuständigkeiten.

Die Inhalte

Europaweit müssen die nationalen KRITIS-Gesetze einheitliche Mindestverpflichtungen für Betreiber kritischer Anlagen festlegen. Dafür definiert das deutsche KRITIS-Dachgesetz die betroffenen Sektoren, die Anforderungen an die Betreiber der Anlagen und die erforderlichen Maßnahmen, Berichtspflichten und das Meldewesen. Nach dem All-Gefahren-Ansatz sollen alle erdenkbaren Risiken abgedeckt werden, die durch Natur oder Mensch verursacht werden können, vom Unwetter über menschliches Versagen bis zur Sabotage.

Betroffene Sektoren sind:

- Energie
- Transport und Verkehr
- Finanz- und Versicherungswesen
- Gesundheitswesen
- Wasser (Trinkwasser und Abwasser)
- Ernährung
- Informationstechnik und Telekommunikation
- Weltraum
- Öffentliche Verwaltung
- Siedlungsabfallentsorgung

Grundsätzlich zählen zu den von KRITIS definierten „kritischen Anlagen“ Einrichtungen, die essenziell für die Gesamtversorgung in Deutschland sind.

KRITIS-Sektor Energie
(Strom, Gas, Kraftstoff, Wärme)

KRITIS-Sektor Transport und Verkehr

KRITIS-Sektor Wasser
(Trinkwasser und Abwasser)

Anlagenkategorien und Schwellenwerte der BSI-Kritisverordnung

Die Verordnungen definieren für jeden Sektor die betroffenen **Anlagenkategorien und Schwellenwerte**, ab welcher Größenordnung eine Anlage unter das KRITIS-Gesetz fällt.

Die für KRITIS zuständige zentrale Anlaufstelle ist das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK). Betreiber müssen ihre kritische Anlage zunächst auf einer zentralen Plattform **registrieren und eine Kontaktstelle oder Person als Ansprechpartner** benennen. Anschließend müssen sie eine **Risikoanalyse und Risikobewertung** ihrer Anlage vornehmen. Sofern nicht bereits durch andere Verpflichtungen geschehen, müssen sie „geeignete und verhältnismäßige, sicherheitsbezogene und organisatorische **Maßnahmen** zur Gewährleistung ihrer Resilienz treffen“, wie es im Gesetzentwurf heißt. Dabei soll der Stand der Technik eingehalten werden. Als „verhältnismäßig“ gilt, wenn der Aufwand angemessen im Vergleich zu den Folgen des Ausfalls oder der Beeinträchtigung erscheint.

Die Maßnahmen sollen

- Vorfälle verhindern,
- einen angemessenen physischen Schutz der Räumlichkeiten und kritischen Infrastrukturen sicherstellen,
- den Betreiber in die Lage versetzen, auf Vorfälle zu reagieren, sie abzuwehren und ihre Folgen zu begrenzen,
- nach Vorfällen die Wiederherstellung sicherstellen,
- ein angemessenes Sicherheitsmanagement mithilfe der Mitarbeitenden oder externer Dienstleister gewährleisten.

In einem Resilienzplan müssen Betreiber ihre getroffenen Maßnahmen dokumentieren und ihn regelmäßig aktualisieren. Störungen von kritischen Anlagen müssen umgehend über die Kontaktstelle gemeldet werden.

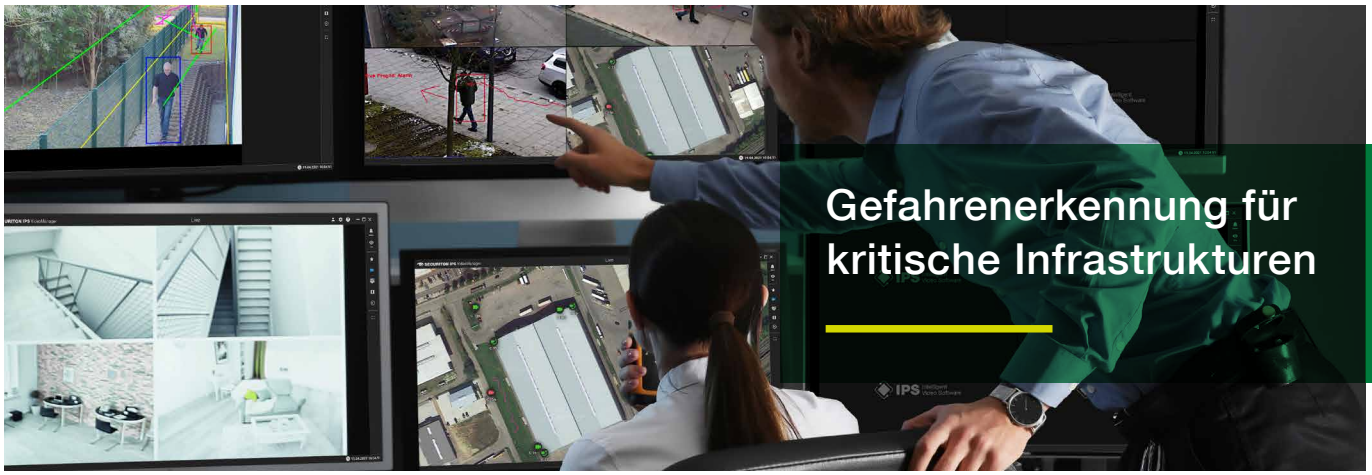
Der Zeitplan

Bis 17. Oktober 2024 müssen alle europäischen Mitgliedstaaten die CER-Richtlinie in nationales Recht umgesetzt haben.

Der Gesetzentwurf vom Dezember 2023 soll im Jahr 2024 das parlamentarische Verfahren durchlaufen. Das Gesetz selbst tritt dann am Tag nach seiner Verkündung in Kraft – mit zwei Ausnahmen: Die Regelungen zu den Pflichten der Anlagenbetreiber sollen erst zum 1. Januar 2026 und zeitlich gestaffelt Inkrafttreten, die Bußgeldvorschriften zum 1. Januar 2027 bzw. ebenfalls zeitlich gestaffelt.

Umgehend nach Inkrafttreten der für ihren Sektor gültigen Rechtsverordnung müssen Betreiber ihre kritische Anlage registrieren und dem BKK eine Kontaktstelle/-person nennen. Erstmalig neun, teilweise auch zehn Monate nach der Registrierung müssen Betreiber eine Risikoanalyse und -bewertung vornehmen und dann spätestens alle vier Jahre wiederholen. Der von ihnen zu erstellende Resilienzplan mit allen Maßnahmen zur Gewährleistung der Widerstandsfähigkeit ihrer Anlage muss zu einem Termin nachgewiesen werden, den das BKK bei der Registrierung mitteilt, anschließend alle zwei Jahre.

> “Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.”
>
> Bundesamt für Sicherheit in der Informationstechnik (BSI)



Gefahrenerkennung für kritische Infrastrukturen

Moderne Systeme zur Gefahrendetektion und -abwehr

Die Bedrohungsszenarien für jeden Sektor und jede kritische Anlage sind höchst individuell. Im Kern müssen jedoch alle Maßnahmen darauf abzielen, unbefugtes Eindringen in die Objekte selbst und Angriffe drauf zu erkennen und wenn möglich zu verhindern, aber auch die Sicherheitstechnik selbst zu sichern, sodass Sabotage-Angriffe umgehend und automatisch erkannt werden. Zudem geht es um die wirksame Überwachung des Umfelds, Perimeter genannt, denn schon herumlungernde Personen, die beispielsweise Situationen vor Ort beobachten oder Details ausspähen, könnten bereits eine Bedrohung darstellen.

Die Sicherheitsbranche beschäftigt sich bereits seit vielen Jahren mit dem Objekt- und Perimeterschutz für kritische Infrastrukturen, der integrative Systemtechnologien in einem Gesamtsystem vereint – dazu gehören:

- Hochfunktionale intelligente Videosicherheitssysteme
- Zaundetektion
- Einbruchschutz
- Zutrittskontrolle
- Systeme zur Drohnendetektion und -abwehr

Das Know-how namhafter Sicherheitsanbieter ist immens, die Alarmierungs- und Sicherheitssysteme beinhalten etablierte Standards für Hochsicherheitsbereiche. Mit lückenloser Erfassung und Verifikation von Gefahren und Angriffen geben sie dem eingesetzten Sicherheitspersonal höchstmögliche technische Unterstützung mit akzeptabler Täuschungsalarmrate. Hierfür kommt teilweise schon künstliche Intelligenz (KI) in Form von neuronalen Netzen zum Einsatz, deren Aufgabe es ist, z. B. die Objektklassifikatoren zu erweitern und Störobjekte auszufiltern, um so die Rate der unerwünschten Alarme stetig zu reduzieren. In der gemeinsamen Entwicklung passgenauer Sicherheitskonzepte mit dem Auftraggeber gilt es, durch Betrachtung von Gefahren und Risiken die Schutzziele zu bestimmen und die erforderlichen Maßnahmen entsprechend auszulegen. Dabei sind alle Skalierungsmöglichkeiten gegeben – von der Kleinstlösung bis hin zur intelligenten Vernetzung von Systemen, mit Multi-Site-Management (MSM) auch über Standortgrenzen hinweg. Letzteres kann erforderliche Einsatzkräfte vor Ort nicht ersetzen, aber deutlich entlasten, denn es gewährleistet eine lückenlose Absicherung mithilfe intelligenter Videoanalyse und Videomanagement aus einem Guss.

Zudem kann das MSM auf eine ständig besetzte Notruf- und Serviceleitstelle (NSL) aufgeschaltet werden, die im Alarmfall die Einsatzkräfte mit Live-Informationen unterstützt. So kann die Auslagerung der Organisationsmaßnahmen die Betreiber kritischer Anlagen von der Bereitstellung eines erhöhten Personalbedarfs entlasten, denn durch das KRITIS-Dachgesetz kommen auf sie ohnehin zum Teil erhebliche Investitionen in moderne Technik zu.

Keine Frage: Physische Sicherheit ist ohne IT-Sicherheit nicht zu haben. Um die physische Absicherung von Objekten durch Einsatz intelligenter Systeme zu gewährleisten, ist mittlerweile auch ein gewisses Maß an IT-Sicherheit zwingend erforderlich. So ist es unabdingbar, neben den baulichen sowie elektronischen Sicherheitseinrichtungen auch den Aspekt der IT-Sicherheit in Verbindung mit den eingesetzten IT-basierten Systemen zu betrachten. Denn schlussendlich müssen robuste Objekt- und Perimeterschutzsysteme selbst auch IT-Angriffen standhalten.

Entsprechend konzipierte Systeme für den Hochsicherheitsbereich bieten systemeigene IT-Sicherheitskomponenten, die sie zum einen vor Angriffen von außen schützen und zum anderen mithilfe von Hardware-Redundanzen

Sicherheitskonzepte für den Objekt- und Perimeterschutz

Vielseitige Sicherheitslösungen für den Luftverkehr

Gefahrendetektion in sensiblen Bereichen im Gesundheitswesen

Videosicherheit für höchste Transparenz

über mehrere Server höchstmögliche Verfügbarkeit gewährleisten – sowohl in Bezug auf die drahtgebundene als auch drahtlose Übertragung.

Videosicherheitssysteme zur Überwachung sensibler Bereiche

Überwachungskameras zum Schutz sensibler Anlagen sind keine Neuigkeit. Ihre stetige Beobachtung und gleichzeitige Beurteilung bindet jedoch Sicherheitspersonal – und ermüdet oft schon nach kurzer Zeit selbst gut ausgebildete Fachkräfte. **Moderne Videosicherheitsanlagen** erkennen mithilfe von Analysemodulen gefährliche Situationen bereits während ihrer Entstehung und lösen automatisch Alarm aus – etwa sobald sich im öffentlichen Personennahverkehr Personen im Gleisbett aufhalten oder wenn unbefugte Personen in kritische Bereiche der Trinkwasserversorgung eindringen.

Algorithmen, die Videobilder nach vordefinierten Kriterien analysieren und auf Pixelveränderungen hin auswerten, entscheiden darüber, ob Unregelmäßigkeiten beziehungsweise Risiken vorherrschen. Quasi ein automatisiertes Frühwarnsystem. Die Veränderungen werden nach Größe, Richtung und Strecke von Objekten, beispielsweise Personen, analysiert.

Speziell für kritische Infrastrukturen ist der seit vielen Jahren betriebsbewährte Videoanalysesensor CIP (Critical Infrastructure Protection) fester Bestandteil in Perimeterschutzkonzepten bei zahlreichen Endanwendern – nicht nur im Bereich kritischer Infrastrukturen. Die Bedrohungsszenarien sind individuell. Im Kern geht es jedoch immer darum, unbefugtes Eindringen und somit Angriffe zu erkennen und darüber hinaus die Sicherheitstechnik selbst zu sichern, sodass Sabotageangriffe schon bei deren Versuch automatisch erkannt werden.

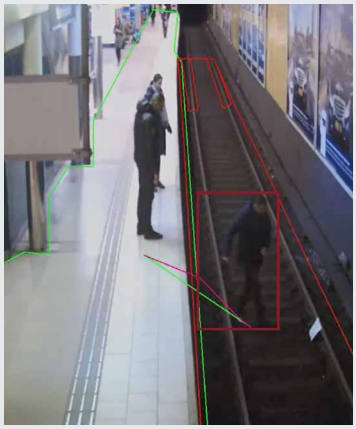
Zudem steht auch die wirksame Überwachung des Umfeldes im Fokus, denn bereits herumlungernde Personen bringen ein erhöhtes Bedrohungspotenzial mit sich. So können im Sinne der Manipulationssicherheit beispielsweise Täter schon frühzeitig erkannt werden, wenn sie versuchen, Zugänge wie Tore und Türen zu überwinden. Den Kameras entgeht nichts, und die intelligente Videodetektion ist der zuverlässige Wächter, der wirksam den Schutz der Umgebung im Griff hat.

Für das Sicherheitspersonal in der Zentrale ist jeder alarmauslösende Grund sofort auf den Bildschirmen ersichtlich. Es kann in der Folge mögliche Unbefugte direkt ansprechen und zum Verlassen des Bereichs auffordern. Geschieht das nicht, ist es möglich, Eindringlinge mit zusätzlichen Kameras auf dem Gelände zu verfolgen – zur Beobachtung, späteren Rekonstruktion und Beweissicherung. Mithilfe der intelligenten Verknüpfung mehrerer Überwachungskameras entsteht eine völlig eigenständige Objektverfolgung. Durch die jeweiligen Kamerabilder visualisiert, sowohl als Livebild als auch auf dem Geländeplan, lassen sich komplexe Alarmszenarien einfach überblicken.

Bestens unterstützt durch die Symbiose aus Videomanagement und Videoanalyse, können umgehend Gegenmaßnahmen eingeleitet werden. Um die Sicherheit beispielsweise im Bahnverkehr zu wahren, können Interventionskräfte oder der zentrale Wachdienst alarmiert werden.

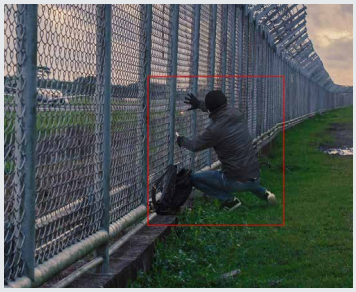
Videobilder werden automatisch gesichert und können DSGVO-konform mit Verschleierung oder Maskierung versehen werden – zum Schutz der Privatsphäre von Unbeteiligten. Bei einer späteren Strafverfolgung könnten Befugte die Inhalte durch eine Passworteingabe wieder sichtbar machen.

Eine zusätzliche Sicherungsmaßnahme etwa für den Trinkwasserschutz kann die Abschottung von Versorgungsleitungen sein.



Sicherheitsdetektion am Bahnsteig und im Gleisbett

Intelligente Videotechnik alarmiert in Echtzeit bei Eindringversuchen



Automatisierte Gefahrendetektion an den Außengrenzen von Arealen

Drohnen – neue Gefahren im bodennahen Luftraum

Zaundetektion – intelligente mechanische Barrieren
Zäune können Grundstücksgrenzen oder juristische Außengrenzen eines Sicherungsbereiches markieren und sind zunächst einmal ein Hindernis für Personen, die sich unbefugt Zutritt verschaffen möchten. Moderne Sicherheitszäune sind intelligente Systeme, die Sicherheitsbereiche wie Flug- oder Seehäfen oder Umspannwerke schützen.

Elektronisch überwachte Zäune sichern rund um die Uhr zuverlässig die Grundstücks- oder juristische Außengrenze, ohne dass die eingesetzte Technik für Angreifer zu erkennen ist. Sobald der Stromkreis im Innern der Drähte durch Demontage, Aufhebeln oder Durchtrennen von Zaunteilen unterbrochen wird, löst das System automatisch Alarm aus. Auch Überklettern kann mithilfe moderner Zäune detektiert werden, die über ein Alarmmeldesystem oder Videosicherheitssystem umgehend das Sicherheitspersonal informieren. Zusatzeinrichtungen zur Beleuchtung oder Beschallung können das Sicherheitskonzept abrunden.

Zutrittskontrolle und Einbruchschutz – das beruhigende Gefühl von Sicherheit
Moderne Systeme zur Zutrittskontrolle und für den Einbruchschutz sorgen dafür, dass nur befugte Personen in Sicherheitsbereiche kritischer Infrastrukturen gelangen, um beispielsweise Produktionshallen der Lebensmittelindustrie vor Verunreinigungen zu schützen oder definierte Bereiche in Krankenhäusern etwa vor unerlaubtem Zugriff auf Medikamente zu bewahren.

Präzise definierte Zutrittsberechtigungen regeln, wer wann welches Gebäude, welchen Trakt oder Raum betreten darf. Die modular aufgebauten Systeme sind flexibel einsetzbar und lassen sich für alle Anlagengrößen skalieren. Auch eine überregionale Vernetzung verschiedener Standorte ist möglich.

Durch Kombination von Zutrittskontrolle mit Einbruch-, Überfall- und Störmeldetechnik entsteht eine ganzheitliche und vernetzte Sicherheitslösung, die Alarm schlägt, wenn sich unbefugte Personen Zutritt zu kritischen Anlagen oder Hochsicherheitsräumen verschaffen.

Drohnensicherheitssysteme gegen die neue Gefahr aus der Luft und als digitale Wächter
Einzelne Drohnen oder Drohnenschwärme stellen nicht nur eine Gefahr für den Luftverkehr an Flughäfen und Landeplätzen für Helikopter dar. Auch für alle anderen Arten von kritischen Anlagen können sie ein Risiko aus der Luft bedeuten.

Drohnensicherheitssysteme erkennen Drohnen oder Drohnenschwärme teilweise sogar schon beim Einschalten der Fernbedienung, können sie lokalisieren und aktiv verfolgen. Das Sicherheitspersonal ist jederzeit über den aktuellen Aufenthaltsort der Drohnen selbst informiert sowie den Standort der Piloten mitsamt der Fernbedienungen. Ihm stehen Daten zu Flugbahn, Flughöhe und Drohnentyp zur Verfügung, damit es frühzeitig Maßnahmen einleiten kann. Moderne Abwehrsysteme sind zudem in der Lage, nicht kooperative Drohnen beim Eintritt in eine Schutzzone kontrolliert zu übernehmen und in einem definierten Areal zu landen, sodass Schaden vom Schutzziel abgewendet werden kann.

Drohnen können aber auch als digitale Wächter die Einsatzkräfte unterstützen. Wenn etwa die Perimetersicherungssysteme einen Manipulations- oder Übersteigversuch an einem abgelegenen Teil des Zauns einer weitläufigen kritischen Anlage meldet, kann es umgehend Einsatzdrohnen aktivieren, die mithilfe der übermittelten Geodaten den Ort anfliegen und durch Live-Aufnahmen des Geschehens vor Ort das Personal der Sicherheitszentrale immer auf dem aktuellen Stand halten.

Barrieren mit Intelligenz: Zaundetektion für Hochsicherheitsbereiche

Zutrittskontrolle: Nur befugte Personen gelangen in gesicherte Bereiche

Schutz vor Gefahren aus der Luft: Drohnendetektion und -abwehr

Dome Security: Umfassender Objekt- und Perimeterschutz

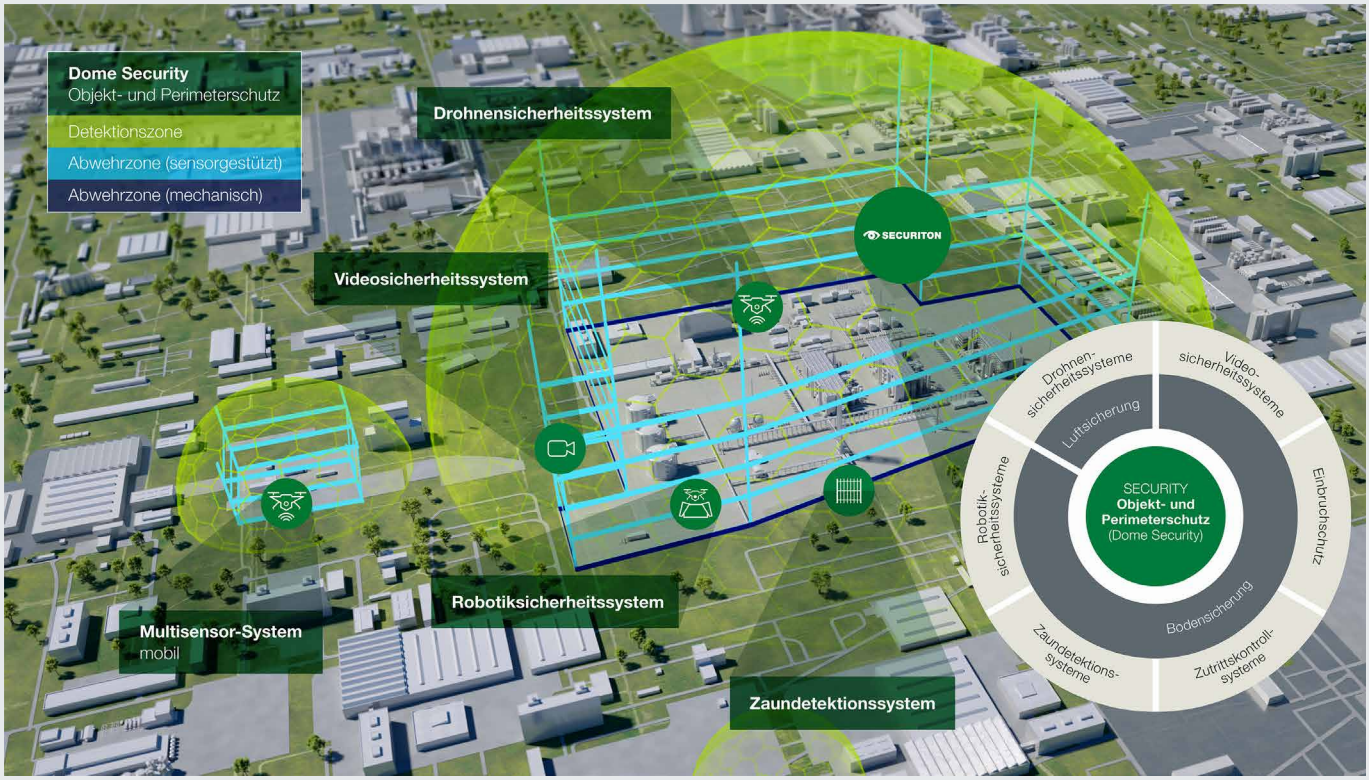
Sicherheit aus erfahrener Hand von Securiton Deutschland – auch für kritische Infrastrukturen der Zukunft
Bei der Entwicklung umfangreicher Sicherheits- und Schutzkonzepte für kritische Einrichtungen ist ein erfahrener und kompetenter Partner unerlässlich. Securiton Deutschland versteht es als Anwendungsspezialist mit jahrzehntelanger Erfahrung, mit geeigneten Technologien „Made in Germany“ individuelle Schutzkonzepte zu erstellen und zum Einsatz zu bringen.

Für den Objekt- und Perimeterschutz entwickelt Securiton Deutschland maßgeschneiderte Lösungen nach Sektor, Bedarf und Anlagengröße. Das dabei entstehende Gesamtkonzept wird „Dome Security“ genannt, da es sich wie eine schützende Kuppel über Freiflächen und Gebäude legt und dafür intelligente Systeme zum Schutz und zur Überwachung von Boden und Luftraum kombiniert.

Das Geschäftsfeld Energie von Securiton Deutschland wurde bereits 1998 gegründet. Es berät und betreut Stakeholder in allen Sicherheitsfragen – von der Energieerzeugung über die Energieverteilung bis zur Energiespeicherung.

Diese langjährige Erfahrung bringt Securiton Deutschland auch in die Initiative Get H2 ein, in der es seit 2023 Mitglied ist, um als ein Vorreiter der Branche sein Know-how in die Entwicklung einer stabilen und sicheren Wasserstoffwirtschaft einzubringen. Denn zweifellos wird die Wasserstoffversorgung künftig zu den kritischen Infrastrukturen in Deutschland gehören und eine Absicherung der Produktionsanlagen und Transportwege im Sinne des KRITIS-Dachgesetzes erfordern.

Aktuelle Informationen finden Sie auch auf unserer Website: www.securiton.de/kritis



Der findigste Anwendungs-spezialist für Sicherheit

Branchen verstehen – individuelle Lösungen entwickeln

Versorgungssicherheit ist ein hohes Gut

Anlagen schützen, Energieversorung sichern

Internationale Gipfel-treffen

Drohnen detektieren, Piloten lokalisieren und frühestmöglich inter-venieren

Food Defense

Gegen vorsätzliche Ver-unreinigung von Lebens-mitteln in der Produktion

Schutzkuppel für Justiz-vollzugsanstalten

Drohnendetektion und -abwehr verhindern Ab-würfe von Drogen und Waffen

Weil der Mensch zählt

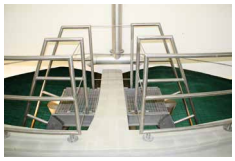
Mehr Effizienz im Pflege-alltag mit Kommunika-tionssystemen und Personalsicherheit in der Notaufnahme

Bahngleisüberwachung mit Intelligenz

Menschen sind im Gleis-bett in Lebensgefahr – Videosicherheitssysteme warnen rechtzeitig

Kunst- und Kultur-schätze bewahren

Museen, Bibliotheken und Archive benötigen Schutz vor Kriminellen, Umwelt-einflüssen und Elementar-schäden



Sauberes Trinkwasser – ganz sicher

Intelligente Videosicher-heitssysteme machen Gefahren transparent und verhindern Sabotage

Prozessüberwachung im Müllkraftwerk

An 365 Tagen im Jahr Ausfallzeiten und Still-stände vermeiden

Physische Sicherheit – auch für Rechenzentren

Unternehmensdaten werden mit kombinierten Sicherheitssystemen wirksam geschützt

Securiton Deutschland
Alarm- und Sicherheitssysteme

Hauptsitz: Von-Drais-Straße 33
77855 Achern | DE
Tel. +49 7841 6223-0

www.securiton.de

Ein Unternehmen der
Securitas Gruppe Schweiz

SECURITON