1/2026

KRITIS inside

DAS FACHMAGAZIN FÜR KRITISCHEN INFRASTRUKTURSCHUTZ

Jetzt neu!
ERSTAUSGABE

IM INTERVIEW

Holger Berens,
Vorstandsvorsitzender,
Bundesverband für den Schutz Kritischer Infrastrukturen e.V. (BSKI)

TECHNOLOGIE & INNOVATION

High-End-Lösungen für den KRITIS-Schutz

BEDROHUNGSLAGEN & TRENDS

Mission #SicheresGerätehaus – Hintergrund & Perspektiven

BEST PRACTICES

Absicherung eines Solarparks mittels Perimeterschutz

videoalarm.de

ERSTAUSGABE *KRITIS inside*

NEW

KRITIS inside ist das neue Fachmagazin für Kritischen Infrastrukturschutz, das mit der vorliegenden Ausgabe 1/2026 erstmals und künftig vier Mal jährlich erscheint. In einer Zeit, in der Versorgungssicherheit, Krisenvorsorge und Resilienz zunehmend an Bedeutung gewinnen, bietet das Magazin eine fundierte und praxisnahe Informationsplattform.

Die Publikation beleuchtet aktuelle Entwicklungen, gesetzliche Rahmenbedingungen, Technologien und Best-Practice-Ansätze aus allen relevanten KRITIS-Sektoren. Dabei steht im Mittelpunkt, wie Organisationen und Einrichtungen ihre Sicherheits- und Resilienzstrategien wirksam weiterentwickeln können.

KRITIS inside richtet sich an:

- ***kommunale Entscheider und Behörden***
- ***Führungskräfte aus Feuerwehr und BOS***
- ***Betreiber Kritischer Infrastrukturen***
- ***Sicherheits- und Krisenmanager***
- ***Anbieter sicherheitsrelevanter Technologien***

EDITORIAL

BASTIAN RAUEN
Herausgeber *KRITIS inside*

Liebe Leserinnen und Leser,

die Welt des Kritischen Infrastrukturschutzes steht an einem Wendepunkt. Digitalisierung, geopolitische Spannungen und technologische Disruptionen stellen unsere Sicherheitsarchitektur auf die Probe – und eröffnen zugleich neue Chancen. Sicherheitstechnische Innovationen, von KI-gestützter Sensorik über adaptive Alarmkonzepte bis hin zu resilienten Netzarchitekturen, werden zum entscheidenden Faktor für die Handlungsfähigkeit moderner Gesellschaften.

Mit dem **KRITIS-Dachgesetz** hat Deutschland einen wichtigen Schritt hin zu einem einheitlichen Ordnungsrahmen getan. Doch die Umsetzung zeigt: Der Teufel steckt im Detail. Viele Betreiber und Kommunen stehen vor der Herausforderung, technische und organisatorische Schutzmaßnahmen in Einklang mit knappen Ressourcen und komplexen Meldepflichten zu bringen. Ein wachsendes Risiko geht dabei von oben aus – im wahrsten Sinne des Wortes: **Drohnen** werden zunehmend als potenzielle Gefahr für kritische Anlagen erkannt. Was einst ein Werkzeug für Inspektion und Logistik war, kann heute zur Waffe oder Spionageplattform werden. Hier braucht es klare rechtliche Leitplanken, aber auch technische Abwehrsysteme, die verlässlich wirken. Gleichzeitig zeigt sich in den Kommunen ein bemerkenswerter Trend: **Mission #SicheresGerätehaus**. Feuerwehren rüsten ihre Standorte mit intelligenten Alarmsystemen, Wärmebildkameras und automatisierten Brandfrüherkennungssystemen aus – ein starkes Signal für Selbstschutz, Prävention und Modernisierung.

Für unsere Erstausgabe konnten wir mit Holger Berens, den Vorstandsvorsitzenden des Bundesverband für den Schutz Kritischer Infrastrukturen e.V. (BSKI) gewinnen, der einen Einblick in aktuelle Entwicklungen, Herausforderungen und Zukunftsperspektiven des KRITIS-Schutzes gibt. Sein Fazit: Sicherheit muss als kontinuierlicher Prozess verstanden werden – interdisziplinär, vernetzt und innovationsgetrieben.

Bleiben wir also neugierig, kritisch und mutig – denn Sicherheit ist keine Frage des Zustands, sondern der Haltung.

Herzlich,

Ihr Bastian Rauen

INHALT 1/2026

IMPRESSUM

Herausgeber:
r2 Überwachungstechnik GmbH/ videoalarm.de
Mainzer Str. 44
56068 Koblenz
V. i. S. d. P.:
Bastian Rauen, Geschäftsführer
Tel.: 0261 - 89 99 99 0
b.rauen@videoalarm.de

Gestaltung & Redaktion:
Martina Kollig / medienbüro makopress
Mainzer Str. 44
56068 Koblenz
m.kollig@makopress.de

Fotonachweis:
Volker M. Bruns, Martina Kollig, Concepture GmbH, AJAX, KI

Erscheinungsweise:
Das Fachmagazin erscheint vier Mal im Jahr.
Erstauflage: 2.500 Exemplare

Anzeigen:
Frank Balschuweit, Tel.: 0261 - 89 99 99 10

KRITIS-DACHGESETZ: DER GANZ GROSSE WURF ?

Die Sicherung kritischer Infrastrukturen wird in Deutschland neu gedacht. Mit dem KRITIS-Dachgesetz entsteht erstmals ein einheitlicher Rechtsrahmen, der nicht nur IT-Sicherheit, sondern auch den physischen Schutz und die organisatorische Resilienz zentral regelt. Nach Jahren sektorspezifischer Einzelregelungen soll das Dachgesetz die bestehenden Lücken schließen – und Deutschland besser gegen hybride Bedrohungen wappnen.

Vom Cyberfokus zur Gesamtresilienz

Während bisher vor allem das IT-Sicherheitsgesetz und die NIS-2-Richtlinie die Anforderungen an Betreiber regelten, geht das KRITIS-Dachgesetz deutlich weiter. Es setzt die EU-CER-Richtlinie (Critical Entities Resilience Directive) um, die seit 2023 gilt und in allen Mitgliedsstaaten eine umfassende Schutzpflicht für Betreiber essenzieller Einrichtungen verlangt.

Ziel ist es, dass Versorgungssysteme auch bei Naturkatastrophen, Sabotage, Terror oder technischen Ausfällen funktionsfähig bleiben. Damit verlagert sich der Fokus von der reinen Cyberabwehr hin zu einer ganzheitlichen Resilienzstrategie – physisch, organisatorisch und digital.

Der aktuelle Stand *(a.d.R. Dezember 2025)*

- Im September 2025 hat die Bundesregierung den Gesetzentwurf verabschiedet, Anfang November wurde er im Bundestag in erster Lesung beraten und an den Innenausschuss überwiesen. Das parlamentarische Verfahren läuft derzeit; Fachanhörungen sind für Dezember vorgesehen.
- Das Inkrafttreten ist nach aktuellem Stand für Anfang 2026 geplant. Viele Regelungen – insbesondere Meldepflichten, Auditverfahren und Sanktionsmechanismen – sollen gestaffelt in Kraft treten.

GESETZESLAGE

Für wen gilt das Gesetz?

Das Dachgesetz richtet sich an Betreiber sogenannter kritischer Anlagen – Einrichtungen, die wesentlich für die Versorgung der Bevölkerung oder für das öffentliche Leben sind. Dazu gehören:

- **Energie- und Wasserversorgung**
- **Abwasserentsorgung**
- **Informations- und Kommunikationstechnik**
- **Behörden und Organisationen mit Sicherheitsaufgaben**
- **Transport und Verkehr**
- **Gesundheitswesen**
- **Ernährung**
- **Öffentliche Verwaltung**
- **Weltrauminfrastruktur**

Die Schwellenwerte, ab wann ein Betrieb als kritisch gilt, sollen per Rechtsverordnung festgelegt werden. Maßgeblich sind unter anderem Versorgungsumfang, gesellschaftliche Relevanz und Vernetzung mit anderen Infrastrukturen. Schätzungen zu Folge betrifft das KRITIS-Dachgesetz rund 30.000 Unternehmen bzw. Institutionen.

Was bringt das Gesetz?

- Einheitliche Mindeststandards für physischen und organisatorischen Schutz – erstmals bundeseinheitlich.
- Pflicht zu Risiko- und Resilienzanalysen: Betreiber müssen Schwachstellen bewerten und Konzepte dokumentieren.
- Meldepflichten bei erheblichen Störungen oder Angriffen.
- Zentrale Zuständigkeiten bei Bund und Ländern, insbesondere durch eine enge Verzahnung von Bundesamt für Sicherheit in der Informationstechnik (BSI) und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK).
- Bußgeldtatbestände bei Nichterfüllung von Pflichten.

Der Bund verfolgt damit das Ziel, den Flickenteppich sektoraler Regelungen zu beenden und eine durchgängige Sicherheitsarchitektur zu schaffen.

Was Betreiber jetzt beachten müssen

Obwohl das Gesetz noch im parlamentarischen Verfahren ist, sollten Betreiber bereits jetzt aktiv werden. Erfahrungsgemäß sind Übergangsfristen knapp bemessen – und der Anpassungsaufwand groß.

Besonders wichtig sind:

- **die Identifikation, ob man als „kritische Anlage“ gilt,**
- **die Bestandsaufnahme bestehender Schutzmaßnahmen,**
- **sowie die Erarbeitung eines Resilienzplans.**

Frühzeitige Vorbereitung sichert Handlungsspielraum – und vermeidet Bußgelder, wenn die Pflichten greifen.

FAZIT: Sicherheit wird zur strategischen Managementaufgabe

Das KRITIS-Dachgesetz markiert den Schritt hin zu einem modernen, ganzheitlichen Schutzsystem für Deutschlands lebenswichtige Infrastrukturen. Es setzt erstmals einen einheitlichen Ordnungsrahmen, der sektorübergreifend Mindeststandards für Resilienz, Prävention und Krisenreaktion definiert. Zugleich steigt der Handlungsdruck auf Betreiber, ihre Sicherheitskonzepte strukturiert zu überprüfen und weiterzuentwickeln. Damit wird der Schutz kritischer Infrastrukturen zunehmend zur strategischen Managementaufgabe auf Führungsebene. Die kommenden Monate werden zeigen, ob der Gesetzgeber die Balance zwischen ambitionierten Sicherheitszielen und praktischer Umsetzbarkeit findet.

Für Betreiber heißt das: Jetzt handeln – nicht warten.

Monitoring-Timeline KRITIS-Dachgesetz

- September 2025 – Kabinettsbeschluss über den Regierungsentwurf (BMI)
- Oktober 2025 – Veröffentlichung der Entwurfsfassung und Verbändeanhörungen
- 6. November 2025 – Erste Lesung im Bundestag, Überweisung an Innenausschuss
- Dezember 2025 – Öffentliche Fachanhörungen im Innenausschuss (geplant)
- Januar 2026 – Zweite/ Dritte Lesung im Bundestag (wahrscheinlich)
- Februar 2026 – Beratung im Bundesrat
- März 2026 – Verkündung im Bundesgesetzblatt (voraussichtlich)
- Q2 2026 – Inkrafttreten der ersten Regelungen (Registrierung, Risikoanalysepflichten)
- Q4 2026 / Q1 2027 – Staffelweise Wirksamkeit der Bußgeld- und Meldepflichten

CHECKLISTE FÜR BETREIBER KRITISCHER ANLAGEN

1. Analyse & Einordnung

- [ ] Prüfen, ob das eigene Unternehmen oder die Einrichtung als „kritische Anlage“ gilt (Versorgungsumfang, Relevanz, Vernetzung).
- [ ] Verantwortliche Person oder Stelle für KRITIS-Compliance benennen.

2. Risiko- und Resilienzbewertung

- [ ] Gefährdungsanalyse erstellen: physische Risiken, Cyberrisiken, Abhängigkeiten.
- [ ] Notfall- und Wiederanlaufkonzepte prüfen oder entwickeln.
- [ ] Dokumentation zentral anlegen (auditfähig).

3. Schutzmaßnahmen & Infrastruktur

- [ ] Zutrittskontrollen, Videoüberwachung, Brandschutz und Redundanzen überprüfen.
- [ ] Kooperation mit Sicherheits- und Wartungsdienstleistern prüfen.
- [ ] Schnittstellen zwischen IT-Sicherheit und physischem Schutz abstimmen.

4. Melde- und Kommunikationswege

- [ ] Zuständige Aufsichtsbehörden (BSI, BBK, Landesstellen) identifizieren.
- [ ] Interne Prozesse zur Störungs- und Ereignismeldung vorbereiten.
- [ ] Kommunikationsplan für Krisenfälle (intern/ extern) festlegen.

5. Governance & Compliance

- [ ] Schulungen für Sicherheits- und Führungspersonal planen.
- [ ] Haftungs- und Verantwortlichkeitsfragen klären.
- [ ] Regelmäßiges Monitoring des Gesetzgebungsverfahrens (Bundestag, BMI).

6. Frühzeitige Umsetzung

- [ ] Maßnahmen priorisieren, Budget und Zeitrahmen definieren.
- [ ] Umsetzungsetappen dokumentieren – Nachweispflicht!
- [ ] Frühzeitiger Austausch mit Fachverbänden (z. B. BSKI, DVGW, VDE, BHE).

INNOVATION TRIFFT VERANTWORTUNG: HIGH-END-LÖSUNGEN FÜR DEN KRITIS-SCHUTZ

WIE EIN DEUTSCHER SICHERHEITSANBIETER MIT MODULAREN SYSTEMLÖSUNGEN, KI-GESTÜTZTER ÜBERWACHUNG UND SMARTER BRANDWARNTECHNIK DEN STANDARD FÜR DEN SCHUTZ KRITISCHER INFRASTRUKTUREN NEU DEFINIERT.

In einer Zeit, in der Bedrohungen zunehmend hybrid, vernetzt und unberechenbar auftreten, genügt klassische Sicherheitstechnik längst nicht mehr. Der Schutz Kritischer Infrastrukturen verlangt nach integrativen Konzepten, die physische, digitale und organisatorische Sicherheitsmechanismen zu einem intelligenten Gesamtsystem vereinen. Ein Unternehmen, das diese Entwicklung seit Jahren konsequent mitgestaltet, ist die r2 Überwachungstechnik GmbH/ videoalarm.de aus Koblenz. Das Team aus Sicherheitsexperten und Facherrichtern hat sich darauf spezialisiert, hochmoderne Sicherheitslösungen zu entwickeln, die vom Perimeterschutz über Alarmsysteme bis hin zu brandschutztechnischen Innovationen reichen – alles aus einer Hand und abgestimmt auf die spezifischen Anforderungen von KRITIS-Betreibern.

Leitstelle nach: *Alarmsystem:*

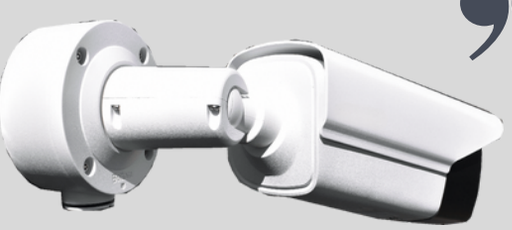
VdS | Alarm-verifikation nach VdS 3415 | DIN EN GRAD II | DSGVO-konform

TECHNOLOGIE & INNOVATION

VON DER RISIKOANALYSE BIS ZUR LEITSTELLE

Der erste Schritt jedes Projekts beginnt mit einer fundierten Risikoanalyse: Welche Bedrohungsszenarien sind realistisch? Wo liegen Schwachstellen in der bestehenden Infrastruktur? Und welche Schutzmaßnahmen sind wirklich sinnvoll? Auf dieser Basis entstehen maßgeschneiderte, herstellerunabhängige Sicherheitskonzepte – optimiert für Effizienz, Integration und Normkonformität.

Das Ergebnis sind ganzheitliche Lösungen, die alle Ebenen der Sicherheitsarchitektur abdecken: intelligente Alarm- und Videosysteme, smarte Zutrittskontrolle, Brandschutz, Sprachalarmierung und 24/7-Überwachung durch eine zertifizierte Notruf- und Serviceleitstelle. Diese Leitstelle gehört zu den modernsten Europas. Sie ist rund um die Uhr besetzt, wertet eingehende Signale in Echtzeit aus, prüft Alarme auf Plausibilität und initiiert im Ernstfall sofortige Interventionsmaßnahmen – vom Kontaktieren der Polizei bis zur Alarmierung der Feuerwehr.



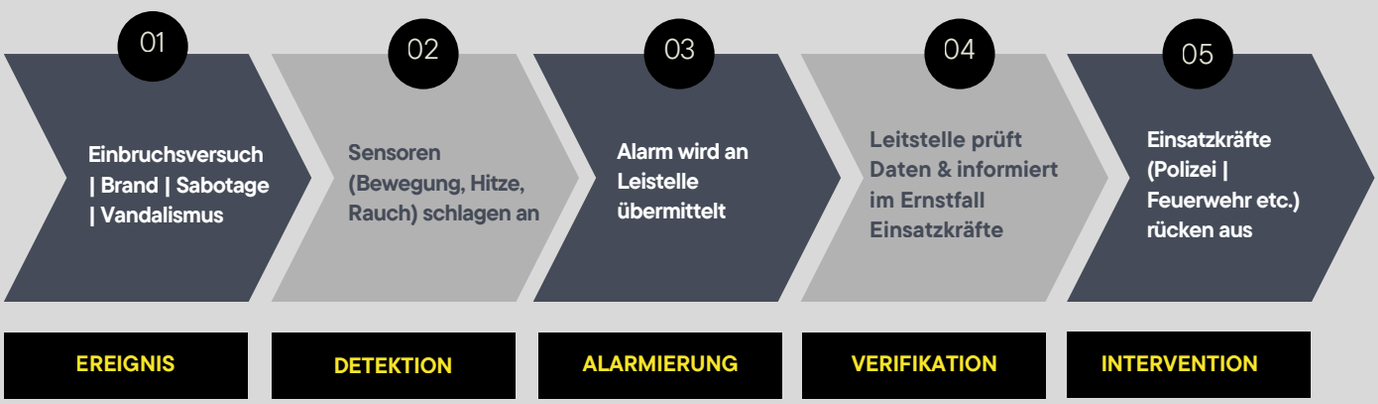
Ein System ist immer nur so sicher wie die Menschen und Prozesse, die es überwachen. Deshalb setzen wir auf permanente Verfügbarkeit, zertifizierte Qualität und aufeinander abgestimmte Technik.

Bastian Rauen,
videoalarm.de

DETEKTIEREN, ALARMIEREN, INTERVENIEREN

Herzstück vieler Sicherheitskonzepte ist das Alarmsystem videoalarm.de – eine drahtlose Funkalarmanlage mit integrierter Videoübertragung und direkter Leitstellenanbindung. Das Prinzip folgt einem klaren Dreiklang: Detektieren, alarmieren, intervenieren.

Löst ein Bewegungsmelder aus, sendet das System automatisch eine kurze Videosequenz an die VdS-zertifizierte Leitstelle, wo das Material sofort analysiert wird. Fehlalarme werden zuverlässig ausgeschlossen, und im Ernstfall erfolgt die Alarmierung von Einsatzkräften (Polizei, Feuerwehr, etc.) binnen Sekunden.



Ein besonderer Vorteil: Das System arbeitet DSGVO-konform – Videosequenzen werden ausschließlich im Alarmfall übertragen. Zusätzlich ist videoalarm.de modular erweiterbar, etwa um das **Sicherheitspaket „Blackout“** mit aktiver Innenraumvernebelung. Im Alarmfall füllt dichter Nebel binnen Sekunden die Räume, nimmt Eindringlingen jede Orientierung und verhindert Diebstahl oder Vandalismus.

Für temporäre oder schwer zugängliche Areale gibt es das System auch als **mobile Version „dein-bauwaechter.de“** – kompakt, autark und ideal für Baustellen, Lagerhallen oder Freiflächen ohne Netz- oder Stromanbindung.

Robust, vielseitig, abschreckend die dein-bauwaechter.de Turmlösung.

TECHNOLOGIE & INNOVATION

KI IM EINSATZ – INTELLIGENTE SICHERHEIT MIT WEITBLICK

Künstliche Intelligenz revolutioniert den Objektschutz: Moderne Kameras werten Bilddaten direkt im Gerät aus und erkennen in Sekunden, ob eine Bewegung relevant oder harmlos ist. So wird aus passiver Überwachung aktive Prävention – ein Meilenstein für KRITIS-Betreiber, die auf Zuverlässigkeit und Echtzeitreaktion setzen.

Moderne Sicherheitsarchitektur setzt heute auf künstliche Intelligenz – nicht als Zusatz, sondern als Kernkomponente. Die intelligenten Kamerasysteme von videoalarm.de analysieren Bilddaten direkt im Gerät und erkennen in Sekundenbruchteilen, ob eine Bewegung oder Veränderung tatsächlich eine Gefahr darstellt. So werden Fehlalarme drastisch reduziert und Einsatzkräfte gezielt informiert.

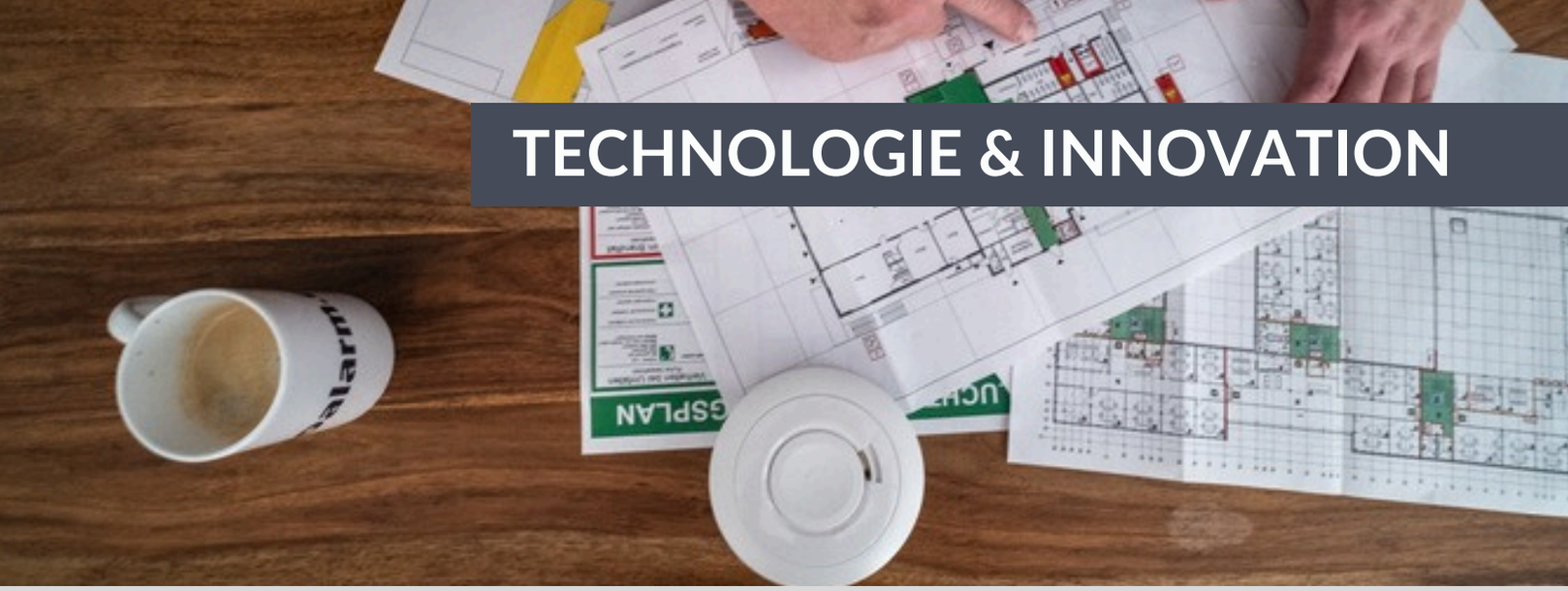
Besonders in weitläufigen oder sensiblen KRITIS-Arealen liefert die Kombination aus Echtzeitbildern und KI-basierter Bewertung einen entscheidenden Vorsprung: Risiken werden erkannt, bevor sie zu Vorfällen werden. Das Ergebnis ist eine präzise, datenschutzkonforme Überwachung – effizient, vorausschauend und ressourcen-schonend.

PRAXISNUTZEN

Die Kombination aus KI, Live-Video und Leitstellenanbindung schafft ein adaptives Frühwarnsystem, das Risiken erkennt, bevor sie zu Störungen oder Angriffen führen – und damit wertvolle Reaktionszeit gewinnt. Durch die automatische Priorisierung von Ereignissen werden Fehlalarme reduziert und Einsatzkräfte gezielt dorthin gelenkt, wo tatsächlich Handlungsbedarf besteht. Gleichzeitig ermöglicht die Videoanalyse eine lückenlose Dokumentation für Nachverfolgung, Beweisführung und Optimierung von Sicherheitsprozessen.

VORZÜGE AUF EINEN BLICK

- Frühzeitige Gefahrenerkennung durch KI-basierte Bildanalyse.
- Reduzierung von Fehl- und Falschalarmen.
- Sofortige Alarmverifizierung in der Leitstelle.
- Datenschutzkonforme Echtzeitüberwachung.
- Ideal für großflächige oder kritische Infrastrukturen.



TECHNOLOGIE & INNOVATION

BRANDSCHUTZ 4.0: FRÜHWARNUNG, DIE LEBEN RETTET

In kritischen Infrastrukturen kann ein Brand weit mehr als nur Sachschäden verursachen – er gefährdet Menschenleben, Versorgungssicherheit und Betriebsstabilität ganzer Regionen. Entsprechend hoch sind die Anforderungen an moderne Brandfrüherkennungssysteme. videoalarm.de setzt hier auf ein intelligentes Zusammenspiel aus Thermalkamera-basierter Früherkennung und zertifizierter Brandwarntechnik nach VDE V 0826-2.

Bereits in der Entstehungsphase registrieren hochempfindliche Thermalkameras minimale Temperaturveränderungen, die für das menschliche Auge noch unsichtbar sind. Die Systeme erkennen Hitzequellen und thermische Anomalien frühzeitig – noch bevor Rauch oder offene Flammen entstehen. In Sekunden werden diese Informationen an die ständig besetzte Leitstelle übertragen, wo die Daten in Echtzeit analysiert und bewertet werden.
So kann die Feuerwehr oder das interne Einsatzteam zielgenau und schnell informiert werden: mit präziser Angabe, wo sich ein Brand entwickelt und wie er sich ausbreitet.

Ajax EN54 Line – zertifizierte Brandwarnanlage für Gewerbe und Kommunen / BWA gemäß VDE V 0826-2

Vernetzte Sicherheit mit AJAX-Brandwarnanlage nach VDE V 0826-2

Ein zentraler Bestandteil der Brandschutzstrategie ist die Integration der AJAX-Brandwarnanlage, die nach VDE V 0826-2 ausgelegt ist – der maßgeblichen Richtlinie für funkvernetzte Brandwarnsysteme in Nichtwohngebäuden und Sonderbauten. Diese Norm legt fest, dass solche Systeme eine zuverlässige, dauerhafte Alarmierung und Übertragung gewährleisten müssen – inklusive sicherer Funkkommunikation, Echtzeitstatus und kontinuierlicher Selbstüberwachung.

TECHNOLOGIE & INNOVATION

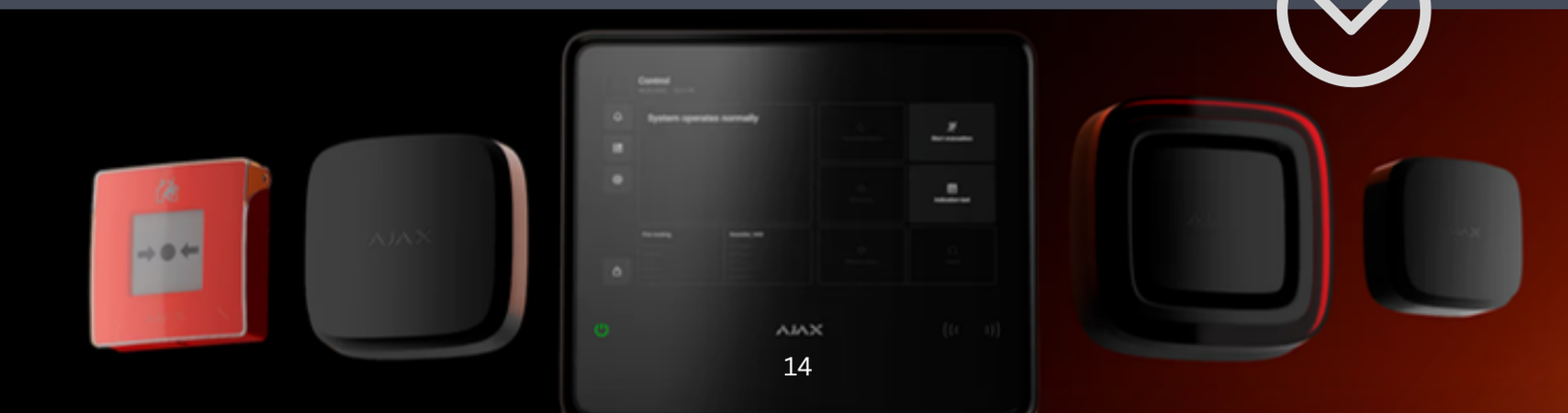
Das System von AJAX erfüllt diese Anforderungen nicht nur, sondern geht technisch noch darüber hinaus: Funkvernetzte Rauch-, Wärme- und Kohlenmonoxidmelder bilden ein intelligentes, selbstüberwachendes Netzwerk. Sie kommunizieren drahtlos miteinander, erkennen Brandereignisse sekundenschnell und alarmieren mehrstufig – akustisch vor Ort, digital über App und cloudbasiert an die Leitstelle.

Früherkennung als Schlüsselfaktor für Resilienz

Mit der Verbindung aus Thermaltechnologie, KI-gestützter Analyse und normkonformer Brandwarntechnik schafft videoalarm.de eine neue Qualität der Brandsicherheit im KRITIS-Umfeld. Das System erkennt Brände, bevor sie entstehen, alarmiert, bevor Menschen gefährdet werden – und schützt damit, was im Ernstfall unbezahlbar ist: Zeit, Leben und Infrastruktur.

VORZÜGE AUF EINEN BLICK

- Normkonforme Sicherheit: Vollständige Übereinstimmung mit VDE V 0826-2 für Brandwarnanlagen in gewerblichen und öffentlichen Gebäuden.
- Doppelte Sicherheitsebene: Kombination aus lokaler Alarmierung und zentraler Leitstellenanbindung.
- Keine Verkabelung notwendig: Ideal für Nachrüstungen, modulare Gebäude und Außenbereiche.
- Zuverlässige Funkkommunikation: Auch bei Strom- oder Netzwerkausfall bleibt das System aktiv.
- Minimierung von Falschalarmen: Intelligente Sensorfusion analysiert Rauch, Temperatur und Gaskonzentration gemeinsam.
- Cloudbasierte Überwachung: Permanente Kontrolle und Wartung aus der Ferne – revisionssicher und datenschutzkonform.



TECHNOLOGIE & INNOVATION

PERIMETERSCHUTZ – SICHERHEIT BEGINNT AM RAND

Perimeterschutz bildet die erste Verteidigungslinie im Sicherheitskonzept kritischer Infrastrukturen. Hochsensible Sensoren und Analysesysteme erfassen Bewegungen, Vibrationen und Annäherungen zuverlässig – und unterscheiden automatisch, ob es sich um Menschen, Tiere oder Fahrzeuge handelt. So entsteht ein präzises, lückenloses Frühwarnsystem entlang der äußeren Grenzen eines Areals.

Ein wirksamer Schutz kritischer Infrastrukturen beginnt an der äußeren Grenze eines Areals – dort, wo erste Annäherungen erkannt und abgewehrt werden müssen. Die Perimetersysteme von videoalarm.de detektieren Bewegungen, Vibrationen und Erschütterungen zuverlässig und können dank intelligenter Sensorik unterscheiden, ob es sich um Personen, Fahrzeuge oder Tiere handelt. So lassen sich Fehlalarme minimieren und potenzielle Eindringlinge schon vor dem eigentlichen Zugriff stoppen. Die Systeme arbeiten autark, sind flexibel skalierbar und lassen sich nahtlos in übergeordnete Sicherheitsnetzwerke integrieren. Damit wird der Perimeterschutz zum ersten, aber entscheidenden Baustein einer mehrstufigen Sicherheitsstrategie für KRITIS-Betreiber.

PRAXISNUTZEN

Gerade für Energieparks, Kläranlagen oder großflächige Betriebsgelände ist der Perimeterschutz ein unverzichtbarer Bestandteil moderner Sicherheitsstrategien – er stoppt Gefahren dort, wo sie entstehen.

VORZÜGE AUF EINEN BLICK

- Frühzeitige Erkennung von Annäherungen und Eindringversuchen.
- Intelligente Differenzierung von Mensch, Tier und Fahrzeug.
- Minimierung von Fehlalarmen durch präzise Sensorik.
- Autarkes, flexibel skalierbares Systemdesign.
- Integration in bestehende Sicherheitsarchitekturen.

RESILIENZ DURCH VERNETZUNG UND SERVICE

VIDEOALARM.DE

- Intelligente ganzheitliche Konzepte.
- Entwicklung herstellerunab-hängigen Lösungen, die optimal an die konkreten Erfordernisse angepasst sind.
- Know-how vom Schutzkonzept bis zur Inbetriebnahme unterschiedlicher Systeme.
- Ein Ansprechpartner bei der Planung und Umsetzung auch komplexere Projekte.
- Breites Portfolio für vielfältige Anforderungen.
- Integration bereits bestehender Infrastrukturen.
- Durchgängiges Servicekonzept mit einem breiten Portfolio an Dienstleistungen.
- Serviceverfügbarkeit 24/7.
- Erfüllung aktueller Normen und Richtlinien.

Was die Lösungen von videoalarm.de besonders auszeichnet, ist die Verknüpfung von Technologie, Dienstleistung und Strategie. Von der ersten Risikoanalyse über die Projektierung bis zur 24/7-Wartung kommt alles aus einer Hand.

Bestehende Infrastrukturen werden integriert, neue Komponenten intelligent ergänzt – ohne Systembrüche oder Schnittstellenprobleme. Mit dieser Philosophie positioniert sich das Unternehmen als einer der wenigen Anbieter, die den KRITIS-Schutz ganzheitlich denken: von der physischen Sicherung über den Datenschutz bis hin zur operativen Resilienz.

IM GESPRÄCH MIT DEM BSKI ÜBER DAS KRITIS-DACHGESETZ UND DIE ZUKUNFT DES INFRASTRUKTURSCHUTZES

Deutschland steht an einer sicherheitspolitischen Wegmarke. Mit dem KRITIS-Dachgesetz will die Bundesregierung erstmals alle wesentlichen Betreiber kritischer Infrastrukturen in einem bundeseinheitlichen Rechtsrahmen zusammenführen – und den Fokus von der Cyberabwehr hin zum physischen Schutz und zur Resilienz erweitern. Doch was bedeutet das in der Praxis für Unternehmen, Versorger und öffentliche Einrichtungen? Welche Pflichten kommen auf Betreiber zu – und welche Chancen bietet das Gesetz für einen zeitgemäßen Schutzsystemansatz?

Wir sprachen mit Holger Berens, Vorstandsmitglied des Bundesverbandes für den Schutz Kritischer Infrastrukturen e.V. (BSKI), über den aktuellen Stand des Gesetzgebungsverfahrens, typische Stolpersteine bei der Umsetzung und die Trends, die den Infrastrukturschutz der Zukunft prägen werden.

Herr Berens, das KRITIS-Dachgesetz soll den Schutz kritischer Infrastrukturen in Deutschland auf eine neue Grundlage stellen. Wie bewerten Sie den aktuellen Gesetzesentwurf – ist er ein echter Fortschritt oder eher ein bürokratischer Balanceakt?

Holger Berens: Der Gesetzesentwurf ist ein echter Fortschritt, denn er schließt eine regulatorische Lücke, bringt physischen Schutz auf Augenhöhe mit IT-Sicherheitsregelungen, schafft Durchsetzungsinstrumente und harmonisiert nationales Recht mit EU-Vorgaben.
Gleichzeitig ist das Vorhaben ein bürokratischer Balanceakt, weil der Erfolg nicht allein am Gesetzestext hängt, sondern maßgeblich von klaren Schnittstellenregelungen, praktikablen Definitionen, Vollzugsressourcen und flankierenden Unterstützungsmaßnahmen abhängt.

HOLGER BERENS
Vorstandsvorsitzender BSKI e.V.

IM INTERVIEW

Der BSKI hat sich früh in den Diskussionsprozess eingebracht. Welche Punkte aus Sicht der Sicherheitsfachverbände wurden im bisherigen Entwurf gut umgesetzt – und wo sehen Sie noch Nachbesserungsbedarf?

Holger Berens: Das KRITIS-Dachgesetz greift zentrale Forderungen der Sicherheitsfachverbände auf, etwa mehr Verbindlichkeit, klarere Mindeststandards und ein einheitlicher Ordnungsrahmen für den physischen Schutz. Damit wird die bislang zersplitterte Regulierung erstmals praktikabler – und für viele Betreiber überhaupt erst handhabbar. Als positiv zu bewerten ist, dass der Entwurf durchsetzbare Melde- und Nachweispflichten sowie Sanktionsmechanismen enthält. Dennoch bleibt er an vielen Stellen sehr abstrakt.

Nennen Sie doch ein paar Beispiele…

Holger Berens: Die vorgesehenen Schwellenwerte sind bislang zu stark an quantitativen Größen orientiert und bilden reale Systemabhängigkeiten nur unzureichend ab – kritische Punkte können so durchfallen. Auch die Risikoanalyse bleibt ohne klaren methodischen Rahmen zu vage; ohne vorgelagerte Risikoabschätzung fehlt vielen Einstufungen die Belastbarkeit.

Wo liegen Ihrer Einschätzung nach die größten praktischen Hürden?

Holger Berens: Die größte Hürde liegt in der abstrakten Ausgestaltung der Anforderungen. Deutschland hat Unternehmen über Jahre vor allem im Cyberbereich nach BSI-Logik reguliert – der physische Schutz wird jetzt erstmals umfassend und verpflichtend adressiert. Viele Betreiber müssen daher völlig neue Prozesse, Bewertungsmethoden und Verantwortlichkeiten aufbauen. Die Kombination aus abstrakten Vorgaben, fehlenden physischen Sicherheitsstandards und bislang cyberzentrierten Strukturen führt zu hoher Unsicherheit, wie Anforderungen konkret auszulegen sind.

Viele Verantwortliche fragen sich, was konkret auf sie zukommt. Welche ersten Schritte sollten Betreiber jetzt unternehmen, um sich rechtzeitig auf das Inkrafttreten des Gesetzes vorzubereiten?

Holger Berens: Wer bisher schon unter die BSI-Schwellen fiel, ist auch künftig betroffen – neu ist, dass weitere Sektoren in den regulatorischen Fokus rücken. Verantwortliche sollten aktiv werden. Der erste Schritt besteht darin, kritische Prozesse und die dazugehörigen Assets im eigenen Unternehmen systematisch zu identifizieren. Darauf aufbauend sollte eine ganzheitliche Risikoanalyse erfolgen, die nicht nur IT- und Cyberrisiken, sondern auch physische Bedrohungen berücksichtigt. Auf Basis dieser Analyse lassen sich gezielt Maßnahmen ableiten und priorisieren.

Wie gut sind Unternehmen hierzulande denn überhaupt auf physische Angriffe, Sabotage oder hybride Bedrohungen vorbereitet?

Holger Berens: Hier muss man zwischen offenen und geschlossenen Systemen unterscheiden. Geschlossene Systeme wie Rechenzentren oder Kraftwerke verfügen in der Regel über Perimeterschutz, Zutrittskontrollen, Videoüberwachung und klar definierte Sicherheitskonzepte – hier ist die Vorbereitung vergleichsweise gut. Bei offenen, großflächigen Infrastrukturen wie etwa dem Schienennetz, Stromleitungen oder Solarparks ist hundertprozentige Sicherheit naturgemäß schwierig. Wir leben in einer gefährlichen Zeit. Die geopolitische Lage, die verschärfte Bedrohungslage, zunehmende Sabotageakte und neue Gefahren – Stichwort Drohnen – stellen Unternehmen vor erhebliche Herausforderungen. Schutzmaßnahmen müssen über einzelne Anlagen hinausgehen: Redundanzen und Ausfallkonzepte sind nötig, damit kritische Systeme im Ernstfall weiter funktionsfähig bleiben.

> ***Wichtig ist, KRITIS-Schutz nicht isoliert zu betrachten, sondern ganzheitlich zu denken.***

Hat Deutschland beim KRITIS-Schutz verschlafen?

Holger Berens: Politisch ist der Handlungsbedarf ja längst erkannt, die Umsetzung hinkt jedoch hinterher: Ursprünglich sollte das KRITIS-Dachgesetz bereits im Oktober 2024 in Kraft treten, seit November liegen nun Bundesratsstatements vor – eine Verabschiedung ist aber frühestens im zweiten Quartal 2026 zu erwarten. Hier zeigt sich, dass die Politik zu spät reagiert und regulatorische Prozesse oft langwierig sind. Die wirtschaftliche Seite hingegen agiert proaktiver: Unternehmen haben schließlich ein ureigenes Interesse daran, sich zu schützen und setzen Maßnahmen bereits eigeninitiativ um, unabhängig von gesetzlichen Vorgaben.

Der Gesetzgeber spricht von „Resilienz“ als Leitprinzip. Was bedeutet Resilienz im praktischen Alltag – und wie lässt sie sich erreichen?

Holger Berens: Resilienz bedeutet die Fähigkeit, Störungen und Krisen zu widerstehen, sich schnell zu erholen und den Betrieb aufrechtzuerhalten. Praktisch zeigt sich das in klaren Notfallplänen, redundanten Systemen, geschultem Personal und einer kontinuierlichen Risikoanalyse. Wichtig ist, KRITIS-Schutz nicht isoliert zu betrachten, sondern ganzheitlich zu denken. Wesentlich sind drei Komponenten: Die physische Sicherheit, also bauliche, technische und operative Schutzmaßnahmen; die Informationssicherheit, das heißt die Umsetzung der NIS2-Richtlinie und kontinuierliche informations- sowie betriebstechnologische Sicherheitsmaßnahmen aber auch die Unternehmenskultur, Sensibilisierung, Qualifizierung und engagierte Unternehmensführung.

Das Gesetz sieht eine stärkere Rolle von Bund, Ländern, BSI und BBK vor. Wie wichtig ist aus Ihrer Sicht eine enge Kooperation zwischen Behörden, Betreibern und privaten Sicherheitsdienstleistern?

Holger Berens: Kooperation ist der Schlüssel. Resilienz lässt sich nur durch praktische Umsetzung, Erfahrungsaustausch und kontinuierliche Kommunikation realisieren – Gesetzestexte allein reichen nicht aus. In der Praxis hat sich gezeigt, dass starke Communities, Verbandsarbeit, Arbeitskreise und branchenspezifische Netzwerke wesentlich sind, um Standards zu definieren, Best Practices zu teilen und neue Bedrohungen frühzeitig zu adressieren. Veranstaltungen wie die *protekt* in Leipzig, die vom BSKI mit ausgerichtet wird, spielen dabei eine zentrale Rolle: Als Leitkonferenz für KRITIS-Experten bringt die *protekt* Behörden, Betreiber, Forschung und Sicherheitsindustrie zusammen, ermöglichet den direkten Dialog und fördert den praxisnahen Erfahrungsaustausch.
Gemeinsam mit dem *Bundesverband Sicherheitstechnik e.V.* (BHE) arbeitet das BSKI aktuell daran, konkrete Vorgaben für physische Sicherheit zu erstellen – mit dem Ziel, physische Sicherheitsstandards zu vereinheitlichen.

Wenn Sie den Blick nach vorn richten: Welche Trends oder Innovationen werden den KRITIS-Schutz in den nächsten Jahren am stärksten verändern?

Holger Berens: KI ist zweifelsohne der zentrale Treiber: KI-gestützte Risikoanalysen und Anomalieerkennung ermöglichen schon jetzt, Störungen frühzeitig zu identifizieren, bevor sie kritisch werden. Sensorische Videoüberwachung, Robotics und automatisierte Frühwarnsysteme werden an Bedeutung gewinnen und die operative Reaktionsfähigkeit erheblich steigern.
Durch Drohnen sind neue Bedrohungsszenarien entstanden: Sie können zwar verlässlich detektiert werden, es fehlt jedoch an effektiven Abwehrstrategien – hier sind in den kommenden Jahren innovative Lösungen zu erwarten. Insgesamt verschiebt sich der Fokus von reaktiver Sicherheit hin zu proaktiver, daten- und KI-gestützter Resilienz.

Vielen Dank für das Gespräch.

ÜBER DEN BSKI

Der Bundesverband für den Schutz Kritischer Infrastrukturen e.V. (BSKI) ist die zentrale Plattform für Betreiber, Hersteller, Sicherheitsdienstleister und Forschungseinrichtungen im Bereich KRITIS-Schutz. Der Verband bündelt Fachwissen, vertritt Betreiberinteressen gegenüber Politik und Behörden und fördert den interdisziplinären Austausch zwischen Wirtschaft, Wissenschaft und öffentlicher Hand.

www.bski.de

MISSION #SICHERESGERÄTEHAUS

Wenn Schutzräume selbst Schutz brauchen: In Hatzenport an der Mosel wurde das Feuerwehrgerätehaus der Freiwilligen Feuerwehr zum Vorreiterprojekt in Sachen Sicherheit. Im Rahmen des Leuchtturmprojekts „Sicheres Feuerwehrhaus“ stattete videoalarm.de die Einrichtung kostenfrei mit modernster Einbruch- und Brandmeldetechnik aus – ein starkes Signal für den Schutz kritischer Infrastruktur und das Ehrenamt zugleich.

Feuerwehrhäuser sind mehr als nur Gebäude – sie sind Dreh- und Angelpunkte lokaler Gefahrenabwehr. Wenn sie beschädigt oder gar zerstört werden, stehen ganze Gemeinden im Ernstfall ungeschützt da. Genau hier setzt das Projekt an: Das Gerätehaus der Freiwilligen Feuerwehr Hatzenport (Mosel, Rheinland-Pfalz) wurde im Frühjahr 2025 mit einem vernetzten Einbruch- und Brandmeldesystem ausgestattet, das 24 Stunden am Tag mit einer zertifizierten Notruf- und Serviceleitstelle verbunden ist.

Intelligente Rauch- und Hitzemelder, Bewegungsdetektoren und eine Echtzeit-Alarmübertragung sorgen dafür, dass jede Unregelmäßigkeit sofort erkannt und bewertet wird. So bleibt die Einsatzfähigkeit der Feuerwehr jederzeit gewährleistet – selbst dann, wenn kein Kamerad vor Ort ist.

BEDROHUNGSLAGEN & TRENDS

Ein Projekt mit Herz und Verantwortung

Initiiert wurde die Maßnahme von videoalarm.de, einem Unternehmen mit jahrzehntelanger Erfahrung im Bereich sicherheitstechnischer Lösungen für Unternehmen, Behörden und kommunale Einrichtungen. Für Geschäftsführer Bastian Rauen ist das Projekt mehr als ein technischer Beitrag – es ist ein persönliches Anliegen:
„Feuerwehrhäuser sind Herzstücke unserer Sicherheitsstruktur – sie müssen einsatzbereit und geschützt sein. Als Sicherheitsdienstleister sehen wir es als unsere Verantwortung, ein Bewusstsein dafür zu schaffen, wie wichtig es ist, solche sensiblen Einrichtungen abzusichern. Mit unserem System leisten wir einen aktiven Beitrag zum Schutz der Einsatzkräfte und der Bevölkerung.“

Rauen weiß, wovon er spricht – er war selbst über 20 Jahren ehrenamtlich in der Freiwilligen Feuerwehr aktiv. *„Durch mein eigenes Engagement kenne ich die Herausforderungen aus erster Hand. Dieses Projekt liegt mir auch persönlich am Herzen.“*

HINTERGRUND

Feuerwehrgerätehäuser sind zunehmend Ziel krimineller Angriffe und schwerwiegender Brandereignisse. Einzelne Polizeimeldungen belegen eine steigende Anzahl von Einbrüchen, bei denen wichtige Rettungsgeräte wie Spreizer oder hydraulische Scheren gestohlen wurden. Diese Geräte sind nicht nur materiell wertvoll, sondern essenziell für Einsätze, etwa bei Verkehrsunfällen. Parallel dazu gab es auch in 2025 wieder Brandfälle mit enormem Schaden: In Stadtallendorf brannte ein Feuerwehrhaus neueren Datums komplett ab (Sachschaden über 20 Mio. €), in Treffurt zerstörte ein Brand ein Gerätehaus mit fünf Fahrzeugen (rund 7 Mio. € Schaden). Das Risiko ist nicht ausschließlich lokal – vielmehr spiegelt es ein strukturelles Problem: Viele Gerätehäuser sind nachts unbesetzt, was Tätern eine große Chance bietet. Gleichzeitig fehlen vielerorts flächendeckend zuverlässige Statistiken, weil solche Delikte nicht gesondert systematisch erfasst werden. Der Deutsche Feuerwehrverband und die Vereinigung zur Förderung des Deutschen Brandschutzes (vfdb) arbeiten aktiv daran, mit der „Deutschen Brandstatistik“ genau das zu ändern und zukünftig belastbare Daten für alle Feuerwehren bereitzustellen.
Fakt ist: Die Gefahr von Einbruch und Brand in Feuerwehrhäusern ist real – und Maßnahmen zur Sicherung dieser kritischen Infrastruktur werden dringlicher denn je.

Ein Gewinn für Ehrenamt und Bevölkerung

Auch vor Ort ist die Freude groß. Für die Freiwillige Feuerwehr Hatzenport bedeutet die neue Sicherheitsausstattung ein Stück mehr Ruhe – und Wertschätzung für das, was sie leisten.
Das Projekt zeigt, dass die Arbeit der ehrenamtlichen Helferinnen und Helfer gesehen wird – und dass Sicherheit auch für sie kein Zufall sein darf.

> ***Für uns Ehrenamtliche ist es eine große Erleichterung, zu wissen, dass unser Gerätehaus jetzt rund um die Uhr überwacht wird. Das stärkt unsere Einsatzfähigkeit und gibt uns Sicherheit.***
>
> Christian Ostrowski,
> Wehrführer Löschgruppe Hatzenport

Dank der modernen Sicherheitslösung können die Einsatzkräfte im Brandfall schneller reagieren und Schäden effektiv verhindern. Die Alarmmeldungen werden in Echtzeit weitergeleitet, sodass bei Bedarf sofort entsprechende Maßnahmen ergriffen werden können. Gleichzeitig bietet das System Schutz vor unbefugtem Zugriff und Vandalismus, was den langfristigen Werterhalt der Ausrüstung sichert. Neben der Sicherheit für die Feuerwehrleute selbst profitieren auch die Bürgerinnen und Bürger von der verlässlicheren Einsatzbereitschaft. Ein echter Gewinn für die gesamte Gemeinde.

Für die Sicherung des Feuerwehrhauses nebst Einsatzfahrzeug, Gerätschaften & Ausrüstung wurden verbaut:

6 Rauchmelder
2 Kameramelder
1 Zentraleinheit mit Bedienteilen nach DIN Grad 2

BEDROHUNGSLAGEN & TRENDS

Vorbild mit Signalwirkung

Das Projekt ist bewusst als Leuchtturmprojekt angelegt – mit dem Ziel, bundesweit Nachahmer zu finden. Denn in den vergangenen Monaten kam es deutschlandweit vermehrt zu Bränden und Einbrüchen in Feuerwehrgerätehäusern. Die Folgen: beschädigte Einsatzfahrzeuge, ausgefallene Technik – und gefährdete Reaktionsfähigkeit im Ernstfall.

Mit dem Projekt #SicheresGerätehaus will videoalarm.de zeigen, wie moderne Sicherheitstechnik helfen kann, Einsatzbereitschaft, Infrastruktur und Ehrenamt gleichermaßen zu schützen.

„*Wir hoffen, dass dieses Projekt Schule macht – in Rheinland-Pfalz, aber auch weit darüber hinaus*“, sagt Bastian Rauen. „*Sicherheit beginnt dort, wo diejenigen geschützt werden, die täglich für unsere Sicherheit sorgen.*“

#SICHERESGERÄTEHAUS

EIN SICHERES GERÄTEHAUS – DAS IST NICHT NUR EIN PROJEKT, SONDERN EIN MISSION: SICHERHEIT FÜR DIE, DIE SICHERHEIT GEBEN.

Fazit: Ein Modell, das Schule machen sollte

Das Leuchtturmprojekt in Hatzenport steht sinnbildlich für die Zukunft kommunaler Sicherheitsarchitektur: intelligent, vernetzt, praxisnah. Durch die Kombination aus Brandwarn- und Einbruchmeldetechnik, Leitstellenanbindung und ehrenamtlichem Engagement wird sichtbar, wie moderne Technologie echten gesellschaftlichen Mehrwert schaffen kann.

ABSICHERUNG EINES SOLARPARKS MITTELS PERIMETERSCHUTZ

Photovoltaikanlagen zählen zu den zentralen Pfeilern der Energiewende – und damit auch zu den sensiblen Objekten der kritischen Infrastruktur. Der betreffende Solarpark in St. Wedel/ Saarland produziert jährlich 3,3 Millionen Kilowattstunden Strom und umfasst 14 600 Solarmodule auf einer Freilandfläche von mehreren Hektar. Eine Herausforderung für jeden Sicherheitsplaner: das gesamte Gelände effektiv gegen Sabotage, Einbruch, Diebstahl und Vandalismus abzusichern – bei gleichzeitigem Anspruch an Wirtschaftlichkeit, Nachhaltigkeit und Systemintegration.

DIE AUFGABE

SCHUTZ EINES ENERGIEVERSORGERS UNTER KRITIS-BEDINGUNGEN

Energieparks gelten als besonders gefährdete Objekte – nicht nur wegen des materiellen Werts der Komponenten, sondern auch aufgrund ihrer strategischen Bedeutung für die Stromversorgung. Ziel war es daher, den Solarpark so zu sichern, dass potenzielle Angriffe bereits an der Außengrenze erkannt und gestoppt werden.

DIE LÖSUNG

INTELLIGENTE VERNETZUNG VON PERIMETERSCHUTZ UND VIDEOANALYSE

videoalarm.de entwickelte ein mehrstufiges Sicherheitskonzept, das Zaundetektion und KI-gestützte Videoerkennung zu einem geschlossenen, autarken Schutzsystem verbindet. Für eine durchgehende Sicherung des gesamten Außengeländes setzt das System auf Infrarot- und Mikrowellentechnik, die in regelmäßigen Abständen von etwa 28 Metern installiert ist. So bleibt das Objekt selbst bei widrigen Wetterbedingungen wie Regen, Nebel oder starken Lichtwechseln zuverlässig geschützt.
Sobald eine der Komponenten eine Auffälligkeit registriert, wird eine Live-Videosequenz in Echtzeit an die zertifizierte Notruf- und Serviceleitstelle übermittelt. Dort bewertet geschultes Leitstellenpersonal die Lage und leitet unmittelbar die vereinbarten Interventionsmaßnahmen ein – ob Polizei, Sicherheitsdienst oder Betreiberalarmierung.

BEST PRACTICES

DAS VORGEHEN

VON DER ANALYSE ZUR UMSETZUNG

Bereits in der Planungsphase führte videoalarm.de eine detaillierte Risikoanalyse und eine Vor-Ort-Begehung durch. Gemeinsam mit dem Betreiber wurden konkrete Sicherheitsziele und Prioritäten definiert. Auf dieser Basis entstand ein individuell zugeschnittenes Konzept, das technische Präzision mit organisatorischer Klarheit verbindet.

Neben der Installation modernster Hardware legte das Unternehmen besonderen Wert auf Skalierbarkeit und Zukunftsfähigkeit: Das System kann bei Bedarf erweitert oder an neue Flächenmodule angepasst werden – ohne Systembruch oder zusätzliche Verkabelung.

DAS ERGEBNIS

FRÜHWARNSYSTEM MIT 360°-RUNDUMSCHUTZ

Heute ist der Solarpark durch ein engmaschiges, KI-gestütztes Überwachungssystem geschützt, das nicht nur erkennt, sondern aktiv reagiert. Fehlalarme sind nahezu ausgeschlossen, die Reaktionszeiten minimal. Dank der intelligenten Vernetzung von Sensorik, Video und Leitstelle erfüllt das Projekt höchste Anforderungen an KRITIS-Schutz und Datenschutz gleichermaßen.

Das Ergebnis: maximale Sicherheit bei minimalem Personalaufwand – und ein Best-Practice-Beispiel dafür, wie moderner Perimeterschutz im Energiesektor aussehen kann.

SICHERHEIT IST EIN PROZESS

Mit dem Projekt im Saarland zeigt videoalarm.de, wie sich technologische Innovation und operative Resilienz vereinen lassen. Der Solarpark in St. Wedel gilt heute als Referenzanlage für effizienten, daten-getriebenen Perimeterschutz im KRITIS-Sektor Energie – und als Beleg dafür, dass intelligente Sicherheitstechnik die Basis einer stabilen Energiezukunft ist.

Die Herausforderungen an den Infrastruktur-schutz wachsen – nicht nur technisch, sondern auch regulatorisch. Unternehmen, die hier Verantwortung übernehmen, müssen Systeme entwickeln, die verlässlich, adaptiv und zukunftsfähig sind.

videoalarm.de zeigt, wie das gelingt: mit modularen Sicherheitslösungen, durchgängiger Servicearchitektur und einem tiefen Verständnis für die komplexen Anforderungen moderner KRITIS-Betreiber. Sicherheit wird hier nicht als starres System verstanden, sondern als lebendiger Prozess, der sich mit jeder Innovation weiterentwickelt.

> ***Was früher Sicherheit war, ist heute Resilienz. Und Resilienz beginnt dort, wo Technologie auf Verantwortung trifft.***

Bastian Rauen,
videoalarm.de

videoalarm.de

DER SICHERHEITSEXPERTE

R2 ÜBERWACHUNGSTECHNIK GMBH / VIDEOALARM.DE

Telefon/
0261 - 89 99 99 0

Email/
info@videoalarm.de

Website/
www.videoalarm.de

Standorte/

Niederlassung West:
Mainzer Str. 44
56068 Koblenz

Niederlassung Ost:
Gasanstalt 1A
06311 Helbra