34. JAHRGANG | Dezember 2025 | AUSGABE 12 | 17 €

GIT SICHERHEIT

30 926

MAGAZIN FÜR SAFETY UND SECURITY

Ausgabe ONLINE lesen:

Titelthema ab Seite 28:

Auf dem Weg zur ISO 27001

Florian Rabe: IT-Sicherheit als strategischer Pfeiler von GU BKS SERVICE

HEFT IM HEFT

EINBRUCH
PERIMETER
ZUTRITT
ab S. 32

WILEY

interflex
UPGRADES YOUR WORK

Zutritt. Sicher. Steuern.

Jetzt mehr erfahren.

Lösungen der Zutrittskontrolle für den Schutz kritischer Infrastrukturen

Als erfahrener KRITIS-Partner unterstützen wir seit 50 Jahren branchenübergreifend bei der Umsetzung gesetzlicher und individueller, betrieblicher Sicherheitsanforderungen.

- **Flexibles Software-System IF-6040** – Mit der modular erweiterbaren, cloudfähigen Plattform erfüllen Sie aktuelle Sicherheitsanforderungen (aus NIS2, KRITIS-DG und CRA) und schützen Ihr Personal, Vermögenswerte und kritische Anlagen.
- **Modernes Identitäts- und Berechtigungsmanagement** – Behalten Sie den Überblick über das Sicherheitskonzept Ihrer Organisation und erhalten Sie für Audits lückenlos nachprüfbare, DSGVO-konforme Zutrittsreports.
- **Breites Portfolio an Zugangskomponenten** – Die Kombination aktueller Sicherheitstechnologien mit den batteriebetriebenen, elektronischen Schließkomponenten sowie die hohe Integrationsfähigkeit mit weiteren Sicherheitsmaßnahmen bringt Ihnen nachhaltigen Investitionsschutz und erhöht den Schutzlevel für Ihre Organisation.
- **Inhouse-Services** – Mit der Interflex-Gesamtlösung setzen Sie auf Sicherheitslösungen aus einer Hand, sowie einem Rund-um-Service von Beratung über Konfiguration und Implementierung bis zur Wartung.

A BRAND OF ALLEGION

Interflex Datensysteme GmbH · 07 11 / 13 22-0 · www.interflex.com

Chefsache Sicherheit

Du liebe Zeit, schon wieder Dezember. Während draußen die letzten Blätter fallen und die ersten Lebkuchen im Büro verschwinden, drehen wir in der Sicherheitsbranche noch einmal richtig auf. Denn eines ist sicher: Das Jahr 2025 hatte es in sich – und das nicht nur, weil die Passwort-Post-its langsam ausgehen.

Bevor wir alle in den wohlverdienten Winterschlaf oder zumindest in die Feiertage abtauchen, werfen wir gemeinsam einen Blick auf die Highlights dieser Ausgabe.

Gleich auf Seite 10 wartet ein Interview mit Sven Dawson, dem Sicherheitschef von Airbus Defence and Space. Hier geht's nicht um Flugmeilen, sondern um echte Sicherheit: Wie schützt man eigentlich ein Unternehmen, das zwischen Kampfjet und Weltraumforschung alles abdeckt? Und wie bleibt man dabei noch souverän, wenn die Weltlage alles andere als ruhig ist? Lesenswert – nicht nur für Luftfahrt-Fans.

Ein weiteres Highlight ist das Ranking der führenden Sicherheitsdienstleister in Deutschland auf Seite 20. Die Lünendonk-Liste zeigt nicht nur die aktuellen Marktbewegungen, sondern beleuchtet auch, wie Digitalisierung, Robotik und Fachkräfteentwicklung die Branche nachhaltig verändern. Die Studie macht deutlich, dass moderne Sicherheitsdienstleistungen heute weit mehr sind als klassische Bewachung – sie sind technologiegestützt, vernetzt und integraler Bestandteil unternehmerischer Wertschöpfung.

Unser Titelthema ab Seite 28 nimmt Sie mit zu GU BKS Service. Hier dreht sich alles um Informationssicherheit und den Weg zur ISO 27001. Klingt trocken? Ist es ganz und gar nicht! Denn hier wird gezeigt, wie man aus einer Norm ein echtes Erfolgsprojekt macht – und warum Vertrauen und Verantwortung dabei mehr sind als nur Buzzwords.

Ab Seite 32 gibt's das „Heft im Heft: Einbruch, Perimeter, Zutritt". Besonders ans Herz legen möchten wir Ihnen beispielsweise das Interview mit Prof. Andreas Hasenpusch (S. 32). Hier erklärt er, warum Perimeterschutz heute mehr ist als ein Zaun mit Alarmanlage. Auf Seite 36 erläutern wir mit Heiko Viehweger, wie moderner Perimeterschutz wirklich funktioniert – Stichwort: Sensorik, Datenmanagement und ein bisschen Hightech-Zauberei. Und auf Seite 42 wird gezeigt, wie Photovoltaik-Anlagen nicht nur Strom, sondern auch Sicherheit liefern – mit smarter Schließtechnik und cleveren Zutrittskonzepten.

Wer zwischendurch Hunger bekommt, sollte auf Seite 58 vorbeischauen: Dort geht's um Brandschutz in der Gastronomie. Wie man ein historisches Amtshaus in ein modernes Dorfgasthaus verwandelt und dabei den Denkmalschutz nicht in Flammen aufgehen lässt – das ist nicht nur für Architekten spannend.

OT-Fans kommen auf Seite 62 auf ihre Kosten: OT-Security, IEC 62443 und die Frage, wie Produkthersteller ihre Entwicklung wirklich sicher machen. Acht „Practices", die nicht nur für Nerds interessant sind.

Und weil Sicherheit auch tragbar sein muss, gibt's auf Seite 70 unseren großen Produktvergleich Schutzjacken. Multinorm, multitalentiert, multistylish – hier finden Sie garantiert die richtige Jacke für jeden Einsatz. Und falls Sie sich fragen, ob das alles wirklich bequem ist: Probieren geht über Studieren.

Zum Schluss bleibt uns in der Redaktion nur eines: Danke zu sagen. Für Ihre Treue, liebe Leserinnen und Leser, für Ihr Feedback und Ihre Neugier. Ohne Sie wäre die GIT SICHERHEIT nur halb so spannend – und vermutlich auch nur halb so sicher.

Kommen Sie gut durch den Jahreswechsel, bleiben Sie gesund und neugierig – und freuen Sie sich mit uns auf ein sicheres, innovatives und vielleicht auch ein bisschen entspannteres 2026! GIT

Herzlichst, Ihr

Steffen Ebert
für das Team GIT SICHERHEIT

TITELTHEMA

Auf dem Weg zur ISO 27001

Informationssicherheit als strategischer Pfeiler von GU BKS SERVICE

ab Seite 28

GIT-SICHERHEIT.DE/DE/PRODUKTE
PRODUCTS FOR PROFESSIONALS
Produkt- und Lead-Plattform für Sicherheit

Sven Dawson

Boris Bärmichl

Florian Rabe

Andreas Hasenpusch

MANAGEMENT

HEFT IM HEFT | EINBRUCH I PERIMETER I ZUTRITT

Heiko Viehweger

Andreas Bollu

Mark Heim

CYBER-SECURITY

BRANDSCHUTZ

RUBRIKEN

SAFETY

INDEX

QUICK-FINDER

ORGANISATIONEN, INSTITUTIONEN UND UNTERNEHMEN IM HEFT

NEWS

Florent Badiou übernimmt die Leitung von Slat

Mit über 20 Jahren Erfahrung in der Industriebranche übernimmt Florent Badiou die Position des CEO bei Slat. Seine Laufbahn ist geprägt von Führungsverantwortung in Frankreich und Europa, stets mit der Überzeugung, dass nachhaltiger Erfolg auf Zuhören, klaren Zielen und der Stärke des Teams beruht.

Florent Badiou

Bei Fagerhult (Premium-Hersteller von Beleuchtungslösungen), verantwortete er die Aktivitäten in Frankreich und Südeuropa, leitete die kommerzielle Strategie, steuerte die finanzielle Performance und trieb das internationale Wachstum voran. Zuvor war er in leitender Position bei der Aldes-Gruppe tätig (Spezialist für Lüftungs- und Wohnkomfortlösungen), wo er Transformationsprojekte realisierte, Supply-Chain-Strukturen aufbaute und marktorientierte Vertriebsmodelle im Bereich Brandschutz und Lüftung erfolgreich umsetzte. Diese Stationen prägten seinen ganzheitlichen Blick von der Analyse der Markterwartungen bis zur operativen Umsetzung.

Slat stehe für Qualität, Zuverlässigkeit und technologische Exzellenz in der sicheren Stromversorgung kritischer Infrastrukturen, so Florent Badiou. Ihn begeistere die Fähigkeit des Unternehmens, technisches Know-how, Agilität und Kundennähe zu verbinden, ein Fundament, das man gemeinsam weiter ausbauen werde. Als CEO verfolge er drei klare Ziele: die Präsenz von Slat auf strategischen europäischen Märkten, insbesondere in Deutschland, zu stärken, Innovationen in enger Zusammenarbeit mit Partnern zu beschleunigen und eine einwandfreie Umsetzung in allen Kundenprojekten sicherzustellen.

Die Sicherheitsbranche sieht er mit tiefgreifenden Veränderungen und gleichzeitig spannenden Herausforderungen konfrontiert: zunehmende Anforderungen an Versorgungssicherheit, strengere Normen, die wachsende Bedeutung der Cybersicherheit sowie der Wandel hin zu mehr Energieeffizienz und Nachhaltigkeit. „Die Akteure müssen Lösungen entwickeln, die robust, interoperabel und zukunftsfähig sind. Slat ist genau an dieser Schnittstelle positioniert. Das macht diese Aufgabe so spannend“, so Florent Badiou. **www.slat.com/de**

Barox: Reinhard Florin wird Vice President of North America Sales

Die Barox Kommunikation GmbH baut ihre Vertriebsaktivitäten in Nordamerika auf. Dazu wurde Reinhard Florin zum Vice President of North America Sales berufen. In seiner neuen Rolle wird Reinhard Florin die Go-to-Market-Strategie für Nordamerika entwickeln und umsetzen sowie ein Team aus Vertriebs- und Support-Spezialisten führen. Mit dieser Verstärkung bringt das Unternehmen sein bewährtes Produktportfolio gezielt auf den nordamerikanischen Markt. Reinhard Florin hat mehr als 30 Jahre Erfahrung in leitenden Positionen im Bereich Netzwerktechnologie und einige der bekanntesten Marken maßgeblich geprägt, zuletzt als Global General Manager von Comnet by Acre. „Barox hat ein einzigartiges Portfolio an Netzwerkprodukten, das speziell auf die hohen Anforderungen von Video-Sicherheitsnetzwerken in kritischen Infrastrukturen zugeschnitten ist“, so Reinhard Florin. **www.barox.de**

Reinhard Florin

Deutsche Bundesministerin besuchte ACE Schmersal in Boituva

Im Vorfeld der Weltklimakonferenz COP30 in Belém besuchte die deutsche Bundesministerin für wirtschaftliche Zusammenarbeit und Entwicklung, Reem Alabali-Radovan, das Unternehmen ACE Schmersal in Boituva (São Paulo) und unterzeichnete einen Finanzierungsvertrag über 18 Millionen Brasilianische Real (BRL), dies entspricht rund 2,75 Millionen Euro. ACE Schmersal ist Teil der international tätigen Schmersal Gruppe. Die Mittel stammen aus dem Förderprogramm ImpactConnect, das von der Deutschen Entwicklungsfinanzierungsgesellschaft (DEG) durchgeführt und vom Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ) finanziert wird. Die Investition ermöglicht die Erweiterung der Fertigung, die Anschaffung neuer Maschinen sowie die Installation von Solaranlagen, die ausreichend Energie für den gesamten Betrieb des Unternehmens erzeugen können. Die Initiative fördert zudem Innovation, Nachhaltigkeit und die Schaffung neuer Arbeitsplätze in der Region.

www.schmersal.com

Beim Besuch des brasilianischen Tochterunternehmens von Schmersal in Boituva unterzeichnete Reem Alabali-Radovan (Mitte), Bundesministerin für wirtschaftliche Zusammenarbeit und Entwicklung, gemeinsam mit DEG-Geschäftsführerin Monika Beck (2. v. l.) und ACE-Schmersal-Geschäftsführer Rogério Baldauf (g. r.) ein Förderabkommen im Rahmen des Programms ImpactConnect

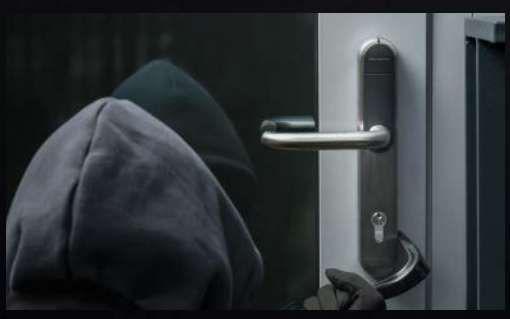
Simons≡Voss technologies

A BRAND OF ALLEGION

Die Sicherheit smart im Griff

Mechatronischer Beschlag für Außentüren
SmartHandle AX Advanced

Wasserfest und staubgeschützt
mit Schutzklasse IP66



Zertifizierter
Einbruchschutz ES3

Mehr
Informationen

Vom Start-up zum Big Player – 30 Jahre SimonsVoss

Erfolgsstorys beginnen häufig mit einer kleinen, aber zündenden Idee und dem Glauben daran, dass etwas Großes daraus werden kann. So auch im Fall der SimonsVoss Technologies GmbH – gegründet von Visionären, die den Markt der Schließsysteme revolutionierten und vom kleinen Start-up zum Big Player wurden.

Hinter dem Firmennamen von SimonsVoss stecken innovative Köpfe: Ludger Voss und ein Kompagnon aus Studienzeiten gründeten im November 1995 – angetrieben von der Vorstellung eines neuartigen Kompaktsystems für die Zutrittskontrolle – ihre Firma. Dazu mieteten sie im Münchner Stadtteil Schwabing ein kleines Büro auf einem Dachboden und holten sich mit Herbert Meyerle einen Systemarchitekten und Strategen ins Boot. Gemeinsam wollten sie die bisher mechanisch geprägte Schließtechnik technologisch erneuern.

Zunächst war das entwickelte digitale Einsteckschloss jedoch zu teuer und es gab zu viele Türvarianten. Im Herbst 1997 hatte das Team die weiterführende Idee, das System in die Knäufe von Schließzylindern zu integrieren. 1998 gab es dazu die ersten erfolgreichen Prototypen des „3060“. Fachhändler in der Branche sahen darin sofort ein enormes Potenzial und so nahm die Erfolgsstory ihren Lauf. Die Zahlen können sich sehen lassen: Seit der Gründung wurden rund 4.400.000 Schließungen installiert und an die 10.000.000 Transponder zum Einsatz gebracht.

Heute ist SimonsVoss ein europäischer Technologieführer digitaler Schließsysteme, 2015 wurde das Unternehmen eine Marke von Allegion und ist mit über 2.000 Fachhandelspartnern in Europa und weltweit vertreten. Unter dem Motto „The finest in keyless security“ entwickelt das Unternehmen seine nach dem Baukasten-Prinzip gestalteten Lösungen immer weiter, um Objekte aller Art und Größe mit einer auf den Bedarf abgestimmten Zutrittssteuerung absichern zu können.

Dabei gibt es drei große Bausteine für den Zugang zur „Keyless World“: das System 3060 und den Digital Cylinder AX als digitale Schließlösungen für Großunternehmen und öffentliche Einrichtungen, Smart Intego zur Integration in bestehende Gebäudetechniksysteme und Mobile Key als digitale Schließlösung für kleine und mittlere Gewerbeeinheiten sowie für Objekte mit bis zu 20 Türen.

Denn kein Gebäude ist zu klein oder zu historisch – für jedes gibt es eine passgenaue Lösung hinsichtlich Funktion und Design. Maximale Flexibilität gilt auch in Hinblick auf die unterschiedlichen Bereiche eines Gebäudes, für die es entsprechende digitale Schließprodukte gibt – vom Schließzylinder über SmartHandle-Türbeschläge bis hin zum Vorhängeschloss.

Zum Credo des Unternehmens gehört neben Innovationskraft, Qualitäts- und Servicedenken auch das Bekenntnis zum Standort Deutschland: Die Firmenzentrale liegt in Unterföhring bei München, das Fertigungs- und Logistikzentrum in Osterfeld. Der erweiterte Standort in Sachsen-Anhalt feierte 2023 sein 10-jähriges Bestehen.

Die Produktion von SimonsVoss in Osterfeld

Auf einer Fläche von 6.500 Quadratmeter sind dort Wareneingang, Fertigung, Lager, Versand, Qualitätsmanagement sowie After-Sales-Service vereint. Ein nachhaltiges Energiekonzept für die Gebäude sorgt für einen möglichst kleinen ökologischen Fußabdruck.

„Der Standort ermöglicht eine Verdoppelung der Fertigungskapazität unserer digitalen Zylinder, unserer digitalen Türbeschläge SmartHandle und der SmartRelais. Damit ist ein weiterer Schritt getan, unser Wachstum nachhaltig abzusichern und unsere Marktposition auszubauen“, so Bernhard Sommer, Geschäftsführer von SimonsVoss, bei der Eröffnung vor zwölf Jahren. 2020 folgte die Erweiterung der Produktion durch einen Neubau.

„Never give up ... der Weg zum Erfolg ist hart“, resümierte Ludger Voss in einem Interview im gleichen Jahr, in das auch das 25-jährige Bestehen des Unternehmens fiel. Dass SimonsVoss heute eine führende Rolle im europäischen Markt hat, erklärt der Firmengründer sich so: „Wir haben mit unserer Idee im Prinzip einen komplett neuen Markt erschlossen und dabei die Erfahrung gemacht, dass man als Hersteller immer ein Gesamtsystem braucht, um erfolgreich zu sein. Zum Erfolg beigetragen hat auch ein Stamm von langjährigen Mitarbeitenden, durch die das Know-how im Unternehmen geblieben ist und viele Innovationen erst möglich waren.“

Auf diesem Kurs ist SimonsVoss auch weiterhin unterwegs, für 2026 sind im Software- und im Produktbereich wiederum Neuheiten angekündigt. „SimonsVoss wird künftig neben der Weiterentwicklung der digitalen Schließsysteme auf eine zukunftsorientierte Softwareplattform setzen. Hier sehen wir viel Potenzial im Bereich von Cloud-Lösungen, moderner Software und Integrationen. Die Anforderungen unserer Kunden stehen dabei im Mittelpunkt unserer Strategie zur technologischen Weiterentwicklung“, kündigt Marcus Alt, CTO und Head of Research and Development bei SimonsVoss, an. **www.simons-voss.com**

BHE: Positive Entwicklung im Sicherheitsmarkt setzt sich fort

Die aktuelle Herbst-Konjunkturumfrage des BHE Bundesverband Sicherheitstechnik zeigt eine weiterhin stabile und leicht positive Entwicklung im Sicherheitsmarkt. Die Facherrichter bewerten ihre derzeitige Geschäftslage mit der Note 2,02 und damit etwas besser als im Frühjahr 2025 (2,09). Gleichzeitig ist dies der drittbeste Wert seit Anfang 2020. Fast 75 Prozent der Betriebe bezeichnen ihre aktuelle Marktsituation als „gut“ oder „sehr gut“. Der Anteil an Betrieben, die eine „schlechte Geschäftslage“ beklagen, beträgt wie im Frühjahr knapp 4 Prozent. Als „sehr schlecht“ wird die Situation aber von keinem Unternehmen beurteilt. In den einzelnen Kundengruppen zeigen sich unterschiedliche Tendenzen. Der Privatsektor verbessert sich leicht auf 2,94 (Frühjahr 2025: 2,95; Herbst 2024: 3,08) und erreicht damit den besten Wert seit Frühjahr 2023. Der gewerbliche Bereich verschlechtert sich minimal auf 2,26 (Frühjahr 2025: 2,20), bewegt sich aber weiterhin auf gutem Niveau. **www.bhe.de**

Fachpressegespräch der ZVEI-Arge Fachplaner und Errichter

Am 4. November 2025 lud der ZVEI Fachverband Sicherheit zum Fachpressegespräch der ZVEI-Arge Planer und Errichter. Im Fokus standen aktuelle Entwicklungen rund um die DIN VDE 0833-1, neue Konzepte für Brandmelde- und Sprachalarmanlagen sowie der Einsatz von Künstlicher Intelligenz (KI) in der Sicherheitsbranche. Christian Kühn als Vorsitzender des Vorstands in der Arge Errichter und Planer des ZVEI leitete das Gespräch ein und stellte die Überarbeitung der DIN VDE 0833-1 vor, die zentrale Anforderungen an Gefahrenmeldeanlagen für Brand, Einbruch und Überfall regelt. Ziel ist es, Planung, Installation, Betrieb und Instandhaltung effizienter und praxisnäher zu gestalten. Ein wesentlicher Fortschritt ist die Einführung einer einheitlichen „Sprache“ und klarer Definitionen, was die Zusammenarbeit aller Beteiligten erleichtert.

www.zvei.org

Vorstand der ZVEI Arbeitsgemeinschaft Errichter und Planer (v.l.n.r.): Percy Görgens (Mitglied des Vorstands), Christian Kühn (Vorsitzender) und Klemens Siebers (stv. Vorsitzender)

Aus Kemas wird Keba

Kemas hat sich in den vergangenen 35 Jahren als Spezialist für Übergabeautomation und Sicherheitslösungen etabliert. Bereits seit 2016 ist das Unternehmen Teil der in Österreich ansässigen, international tätigen Keba Gruppe und in dieser Zeit kontinuierlich gewachsen. Mit Keba verbindet das Unternehmen die beiderseitige jahrzehntelange Erfahrung und das breite Know-how in der Übergabeautomation sowie die Leidenschaft, Prozesse intelligenter und effizienter zu gestalten zum Nutzen der Kunden. Ab dem 1. April 2026 soll die enge Verbindung auch im Firmennamen und Auftritt sichtbar gemacht werden, deshalb firmiert das Unternehmen unter dem neuen Namen: Keba Handover Automation Germany GmbH. Mit dem neuen Namen schlage man das nächste Kapitel der Unternehmensgeschichte auf. Mit einer stark zukunftsorientierten Ausrichtung wolle man das Wachstum in den nächsten Jahren weiter vorantreiben und gemeinsam mit Kunden und Partnern an die Erfolge der letzten Jahre anschließen.

www.kemas.de

Von Kampfjet bis Weltraumforschung

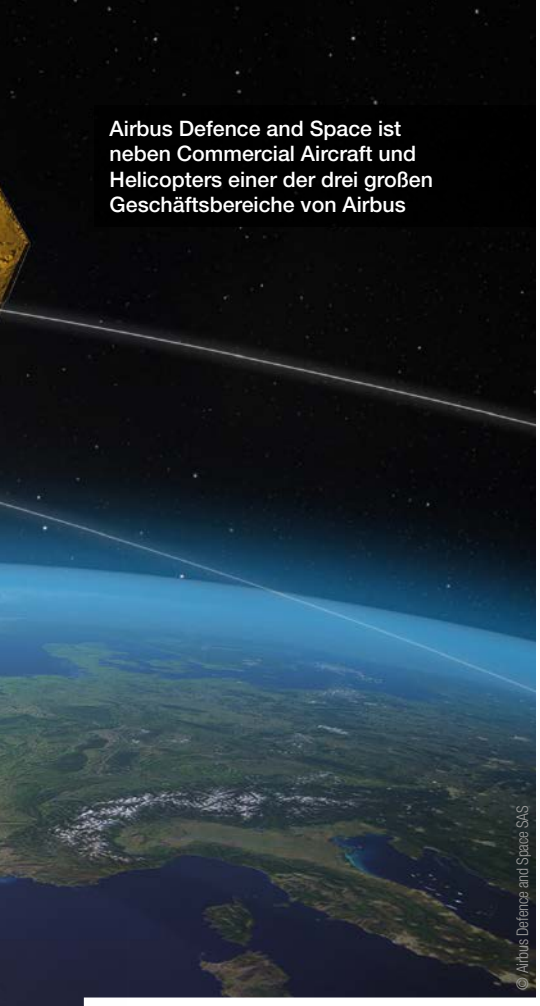
Sicherheit bei Airbus Defence and Space

Die Zeitläufte rücken die Bedeutung von Verteidigungs- und Sicherheitsfähigkeit in Europa schärfer denn je ins Bewusstsein. Als einer der führenden Akteure in den Bereichen Luftverteidigung, Satellitentechnologie, Cybersecurity und Weltraum ist das Airbus Defence and Space nicht nur ein Industriegigant, sondern ein strategischer Pfeiler für die Sicherheit des Kontinents. Wie reagiert ein global agierendes Unternehmen wie Airbus auf diese Herausforderungen? Wie schützt es seine Standorte, Technologien und Mitarbeitenden in einer Zeit, in der physische und digitale Bedrohungen stetig zunehmen? Und welche Verantwortung trägt die Industrie im Dialog mit Politik und Behörden, um Europas Resilienz zu stärken? GIT SICHERHEIT sprach mit Sven Dawson, Head of Corporate Security Airbus Defence and Space.

Herr Dawson, vielen Dank, dass Sie sich in diesen Zeiten noch Extrazeit für dieses GIT SICHERHEIT-Gespräch nehmen. Die öffentliche Aufmerksamkeit für die Defence- und Space-Sparte von Airbus war vermutlich selten so stark wie in diesen Wochen und Monaten?

Sven Dawson: Das stimmt, die öffentliche Aufmerksamkeit für Airbus Defence and Space ist in den vergangenen Monaten deutlich gestiegen. Für uns bedeutet das eine große Verantwortung – aber auch eine Chance. Wir sind mit unseren Programmen und Technologien in den Bereichen Luftverteidigung, Aufklärung, Satellitenkommunikation, Cybersecurity und Weltraum ein zentraler Partner, wenn es darum geht, Europas Handlungsfähigkeit zu sichern. Gleichzeitig nehmen wir wahr, dass auch in der Gesellschaft ein neues Verständnis dafür wächst, wie wichtig Resilienz, Verteidigungsbereitschaft und technologische Souveränität sind. Dass Airbus Defence and Space dabei so stark im Fokus steht, zeigt: Wir sind nicht nur ein Industrieunternehmen, sondern ein strategischer Pfeiler europäischer Sicherheit.

Bevor wir die aktuelle Lage weiter vertiefen, lassen Sie uns zunächst über Airbus Defence and Space selber sprechen – also über den Geschäftsbereich,



Airbus Defence and Space ist neben Commercial Aircraft und Helicopters einer der drei großen Geschäftsbereiche von Airbus

© Airbus Defence and Space SAS

grammen wie dem Eurofighter oder der kommenden Eurodrohne über Satellitenkommunikation, Aufklärungssysteme und Cybersecurity bis hin zu Weltraumtechnologien, die von der Erdbeobachtung bis zur interplanetaren Exploration reichen.

In Deutschland sind wir an mehreren wichtigen Standorten vertreten, die jeweils eigene Schwerpunkte haben. Wir bündeln Luftfahrt-, Verteidigungs- und Weltraumkompetenzen unter einem Dach und können so integrierte, zukunftsorientierte Systeme entwickeln – etwa im Rahmen des Future Combat Air System (FCAS), das Luft-, Weltraum- und Cyber-Domänen miteinander verbindet. Kurz gesagt: Airbus Defence and Space vereint Spitzentechnologie, starke Standorte u.a. in Deutschland und sicherheitspolitische Verantwortung – und leistet damit einen entscheidenden Beitrag zu Europas Souveränität.

Herr Dawson, Sie sind Head of Corporate Security und National Security Representative Germany. Geben Sie uns einen Überblick über Ihren Verantwortungsbereich?

Als National Security Representative Germany vertrete ich zudem die sicherheitsrelevanten Interessen von Airbus gegenüber staatlichen Stellen und Behörden in Deutschland. Das umfasst unter anderem die enge Zusammenarbeit mit Ministerien, Nachrichtendiensten und Sicherheitsbehörden, insbesondere bei Themen wie nationale Geheimschutzanforderungen, Zulassungen und der Einhaltung gesetzlicher Vorgaben.

Mit meinem Team arbeiten wir täglich daran, Risiken frühzeitig zu erkennen, Bedrohungen effektiv zu managen und die Resilienz des Unternehmens zu stärken. Dabei geht es nicht nur um den physischen Schutz, sondern auch um die Absicherung sensibler Daten, Technologien und Programme, die für die nationale und europäische Sicherheit von strategischer Bedeutung sind.

Unser Ziel ist es, Airbus Defence and Space als verlässlichen und sicheren Partner für unsere Kunden, die Bundeswehr, die NATO und andere Institutionen zu positionieren.

© Airbus Defence and Space SAU. P.PIGEYRE/MASTERFILMS

Luftfahrt-, Verteidigungs- und Weltraumkompetenzen werden bei Airbus Defence and Space unter einem Dach gebündelt. Im Bild: Flugzeug der deutschen Luftwaffe

der sich mit Verteidigungs- und Raumfahrttechnologien befasst. Die Bandbreite ist ja gewaltig – vom Kampfjet bis zur Weltraumforschung...

Sven Dawson: Airbus Defence and Space ist einer der drei großen Geschäftsbereiche von Airbus – neben Commercial Aircraft und Helicopters – und deckt ein außerordentlich breites Spektrum ab. Unser Auftrag reicht von klassischen Verteidigungspro-

Sven Dawson: In meiner Funktion als Head of Corporate Security bei Airbus Defence and Space bin ich verantwortlich für den Schutz unserer Mitarbeitenden, Standorte, Informationen, Technologien und Produkte. Dazu gehört ein breites Spektrum an Sicherheitsbereichen — von klassischer Werks- und Personensicherheit über Informations- und Cybersicherheit bis hin zum Schutz kritischer Technologien und Infrastrukturen.

Könnten Sie uns – vielleicht anhand von ein paar Beispielen – beschreiben, welche Veränderungen angesichts der weltpolitischen Lage bei Airbus Defence and Space vorgenommen wurden?

Sven Dawson: Die Lage hat uns veranlasst, unsere Sicherheitsarchitektur noch einmal deutlich zu schärfen. Wir haben u.a. drei zentrale Handlungsfelder verstärkt: Da ist zunächst die physische Objektsicherung:

Bitte umblättern ▶

Hier haben wir unsere Schutzmaßnahmen für kritische Standorte, Entwicklungszentren und Produktionsstätten ausgebaut. Dazu gehören unter anderem erweiterte Zugangskontrollen, eine verstärkte Videoüberwachung und eine engere Zusammenarbeit mit Sicherheitsbehörden.

Dazu kommt der Bereich Cyberabwehr und Informationssicherheit: Wir haben unsere Verteidigungsstrukturen erheblich verstärkt, investieren in modernste Threat-Detection-Technologien, bauen Security Operations Centers aus und arbeiten intensiv mit staatlichen Partnern, um gemeinsam gegen Cyberangriffe vorzugehen.

Das dritte dieser zentralen Handlungsfelder ist der Schutz kritischer Technologien und Programme. Gerade weil wir an Projekten von nationaler und europäischer Sicherheitsrelevanz arbeiten, haben wir zusätzliche Maßnahmen zum Schutz sensibler Informationen und Entwicklungsdaten eingeführt. Hier spielt auch die enge Abstimmung mit Behörden wie z. B. dem Bundesministerium für Wirtschaft und Energie (BMWE) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) eine wichtige Rolle.

Darüber hinaus haben wir das Thema Awareness stark priorisiert: Unsere Mitarbeiter sind der entscheidende Faktor für Sicherheit. Deshalb investieren wir verstärkt in Schulungen und Sensibilisierungsprogramme, um das Sicherheitsbewusstsein in allen Bereichen weiter zu erhöhen.

© Airbus Defence and Space - PHOTO ESKENAZI DOMINIQUE_0606186617

Airbus Defence and Space ist in den Bereichen Luftverteidigung, Aufklärung, Satellitenkommunikation, Cybersecurity und Weltraum ein zentraler Partner, wenn es darum geht, Europas Handlungsfähigkeit zu sichern

© Airbus Defence and Space SAS

Austausch und Nähe zwischen Behörden und Industrie gestalten sich in Deutschland ganz anders als etwa in Frankreich oder Spanien. Bevor Sie in die Industrie wechselten, waren Sie selbst zwölf Jahre lang in einer Behörde tätig. Wo sehen Sie hier die Unterschiede?

Sven Dawson: Die deutschen Behörden unterliegen - leider noch immer - gesetzlichen Auflagen, die die Zusammenarbeit und den engen Austausch mit der Wirtschaft nicht immer vorsehen oder gar fordern. Hier sind uns andere Staaten, wie z. B. die von Ihnen erwähnten weit voraus. Aber auch hier sehen wir ein zunehmendes Interesse deutscher Behörden und eine daraus resultierende Intensivierung des Austausches.

Wo sehen Sie Verbesserungsbedarf in diesem Punkt – auch hinsichtlich des Zugangs zu Informationen, Frühwarnungen, Spionageabwehr, Drohnenüberflüge und dergleichen?

Sven Dawson: Es gibt einen erheblichen Verbesserungsbedarf in der Organisation dieses Austausches und der Zusammenarbeit. Aktuell mangelt es an gezielten Absprachen oder gar einer Koordination auf Behördenebene. Die Wirtschaft ist hier bereits abgestimmt und auch mit unseren Verbänden in stetigem Austausch. Ein weiterer großer Wunsch aus der Wirtschaft ist die Schaffung eines einheitlichen nationalen Lagebildes, welches die verschiedenen

Der Verantwortungsbereich von Sven Dawson reicht von klassischer Werks- und Personensicherheit über Informations- und Cybersicherheit bis hin zum Schutz kritischer Technologien und Infrastrukture

Layer, z. B. die Cyberlage, für alle Akteure aus Wirtschaft, Behörden und Institutionen abbildet.

Schauen wir etwas näher auf die Cyberangriffe. Haben sie zugenommen? Immerhin geht es bei Ihnen ja um hoch schützenswertes technologisches und verteidigungsrelevantes Know-how – man braucht nur an Kampfjets oder Hubschrauber zu denken...?

Sven Dawson: Ja, wir beobachten seit einigen Jahren eine deutliche Zunahme von Cyberangriffen – sowohl in Quantität als auch in Komplexität. Hier geht es nicht nur um klassische Industriespionage, sondern zunehmend auch um staatlich gesteuerte Angriffe, die darauf abzielen, Know-how abzugreifen oder kritische Systeme zu stören.

Unsere Antwort darauf ist eine konsequente Stärkung unserer Cyber-Resilienz. Wir haben unsere Security Operations Centers erweitert, investieren massiv in Threat-Intelligence-Technologien und arbeiten eng mit nationalen und europäischen Behörden sowie Partnern zusammen. Unser Ansatz ist ganzheitlich: Wir kombinieren modernste Technologien, kontinuierliche Mitarbeitersensibilisierung und eine enge internationale Vernetzung, um Bedrohungen frühzeitig zu erkennen und abzuwehren. Gleichzeitig gilt: Absolute Sicherheit gibt es nicht. Entscheidend ist, dass wir unsere Reaktionsgeschwindigkeit und unsere Fähigkeit zur Schadensbegrenzung stetig verbessern.

Cyberattacken sind ein Thema auch für kleinere Zulieferer. Wie gehen Sie mit dieser Thematik entlang der Lieferketten bei Airbus um?

Sven Dawson: Sie haben völlig recht: Cyberangriffe machen nicht an den Werkstoren von Airbus halt. Gerade kleinere Zulieferer, die oft über weniger Ressourcen im Bereich IT-Sicherheit verfügen, geraten zunehmend in das Visier von Angreifern. Da unsere Lieferkette ein integraler Bestandteil unserer Sicherheitsarchitektur ist, haben wir das Thema Supply-Chain-(Cyber)security zu einem strategischen Schwerpunkt gemacht.

Konkret heißt das: Wir haben klare Sicherheitsstandards und -anforderungen etabliert, die für alle Partner gelten und regelmäßig überprüft werden. Wir führen Audits und Assessments durch, um mögliche Schwachstellen frühzeitig zu identifizieren. Außerdem unterstützen wir unsere Zulieferer durch Schulungen, Best-Practice-Programme und Beratung, damit auch kleinere Unternehmen ihr Sicherheitsniveau anheben können. Und wir arbeiten eng mit nationalen und europäischen Behörden sowie anderen Unternehmen zusammen, um einheitliche Standards entlang der gesamten Lieferkette sicherzustellen.

Herr Dawson, Europa will und muss mehr für seine Verteidigung tun und ausgeben. Wenn dies die Nachfrage erhöht, dann ist ja auch eine Verschärfung des allerorten ohnehin bestehenden Problems des Fachkräftemangels absehbar. Wie sieht das bei Airbus aus – bei „Blue Collar"- und „White Collar"-Mitarbeitern?

Sven Dawson: Unser Ansatz ist mehrgleisig: Wir investieren massiv in die Ausbildung junger Menschen, bauen duale Studiengänge und Ausbildungsprogramme aus und arbeiten eng mit Universitäten und Fachhochschulen zusammen. Wir wollen als moderner, internationaler Arbeitgeber überzeugen – durch flexible Arbeitsmodelle, Entwicklungsmöglichkeiten und den einzigartigen Mehrwert an technologisch führenden und sicherheitsrelevanten Projekten wie z. B. FCAS oder Space-Programmen mitzuwirken. Wir fördern zudem interne Weiterqualifizierung, um Mitarbeiter gezielt auf neue Anforderungen vorzubereiten – gerade in Zukunftsfeldern wie Cybersecurity, KI und digitaler Systemintegration. Wir setzen bewusst auf Diversität und internationale Talente, um den Fachkräftemangel abzufedern und gleichzeitig Innovationskraft zu stärken.

Welche Besonderheiten gibt es im Zusammenhang mit Rüstungsgütern, etwa hinsichtlich erforderlicher Sicherheitsüberprüfungen?

Sven Dawson: Der Umgang mit Rüstungsgütern unterliegt ganz besonderen Anforderungen – und das zu Recht. Konkret bedeutet das, dass für Mitarbeiter in sensiblen Bereichen Sicherheitsüberprüfungen nach den gesetzlichen Vorgaben verpflichtend sind. Diese Prüfungen werden in enger Abstimmung mit den zuständigen staatlichen Stellen durchgeführt und sind Voraussetzung dafür, dass jemand an klassifizierten Projekten arbeiten darf. Darüber hinaus gelten strikte Geheimschutzauflagen, Exportkontrollvorschriften und Genehmigungsverfahren, die wir in unseren Prozessen fest verankert haben. Airbus Defence and Space verfügt als Deutschlands größter Akteur in diesem Bereich selbstverständlich über die entsprechenden Strukturen und Compliance-Mechanismen, um diese Anforderungen konsequent einzuhalten. Wir sehen diese Vorgaben nicht als Hürde, sondern als zentrales Element des Vertrauens, das Kunden wie die Bundeswehr, die NATO oder europäische Partner in uns setzen. Wer mit Rüstungsgütern arbeitet, trägt eine besondere Verantwortung – und wir nehmen diese sehr bewusst wahr. GIT

Airbus Defence and Space GmbH
www.airbus.com

Sicherheit neu denken

Fachvorträge und Diskussionen zu Migration, Wirtschaftskriminalität, Datenschutz und europäischer Souveränität prägten den 11. Bayerischen Sicherheitstag von BVSW und BDSW

Reza Ahmari, Grenzschutzagentur Frontex

Der 11. Bayerische Sicherheitstag von BVSW und BDSW brachte am 18. und 19. November 2025 im Münchner „Paulaner am Nockherberg" Fachleute aus Wirtschaft, Behörden und Sicherheitsdienstleistern zusammen. Im Mittelpunkt: aktuelle Herausforderungen wie hybride Bedrohungen, Migration, Wirtschaftskriminalität, Datenschutz und europäische Sicherheit. Vorträge, Diskussionen und ein Dialogforum boten praxisnahe Einblicke in zentrale Entwicklungen der Sicherheitsbranche.

Der Bayerische Sicherheitstag, der in diesem Jahr zum elften Mal stattfand, wurde von BVSW und BDSW gemeinsam ausgerichtet. Die Veranstaltung richtete sich an Vertreterinnen und Vertreter aus Wirtschaft, Behörden und Sicherheitsdienstleistern und bot die Gelegenheit, sich über aktuelle Entwicklungen im Bereich Sicherheit zu informieren und zu vernetzen.

Sicherheitspartnerschaften und ganzheitliches Denken

Bereits zur Eröffnung der in der Fachwelt etablierten Netzwerkveranstaltung gaben Werner Landstorfer, Präsident des BDSW, und Markus Klaedtke, seit Juli 2025 neuer Vorstandsvorsitzender des BVSW, das Motto „Sicherheit neu denken" aus, das sich denn auch wie ein roter Faden durch das Programm zog. Die Bedeutung von Kooperation und Innovation wurde von den Veranstaltern betont, um den vielfältigen Herausforderungen im Sicherheitsbereich zu begegnen.

In einer Videobotschaft hob der Bayerische Innenminister Joachim Herrmann die Bedeutung von Investitionen in Personal und Ausrüstung der Polizei hervor. Er betonte, dass Sicherheit ein zentrales Anliegen der Politik sei.

Die Notwendigkeit, Sicherheit ganzheitlich zu denken und die Zusammenarbeit zwischen Behörden, Wirtschaft und Dienstleistern zu stärken, wurde von den Verbands-Chefs Landstorfer und Klaedtke zu Beginn des eigentlichen Vortragsprogramms noch einmal unterstrichen.

Grenzschutz und Migration: Herausforderungen für Europa

Reza Ahmari erläuterte die Aufgaben und Herausforderungen der europäischen Grenzschutzagentur Frontex. Sie ist für die Kontrolle der EU-Außengrenzen verantwortlich. Ahmari zeigte, welche Aufgaben Frontex zur Erfüllung dieser Mission übernimmt. An erster Stelle steht die Unterstützung der EU-Mitgliedsstaaten bei der Sicherung ihrer Grenzen, wobei insbesondere bei der Überwachung der Küsten ein hoher technischer Aufwand betrieben wird. Zudem kooperiert Frontex eng mit nationalen Behörden und EU-Agenturen, um grenzüberschreitende Kriminalität zu bekämpfen, wie Schmuggel oder Menschenhandel. Ein weiterer Schwerpunkt liegt auf der Analyse potenzieller Risiken, die zur Auslösung erhöhter Flüchtlingsströme führen könnten. Aktuelle Vorfälle: siehe Online-Bericht (QR rechts oben).

Wirtschaftskriminalität und Betrugsprävention im Fokus

Alexander Resch, Leiter der Einheit für Finanzkriminalität bei Europol, gab Einblicke in die Arbeit der europäischen Polizeibehörde. Er erläuterte, dass Europol die Mitgliedstaaten bei der Bekämpfung von Korruption, Geldwäsche, Produktpiraterie und Betrug unterstützt. Resch verwies auf konkrete Fälle wie die Operation Jumita in Spanien und die Bekämpfung von Umsatzsteuerbetrug.

Ein besonderes Augenmerk legte er auf die zunehmende Bedrohung durch CEO-Fraud und Phishing-Angriffe, die Unternehmen aller Größenordnungen betreffen können. Resch warnte eindringlich vor der Gefahr, die noch einmal vermehrt von gefälschten E-Mails und betrügerischen Zahlungsanweisungen ausgeht.

Europäische Souveränität und wirtschaftliche Herausforderungen

Sabine Seeger-Regling, Senior Advisor und Europa-Korrespondentin, beleuchtete die Rolle Europas in einer neuen Weltordnung. Sie stellte fest, dass Europa zwischen den Großmächten USA, China und Russland zunehmend eigenständige Strategien entwickeln müsse. Seeger-Regling wies auf die wirtschaftlichen Herausforderungen hin, darunter eine anhaltende Rezession und Handelskonflikte. Sie betonte die Notwendigkeit, bürokratische Hürden abzubauen und die Souveränität Europas zu stärken.

Die Referentin hob hervor, dass die Transformation im Sicherheitsbereich alle gesellschaftlichen Akteure einbeziehe und eine stärkere Einbindung der Bevölkerung erforderlich sei.

Datenschutz auf Kosten der Sicherheit? Balanceakt für die Gesellschaft

Prof. Dr. Thomas Petri, Landesbeauftragter für Datenschutz in Bayern, thematisierte in seinem Impulsvortrag die Unterschiede im Datenschutz zwischen Europa, den USA und China. Er betonte die Bedeutung des Grundrechtsschutzes und warnte vor einer zu zentralisierten Datenschutzregelung. In der anschließenden Podiumsdiskussion diskutierten Petri, Christian Huber (Polizeipräsidium München) und Torsten Malt (DB Sicherheit GmbH) die Herausforderungen bei der Vereinbarkeit von Datenschutz und Sicherheitsanforderungen.

Die Diskussion zeigte, dass der Einsatz von Technologien wie Bodycams und Videotürmen eindeutig zur Erhöhung der Sicherheit beitrage, jedoch stets im Einklang mit den Grundrechten stehen muss. Beispielsweise die Videotürme – deutlich erkennbar im „Polizei-Design" – leisteten, so Huber, in München gute Dienste für die Sicherheit der Bürgerinnen und Bürger der Stadt. Die Podiumsdiskutanten forderten eine stärkere Digitalisierung und den Abbau bürokratischer Hürden, um die Effizienz im Sicherheitsbereich zu steigern.

Zukunftsthema ganzheitliche Sicherheit: Anforderungen und Perspektiven

Im abschließenden Dialogforum diskutierten BVSW-Vorstand Ernst Steuger und BDSW-Präsident Werner Landstorfer über die zukünftigen Schwerpunkte der Sicherheitsbranche. Sie betonten die Notwendigkeit, Regularien zu vereinfachen und die Anerkennung von Sicherheitsdiensten als systemrelevant voranzutreiben. Die Referenten wiesen darauf hin, dass technologische Lösungen wie Drohnenabwehrsysteme zwar verfügbar seien, deren Einsatz jedoch rechtliche Klarheit erfordere.

Zudem wurde die Bedeutung der Vorbereitung auf Krisenfälle und die Rolle der sicherheitsrelevanten Industrie hervorgehoben. Die Diskussion machte deutlich, dass eine enge Zusammenarbeit zwischen Staat, Wirtschaft und Gesellschaft erforderlich ist, um den zukünftigen Anforderungen an die Sicherheit gerecht zu werden.

Fazit

Der 11. Bayerische Sicherheitstag zeigte, dass die Sicherheitsbranche vor vielfältigen Herausforderungen steht, die von Migration und Wirtschaftskriminalität über Datenschutz bis hin zu Fragen der europäischen Souveränität reichen.

Die Veranstaltung unterstrich die Bedeutung von Kooperation, Innovation und einer ausgewogenen Balance zwischen Sicherheit und Grundrechten. Die Diskussionen und Vorträge lieferten wertvolle Impulse für die Weiterentwicklung der Sicherheitsstrategie in Bayern und darüber hinaus. GIT

BVSW | BDSW
www.bvsw.de | www.bdsw.de

Auch 2026 wird der Bayerische Sicherheitstag erneut stattfinden. Unverbindliche Informationen und Vorab-Zugriff auf die begrenzten Plätze sind erhältlich per E-Mail an mail@bdsw.de oder info@bvsw.de, Stichwort „Bayerischer Sicherheitstag 2026"

Gastgeber des 11. Bayerischen Sicherheitstages: BVSW-Vorstand Ernst Steuger, BVSW-Vorstandsvorsitzender Markus Klaedtke, BDSW-Geschäftsführer Andreas Paulick, BVSW-Geschäftsführerin Caroline Eder, BDSW-Präsident Werner Landstorfer, Moderator Oliver Luxenburger


© Boris Bärmichl

Jetzt oder nie

Zur digitalen Souveränität Europas

Bei digitalen Technologien ist Europa weitestgehend auf Importe angewiesen. Diese Abhängigkeit wird zunehmend zum Problem. Dabei wäre es bereits heute möglich, mit europäischen Lösungen digitale Souveränität zu erreichen. Wenn jetzt alle entschieden handeln, könnte Europa das Blatt noch rechtzeitig wenden. Ein Beitrag von Boris Bärmichl, Vorstand der Digitalsparte beim Bayerischen Verband für Sicherheit in der Wirtschaft, BVSW.

Digitale Souveränität umschreibt die Fähigkeit, die Kontrolle über die digitalen Grundlagen unserer Gesellschaft zu behalten. Sie startet bei der technologischen Souveränität, also der Fähigkeit, die eingesetzten Systeme selbst zu gestalten. Darauf baut die Datensouveränität auf, die Kontrolle darüber, wer Zugang zu Informationen hat und wie diese verarbeitet werden. Zusammen bilden sie die Basis für wirtschaftliche Souveränität, die sich durch eine Unabhängigkeit von außereuropäischen Plattformen und Anbietern auszeichnet. Wer in allen drei Bereichen eigenständig und selbstbestimmt bleibt, kann seine Stellung in der dynamischen digitalisierten Welt langfristig behaupten. Doch Europa hat einen erheblichen Aufholbedarf in Sachen digitaler Souveränität.

Tech-Giganten und die Macht der Daten

US-Anbieter stellen rund 70 Prozent der Cloud-Infrastrukturen, Suchmaschinen stammen zu 90 Prozent aus Ländern außerhalb Europas. Ein ähnliches Bild zeigt sich in den Bereichen KI-Entwicklung, Chip-Produktion und Social Media: amerikanische und chinesische Anbieter dominieren das Angebot, während der Wettbewerb für europäische Unternehmen durch fehlende Skaleneffekte und fragmentierte Märkte erschwert wird.

Der heutige Digitalmarkt wird zum größten Teil von fünf Konzernen beherrscht: Jedes Dokument, jede E-Mail, jede Sprachnachricht oder jede beliebige andere digitale Information kommt irgendwann mit den Lösungen der „Big Five" in Berührung, also mit Alphabet, Amazon, Apple, Meta oder Microsoft. Diese Tech-Giganten erzielen einen Umsatz von rund 1,6 Billionen US-Dollar jährlich. Doch damit nicht genug: Zusätzlich erhalten sie einen umfassenden Überblick über die weltweite Informationslage, was unter Umständen wertvoller sein kann als das verdiente Geld.

Regierungen sind sich der Macht dieser Daten bereits seit Langem bewusst und haben Technologie zu einem Teil ihrer Geopolitik gemacht.

Der Preis der Abhängigkeit

Mittlerweile ist es nicht mehr zu übersehen, dass diese digitalen Abhängigkeiten verschiedene Risiken bergen. US-Behörden haben über den Patriot Act und den Cloud Act die Möglichkeit, auf Daten zuzugreifen, die in Europa erzeugt und gespeichert werden. Unter Umständen gelangen diese Behörden so an Informationen, die dem europäischen Datenschutz unterliegen.

Quasi-Monopolisten können außerdem nahezu beliebige Preissteigerungen durchsetzen. Die Ausgaben des Bundes für Microsoft-Lizenzen sind hier nur ein Beispiel: Während die Kosten 2017 noch bei 74 Millionen Euro lagen, betrugen sie 2024 bereits 204,5 Millionen.

Auch ein Anbieterwechsel ist oft mit großem Aufwand verbunden, was den Handlungsspielraum der betroffenen Organisationen einengt. Cloudanbieter verlangen oft hohe Migrationskosten und erschweren so einen Umzug. In anderen Fällen lassen sich Dateien nur mit der proprietären Software öffnen, sodass ein Wechsel zu anderen Anbietern unmöglich wird.

Schlummernde Chancen überall

Es gibt aber auch gute Nachrichten, denn Europa hat im Digitalbereich viele Stärken vorzuweisen. In puncto Datenschutz ist Europa Vorreiter. Nirgendwo sonst wird das Recht an den eigenen Daten so hoch gehandelt, und das ist langfristig der entscheidende Faktor für Unabhängigkeit. Europa ist auch in der Forschung herausragend, insbesondere im Bereich der Künstlichen Intelligenz und des Quantencomputings. Zahlreiche wissenschaftliche Akteure arbeiten an der Entwicklung von Quantentechnologien und neuen Möglichkeiten von KI, oft in enger Kooperation mit der Industrie. Qualität, Präzision und Innovationen gehören zur Ingenieurskultur. Und obwohl es manchmal als Hemmschuh betrachtet wird, so ist das regulatorische Know-how in der Europäischen Union Granat für passgenaue Rahmenbedingungen. Auf diese Weise wird sichergestellt, dass Innovationen im Technologiebereich der gesamten Gesellschaft zugutekommen.

Mut zum Risiko

Bevor neue Technologien jedoch anfangen zu skalieren, wandern zahlreiche Start-ups in die USA oder nach Asien ab. Dort steht deutlich mehr Wagniskapital zur Verfügung, um Innovationen schneller voranzubringen. In Europa dagegen sind junge Unternehmen oft mit bürokratischen Hürden konfrontiert. Banken fordern Sicherheiten, die Start-ups in der Entwicklungsphase meistens nicht aufbringen können. Klassische Finanzierungsmöglichkeiten sind in der Regel auf bewährte Geschäftsmodelle ausgerichtet und weniger auf visionäre Ideen, die erst in der Zukunft Gewinne erzielen.

Ein weiteres Thema ist das Mindset. In der europäischen Politik, Verwaltung und Gesellschaft herrscht eine gewisse Skepsis gegenüber neuen Technologien vor. Manchmal werden Datenschutz, Regulierung und ethische Bedenken so restriktiv ausgelegt, dass Innovationen eher gebremst als gefördert werden.

Bitte umblättern ▶


Safety first. Für eine sichere und stabile Energieversorgung.
Setzen Sie als Energieversorger auf ganzheitliche Sicherheit. Bosch Building Technologies schützt Ihre physische und digitale Infrastruktur: Planung, Umsetzung und Wartung – alles aus einer Hand.
www.boschbuildingtechnologies.com
Technik fürs Leben
BOSCH

Technische Innovationen kommen in immer kürzeren Abständen auf den Markt und bieten neue Möglichkeiten für die Sicherheit. Wichtige Trends werden am 21./22. April 2026 wieder auf der BVSW SecTec vorgestellt. Ernst Steuger, BVSW-Vorstand und Geschäftsführer der Nürnberger Wach- und Schließgesellschaft, gab uns einen Überblick.

Ernst Steuger, BVSW-Vorstand und Geschäftsführer der Nürnberger Wach- und Schließgesellschaft

Trends im 360°-Überblick

Zukunft der Sicherheitstechnik – auf der BVSW SecTec

„Technik spielt in der Sicherheit eine immer wichtigere Rolle. Mit der BVSW SecTec wollen wir Unternehmen eine Orientierung bieten, welche Technologien das Potenzial haben, die Sicherheit zu verbessern und effizienter zu gestalten“, so Ernst Steuger.

Kollege Roboter kommt

Der Fachkräftemangel ist in der Sicherheitsbranche weiterhin ein heikles Thema. Die Entwicklungen in der Robotik können helfen, das Problem in einigen Bereichen zu entschärfen. Insbesondere bei der Überwachung von großen Arealen erweisen sich Roboter schon heute als besonders hilfreich - zu sehen bereits auch auf der SecTec 2025. „Einige Außengelände beispielsweise umfassen 15 bis 40 Kilometer Zaun“, so Steuger. „Auf einem so großen Gebiet ist die Überwachung mithilfe von Kameras aufwändig, beginnend von den Erdarbeiten und der Verlegung von Anschlusskabeln bis hin zur Wartung der Geräte.“ Ein Roboter hingegen, der mit Kameras ausgestattet ist, kann die Außengrenzen des Geländes abfahren.

Fortsetzung ▶

Zusammenarbeit stärken

Schon heute gibt es eine ganze Reihe europäischer Technologieunternehmen, die alles zur bereitstellen könnten, was für die digitale Souveränität Europas erforderlich ist. Noris Network, Ionos und OVH Cloud sind Beispiele für Cloud-Anbieter mit DSGVO-konformen Rechenzentren und konkurrenzfähigen Services. Im Bereich „Security & Identity“ bieten Unternehmen wie Secunet, Nevis oder Eviden Lösungen für Authentifizierung, Verschlüsselung und IT-Sicherheit.

Für besonders kritische Anwendungen stehen souveräne Datenökosysteme und europäische KI-Modelle zur Verfügung, beispielsweise von N8N oder U-KNOW.AI. Die Aufzählung zu vervollständigen, würde den Rahmen hier sprengen. Es gibt über 800 herausragende europäische Unternehmen, die von der Hardware über die Cloud bis zur KI alles bieten, was für Europas digitale Souveränität gebraucht wird.

Kurswechsel jetzt

Die Zeit drängt: Gefragt sind jetzt mutige Investitionen, schnelles Handeln und Risikofreude für Innovationen. Europa verfügt über die Technologie, die Unternehmen und die Talente – jetzt braucht es nur noch den gemeinsamen Willen, diese zusammenzubringen. Öffentliche Hand, Mittelstand und Start-ups müssen enger zusammenarbeiten, denn die notwendige Skalierung lässt sich nur gemeinsam erreichen. Außerdem müssen wir die digitalen Kompetenzen auf allen Ebenen stärken – von der Schule bis zur Führungsetage im Großkonzern. Nicht zuletzt müssen die Erfolgsgeschichten europäischer Technologieunternehmen sichtbarer werden, um Vertrauen aufzubauen und Nachfrage zu schaffen.

Digitale Souveränität ist keine Utopie, sondern eine Frage des entschlossenen Handelns. Lassen Sie uns diese Herausforderung gemeinsam angehen. GIT

BVSW
www.bvsw.de

Was am besten und wirtschaftlichsten ist, hängt immer vom Schutzziel im Einzelfall ab. Sollte die Kamera eine Unregelmäßigkeit erfassen, beispielsweise einen beschädigten Zaun, wird das Bild an die Alarmempfangsstelle gesendet. Ein Mitarbeiter hat dann die Möglichkeit, sich auf die Kamera aufzuschalten, um sich die Situation genauer anzusehen und weitere Schritte einzuleiten.

Nicht nur im Außenbereich sind die Roboter eine große Hilfe: In Lagerhallen und Logistikzentren werden laufend Waren bewegt, so dass der Sichtbereich von fest installierten Kameras gelegentlich eingeschränkt sein kann. Roboter können auch in solchen Einsatzszenarien für Sicherheit sorgen und Mitarbeiter aus der Zentrale bei Bedarf mit auf einen virtuellen Rundgang nehmen. Große Fortschritte gibt es aktuell auch im Bereich der humanoiden Roboter, die ein noch breiteres Aufgabenspektrum abdecken können. „Diese Roboter sind in der Lage, Kontrollgänge in Bürogebäuden durchzuführen und eventuell offen gelassene Fenster zu schließen oder vergessene Kaffeemaschinen auszuschalten."

Nächste BVSW SecTec
21./22. April 2026 in München

Auch Drohnen sind mittlerweile in der Sicherheit nicht mehr wegzudenken und kommen gerade bei der Überwachung von Außenflächen zum Einsatz. In Zusammenarbeit mit Robotern lässt sich das Leistungsspektrum von beiden Technologien erweitern: „Angenommen ein Roboter entdeckt eine Beschädigung am Zaun, dann kann die Drohne Personen auf dem Gelände lokalisieren, die sich eventuell Zutritt verschafft haben", so Steuger.

LiDAR-Systeme: Licht ins Dunkel

Eine Möglichkeit, sein Umfeld zu überwachen, bietet die LiDAR-Technologie (Light Detection And Ranging). Dabei tasten Laserstrahlen die Umgebung ab und können so sehr genaue Abbilder von Gegenständen, Tieren und Personen erstellen. Ein wesentlicher Pluspunkt gegenüber bildgebenden Technologien ist der Datenschutz: „Ein LiDAR-Sensor erfasst die Umrisse und kann somit Personen detektieren, nicht aber deren Gesicht erkennen und wird somit strengen Vorgaben zum Datenschutz gerecht."

Perimeterschutz
Siehe auch ab Seite 32

Außerdem liefern LiDAR-Systeme zuverlässige Überwachungsdaten unabhängig von Wetter oder Tageszeiten.

Künstliche Intelligenz auf dem Vormarsch

Die Verknüpfung von Technologien bietet in unterschiedlichen Bereichen immer leistungsstärkere Gesamtsysteme und in viele Lösungen wird Künstliche Intelligenz integriert. Mittels künstlicher Intelligenz lassen sich die biometrischen Merkmale in Gesichtern vermessen, also beispielsweise der Abstand der Augen oder die Länge der Nase. Anhand dieser Merkmale ist KI in der Lage, Gesichter wiederzuerkennen, ohne sie bildlich darzustellen. Auch hier lassen sich die Vorgaben zum Datenschutz einhalten.

Mit entsprechender Software für Kameras, bietet KI damit entscheidende Vorteile beispielsweise bei der Überwachung von Supermärkten und anderen öffentlich zugänglichen Räumen: Wird eine Person erkannt, die Hausverbot hat, wird sie auf den Bildern der Überwachungskameras markiert. Der Sicherheitsdienst kann den Weg der Person nachverfolgen, um weitere Maßnahmen einzuleiten.

Smarte Zutrittssysteme

Zutrittssysteme regeln heute weit mehr als nur den Einlass. Mittlerweile gibt es Lösungen, die sich zusätzlich als Lotsendienste zur Navigation durch Firmengebäude und Werksgelände einsetzen lassen. Dafür brauchen Besucher ihr Smartphone, auf dem sie die Ortungsdienste angeschaltet lassen müssen. Nach dem Zutritt bekommen sie eine Wegbeschreibung vorgezeichnet, die sie zu ihrem Ziel führt. Mittels Geofencing wird dafür gesorgt, dass die Besucher die vorgegebene Route nicht verlassen.

Hohe Anforderungen an Errichter

Die Möglichkeiten der Sicherheitstechnik wachsen schnell. Errichter spielen vor diesem Hintergrund eine Schlüsselrolle: Sie müssen die Integration unterschiedlicher Technologien meistern. Statt einzelnen Systemen sind zukünftig immer öfter komplexe, vernetzte Lösungen gefragt, die miteinander kommunizieren. „Die Herausforderung liegt darin, die richtige Kombination aus Hard- und Software zu finden und dabei die individuellen Anforderungen der Auftraggeber sowie die gesetzlichen Vorschiften zu berücksichtigen", erklärt Steuger.

Aspekte wie Datenschutz, Benutzerfreundlichkeit und Skalierbarkeit spielen dabei eine entscheidende Rolle. Ebenso wichtig ist die regelmäßige Wartung und Aktualisierung der Systeme, um mit den neuesten technologischen Entwicklungen Schritt zu halten. Letztlich sind Errichter nicht nur technische Dienstleister, sondern strategische Partner für Unternehmen, die ihre Sicherheitsinfrastruktur zukunftssicher gestalten wollen.

Infos rund um diese Trends wurden bereits auf der BVSW SecTec 2025 präsentiert – weitere Neuheiten werden auch bei der nächsten Ausgabe wieder zu sehen sein, dann am 21./22. April, erneut in München. Vorab-Anmeldung unter www.bvsw.de GIT

BVSW e.V.
www.bvsw.de

Sicherheitsdienstleister werden digital

Lünendonk-Liste „Sicherheitsdienstleistungen in Deutschland“ 2025

Seit 2009 beobachtet Lünendonk den Markt für Sicherheitsdienstleistungen. Die aktuelle Ausgabe der Marktstudie basiert auf der Analyse von 50 führenden Anbietern. Sie beleuchtet aktuelle Trends wie den zunehmenden Einsatz von digitalen Technologien, Robotiklösungen und die Qualifizierung von Sicherheitspersonal zur Gewährleistung von Effizienz, Qualität und Kontinuität der Sicherheitsleistungen. Bei den Top 25 Sicherheitsdienstleistern meldet die Untersuchung ein Wachstum von 7,5 %.

Die 25 führenden Sicherheitsdienstleister in Deutschland erzielen im Geschäftsjahr 2024 ein Umsatzwachstum von 7,5 Prozent und vergrößern ihren Personalbestand um 2,2 Prozent. Um die Effizienz, Qualität und Kontinuität der Sicherheitsleistungen auch in einem herausfordernden wirtschaftlichen Umfeld zu gewährleisten, setzen die Dienstleister zunehmend auf digitale Technologien, Robotiklösungen und die berufsbegleitende Qualifizierung ihres Sicherheitspersonals. Dies sind Ergebnisse der neuen Lünendonk-Studie „Sicherheitsdienstleistungen in Deutschland“.

Ranking

Die 25 führenden Sicherheitsdienstleister in Deutschland erwirtschafteten im Geschäftsjahr 2024 zusammen 5.398,6 Millionen Euro und repräsentieren damit rund 40 Prozent des Marktvolumens. Sie beschäftigen insgesamt mehr als 96.500 Personen und vereinen somit gut ein Drittel der Beschäftigten in der deutschen Sicherheitswirtschaft auf sich. An der Spitze der Lünendonk-Liste liegt wie in den Vorjahren die deutsche Landesgesellschaft von Securitas. Mit einem Umsatz von 1.210,0 Millionen Euro erzielte das Unternehmen ein Plus von 4,1 Prozent und vereint allein 9 Prozent des Marktvolumens auf sich.

Auf Rang zwei folgt die Kötter Unternehmensgruppe, die durch die Übernahme der Wako-Gruppe ihren Umsatz um 18,6 Prozent steigern konnte und zugleich 13,6 Prozent mehr Personal beschäftigte. Das Essener Unternehmen erbringt neben Sicherheitsleistungen auch weitere Gebäudeservices und kam 2024 auf einen Gesamtumsatz von 722,0 Millionen Euro.

Die Kieler Wach- und Sicherheitsgesellschaft inklusive Sicherheit Nord belegt mit einem geschätzten Umsatz von 519,0 Millionen Euro (+6,1 %) und 11.750 Beschäf-

Im Geschäftsjahr 2024 erzielte Klüh Security mit 207,1 Millionen Euro Umsatz (+11,2 %) erstmals ein Ergebnis über der 200-Millionen-Marke. Die neue Alarmempfangsstelle und Notruf- und Serviceleitstelle stärkt dabei die Position des Unternehmens als zukunftsorientierter Partner für integrierte Sicherheitslösungen

Unternehmen			Umsatz mit Sicherheit in Deutschland (in Mio. Euro)		Gesamtumsatz (in Mio. Euro)		Sicherheitsmitarbeitende in Deutschland	
2025	2024		2024	2023	2024	2023	2024	2023
1	1	Securitas Holding GmbH, Berlin	1.210,0	1.161,6	1.210,0	1.161,6	20.000	20.000
2	2	Kötter Unternehmensgruppe, Essen 1)	607,0	512,0	722,0	627,0	11.700	10.300
3	3	Kieler Wach- und Sicherheitsgesellschaft mbH & Co. KG, Kiel *)	519,0	489,0	519,0	489,0	11.750	11.750
4	4	Niedersächsische Wach- und Schliessgesellschaft Eggeling & Schorling KG, Hannover 2)	400,0	380,0	400,0	380,0	5.500	5.500
5	6	Wisag Sicherheit & Service Holding GmbH & Co. KG, Frankfurt am Main	292,8	269,2	1.729,0	1.617,3	5.361	5.027
6	5	Pond Security Service GmbH, Erlensee	288,9	312,2	290,1	313,2	4.150	4.015
7	7	Klüh Security GmbH, Düsseldorf	207,1	186,3	615,9	604,5	3.622	3.716
8	8	Piepenbrock Sicherheit GmbH + Co. KG, Osnabrück	200,2	177,8	968,5	886,1	3.837	3.408
9	9	W.I.S. Sicherheit + Service GmbH & Co. KG, Köln	156,4	155,8	156,4	155,8	3.027	3.132
10	11	Stölting Service Group GmbH, Gelsenkirchen 3)	142,1	122,6	319,9	272,5	3.326	3.348
11	12	ICTS Germany Gruppe, Potsdam	139,1	120,2	139,1	120,2	3.051	2.754
12	10	Dussmann Group, Berlin	126,0	123,0	911,0	881,0	2.436	2.557
13	14	Apleona Security Services GmbH, Berlin	121,0	107,6	121,0	107,6	2.230	2.160
14	15	Nürnberger Wach- und Schließgesellschaft mbH, Nürnberg 4)	118,4	101,4	118,4	101,4	2.400	2.200
15	13	Siba security service GmbH, Karlsruhe	115,0	113,0	115,0	113,0	2.400	2.330
16	17	big. bechtold-gruppe, Karlsruhe	88,2	81,6	144,3	136,4	1.598	1.658
17	22	ESD Sicherheitsdienst GmbH, Mühldorf am Inn 5)	85,0	72,8	97,3	84,2	1.466	1.365
18	21	Power Personen-Objekt-Werkschutz GmbH, Hamburg	83,0	75,6	83,0	75,6	1.610	1.600
19	18	Bewachungsinstitut Eufinger GmbH, Frankfurt am Main 6)	82,0	68,4	82,0	68,4	1.270	1.250
20	22	City Schutz GmbH, Schönburg	78,2	72,5	78,2	72,5	1.149	1.176
21	20	All Service Sicherheitsdienste GmbH, Frankfurt am Main	77,0	76,0	139,8	136,9	1.243	1.238
22	16	Ardor SE, Berlin	70,3	84,1	70,3	84,1	821	879
23	19	ISS Facility Services Holding GmbH, Düsseldorf	67,8	76,1	772,7	800,9	1.180	1.420
24	24	Secura protect Holding GmbH, Langenselbold	63,1	66,3	63,1	66,3	932	1.090
25	(-)	WeWatch Security Service GmbH, Berlin *)	61,0	57,3	61,0	57,3	500	494

Fußnoten:

1) Inkl. der in 2024 übernommenen Wako Gruppe.
2) Umsatz inkl. Sicherheitsdienstleistungen von VSU Vereinigte Sicherheitsunternehmen GmbH.
3) Umsatzsteigerung u. a. durch Großauftrag im Rahmen der EM. Inkl. der in 2023 übernommenen ESS - Erlanger Sicherheit- und Service-Gruppe.
4) Umsatzsteigerungen durch Neuaufträge von öffentlichen und militärischen Auftraggebern.
5) Umsatzwachstum durch mehrere Neuaufträge im Banken- und Industriesekto

*) Umsatz und/oder Mitarbeitendenzahlen ganz oder teilweise geschätzt.

tigten Platz drei. An vierter Stelle folgt die Niedersächsische Wach- und Schliessgesellschaft mit der zugehörigen VSU und einem Umsatz von 400,0 Millionen Euro (+5,3 %).

Neu in den Top 5 ist die Wisag Sicherheit & Service, die ihren Umsatz um 8,8 Prozent auf 292,8 Millionen Euro steigerte und damit Pond Security Service verdrängte. Pond verzeichnete einen Rückgang von 7,5 Prozent auf 288,9 Millionen Euro und fällt auf Rang sechs zurück. Auf dem siebten Platz rangiert Klüh, das mit einem Umsatz von 207,1 Millionen Euro (+11,2 %) erstmals die Marke von 200 Millionen Euro überschritten hat. Ebenfalls über dieser Schwelle liegt nun Piepenbrock, das seinen Umsatz um 12,6 Prozent auf 200,2 Millionen Euro steigerte und Platz acht erreicht.

Die W.I.S. aus Köln bleibt mit nahezu stabilem Umsatz von 156,4 Millionen Euro (+0,4 %) auf Rang neun. Neu unter den zehn führenden Anbietern ist die Stölting Service Group, die ihren Umsatz auf 142,1 Millionen Euro steigerte (+15,9 %), unter anderem durch einen Großauftrag im Rahmen der Fußball-Europameisterschaft.

Sicherheitsdienstleistungen werden zunehmend digital

Die private Sicherheitswirtschaft gewinnt in Deutschland spürbar an Bedeutung. Angesichts vielfältiger Krisen und steigender Anforderungen leistet sie einen immer wichtigeren Beitrag zur öffentlichen und unternehmerischen Sicherheit. Parallel dazu wandelt sich das Bild der Branche vom klassischen „Türsteher“ hin zum professionellen, technologiegestützten Dienstleister. Ein wesentlicher Treiber dieser Entwicklung ist auch der anhaltende Personal- und Fachkräftemangel. So nutzt innerhalb der Top 25 bereits die Hälfte der Unternehmen Robotik und moderne Digitallösungen – teils im operativen Einsatz, teils in Pilotprojekten. Besonders hoch ist das Interesse am Einsatz von Drohnen.

„Innovation und Digitalisierung verändern die Sicherheitswirtschaft: Intelligente Zutrittskontrollen, KI-gestützte Videoüberwachung sowie der Einsatz von Robotik und Drohnen erweitern das Leistungsspektrum moderner Sicherheitsdienstleister und setzen neue Maßstäbe für Effizienz und Qualität. Ob sich diese Technologien als fester Bestandteil der Sicherheitsarchitektur etablieren, hängt maßgeblich davon ab, wie überzeugend ihr Nutzen kommuniziert und Vertrauen bei Auftraggebern geschaffen wird“, erklärt Stefan Schubert, Consultant bei Lünendonk & Hossenfelder. „Gleichzeitig gilt es, regulatorische Vorgaben, Wirtschaftlichkeit und Akzeptanz moderner Technologien in Einklang zu bringen.“ GIT

Die Lünendonk-Liste der führenden Sicherheitsdienstleister in Deutschland und alle Ergebnisse der Studie können Sie hier downloaden:

Lünendonk & Hossenfelder GmbH
www.luenendonk.de

Zum Portfolio gehört neben dem vorbeugenden und abwehrenden Brandschutz auch der betriebliche Rettungsdienst

Bei der Ausbildung wird modernes Equipment genutzt, wie es auch bei realen Einsätzen der Fall ist

Wie bei der Berufsfeuerwehr

Betrieblicher Brandschutz und Rettungsdienst aus einer Hand

Ein Brand im Unternehmen, ein medizinischer Notfall im laufenden Betrieb – Szenarien, die niemand erleben möchte, die aber jederzeit Realität werden können. In solchen Momenten entscheidet sich, ob Vorsorge und Ausbildung funktioniert haben: Sind Beschäftigte richtig geschult? Greifen Brandschutzkonzepte zuverlässig? Stehen qualifizierte Fachkräfte bereit, um schnell und professionell zu handeln? Hier setzt die Kötter Unternehmensgruppe an. Mit vorbeugenden und abwehrenden Brandschutzlösungen sowie praxisnahen Spezialschulungen für Rettungs- und Sanitätsdienste bietet sie ein Leistungspaket, das beide Seiten der Sicherheit abdeckt – Prävention und Einsatz.

Dass es sich dabei um ein Thema handelt, das nie an Brisanz verliert, zeigte auch die Florian 2025, die im Oktober in Dresden stattfand. Die Fachmesse, auf der auch die Kötter Unternehmensgruppe vertreten war, bot eine Bühne für aktuelle Entwicklungen rund um Feuerwehr, Zivil- und Katastrophenschutz.

„Brandschutz ist heute weit mehr als die Erfüllung gesetzlicher Vorgaben. Wer Menschen, Sachwerte und Prozesse schützen will, muss vorbeugen und zugleich auf den Ernstfall vorbereitet sein“, sagt Dirk H. Bürhaus, Geschäftsführender Direktor der Kötter Security Gruppe. Kötter Fire & Service bündelt beide Perspektiven: präventiver Brandschutz durch Gefährdungsanalysen, maßgeschneiderte Konzepte und den Aufbau sowie Betrieb von Werk- und Betriebsfeuerwehren – ebenso wie der abwehrende Brandschutz, bei dem wenige Minuten über den Ausgang entscheiden. Hinzu kommt betrieblicher Rettungsdienst, der über die notwendigen Qualifikationen verfügt, um eine umfassende medizinische Versorgung sicherzustellen. Unternehmen profitieren so von ganzheitlichen Lösungen aus einer Hand.

Qualifizierung für Rettungs- und Sanitätsdienste

Zusätzlich wächst die Bedeutung qualifizierter Aus- und Weiterbildung im Rettungswesen. Die Anforderungen an Einsatzkräfte steigen – von Ersthelfern bis hin zu Notfallsanitätern. Hier setzt die Unternehmensgruppe auf ein breites Angebot, das seit der Integration des Ausbildungsspezialisten MedGravity vor drei Jahren deutlich erweitert wurde. Das Portfolio umfasst Trainings für Erst- und Betriebssanitäter ebenso wie vollwertige Ausbildungen für Rettungs- und Notfallsanitäter. Moderne eLearning-Formate und flexible Teilzeitmodelle sorgen dafür, dass Schulungen an individuelle Bedarfe angepasst werden können. Ein zusätzlicher Vorteil: Während eigenes Personal fortgebildet wird, kann das Familienunternehmen seinen Auftraggebern über Arbeitnehmerüberlassung qualifizierte Sanitätskräfte zur vertretungsweisen Übernahme der Aufgaben bereitstellen.

Praxisnahe Trainings

Mit der Kötter Brandschutz- und Rettungsdienstakademie in Stralsund steht zudem eine Einrichtung zur Verfügung, die auf praxisnahes Training setzt. Freiwillige, Berufs- sowie Werk- und Betriebsfeuerwehren können hier eine Vielzahl von Lehrgängen absolvieren – darunter Truppmann- und Truppführer-Ausbildungen, Atemschutzgerätetraining oder die Qualifizierung zur IHK-geprüften Brandschutzfachkraft sowie eine Vielzahl von feuerwehrspezifischen Fachlehrgängen.

Auch Rettungsdienste nutzen die Angebote: von Online-Ausbildungen für Rettungssanitäter bis hin zur dreijährigen Notfallsanitäter-Ausbildung. Besondere Stärke entfaltet die praktische Ausbildung, bei der reale Einsatzfahrzeuge und Ausrüstung genutzt werden – ein entscheidender

Live-Eindrücke vom Ausbildungsangebot und Trainingsequipment der Akademie in Stralsund

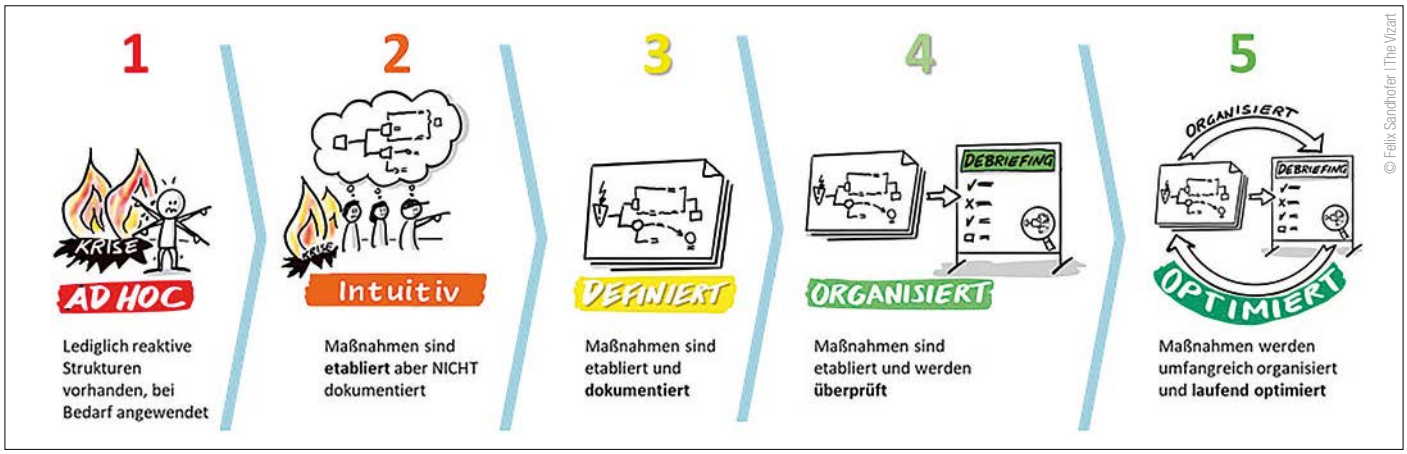
Pluspunkt, um Fachkräfte optimal auf den Einsatz vorzubereiten.

Synergie aus Sicherheit, Service und Weiterbildung

Die Kombination aus Brandschutz, Rettungsdienst und Weiterbildung schafft einen Mehrwert, der weit über einzelne Leistungen hinausgeht. „Wir können unseren Kunden heute nicht nur umfassende Schulungsprogramme anbieten, sondern auch im laufenden Betrieb für Sicherheit sorgen“, betont Dirk H. Bürhaus. Angesichts steigender Anforderungen in Brandschutz und Rettungsdienst bleibt die kontinuierliche Aus- und Weiterbildung ebenso wichtig wie ein durchdachtes Schutzkonzept, das die Resilienz von Unternehmen und Institutionen stärkt. Entscheidend ist das Zusammenspiel: Wer Prävention und Praxis verbindet, schafft die Basis für nachhaltige Sicherheit. GIT

Kötter Services, Essen
www.koetter.de

© Bilder: Kötter Services



Die 5 Stufen des verwendeten Reifegradmodell

Reifeprüfung

Zum Krisenmanagement von Unternehmen und Organisationen im DACH-Raum

Eine Umfrage zum Reifegrad des Krisenmanagements in Deutschland, Österreich und der Schweiz zeigt: Zwar sind die Krisenmanagementsysteme in der Mehrheit der befragten Organisationen dokumentiert, doch erfüllen sie oftmals nicht alle Anforderungen an ein modernes Krisenmanagement. Insbesondere wird die Ausbildung der Mitglieder in den Krisenstäben häufig vernachlässigt. Auch die Belastungssituation in der Stabsarbeit sowie der Umgang mit Dilemmata werden in vielen Organisationen nicht oder nur unzureichend behandelt. Existiert der Krisenplan eines Unternehmens nur auf dem Papier, droht die Gefahr, dass sich Unternehmen in trügerischer Sicherheit wiegen. Ein Beitrag von Max Brägger, Berater bei der Beratungsgesellschaft Verismo.

Im Rahmen einer Reifegradanalyse hat die Verismo zusammen mit Partnern in Ihrem Netzwerk insgesamt 85 Unternehmen aus Deutschland, Österreich und der Schweiz untersucht. Davon zählen 59 Organisationen zu den Großunternehmen mit mehr als 1.000 Mitarbeitern. 29 Unternehmen verstehen sich als Kritische Infrastruktur. Die Bewertung erfolgte durch eine geführte Selbstevaluation, bei der die Teilnehmer ihr Krisenmanagement anhand von 15 Prüfkriterien einschätzten. Grundlage für diese Kriterien war die ISO 22361:2022, der erste international anerkannte Standard für Krisenmanagement.

Zur Bewertung wurde ein fünfstufiges Reifegradmodell verwendet:

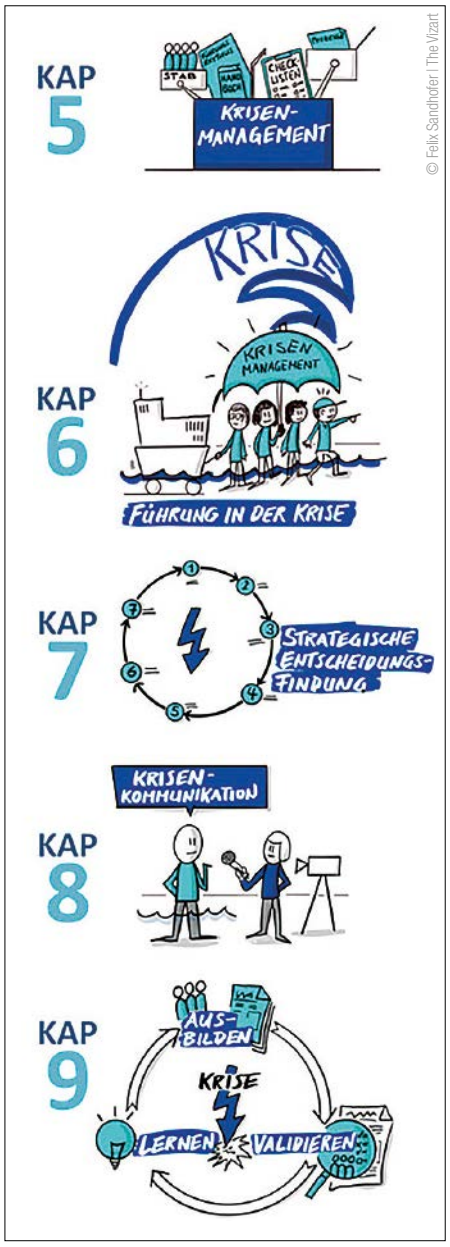
- Stufe 1 – Ad hoc: Lediglich reaktive Strukturen vorhanden
- Stufe 2 – Intuitiv: Maßnahmen sind etabliert, aber nicht dokumentiert
- Stufe 3 – Definiert: Maßnahmen sind etabliert und dokumentiert
- Stufe 4 – Organisiert: Maßnahmen sind etabliert und werden überprüft
- Stufe 5 – Optimiert: Maßnahmen werden umfangreich organisiert und laufend optimiert

Die 15 Prüfkriterien orientierten sich jeweils an den Anforderungen der operativen Kapitel 5 bis 9 der ISO 22361:2022, die unter anderem Themen wie Struktur und Prozesse, strategische Entscheidungsfindung, Krisenkommunikation und kontinuierlicher Verbesserung im Krisenmanagement behandeln. Diese strukturierte Herangehensweise erlaubt eine differenzierte Einschätzung des aktuellen Stands und zeigt auf, in welchen Teilbereichen des Krisenmanagements konkreter Entwicklungsbedarf bestehet.

Oft hohes Niveau

Viele Krisenmanagementsysteme im DACH-Raum zeigten ein überraschend hohes Reifegradniveau. Besonders bemerkenswert ist dies vor dem Hintergrund, dass sich nur 27 der untersuchten Unternehmen explizit an der ISO 22361:2022 orientieren, während 39 Organisationen, also fast die Hälfte, keinen konkreten Standard für ihr Krisenmanagement berücksichtigen. Unternehmen, die ihr Krisenmanagementsystem an der ISO 22361 ausrichten, erreichen dabei hinsichtlich aller Kapitel der Norm höhere Reifegrade und profitieren von einer systematischeren, ganzheitlicheren Herangehensweise.

Die Unternehmen und Organisationen der kritischen Infrastruktur schneiden bei der Standardisierung und Professionalität des Krisenmanagements im Durchschnitt am besten ab, obschon auch in dieser Gruppe nicht alle die ISO 22361 konsequent berücksichtigen. Erwähnenswert ist auch, dass die Umfrage vereinzelte KRITIS-Unternehmen identifiziert hat, deren Krisenmanagement nicht dokumentiert ist. Sie verlassen sich lediglich auf Ad-hoc-Reaktion oder die intuitive Leistung Ihrer Führungskraft, womit Sie den Anforderungen an die Resilienzpläne gemäß der europäischen CER-Richtlinie nicht gerecht werden.



Operative Kapitel der ISO 22361 zum Krisenmanagements

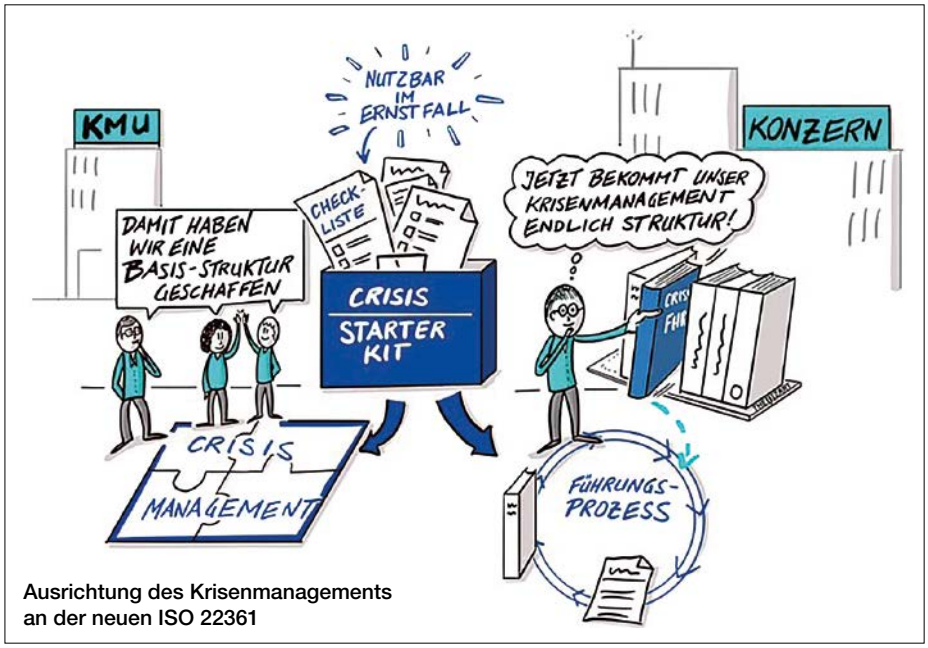
Ein Drittel ohne strukturierte Ausbildung

Die größte Schwachstelle liegt in der Ausbildung der Krisenstabsmitglieder: Ein Drittel der befragten Organisationen verfügt über kein strukturiertes Ausbildungsprogramm. Unzureichende Vorbereitung und Ausbildung der Krisenstabsmitglieder birgt die Gefahr, dass Sie im Ereignisfall ihre Rolle im Krisenstab nicht kennen, was die Entscheidungsfindung verzögern kann. Teils sind die Mitglieder in Anbetracht mangelnder Methodenkenntnis nicht in der Lage, zur strategischen Entscheidungsfindung mittels stringentem Führungsrhythmus im Stab beizutragen.

Weitere Schwächen zeigen die untersuchten Krisenmanagementsysteme im Umgang mit der besonderen Belastungssituation in der Stabsarbeit sowie bei der Bewältigung von Dilemmata in der strategischen Entscheidungsfindung. Werden diese Aspekte vernachlässigt, kann dies die Arbeit eines Krisenstabs nachhaltig negativ beeinflussen, insbesondere wenn dies zu unüberlegten Entscheidungen führt, oder weil schwierige, aber notwenige Entscheidungen vermieden werden und es dem Stab folglich nicht gelingt, „vor die Lage“ zu kommen.

Wenig überraschend kämpfen zudem viele kleine Unternehmen mit weniger als 250 Mitarbeitern auch mit dem formellen Aufbau eines Krisenmanagementsystems. Häufig fehlt nicht nur die strukturierte Implementierung, sondern auch ein definierter Krisenstab. Für größere Unternehmen ist dies hingegen nicht der Fall. Deren häufigsten Schwachstellen liegen vor allem bei den Anforderungen an die Führung in der Krise und der kontinuierlichen Verbesserung ihres Krisenmanagements.

Bitte umblättern ▶



Ausrichtung des Krisenmanagements an der neuen ISO 22361

Große Flächen – smarte Analysen

Neue Generation intelligenter Videoüberwachung

Fortsetzung ▶

Grenzen der Analyse

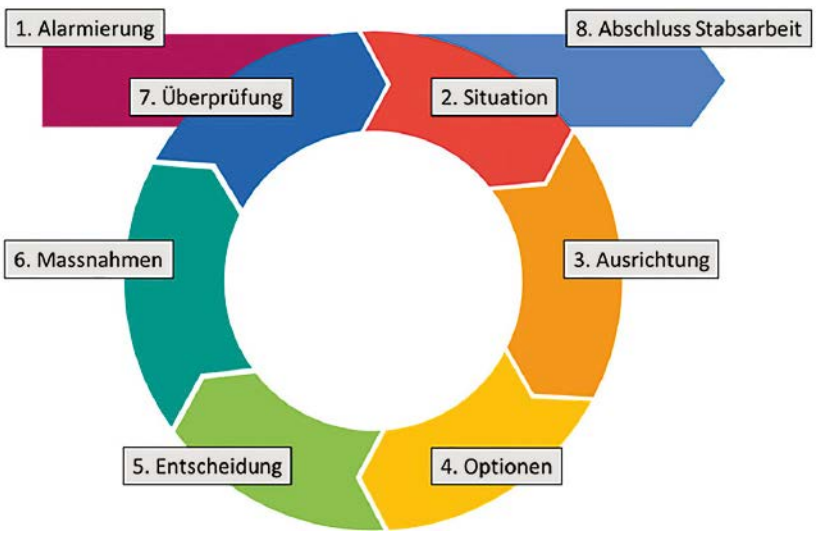
Die Methode der Selbstevaluation stößt bei der kritischen Betrachtung des Krisenmanagements an ihre Grenzen. Subjektive Wahrnehmungen und unternehmenskulturelle Informationsmuster, bei denen Stärken und Erfolge überbetont und Schwächen eher verschwiegen werden, können zu einer Verzerrung der Ergebnisse führen. Zudem haben überwiegend Organisationen an der Reifegradanalyse teilgenommen, die sich bereits vertieft mit dem Thema Krisenmanagement auseinandergesetzt haben. Es ist daher anzunehmen, dass der tatsächliche Reifegrad im DACH-Raum niedriger liegt, als es die Resultate der Analyse vermuten lassen.

Die Ergebnisse der Umfrage zeigen allerdings deutlich, dass es sich lohnt, das eigene Krisenmanagementsystem kritisch zu hinterfragen und gezielt anhand der ISO 22361 weiterzuentwickeln. Für bestehende Systeme empfiehlt sich eine Überprüfung anhand der Norm, um gezielt Abweichungen und Verbesserungspotenziale zu identifizieren. Ein externes Assessment kann dabei eine neutrale und nüchterne Perspektive ermöglichen.

Neue Krisenmanagementsysteme sollten von Beginn an konsequent an der Norm ausgerichtet werden. Erste Unternehmen haben diesen Schritt bereits vollzogen, weitere befinden sich in der Umsetzung.

Seit ihrer Veröffentlichung gilt die Norm als Stand der Technik. Sie wird nicht wieder verschwinden und ihre Bedeutung wird voraussichtlich weiter zunehmen, insbesondere weil die CER-Richtlinie der EU die Anwendung internationaler Standards für die Resilienzpläne der Kritischen Infrastruktur ausdrücklich fördert.

Für beide Wege, sowohl die Überprüfung bestehender Krisenmanagementsysteme und die Entwicklung neuer, existieren bereits praxiserprobte Herangehensweisen und Grundlagen, die eine strukturierte und wirksame Umsetzung der ISO 22361 ermöglichen. GIT



Führungsrhythmus des Krisenstabs gemäß ISO 22361, ergänzt um Alarmierung und Abschluss der Stabsarbeit

Verismo GmbH
www.verismo.ch

Mit der Panomera V8 präsentiert Dallmeier eine Kamera, die modernste Multifocal-Sensortechnologie und künstliche Intelligenz in einem System vereint – für eine lückenlose 180°-Sicht ohne toten Winkel und präziseste Analysen auch auf weitläufigen Flächen.

Panomera V8:
Die neue Generation der intelligenten Videoüberwachung kombiniert nahtlose 180°-Abdeckung mit maximaler Reichweite für smarte Lösungen

Die neue Panomera V8 von Dallmeier erreicht ein Blickfeld von 180 Grad und ermöglicht es, mit acht Linsen, acht Sensoren und acht KI-Chips eine sehr große Fläche zu erfassen – mit nur einer Kamera. Durch ein komplexes Verfahren werden die acht Systeme zu einem großen Übersichtsbild verbunden und die neuronalen Netze logisch verknüpft. Das macht sowohl menschliche Operatoren als auch KI-Assistenz-Systeme deutlich effizienter, präziser und zuverlässiger. So lassen sich die unterschiedlichsten Areale, von Marktplätzen über Logistikflächen bis hin zu Flughafen-Vorfeldern, erfassen und auswerten.

Business-Intelligence-Anwendungen

Ein Alleinstellungsmerkmal der Panomera V8 ist nach Angaben des Unternehmens das lückenlose 180°-Sichtfeld ohne toten Winkel und die Fähigkeit, die neuronalen Netze der acht integrierten KI-Chips logisch zu verknüpfen. Damit entfällt die größte Schwäche vieler Videoanalyse-Systeme: unvollständige, lückenhafte oder doppelte Bilddaten.

Diese Besonderheit bietet die ideale Grundlage für umfassende Analyse-Möglichkeiten sowohl mit den Dallmeier-eigenen KI-Analyse-Apps als auch mit Lösungen von Technologiepartnern. Die vollständige Erfassung einer Szene erlaubt tiefgreifende Auswertungen – sei es zur Vorfallanalyse, für Bewegungsmuster oder zur Nachverfolgung komplexer Abläufe. Damit wird die Panomera V8 zur Basis für eine Vielzahl von Sicherheits- und Business-Intelligence-Anwendungen.

KI für echten Mehrwert

Die Kombination aus durchgängigem Bild, hoher Detailtiefe und der engen Integration intelligenter Analysefunktionen eröffnet Anwendern vielfältige Möglichkeiten. So lassen sich etwa Personen und Objekte sekundenschnell anhand äußerer Merkmale wie Kleidung oder Taschen auffinden, Personen- oder Fahrzeugströme präzise erfassen oder große Areale zuverlässig gegen unbefugtes Eindringen absichern – und das mit deutlich weniger Falschalarmen. Ob zur Steuerung von Warteschlangen, für ein effektives Crowd-Management oder zur Verbesserung des Parkplatzmanagements: Die tiefgreifenden Auswertungsmöglichkeiten bieten nicht nur ein Plus an Sicherheit, sondern helfen auch, operative Prozesse nachhaltig zu optimieren.

AI made in Germany

Die Panomera V8 ist wie alle Dallmeier-Produkte „Made in Germany“ und erfüllt höchste Anforderungen an Qualität, Zuverlässigkeit und Cybersicherheit.

Dies gilt auch für die künstliche Intelligenz: Der Hersteller setzt auf eigens trainierte Netze und behält somit die volle Kontrolle über die Trainingsdaten. Mit diesem Ansatz will das Unternehmen Präzision und Verlässlichkeit steigern und eine Grundlage schaffen für Vertrauen in die Technologie.

Von Sicherheit zu Effizienz

Ob in Smart Cities, Flughäfen, Stadien, Logistikzentren oder im Einzelhandel: Das System ermöglicht es Betreibern, Sicherheit und Wirtschaftlichkeit miteinander zu verbinden. Durch die präzisen Analysen lassen sich Abläufe verbessern, Ressourcen gezielt einsetzen und Kosten senken.

„Mit der Panomera V8 wird die Kamera zu einer wichtigen Datenquelle“, erklärt Christian Linthaler, Chief Sales Officer bei Dallmeier. „Unsere Kunden profitieren nicht nur von maximaler Sicherheit, sondern auch von wertvollen Einblicken in ihre Prozesse – ein doppelter Mehrwert, der weit über klassische CCTV hinausgeht.“

Kosteneffizienz durch weniger Infrastruktur

Wie bei allen Panomera-Modellen weist auch die V8-Serie einen weiteren entscheidenden wirtschaftlichen Vorteil auf: Dank der enormen Abdeckung großer Flächen sind deutlich weniger Kameras, Masten und Kabel notwendig als bei konventionellen Systemen. Das senkt die Total Cost of Ownership (TCO) erheblich – bei gleichzeitig höherem Bedienkomfort.

Das System eignet sich beispielsweise für Smart-City-Anwendungen (städtische Sicherheit und Verkehrsfluss-Analysen), Flughäfen (Passagiermanagement, Perimeterschutz und Parkplatzoptimierung), Stadien und Events (Crowd-Management und Sicherheit in Echtzeit), Logistikzentren und Häfen (Flächenüberwachung und Prozessoptimierung) sowie Industrie und Kritische Infrastrukturen (Schutz sensibler Areale & Arbeitssicherheit). GIT

Die neue Panomera V8 liefert eine 180°-Sicht ohne toten Winkel

Dallmeier
www.dallmeier.com
www.panomera.com

TITELTHEMA

Auf dem Weg zur ISO 27001

Informationssicherheit als strategischer Pfeiler

GU BKS SERVICE steht kurz vor der Zertifizierung nach ISO/IEC 27001 – dem international führenden Standard für Informationssicherheitsmanagement. Damit will das Unternehmen seinen Anspruch unterstreichen, Kundendaten im Projektgeschäft wie auch in der laufenden Betreuung jederzeit nach höchsten Sicherheitsmaßstäben zu schützen.

Die Vorbereitung auf die Zertifizierung war für GU BKS SERVICE ein strategisches Investitionsprojekt: Strukturen wurden professionalisiert, Prozesse vereinheitlicht, Risiken bewertet und technische wie organisatorische Schutzmaßnahmen auf ein neues Niveau gehoben. Ziel war es nicht nur, eine Norm zu erfüllen, sondern ein Informationssicherheitsniveau zu schaffen, das den Anforderungen der Kunden dauerhaft gerecht wird und Vertrauen in die Leistungen des Unternehmens stärkt.

Vertrauen und Verantwortung

Aus Sicht von Patrick Wohlgemuth, Chief Information Security Officer der GU-Gruppe, stehen dabei zwei zentrale Aspekte im Mittelpunkt: Vertrauen und Verantwortung. „Unsere Kunden übertragen uns nicht nur Projekte, sondern oft auch hochsensible Unternehmensdaten. Daher war früh klar, dass Informationssicherheit nicht nur intern gelebt, sondern auch nach außen sichtbar gemacht werden muss. Die ISO/IEC 27001-Zertifizierung ist dafür der international anerkannte Maßstab und bildet zugleich die Basis für weitere regulatorische Anforderungen wie NIS2“. In den vergangenen Monaten wurde das Informationssicherheits-Managementsystem konsequent weiterentwickelt, so Wohlgemuth: „Klare Prozesse, gelebte Governance und ein hohes technisches Sicherheitsniveau prägen heute das Gesamtbild“.

Die intensive Vorbereitung auf die Zertifizierung habe dabei geholfen, Strukturen zu schärfen, Risiken noch präziser zu managen und die organisationale Resilienz stärker in den Mittelpunkt zu rücken. Entscheidend sei dabei die Grundhaltung, sagt CISO Patrick Wohlgemuth: „Informationssicherheit darf kein isoliertes Projekt sein, sondern muss als kontinuierliche Verantwortung in allen Bereichen des Unternehmens verankert sein“. Der eigentliche Wert der Zertifizierung liege darin, „dass gemeinsam eine nachhaltige Sicherheitskultur aufgebaut wurde, die das Unternehmen langfristig stärkt.“

Partner für KRITIS und NIS-2

Die zunehmende Digitalisierung und globale Vernetzung erhöhen die Verwundbarkeit kritischer Infrastrukturen gegenüber Cyberangriffen und physischen Bedrohungen. Mit dem Inkrafttreten der NIS-2-Richtlinie und dem KRITIS-Dachgesetz stehen Unternehmen vor der Herausforderung, ihre Sicherheits- und Resilienzmaßnahmen deutlich zu verstärken. Betroffen sind tausende Organisationen in Deutschland – von Betreibern kritischer Infrastrukturen bis hin zu besonders wichtigen Einrichtungen. Unternehmen müssen künftig ein umfassendes Risikomanagement etablieren und Resilienzpläne entwickeln, die sämtliche Gefahren – von Cyberangriffen bis hin zu Naturkatastrophen – berücksichtigen.

Darüber hinaus sind technische und organisatorische Sicherheitsmaßnahmen nach dem „Stand der Technik“ verpflichtend. Dazu gehören unter anderem Systeme zur Angriffserkennung sowie strenge Zutrittskontrollen. Sicherheitsvorfälle und erhebliche Störungen müssen innerhalb enger Fristen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) gemeldet werden. Ergänzend ist ein kontinuierliches Störungsmonitoring erforderlich, um Vorfälle frühzeitig zu erkennen und zu melden.

Zentrale Plattform

Das Gebäudemanagement- und Organisationssystem GEMOS bietet eine zentrale Plattform zur Integration und Steuerung physischer und digitaler Sicherheitsprozesse. Es erfüllt nicht nur die Anforderungen aus NIS-2 und KRITIS, sondern geht darüber hinaus. GEMOS ermöglicht eine zentrale Sicherheitssteuerung, indem es Meldungen und Anweisungen aus unterschiedlichen Systemen herstellerneutral in einem unabhängigen Risikomanagementsystem bündelt. Das System folgt höchsten

© Ehesan - stock.adobe.com

Lesen Sie das Interview mit Florian Rabe auf der nächsten Seite

Sicherheitsstandards: TLS 1.3-Verschlüsselung, AES-256 nach den Vorgaben des BSI, eine plattformunabhängige Architektur sowie eine webbasierte Bedienoberfläche nach OWASP-Standards.

Auch die Zutrittskontrolle ist integriert: Mit GEMOS Access werden alle Zutrittspunkte zentral überwacht – ein Kernbestandteil der NIS-2-Anforderungen. Zahlreiche Penetrationstests durch externe Prüfstellen bestätigen die Widerstandsfähigkeit des Systems. GEMOS hat alle Tests erfolgreich bestanden und ist für den Einsatz in hochsensiblen kritischen Umgebungen qualifiziert. Bereits ein unangekündigter Penetrationstest bei einem KRITIS-Kunden wurde erfolgreich und mit hervorragendem Ergebnis bestanden. Zudem unterstützt das System Unternehmen bei der Erfüllung gesetzlicher Meldepflichten und beim Störungsmonitoring durch die zentrale Erfassung und Auswertung sicherheitsrelevanter Ereignisse.

Das Gebäudemanagement- und Organisationssystem Gemos bietet eine zentrale Plattform zur Integration und Steuerung physischer und digitaler Sicherheitsprozesse

© 2023 Gorodenkoff/Shutterstock. – stock.adobe.com

Sicherheit in der Lieferkette

Neben modernster Technologie spielt heute die Sicherheit der gesamten Lieferkette eine zentrale Rolle. GU BKS SERVICE positioniert sich bewusst als verlässlicher Partner, der höchste Standards lebt und die Einhaltung regulatorischer Anforderungen innerhalb der gemeinsamen Geschäftsbeziehungen sicherstellt. Durch die Implementierung eines Informationssicherheits-Managementsystems (ISMS) nach ISO 27001 schaffen wir transparente, strukturierte Prozesse und gewährleisten den bestmöglichen Schutz sensibler Informationen – für uns und für unsere Kunden.

Darüber hinaus unterstützt GU BKS SERVICE bei der Erfüllung gesetzlicher Vorgaben aus dem KRITIS Dachgesetz und dem NIS-2 Umsetzungsgesetz und sorgt durch unabhängige Überprüfungen akkreditierter Auditoren für maximale Transparenz. Das Leistungsspektrum reicht von Beratung und Projektierung über Installation und Wartung bis hin zur Modernisierung bestehender Systeme. GIT

GU BKS Service GmbH
www.gu-bks.de

Gelebte Informations-sicherheit

Als integraler Dienstleister der GU-Gruppe bündelt GU BKS SERVICE seit 2023 die technischen, planerischen und organisatorischen Kompetenzen der Marken GU und BKS und stellt mit rund 120 Mitarbeitern und 30 Partnerbetrieben ein bundesweites Servicenetz bereit. Herzstück ist das Gebäudemanagementsystem GEMOS PSIM. Vor dem Hintergrund von KRITIS, KRITIS-Dachgesetz und NIS-2 dient sie als zentraler Baustein moderner Sicherheitsstrategien. GIT SICHERHEIT sprach mit Florian Rabe, Geschäftsführer von GU BKS SERVICE.

© GU BKS Service

GIT SICHERHEIT: Herr Rabe, die Marken GU und BKS kennt praktisch jeder in Deutschland. Sie sind Geschäftsführer der GU BKS SERVICE, der Dienstleistungspartner innerhalb der GU-Unternehmensgruppe. Können Sie uns zum Einstieg kurz die Geschichte Ihres Unternehmens innerhalb der GU-Gruppe erläutern?

Florian Rabe: Die Entscheidung war strategisch. Die technischen Zusammenhänge rund um unsere Produkte – vor allem im elektronischen Bereich – werden immer komplexer. Gleichzeitig erschwert der Fachkräftemangel die Arbeit bei Fachhändlern, Planern und Betreibern. Die Holding wollte unsere Partner damit nicht allein lassen. Deshalb haben wir die bestehenden Dienstleistungsstrukturen systematisch ausgebaut und schließlich in der GU BKS SERVICE gebündelt. Heute stellen wir flächendeckenden technischen Service sicher und unterstützen unsere Kunden mit fundierter, zertifizierter Fachkompetenz.

Was sind die zentralen Schwerpunkte Ihres Portfolios?

Florian Rabe: Unser Fokus liegt auf dem Service für sicherheitsrelevante Systeme rund um Tür, Zutritt und Rettungswege – also elektronische und mechatronische Schließsysteme, Zutrittskontrolle und Fluchttürtechnik. Zusätzlich entwickeln wir detaillierte Feuerwehrpläne, Feuerwehrlaufkarten und umfassende Sicherheits- und Notfallplanungen. Ein weiterer Schwerpunkt ist der Service für das Gebäudemanagementsystem Gemos, das sämtliche sicherheitstechnischen Anlagen zentral visualisiert und steuert. Wir sorgen dafür, dass diese Systeme zuverlässig funktionieren, sicher betrieben werden und im Bedarfsfall schnell Unterstützung verfügbar ist.

Sie sind heute vollwertiger Errichter mit direktem Herstellerbezug und u.a. mit VdS- und ISO-Zertifizierung. Was bedeutet das für Ihre Kunden und Ihre Position im Markt?

Florian Rabe: Unsere Zertifizierungen zeigen: Wir arbeiten durchgehend auf einem hohen technischen und organisatorischen Niveau. Kunden erhalten dadurch langfristig zuverlässigere Systeme, minimierte Folgekosten und einen überdurchschnittlichen Qualitätsstandard. Als Errichter mit direktem Herstellerbezug kombinieren wir tiefes Produktwissen mit praxisnahem Service. Das unterscheidet uns deutlich von Dienstleistern, die nur Teilleistungen erbringen.

Können Sie einmal anhand einer Kundenanforderung beispielhaft erläutern, wie Ihre Funktion als Bindeglied innerhalb der GU-Gruppe in der Praxis aussehen kann?

Florian Rabe: Ein Beispiel: Ein Fachhändler benötigt für ein Objekt eine RWA-Anlage, eine Fluchttürsicherung und ein digitales Schließsystem. Er kann die Produkte beziehen, hat aber oft nicht die Zertifizierungen oder Ressourcen für Montage und Inbetriebnahme. Hier übernehmen wir – inklusive aller Nachweise, der Einrichtung von Berechtigungen und der Schulung der Nutzer. Auch nach der Übergabe bleiben wir Partner: mit Wartungsverträgen, Instandhaltung, Updates und 24/7-Service. So entsteht eine durchgängige Verbindung zwischen Hersteller, Fachhandel und Endkunde.

Herr Rabe, Ihr Unternehmen ist auch durch Zukäufe von Errichtern gewachsen. Was waren das für Unternehmen?

Florian Rabe: Wir haben vor allem klassische Errichterbetriebe aus den Bereichen Brandmelde-, Einbruchmelde- und Videotechnik übernommen sowie ein Unternehmen für Zutrittskontrolle und Zeitwirtschaft. Alle Zukäufe haben unsere technische Kompetenz sinnvoll erweitert.

Was sind Ihre Pläne für die nächste Zeit?

Florian Rabe: Stabilität, Vertrauen und Qualität. Nach einer Verschmelzung müssen Kunden Veränderungen einordnen können. Wir möchten Verlässlichkeit schaffen und unsere erweiterten Fähigkeiten gezielt nutzen, um Bestandskunden noch besser zu unterstützen. Gleichzeitig bauen wir die Zusammenarbeit mit den Fachhandelspartnern weiter aus. Unser Anspruch ist: nicht Wettbewerber zu sein, sondern Servicepartner. Kurz gesagt: Wir konzentrieren uns auf Stabilität, Kundennähe und den Ausbau unserer Servicekompetenz, um nachhaltig Mehrwerte für alle Beteiligten zu schaffen. Zugleich verfolgen wir das Ziel, mit Gemos von BKS verstärkt Projekte im Bereich der Kritischen Infrastrukturen (KRITIS) zu realisieren. GIT

© GIT SICHERHEIT

Neue Ära im Besuchermanagement

Mit dem neuesten Release des Visitor Managements von ID-ware wird das Besuchermanagement noch smarter und schneller. Terminplanung und Zutritt funktionieren ganz von selbst: Meetings werden direkt aus mehreren Microsoft-Konten importiert– manuelle Eingaben sind nicht mehr notwendig. Vor Ort werden Besucher dann automatisch eingecheckt und erhalten umgehend Zutritt zum Ort des Meetings, ohne dass Gastgeber oder Empfang etwas tun müssen. Zudem ist der physische Besucherausweis jetzt Geschichte: Stattdessen bekommen Gäste eine personalisierte E-Mail mit einem QR-Code, der als sicherer digitaler Schlüssel dient – für nahtlosen Zutritt durch Türen und Schranken. Von der Terminplanung bis zum Zutritt ist alles automatisiert und sicher – für ein bequemes Besuchserlebnis ohne Wartezeit. **www.id-ware.com**

PERIMETERSCHUTZ

Datenflut an der Grenze

Aktuelle Themen des Perimeterschutzes

Was derzeit beim Perimeterschutz im Fokus steht, fasst aktuelle Entwicklungen der Sicherheitstechnik weitgehend wie in einem Brennglas zusammen. Moderne Systeme wie Perimeter-Konzentratoren helfen, die Datenflut aus Detektions- und Verifikationssystemen zu strukturieren. Künstliche Intelligenz erkennt Muster und unterstützt die Lagebewertung. Besonders im Fokus: Drohnenerkennung, Durchfahrtsschutz und die Integration autonomer Systeme. GIT SICHERHEIT sprach darüber mit Prof. Dr. Andreas Hasenpusch, u.a. Geschäftsführer des Ingenieurbüros Rathenow BPS und der STC BPS, Professor an der Hochschule für Öffentliche Verwaltung und Vorstand des Verbandes für Sicherheitstechnik.

Prof. Dr. Andreas Hasenpusch, u.a. Geschäftsführer des Ingenieurbüros Rathenow BPS und der STC BPS, Professor an der Hochschule für Öffentliche Verwaltung und Vorstand des Verbandes für Sicherheitstechnik

Herr Prof. Hasenpusch, Lassen Sie uns mit dem Anfang beginnen – mit der Gefährdungseinschätzung: Wie individuell sind der Schutzbedarf und das daraus abgeleitete Schutzkonzept für ein konkretes Projekt?

Andreas Hasenpusch: Beginnen wir mit dem Schutzziel, beispielsweise die Aufrechterhaltung einer Anlagenfunktion, die Verfügbarkeit von Schutzgütern oder die Verhinderung von Umweltgefahren. Dieses Schutzziel ist Gefahren ausgesetzt. Gibt es einen örtlichen und zeitlichen Zusammenhang zwischen dem Schutzgut und den Gefahren sowie möglichen Tätern, die die Gefahren ausnutzen können, entwickeln sich daraus Bedrohungen. Aus der Bewertung von Eintrittswahrscheinlichkeiten und Schadensausmaßen von festgestellten Bedrohungen werden Risiken ermittelt, denen zu begegnen ist. Diese Bewertung muss für jede zu sichernde Liegenschaft einzeln erfolgen oder aus typisierten Einschätzungen abgeleitet werden. Aus der Risikoanalyse ergeben sich Schutzmaßnahmen, die in einem Schutzkonzept zusammengefasst werden. Dieses ist für ein konkretes Projekt in der Regel genau zugeschnitten.

Neben Multilayer-Konzepten ist beispielsweise von szenarienbasierter Risikoanalyse viel die Rede – sind das die aktuellen Strategien für den Aufbau eines effizienten Perimeterschutzes?

Andreas Hasenpusch: Beim Multilayer-Konzept in der Perimetersicherung wird eine Liegenschaft nicht nur mit einer einzigen Schutzmaßnahme, sondern mit mehreren hintereinander oder parallel wirkenden „Schutzschichten" abgesichert. Dadurch entsteht eine Sicherheitsstruktur in der Tiefe, bei der das Überwinden einer Schicht nicht sofort zum vollständigen Verlust der Sicherheit führt. Die Nutzung von Szenarien in der Risikoanalyse setzt vorher an und ist ein bewährtes Instrument. Dabei wird untersucht, wie sich verschiedene Ereignisse auf das Schutzziel auswirken bzw. welche Ereignisse zu Beeinträchtigungen des Schutzziels führen. Dies erfolgt beispielsweise über die Anwendung von Fehlerfortpflanzungsmodellen. Ein anderer Ansatz ist, vom Schutzziel auszugehen und in einer Top-Down-Analyse zu untersuchen, durch welche Ereignisse das Schutzziel beeinträchtigt werden kann. In jedem Fall werden Ereignisse ermittelt, denen entgegengewirkt werden muss. Insofern ist die Betrachtung von Szenarien eine sinnvolle Möglichkeit für eine strukturierte Konzepterstellung. Aus dem Konzept leiten sich Maßnahmen ab, die z.B. in einem Multilayer-Konzept praktisch umgesetzt werden.

Auch im Rahmen des Perimeterschutzes kommt unter Umständen eine unübersehbare Masse von Daten zusammen, die verarbeitet werden müssen?

Andreas Hasenpusch: Es ist festzustellen, dass aufgrund der Anforderungen an die Detektion und der verfügbaren technischen Lösungen in der Perimeterüberwachung oft mehrere Detektions- und Verifikationssysteme zum Einsatz kommen. Diese erzeugen eine große Menge an Daten, die neben den Echtalarmen auch unerwünschte Alarme und Falschalarme umfassen. Insbesondere bei großen Perimeterlängen kommen so viele Informationen zusammen, die an einem zugeordneten Arbeitsplatz abgearbeitet werden müssen. Aktuell erfolgt dabei oft eine Bearbeitung jeder einzelnen Meldung. Aufgrund anderer zu bearbeitender Aufgaben können dabei Zusammenhänge zwischen einzelnen Ereignissen nicht ohne weiteres erkannt werden.

Es gibt Systeme, die hier ansetzen – Stichwort Perimeter-Konzentratoren. Wie sehen die aus?

Andreas Hasenpusch: Aktuell gibt es technische Systeme, die Meldungen aus der Perimeterüberwachung nach verschiedenen Kriterien wie beispielsweise Zeitverlauf und Meldungsreihenfolge strukturieren und

bewerten. Je nach eingestellter Sicherheitsstufe wird ein Alarm erst nach dem Vorhandensein vorgegebener Kriterien erzeugt. Dadurch wird die Anzahl der zu bearbeitenden Meldungen reduziert.

Die Nutzung riesiger Datenmengen ist ja die Kernkompetenz dessen, was wir Künstliche Intelligenz nennen – auch im Perimeterschutz?

Andreas Hasenpusch: Künstliche Intelligenz ist derzeit ein viel verwendetes Schlagwort. Angewandt auf den Perimeterschutz besteht die Aufgabe z.B. darin, übergreifende Muster im Meldungsaufkommen zu erkennen und anzuzeigen, die dem Bediener bei der sequenziellen Erarbeitung von Alarmen nicht auffallen oder auffallen können. In diese Mustererkennung können auch Datenpunkte einfließen, die vielleicht gar nicht aus dem Sicherheitssystem stammen. Die Aufgabe für die Zukunft sollte darin bestehen, in der Datenfusion Muster zu erkennen, die mit Bedrohungen verbunden sein können, und diese anzuzeigen. Im Idealfall hat der Benutzer dann eine Art Lagebild für seinen Schutzbereich als Grundlage für eine sinnvolle Reaktion. Die Maßnahmen zur Meldungsbearbeitung können zukünftig möglicherweise auch unter Einbeziehung entsprechende KI-Algorithmen für den Nutzer abgeleitet und vorgeschlagen werden.

In der Videotechnologie gibt es ja schon länger die intelligente Videoanalyse – auch dort geht es ja um Mustererkennung?

Andreas Hasenpusch: Ja, die intelligente Videoverarbeitung ist bereits seit vielen Jahren in der Anwendung. Ein erster Ansatz war das Erkennen abstrakter Objekte im Bild mittels verschiedener mathematischer Verfahren. Das Verhalten dieser Objekte wurde dann beispielsweise hinsichtlich Bewegung und Größe bewertet. Bei Video mit Mustererkennung oder KI wird letztlich versucht, das Bild über eine Mustererkennung zu „verstehen“. Dabei werden Menschen, Autos usw. als solche erkannt und bewertet. Hier besteht das Risiko, dass z.B. ein Mensch aufgrund einer absichtlich veränderten Ansicht nicht als Mensch erkannt wird. Für Sicherheitsanwendungen ist dies ein Zustand, der möglichst ausgeschlossen sein soll. Hier wäre vielleicht ein Ansatz sinnvoller, bei dem alles zur Meldung führt, was nicht definitiv ohne Risiko ist.

Was erwarten Sie von der noch weiteren Entwicklung der KI für den Perimeterschutz in den nächsten Jahren?

Andreas Hasenpusch: Es ist davon auszugehen, dass die Anzahl der verfügbaren Datenpunkte zunimmt. Mithilfe moderner Techniken der Mustererkennung wird die Interpretation der Daten eine Bewertung ermöglichen. Dies wird die Arbeitsabläufe an den Sicherheitsarbeitsplätzen verändern. Wenn KI in solch sensiblen Bereichen zur Anwendung kommt, muss dabei ihre bestimmungsgemäße Funktion gegeben sein. Voraussetzung hierfür ist Vertrauen in Lieferanten und Errichter.

Bei Perimeterschutz spielt heute die Abwehr von Drohnen eine zunehmende Rolle. Das betrifft insbesondere Kritische Infrastrukturen. Wie entwickelt sich aus Ihrer Sicht die Verteidigung gegen solche Angriffe?

Andreas Hasenpusch: Das Thema Drohnen ist aktuell, denn es vergeht kaum ein Tag, an dem keine Drohnen über Infrastruktureinrichtungen gemeldet werden. Drohnenerkennung und -abwehr sind daher hochaktuelle Themen. Aus meiner Sicht gibt es für den zivilen Einsatz eine Reihe verfügbarer Systeme zur Drohnendetektion, die potentiell zuverlässig arbeiten.

Bei der Drohnenabwehr sieht es anders aus, da die rechtlichen Rahmenbedingungen für gewerbliche Bedarfsträger unzureichend geklärt sind. Hier besteht Regelungsbedarf. Sind die Vorgaben vorhanden, muss sich mit der praktischen Umsetzung auseinandergesetzt werden. Nicht alle möglichen Abwehrmaßnahmen sind beispielsweise in einem städtischen Umfeld umsetzbar. Auch die Zeitspanne zwischen möglicher Detektion und notwendigen Abwehrmaßnahmen ist zu bedenken. Aus meiner Sicht besteht hier noch Forschungs- und Entwicklungsbedarf. Dies wird offenbar auch von staatlichen Stellen so gesehen, da verschiedene Projekte in diesem Bereich gefördert werden.

Auch hier geht es also um die Zusammenführung vieler Systeme, vieler Daten. Das kann man offenbar für den Perimeterschutz insgesamt sagen?

Andreas Hasenpusch: Durch die Einbeziehung aller anfallenden Daten und deren Bewertung ergibt sich tendenziell ein besserer Überblick. Voraussetzung hierfür ist eine vorherige Aufbereitung und Strukturierung der Daten. Dies muss für den Bediener zu einem Mehrwert werden, der ihn bei der Entscheidungsfindung unterstützt.

Lassen Sie uns im Zusammenhang mit dem Perimeterschutz für Kritische Infrastrukturen noch ein Thema herausgreifen: Den Durchfahrtsschutz. Was tut sich hier und warum ist das besonders wichtig?

Andreas Hasenpusch: Beim Durchfahrtschutz geht es kurz gesagt darum, das unbeabsichtigte Überfahren einer Perimeterlinie zu verhindern. Dazu muss bekannt sein, welche Fahrzeugmasse mit welcher Geschwindigkeit aufzuhalten ist.

Aufgrund von Vorfällen in Deutschland wird seit einigen Jahren auch beim Durchfahrtschutz nachgerüstet. Im Fokus der Öffentlichkeit steht dabei vor allem der Schutz von Großveranstaltungen. Allerdings sind auch kritische Infrastrukturen durch Angriffe mit Kfz gefährdet. Daher ist es unverzichtbar, den Zufahrtschutz als Teil der Sicherheitskonzepte für kritische Infrastrukturen zu begreifen. Durchfahrtsschutz ist somit ein elementarer Bestandteil der Sicherung kritischer Infrastrukturen. Dies bezieht sich sowohl auf die Zufahrtspunkte als auch auf den linearen Perimeter. Hier sind abgestimmte Lösungen notwendig.

Zum Abschluss ein Ausblick: Was wird in den nächsten Jahren wichtiger werden im Perimeterschutz?

Andreas Hasenpusch: Aus meiner Sicht wird das Thema Drohnen die Bedarfsträger und die Sicherheitswirtschaft in den kommenden Jahren weiter beschäftigen. Neben den technischen Fragen sind hier auch rechtliche Aspekte zu klären. Ein weiteres Thema ist für mich der Einsatz autonomer auch robotischer Systeme zur Alarmverifikation im Perimeter und möglicherweise auch bei abwehrenden Maßnahmen. GIT

Ingenieurbüro Rathenow
BPS GmbH
www.ibr-bps.de

PERIMETERSCHUTZ

Vom Zaun bis zur Wolke

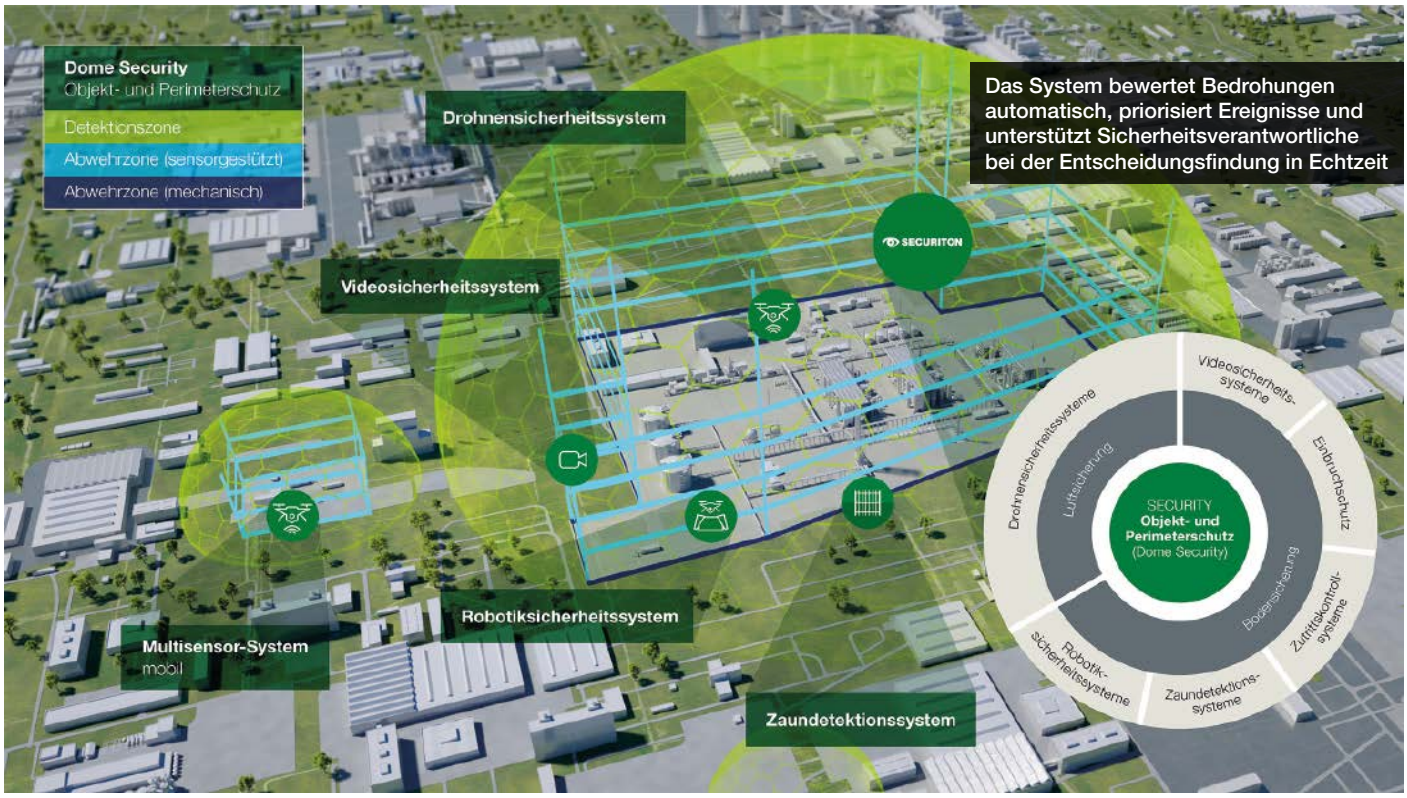
Perimeterschutz unter Einbeziehung des Luftraums

Der klassische Perimeterschutz ist blind für die dritte Dimension. Zäune, Kameras, Bewegungsmelder und Zugangssysteme sichern seit Jahrzehnten zuverlässig das, was auf dem Boden geschieht – doch die Bedrohung kommt längst von oben. Kleine, leise und hochpräzise Drohnen können heute Schadsoftware einschleusen, Daten abgreifen, Schmuggelware transportieren oder ganze Produktionsanlagen lahmlegen. Das Problem: Viele Sicherheitssysteme erkennen sie gar nicht.

Für Unternehmen aus dem Mittelstand oder Betreiber kritischer Infrastrukturen (KRITIS) ist das ein reales Risiko. Während der physische Schutzzaun vielleicht einem Einbruch standhält, öffnet sich über jedem Gelände eine unsichtbare Schwachstelle – der bodennahe Luftraum. Angreifer müssen keine Mauern mehr überwinden, sie fliegen einfach darüber hinweg. Das ändert die Logik der Sicherheit grundlegend: Es reicht nicht mehr, Grenzen zu überwachen – sie müssen räumlich gedacht werden.

Sicherheit wird dreidimensional

Das Konzept der „Dome Security“ von Securiton Deutschland setzt hier an. Es erweitert den klassischen Perimeterschutz in die Höhe und verknüpft Bodensicherung mit Luftraumüberwachung. RF-Sensoren, Radar, Akustiksysteme und intelligente Videotechnik bilden gemeinsam eine Art virtuelle Kuppel über dem Gelände. Diese Kuppel erkennt unautorisierte Flugobjekte frühzeitig – noch bevor sie Schaden anrichten oder unbemerkt Daten sammeln können.



Das Konzept der „Dome Security“ von Securiton Deutschland verknüpft Bodensicherung mit Luftraumüberwachung

Das Entscheidende dabei ist nicht nur die Technik, sondern die Integration. Denn was nützt es, wenn jedes System für sich Alarm schlägt, aber niemand das Gesamtbild sieht? Ein modernes Sicherheitsmanagementsystem verknüpft alle Informationen zu einem konsistenten Lagebild. Es bewertet Bedrohungen automatisch, priorisiert Ereignisse und unterstützt Sicherheitsverantwortliche bei der Entscheidungsfindung in Echtzeit.

Anwendungsfälle mit hoher Relevanz

Ein Energieversorger schützt sein Umspannwerk – bisher mit klassischer Videoüberwachung und Zutrittskontrolle. Plötzlich fliegt eine Drohne über die Anlage, möglicherweise mit einer Kamera oder einem Sprengsatz. Ohne Dome Security bleibt der Vorfall unentdeckt. Mit ihr wird das Flugobjekt im Umkreis erkannt, verfolgt und klassifiziert – und bei Bedarf automatisch abgewehrt.

Ein anderes Beispiel: Ein Produktionsbetrieb mit geistigem Eigentum von hohem Wert. Spionagedrohnen, die Daten oder Bildmaterial sammeln, sind hier keine theoretische Gefahr. Auch hier schließt die „Sicherheitskuppel“ jene Lücke, die herkömmliche Systeme offenlassen – die Grenze zwischen physischem und digitalem Risiko.

Vom linearen Denken zur integrierten Sicherheit

Dome Security markiert damit den Übergang vom zweidimensionalen zum ganzheitlichen Schutz. Perimetersicherheit wird nicht mehr nur als horizontale Linie verstanden, sondern als dreidimensionale Zone – ein Raum, in dem jede Bewegung, am Boden wie in der Luft, Teil eines dynamischen Sicherheitskonzepts ist.

Was früher eine klare Grenze war, ist heute ein intelligentes Netzwerk aus Detektion, Analyse und Reaktion. So entsteht ein Schutzschirm, der sich über Gelände, Gebäude und Luftraum spannt – ein System, das ebenso vorausschauend wie vernetzt arbeitet.

Boden und Himmel als Einheit

Dome Security bedeutet jedoch nicht, dass der Fokus allein auf den Luftraum gelegt wird. Im Gegenteil: Am Boden kommen weiterhin modernste Technologien zum Einsatz – automatisierte Videoüberwachung mit intelligenter Videoanalyse, hochsensible Detektionszäune oder Robotiksysteme, die eigenständig Aufklärung und Bestreifung übernehmen. Zusammen bilden sie das Fundament, auf dem die Schutzkuppel des Luftraums aufbaut. Erst das Zusammenspiel von bodennaher Sicherung und smarter Luftraumüberwachung schafft ein Sicherheitsniveau, das den Herausforderungen der Gegenwart gewachsen ist – vom Zaun bis zur Wolke.

Dome Security, so der Hersteller, ist kein zusätzliches Modul, sondern der logische nächste Schritt – hin zu einem Sicherheitsverständnis, das Bedrohungen nicht nur erkennt, sondern in ihrer gesamten räumlichen und technologischen Tiefe begreift. GIT

Securiton Deutschland
www.securiton.de

© Bilder: Securiton

PERIMETERSCHUTZ

Wirkungsvoller Perimeterschutz

Wie effektiver Perimeterschutz physische Barrieren mit intelligenter Sensorik und integriertem Datenmanagement kombiniert

Heiko Viehweger, Vertriebsleiter DACH bei Hirsch Secure

Der Schutz des Perimeters ist ein zentrales Element der Unternehmenssicherheit, weil er die erste Verteidigungslinie gegen unbefugten Zutritt, Sabotage, Diebstahl oder Spionage bildet. Seine besondere Bedeutung liegt darin, dass er potenzielle Bedrohungen erkennt, verzögert oder ganz abwehrt, bevor sie das eigentliche Betriebsgelände oder kritische Infrastrukturen erreichen.

Ein effektiver Perimeterschutz erkennt Sicherheitsvorfälle schon an der Grundstücksgrenze, noch bevor unbefugte Personen oder Fahrzeuge das Gelände betreten. Dabei kommen moderne Detektionssysteme zum Einsatz, die Eindringlinge präzise erkennen und klassifizieren können. Physische Barrieren wie Zäune, Tore, Schranken oder Mauern erschweren das Eindringen zusätzlich und verschaffen Sicherheitskräften wertvolle Zeit für eine Reaktion; bereits die offensichtliche Präsenz solcher Schutzmaßnahmen wirkt stark abschreckend. Darüber hinaus ist wirkungsvoller Perimeterschutz heute digital vernetzt und in umfassende Sicherheitskonzepte integriert, beispielsweise in Zutrittskontrollsysteme, Videoüberwachung, Gefahrenmanagementsysteme oder Alarmanlagen, was automatisierte Reaktionen ermöglicht und ein genaues Lagebild in der Sicherheitsleitstelle entwirft.

Moderne Detektionssysteme

Physische Barrieren wie Zäune, Tore, Schranken oder Mauern sollen Eindringlinge an der Außengrenze abhalten, sie sind aber nur dann ein effektiver Schutz, wenn sie mit entsprechenden elektronischen Detektionssystemen kombiniert werden. Für relativ einfach zu sichernde Liegenschaften kann eine Detektionsmethode ausreichen, gerade für Anwendungen in Hochsicherheitsbereichen und KRITIS-Standorten ist aber das Kombinieren verschiedener Detektionsmethoden im Perimeterschutz sinnvoll, weil aufgrund der individuellen Standortbedingungen oder auch Witterungseinflüssen keine einzelne Technologie oftmals alle Anforderungen gleichzeitig optimal erfüllt. Jede Methode hat spezifische Stärken – und auch Schwächen, die durch andere Systeme ausgeglichen werden können. Durch die Verknüpfung mehrerer Sensoren entsteht ein robustes mehrschichtiges, intelligentes und falschalarmarmes Gesamtsystem. Um eine gute Kombination von Detektionssystemen wie Videoanalyse, Infrarot, Radar, LiDAR oder Zaunsensorik zu finden, aber auch um beurteilen zu können, ob nicht bereits eine Art der Detektion für den Schutzzweck ausreichend ist, muss man die einzelnen Methoden näher betrachten. Im Abschnitt Praxistipps in der erweiterten Fassung dieses Artikels auf GIT-SICHERHEIT.de geben wir Ratschläge für einen wirkungsvollen Einsatz. Link: https://git-sicherheit.de/de/topstories/wirkungsvoller-perimeterschutz-technologien-anforderungen-und-praxistipps (siehe auch QR-Code unten).

Zaundetektionssysteme

Zaundetektionssysteme übernehmen im physischen Perimeterschutz die Funktion der frühzeitigen Detektion von Eindringversu-

chen an der äußeren Begrenzung eines Schutzobjektes. Sie bilden damit die erste Verteidigungslinie innerhalb eines mehrschichtigen Sicherheitskonzeptes nach dem Prinzip der „Defense in Depth".

Technisch basieren Zaundetektionssysteme auf Sensorik, die mechanische Einwirkungen auf den Zaun – etwa durch Klettern, Schneiden oder Durchtrennen – erfasst und in elektrische Signale umwandelt. Gängige Technologien sind Beschleunigungssensoren, mikrofonische Sensorkabel, piezoelektrische Systeme oder faseroptische (DAS-basierte) Sensoren, die entlang der Zaunlinie installiert werden. Diese Systeme erkennen charakteristische Vibrationsmuster und unterscheiden durch Signalverarbeitung und algorithmische Filterung zwischen realen Angriffen und Störereignissen wie Wind, Regen oder Kleintieren.

Im mehrschichtigen Sicherheitsverbund dient das Zaundetektionssystem der Frühwarnung und Lageerkennung. Es löst eine Alarmmeldung mit präziser Zonenlokalisierung bereits vor bzw. während des Eindringversuchs am Zaun aus, noch bevor das gesicherte Gelände betreten wird. Hierdurch können Videoüberwachungssysteme automatisiert auf den betroffenen Bereich schwenken und Sicherheitskräfte zielgerichtet Maßnahmen in der Alarmkette einleiten. Durch die Integration in ein übergeordnetes Sicherheitsmanagementsystem lässt sich der gesamte Perimeterzustand in Echtzeit überwachen und dokumentieren.

Zaundetektionssysteme besitzen zwar keine physische Barrierewirkung, erhöhen jedoch durch die sofortige Detektion und Alarmierung die Reaktionsgeschwindigkeit und damit die Gesamteffektivität des Perimeterschutzes erheblich. In Kombination mit mechanischen Barrieren, Beleuchtung, Videoanalyse und Zutrittskontrolle bilden sie ein hochwirkungsvolles, mehrschichtiges Schutzkonzept, das sowohl präventiv als auch reaktiv wirkt.

Videoanalyse

Die Videoanalyse mit Videofarb- und Thermalkameras hat sich zu einem zentralen Bestandteil des modernen Perimeterschutzes entwickelt. Sie ermöglicht die automatische Erkennung, Klassifikation und Bewertung von Ereignissen entlang der Schutzlinie und liefert gleichzeitig wichtige visuelle Informationen zur Verifikation und Forensik.

Moderne Videoanalysen erkennen Personen, Fahrzeuge oder Bewegungen und können Falschalarme deutlich reduzieren, wenn sie richtig projektiert und konfiguriert sind. Besonders Thermalkameras zeigen ihre Stärken bei Nacht und schwierigen Lichtverhältnissen: Sie erkennen Wärmequellen unabhängig von Beleuchtung oder Schatten und sind daher ein wertvolles Frühwarninstrument. Allerdings liefern sie kaum visuelle Details und werden deshalb oft durch PTZ-Videokameras ergänzt, die zusätzliche Detailinformation bei der Videoverifikation liefern.

Unabhängige Systemtests und Erfahrungen aus der Praxis zeigen, dass die Leistungsfähigkeit der Systeme stark von den eingesetzten Algorithmen, der Installation und den Umgebungsbedingungen abhängt. Nur wenige Systeme können in allen Bedrohungsszenarien ausreichend überzeugen und unbefugten Zugang zuverlässig erkennen, ohne dabei zu viele Falschalarme zu erzeugen. Witterungseinflüsse, Vegetation, wechselnde Beleuchtung oder Tiere führen immer noch zu Falschauslösungen. Zu viele Falschauslösungen sind - hohe Detektionsqualität vorausgesetzt- bei Installationen mit einer starken Präsenz durch Sicherheitspersonal vor Ort in Einzelfällen noch akzeptabel, da die Lage schnell geklärt werden kann, sie sind aber ein KO-Kriterium bei Anwendungen, bei denen automatisch eine Alarmkette durch externe Interventionskräfte ausgelöst wird. Entscheidend sind daher eine standortspezifische Auswahl und Feinjustierung der Analytik. Systeme, die im Labor gute Ergebnisse liefern, können in der Praxis stark abfallen. Besonders effektiv sind Lösungen, die Videoanalyse mit anderen Sensoren wie Zaunsensorik, LiDAR

Bitte umblättern ▶

oder Infrarotmeldern kombinieren, da so Falschalarme minimiert und Erkennungsraten maximiert werden.

Für Betreiber bedeutet das: Videoanalyse ist in vielen Fällen unverzichtbar, kann aber in sicherheitskritischen Umgebungen nicht uneingeschränkt als alleinige Technologie empfohlen werden. Eine gute Planung umfasst die Kombination von Thermal- und sichtbaren Kameras, klare Zonenlogik und eine Integration in den Alarm-Workflow. Regelmäßige Tests und Kalibrierungen sichern die Performance im Betrieb. Videoanalyse bietet großes Potenzial für den Perimeterschutz – ihre Wirksamkeit hängt jedoch entscheidend von Qualität, Umfeld, Parametrierung und dem intelligenten Zusammenspiel mit anderen Detektionsmethoden ab.

Radarsysteme

Radar wurde von Beginn an für anspruchsvolle Anwendungen eingesetzt, zunächst im Militärbereich sowie zur Navigation von Flugzeugen und Schiffen. Diese Einsatzgebiete stellten hohe Anforderungen an Zuverlässigkeit und Präzision der Radargeräte. Mit der Weiterentwicklung der Technologie wurde Radar auch für den Sicherheitsmarkt verfügbar, kommt bisher jedoch insbesondere nur für eine großflächige Überwachung und freie Flächen zum Einsatz.

Zukünftige Entwicklungen in Chip- und Softwaretechnik sowie Antennendesign versprechen weitere Verbesserungen bei Leistung, Design und Anpassungsfähigkeit von Radarsystemen für den Schutz kritischer Infrastrukturen. Wie ausgiebige Systemtests, z.B. der GIT System Test Perimeter Protection gezeigt haben, sind Radarsysteme aber trotz der relativ hohen Kosten nicht per se anderen Systemen überlegen, sondern müssen wie andere Detektionsmethoden zur Anwendung passen und vor Ort genau eingestellt und optimiert werden. Auch sollte für ein wirksames System zwingend eine Kombination mit z.B. PTZ-Kameras und Videoanalyse durchgeführt werden, die das Alarmereignis der Radarsensorik überprüft und optisch bewertet.

LiDAR

LiDAR-basierte Einbruchserkennung gewinnt an Bedeutung, da sie durch präzise Detektion und hohe Zuverlässigkeit bei nahezu allen Licht- und Wetterbedingungen überzeugt – sogar bei Dunkelheit oder extremen Wetterlagen. LiDAR funktioniert, indem Laserpulse ausgesendet und deren Reflexionen gemessen werden, um eine präzise dreidimensionale Karte der Umgebung zu erstellen, der sogenannten Punktwolke.

Im Bereich der Perimetersicherheit bietet LiDAR mehrere bedeutende Vorteile. Erstens ermöglicht LiDAR eine hochpräzise Erkennung, indem Personen und Fahrzeuge mit einer Genauigkeit im Zentimeterbereich verfolgt werden – oft übertrifft dies herkömmliche Sensoren. Zweitens liefert LiDAR eine gleichbleibende Leistung unter allen Lichtverhältnissen, auch bei völliger Dunkelheit oder schwachem Licht, da es nicht auf Umgebungslicht angewiesen ist. LiDAR sammelt keine personenbezogenen Daten oder Details, sondern lediglich Sensordaten des LiDAR-Systems, wodurch ein reines LiDAR-System vollständig DSGVO-konform ist.

Durch das Erfassen von 3D-Daten kann LiDAR echte Bedrohungen zuverlässig von harmlosen Bewegungen, die durch Tiere, Wetter oder Laub verursacht werden, unterscheiden – dies führt zu einer geringeren Falschalarmrate. Schließlich lassen sich LiDAR-Systeme mit anderen Sicherheitstechnologien wie Kameras kombinieren, um Alarme zu verifizieren und sowohl eine Nah- als auch Fernbereichsüberwachung zu ermöglichen.

Kombiniert man LiDAR mit seiner volumetrischen Erkennungstechnologie und einer fortschrittlichen 3D-Überwachungssoftware, lassen sich Bedrohungen in einer digitalen Darstellung der Realität – einem digitalen Zwilling – visualisieren. Anders als herkömmliche Perimeter-Einbruchmeldesysteme, die sich meist nur auf den Schutz des Zauns konzentrieren, ist ein solches System darauf ausgelegt, komplette Anlagen zu sichern.

Diese Stärken machen LiDAR besonders nützlich für sicherheitskritische Umgebungen wie Flughäfen, Rechenzentren, Kraftwerke, Gefängnisse und Grenzanlagen, wo die Minimierung von Falschalarmen aufgrund der möglichen Störungen und Kosten besonders wichtig ist.

LiDAR ergänzt physische Barrieren um eine intelligente, präzise und frühzeitige Detektion und ist für verschiedenste Einsatzbereiche geeignet – von kleinen bis großen Anlagen sowie für Industrie, Logistik, Behörden und kritische Infrastrukturen.

Mikrowellen- und Passiv-Infrarot-Sensoren

Im modernen Perimeterschutz kommen Mikrowellen- und Passiv-Infrarot-Sensoren (PIR) häufig zum Einsatz, um unbefugte Annäherungen oder Eindringversuche zuverlässig zu erkennen. Beide Technologien ergänzen sich ideal, da sie auf unterschiedlichen physikalischen Prinzipien beruhen und so eine hohe Detektionssicherheit auch unter schwierigen Umweltbedingungen ermöglichen.

Mikrowellensysteme erzeugen ein elektromagnetisches Feld zwischen Sender und Empfänger. Bewegt sich ein Objekt durch dieses Feld, wird das Signal gestört – ein Alarm wird ausgelöst. Diese Technologie eignet sich besonders für den Außenbereich, da Mikrowellen weder durch Dunkelheit noch durch Regen, Nebel oder Schnee beeinträchtigt werden. Typische Anwendungen sind Mikrowellenbarrieren entlang von Zäunen oder Zufahrten sowie volumetrische Systeme zur Absicherung schmaler Geländestreifen. Reichweiten von bis zu 200 Metern pro Linie machen sie zu einer effizienten Lösung für großflächige Areale. Ihre hohe Reichweite verlangt jedoch eine exakte Ausrichtung und stabile Montage, um Fehlauslösungen durch Reflexionen oder bewegte Objekte außerhalb der Zone zu vermeiden.

Passiv-Infrarot-Sensoren (PIR) arbeiten dagegen ohne eigene Strahlung und reagieren auf Veränderungen der Wärmestrahlung im Erfassungsbereich. Sie erkennen zuverlässig die Bewegung von Personen oder warmen Objekten und werden häufig in der Umfeldüberwachung von Gebäuden, an Toren oder in Kombination mit

Videoüberwachungssystemen eingesetzt. PIR-Sensoren sind kostengünstig, energieeffizient und einfach zu installieren, jedoch empfindlich gegenüber extremen Witterungsbedingungen und Temperaturänderungen.

Besonders effektiv sind Kombisysteme, die Mikrowellen- und PIR-Technologie vereinen z.B. ein Dual-Technologie-Volumendetektor für Außenanlagen, der eine hochfrequente Doppler-Radarfunktion (Hyper-Frequenz) und ein Passiv-Infrarot-(PIR-)Modul kombiniert. Solche Systeme lösen nur dann Alarm aus, wenn beide Sensoren gleichzeitig eine Bewegung detektieren. Dadurch lassen sich Falschalarme durch Wind, Regen, Tiere oder Sonneneinstrahlung deutlich reduzieren. Diese Dualtechnologie findet vor allem in sensiblen Bereichen Anwendung – etwa in Energieversorgungsanlagen, Flughäfen oder logistischen Hochsicherheitszonen.

Lichtschrankensysteme

Aktive Lichtschrankensysteme spielen im modernen Perimeterschutz eine zentrale Rolle, da sie eine zuverlässige und unauffällige Methode zur frühzeitigen Erkennung von Eindringlingen bieten. Sie arbeiten mit unsichtbaren aktiven Infrarotstrahlen, die zwischen Sender- und Empfängereinheiten verlaufen. Wird dieser Strahl unterbrochen, löst das System sofort einen Alarm aus. Dadurch lassen sich Grenzverletzungen bereits erkennen, wenn physische Barrieren wie Zäune oder Tore überwunden werden. Auch sind Lichtschrankensystem besonders geeignet, wenn z.B. gar keine Zäune vorhanden sind und man um ein zu schützendes Objekt einen virtuellen Zaun errichten möchte, der ohne Alarmauslösung nicht durchbrochen werden kann.

Ein wesentlicher Vorteil von Lichtschranken liegt in ihrer Flexibilität und ihrem geringen Installationsaufwand. Je nach Modell können sie kabelgebunden oder auch völlig autark (Solar + Funkübertragung) betrieben werden, was sie für unterschiedlichste Umgebungen geeignet macht – von Industriearealen und Energieanlagen über Flughäfen und Logistikzentren bis hin zu temporären Absicherungen bei Veranstaltungen. Sie lassen sich sowohl als alleinstehende Detektionslösung als auch als Ergänzung zur Zaunsensorik oder Videoüberwachung einsetzen.

Lichtschranken ermöglichen eine präzise Linienüberwachung mit klar definierten Detektionszonen. Moderne Systeme bieten dabei zusätzliche Funktionen wie die Unterscheidung zwischen Personen, Tieren und Fahrzeugen, um über die Filterung nach Objektgröße Falschalarme zu reduzieren. Auch in bestehenden Sicherheitsinfrastrukturen lassen sie sich über Schnittstellen und Netzwerkanbindungen einfach integrieren.

Insgesamt bieten Lichtschrankensysteme eine effiziente, skalierbare und wartungsarme Lösung zur Perimeterüberwachung. Sie erhöhen die Detektionssicherheit, schaffen zusätzliche Reaktionszeit und tragen wesentlich dazu bei, ein Gelände lückenlos und frühzeitig gegen unbefugtes Eindringen zu schützen.

Besserer Schutz durch integriertes Datenmanagement und Sensorfusion

Ein wirksamer Perimeterschutz beruht wie gesagt häufig auf einem mehrschichtigen Ansatz, bei dem verschiedene Technologien miteinander kombiniert werden. Ziel ist es, die Sicherheit auch dann aufrechtzuerhalten, wenn eine einzelne Methode ausfallen sollte. Es genügt nicht, lediglich einen Alarm auszulösen, sobald ein Zaun überwunden wird. Vielmehr müssen mehrere Sicherheitsebenen eingerichtet sein, die unbefugte Personen schon vor dem Erreichen besonders schützenswerter Bereiche stoppen oder zumindest verzögern. Damit diese Systeme nicht isoliert arbeiten, sondern als integriertes Gesamtsystem funktionieren, ist ein einheitlicher Ansatz zur Qualifizierung von Ereignissen und Alarmen essenziell. Ein entsprechendes Sicherheitsmanagementsystem ermöglicht einen umfassenden Überblick über die gesamte Sicherheitsinfrastruktur – insbesondere vor dem Hintergrund der zunehmenden Bedeutung des Internets der Dinge (IoT) und wachsender Cyberrisiken.

Die Einführung einer offenen und einheitlichen Sicherheitsplattform verbessert die Situationsübersicht für Sicherheits- und Betriebspersonal erheblich. Verschiedene Teilsysteme – wie Detektionssysteme, Video, EMA und weitere Sicherheitselemente – werden unter einer gemeinsamen Oberfläche gebündelt. Dies erlaubt schnelle Reaktionen und verhindert Zeitverluste, die durch den Wechsel zwischen separaten Systemen entstehen könnten. Moderne Technologien wie Infrarot, Zaunsensoren, verlegte Kabelsensoren, LiDAR und Videoanalytik tragen dazu bei, Bedrohungen frühzeitig zu erkennen und einzuschätzen, zur genauen Bewertung von Gefahren ist jedoch in der Regel eine visuelle Bestätigung erforderlich. Hochauflösende Kameras mit Infrarotfunktion ermöglichen eine schnelle Identifikation und Verfolgung von Zielen. Alarmmeldungen können direkt und mobil an Interventionskräfte weitergeleitet werden.

Physische Identitäts- und Zugangsmanagementsysteme sorgen dafür, dass Zutrittsrechte automatisch und gemäß den Unternehmensrichtlinien angepasst werden – beispielsweise bei einem Personalwechsel. Die zunehmende Vernetzung birgt jedoch auch neue Cyberrisiken, etwa durch unsichere oder falsch konfigurierte Geräte. Deshalb ist es für Sicherheitsverantwortliche unerlässlich, sicherzustellen, dass die Hersteller der eingesetzten Geräte aktuelle Sicherheitsstandards erfüllen und regelmäßige Updates bereitstellen. Ein einheitliches System unterstützt dabei, den Status aller Komponenten zu überwachen und frühzeitig auf Schwachstellen hinzuweisen.

Mit steigender Zahl der eingesetzten Sensoren wächst auch das Datenvolumen, das ausgewertet werden muss. Ein einheitliches System hilft, diese Datenflut durch automatisierte Alarme und digitale Standardarbeitsanweisungen effizient zu managen. So werden Vorfälle unabhängig vom jeweils eingesetzten Schichtpersonal konsistent und effektiv bearbeitet. Die automatische Korrelation von Ereignissen aus verschiedenen Quellen ermöglicht es eventuell auch, Muster zu erkennen und Bedrohungen schneller zu identifizieren.

Ein mehrschichtiger Ansatz stellt außerdem sicher, dass sämtliche Bereiche eines Perimeters zuverlässig überwacht werden – einschließlich potenzieller Schwachstellen wie Zufahrten oder toter Winkel, die mit Kameras allein unter Umständen nicht lückenlos erfasst werden können. Ein entscheidender Vorteil der Sensorfusion ist die deutliche Reduktion von Falschalarmen, was für einen wirtschaftlichen Betrieb von großer Bedeutung ist. Weniger Falschauslösungen bedeuten eine geringere Belastung der Interventionskräfte und erhöhen gleichzeitig die Akzeptanz des Systems bei allen Beteiligten.

Die Kombination und richtige Konfiguration moderner Sensorik – abgestimmt auf die individuellen Bedingungen vor Ort – bildet die Grundlage für einen wirksamen und robusten Perimeterschutz. Regelmäßige Überprüfung, Wartung und Anpassung der Systeme sind ebenso wichtig wie die Einbindung in ein ganzheitliches Sicherheitskonzept. GIT

Erfahren Sie mehr

Praxistipps für die Installation von Perimeterschutz-Systemen sowie Hintergrund-Infos zum KRITIS-Dachgesetz lesen Sie in der erweiterten Fassung des Artikels hier auf GIT-SICHERHEIT.de

Heiko Viehweger, Vertriebsleiter DACH
Hirsch Secure GmbH
www.hirschsecure.de

PERIMETERSCHUTZ

Punktwolken-Landung am Perimeter

Wie 3D-LiDAR die Zaunsicherung revolutioniert

Die Sicherung von Perimetern, insbesondere Zäunen, stellt eine zentrale Herausforderung für die Sicherheitsbranche dar. Traditionelle Technologien wie Videokameras und Thermalkameras stoßen jedoch oft an ihre Grenzen. 3D-LiDAR-Technologie bietet eine Alternative. Sie erstellt präzise 3D-Punktwolken und ermöglicht eine zuverlässige, datenschutzfreundliche und effiziente Überwachung. Die Vorteile, fortschrittliche Funktionen und praxisnahe Einsatzmöglichkeiten von 3D-LiDAR zur Zaunsicherung erläutert Andreas Bollu, Vice President der Business Unit Security bei Blickfeld.

Präzision bei jeder Sichtbedingung, Reduktion von Fehlalarmen und Datenschutzfreundlichkeit – so lassen sich die Vorteile von 3D-LiDAR für die Zaunsicherung auf den Punkt bringen. LiDAR steht für Light Detection and Ranging und nutzt gepulste Laserstrahlen, um die Umgebung präzise dreidimensional zu erfassen. Die Technologie ermöglicht eine genaue Lokalisierung von Objekten sowie die Analyse ihrer Bewegungsmuster im erfassten Raum.

3D-LiDAR-Sensoren sind aktive Messsysteme, die ihre eigene Lichtquelle nutzen und können daher unabhängig von äußeren Lichtverhältnissen operieren. Bei Dunkelheit liefern sie sogar bessere Ergebnisse als bei Tageslicht. Auch unter schwierigen Wetterbedingungen wie Regen, Schnee oder Nebel bleibt LiDAR deutlich zuverlässiger als andere Technologien, wie etwa Kameras, deren Leistung bei schlechten Sichtverhältnissen häufig stark abnimmt.

Die LiDAR-Technologie kann Objekte anhand ihrer Größe und Bewegungsmuster unterscheiden. Dadurch erkennt das System zuverlässig, ob es sich um eine tatsächliche Bedrohung, wie das Eindringen einer Person, oder um ein harmloses Ereignis, wie herabfallende Blätter oder kleine Tiere handelt. Während andere Sensoren Schatten als Objekte wahrnehmen und möglicherweise Fehlalarme auslösen, erkennt das LiDAR-System diese nicht, da es nur reale, reflektierende Objekte detektiert.

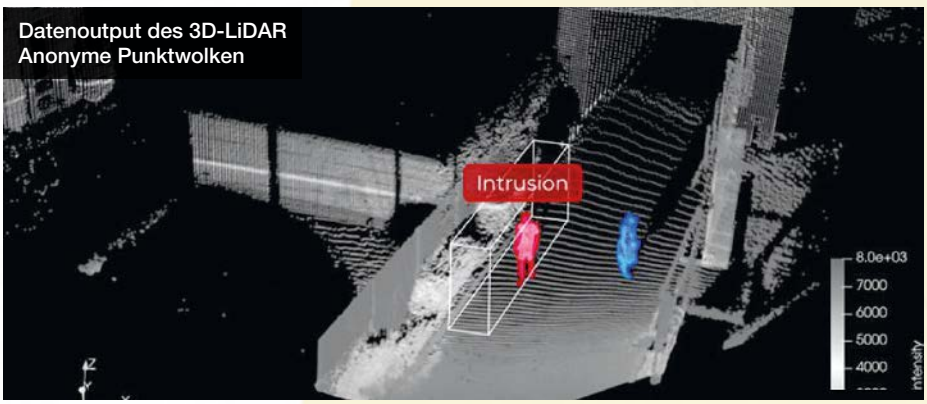
Dazu kommt die Datenschutzfreundlichkeit: LiDAR-Sensoren erfassen ausschließlich geometrische Daten. Diese abstrakten Punktwolken ermöglichen eine DSGVO-konforme Überwachung, da sie keine identifizierenden Merkmale wie Gesichter, Kleidung oder andere persönliche Merkmale enthalten. Dies macht 3D-LiDAR besonders geeignet für Einsätze in sensiblen Bereichen, wie kritischen Infrastrukturen oder öffentlichen Räumen, wo Datenschutz eine hohe Priorität hat.

Erweiterte Software-Features

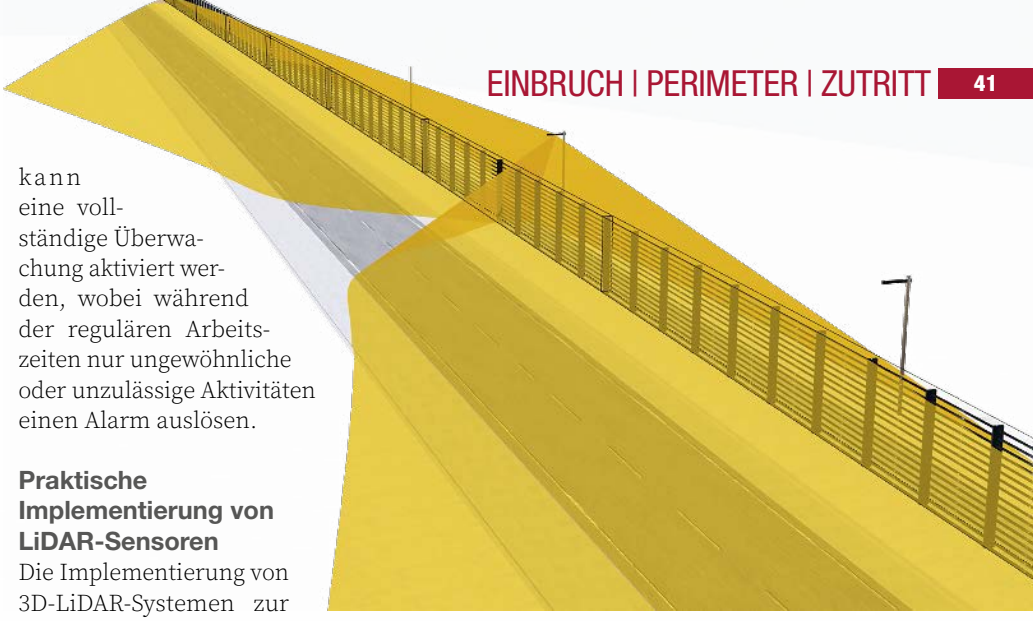
Ein Beispiel für ein 3D-LiDAR-System mit integrierter Datenverarbeitung ist der Blickfeld QbProtect. Der smarte Sensor erfasst detaillierte 3D-Daten, die dann direkt von der Software analysiert werden. Diese intelligenten Algorithmen sorgen dafür, dass Alarme nur dann ausgelöst werden, wenn wirklich eine Bedrohung vorliegt.

Durch die Möglichkeit, präzise 3D-Alarmzonen entlang des Zauns zu definieren, können verdächtige Aktivitäten frühzeitig erkannt und Alarme ausgelöst werden. Diese Zonen können im dreidimensionalen Raum eingerichtet werden, um spezifische Bereiche – sowohl vor als auch entlang des Zauns – genau zu überwachen. Beispielsweise ermöglichen Frühwarnzonen vor dem Zaun es, potenzielle Eindringlinge zu erkennen und deren Bewegungsmuster zu tracken, noch bevor sie den Zaun erreichen.

Verdächtige Objekte werden so lokalisiert und entlang des Zauns verfolgt. Überstiegszonen hingegen werden nur aktiviert, wenn Personen versuchen, den Zaun aktiv zu übersteigen. Ein Hauptalarm löst dann aus, wenn der Zaun tatsächlich überwunden bzw. durchbrochen wurde, und eine akute Sicherheitsbedrohung besteht. Eine solche Zonenaufteilung ermöglicht eine differenzierte Reaktion auf verschiedene Sicherheitsereignisse und optimiert den Ressourceneinsatz.



Datenoutput des 3D-LiDAR
Anonyme Punktwolken



3D-Simulation der versetzen Zaunmontage von zwei LiDAR-Sensoren

Alarmgenerierung nach Objektgröße

Ein wesentlicher Vorteil der 3D-LiDAR-Technologie ist die Fähigkeit, Objekte anhand ihrer Größe und Form zu erkennen. Die Sensoren erfassen nicht nur die Position und Bewegung von Objekten, sondern auch deren Dimensionen. Diese Informationen ermöglichen es, zwischen verschiedenen Arten von Objekten zu unterscheiden, wie etwa Personen, Tieren oder Fahrzeugen. Durch diese Unterscheidung wird die Alarmierung gezielt: Ein Alarm wird nur ausgelöst, wenn eine tatsächliche Bedrohung, wie eine Person, erkannt wird, während kleinere, für die Sicherheit irrelevante Objekte, wie Tiere oder kleine Gegenstände, keine Reaktion hervorrufen. Diese Funktion trägt erheblich dazu bei, Fehlalarme zu reduzieren und die Genauigkeit der Überwachung zu verbessern.

Regelbasierte Alarmlogik

Eine der zentralen Funktionen moderner Sicherheitslösungen ist die Möglichkeit, Alarmlogiken individuell anzupassen, um den spezifischen Anforderungen der jeweiligen Anwendung gerecht zu werden. Nutzer können maßgeschneiderte Alarmregeln definieren, die präzise festlegen, wann und unter welchen Bedingungen Alarme ausgelöst werden. Diese Flexibilität ist besonders vorteilhaft in dynamischen oder komplexen Szenarien, wie sie bei der Zaunsicherung auftreten können.

So lässt sich die Alarmlogik so konfigurieren, dass nur bestimmte Bewegungsmuster und Verweildauern innerhalb eines definierten Bereichs am Zaun einen Alarm auslösen. Diese Anpassung hilft, Fehlalarme durch Tiere oder Umwelteinflüsse, wie etwa durch Laubbewegungen im Wind, zu minimieren. Darüber hinaus können auch andere Faktoren wie die Verfolgungslänge und die Dauer des Eindringens in das Überwachungsgebiet berücksichtigt werden, um verdächtige Aktivitäten noch gezielter zu identifizieren.

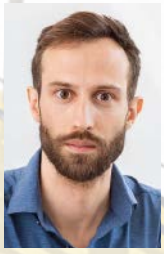
Die Alarmlogik ermöglicht es zudem, verschiedene Sicherheitslevels zu implementieren: Außerhalb der Betriebszeiten kann eine vollständige Überwachung aktiviert werden, wobei während der regulären Arbeitszeiten nur ungewöhnliche oder unzulässige Aktivitäten einen Alarm auslösen.

Praktische Implementierung von LiDAR-Sensoren

Die Implementierung von 3D-LiDAR-Systemen zur Zaunsicherung erfordert eine sorgfältige Planung, um eine effiziente Überwachung zu gewährleisten. Dabei variieren die Montageoptionen der Sensoren je nach Anwendung und Anforderungen. So können LiDAR-Sensoren an Gebäudefassaden montiert werden, orthogonal zum Zaun, um präzise zu erkennen, ob sich eine Person vor oder hinter dem Zaun befindet. Alternativ können die Sensoren an Masten hinter dem Zaun entlang der Perimeterlinie positioniert werden (versetzte Zaunmontage), um eine lückenlose Überwachung über große Entfernungen hinweg zu ermöglichen. Dies ist besonders nützlich in schwer zugänglichen oder weitläufigen Bereichen. Eine weitere Möglichkeit besteht darin, die Sensoren direkt auf dem Zaun anzubringen (direkte Zaunmontage), was ebenso eine kontinuierliche Überwachung der gesamten Perimeterlinie gewährleistet, ohne zusätzliche Masten zu benötigen.

Zusätzlich können LiDAR-Sensoren, je nach Material und Aufbau des Zauns, in der Lage sein, Objekte durch den Zaun hindurch zu erfassen, was eine noch flexiblere Installation ermöglicht, die sich an die unterschiedlichen Gelände- und Umgebungseigenschaften anpasst. Smarte 3D-LiDAR-Sensoren bieten zudem den Vorteil, dass sie die erfassten Daten direkt verarbeiten. Diese Funktion vereinfacht die Integration in bestehende Sicherheitsinfrastrukturen zusätzlich und reduziert den Bedarf an zusätzlicher Hardware, was besonders in abgelegenen Gebieten von Vorteil ist.

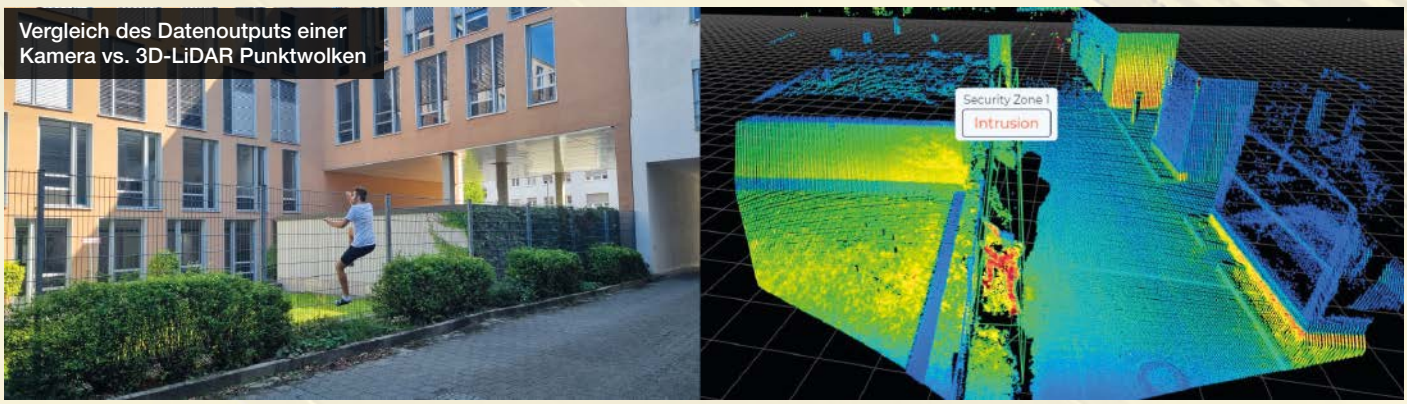
LiDAR-Sensoren wie der Blickfeld QbProtect Smart Security LiDAR lassen sich problemlos in Video-Management-Systeme (VMS) und andere Sicherheitslösungen integrieren. Dank gängiger Standardschnittstellen und Protokolle wie RTSP (Real-Time Streaming Protocol) oder ONVIF können sie nahtlos mit bestehenden Technologien wie Kameras und Zutrittskontrollsystemen verknüpft werden. Dies ermöglicht eine zentrale Steuerung verschiedener Sicherheitskomponenten, ohne umfangreiche Anpassungen an der vorhandenen Infrastruktur vorzunehmen. GIT



Autor:
Andreas Bollu
VP Security Business Unit
bei Blickfeld GmbH

Blickfeld GmbH
www.blickfeld.com

Vergleich des Datenoutputs einer Kamera vs. 3D-LiDAR Punktwolken



Solarparks wie die von Greentech in Nienbüttel betriebene Anlage werden meist auf der „grünen Wiese“ errichtet

ENERGIE UND VERSORGER

In exponierter Lage

Digitale Sicherheit reicht nicht: Intelligente Schließtechnik für Photovoltaik-Parks

Mit der Solarleistung von Photovoltaik-Parks steigt auch die Bedeutung dieser Anlagen für eine versorgungssichere Energieinfrastruktur. Unternehmen wie Greentech, die mit Projektentwicklung, Asset Management, Anlagenbau und Betriebsführung alle Stationen des Photovoltaik-Downstreams abbilden, stehen damit vor der Herausforderung, Solarparks wirksam und langfristig sowie kosteneffizient physisch abzusichern, ohne dabei auf eine flexible Handhabung und Wartungsfreundlichkeit zu verzichten. Bei der Sicherung von sechs Anlagen in Nord- und Süddeutschland setzt das Hamburger Photovoltaik-Unternehmen daher auf das elektronische Schließsystem eCliq der Marke Ikon von Assa Abloy.

Das elektronische Schließsystem eCliq bietet hohen Schutz gegen Manipulation und intelligente Angriffe

Erneuerbare Energien erzeugten im Mai 2025 rund zwei Drittel des in Deutschland produzierten Stroms – ein bisheriger Höchstwert. Laut Angaben der Denkfabrik Agora Energiewende trug dabei allein die Photovoltaik (PV) 29 Prozent bei und lieferte damit mehr Strom als alle fossilen Kraftwerke zusammen. Mit einer installierten Leistung von rund 100 Gigawatt (GW) stellen PV-Anlagen somit schon heute einen unverzichtbaren Baustein der Energieversorgung dar. Das Ziel für den PV-Ausbau in Deutschland liegt jedoch noch höher. Bis zum Jahr 2030 sollen 215 GW erreicht werden.

Großdimensionierte Projekte

Diesen ambitionierten Ausbauzielen leisten auch Solar- und Speicher-Spezialisten wie Greentech durch zahlreiche Projekte Vorschub. Das im Jahr 2008 gegründete Hamburger Unternehmen zählt heute zu den namhaften Anbietern für den Betrieb von PV-Kraftwerken in Europa und verantwortet von der Projektentwicklung, der Planung und dem Anlagenbau sowie technischem und kaufmännischem Asset-Management weitere Leistungen in den Bereichen Engineering, technische Beratung, Finanzierung und Stromvermarktung.

Zuletzt gingen im Juni 2024 im Landkreis Steinburg drei Solarparks von Greentech ans Netz. Zusammen erreichen die Anlagen eine Gesamtkapazität von über 100 MWp (Megawatt Peak) und repräsentieren damit das bislang größte Portfolio des Solar- und

Speicher-Spezialisten. Mit der kleinsten Installation in Nienbüttel nahe dem durch sein Open-Air-Festival bekannten Wacken erreicht das Unternehmen mit 32.580 bifazialen Solarmodulen, verteilt auf einer Fläche von rund 17 Hektar, eine maximale Leistungskapazität von 21,45 MWp. Auch im Süden Deutschlands treibt Greentech den Ausbau der Kapazitäten mit insgesamt drei Anlagen in Großheirath und Untersiemau voran.

Kritische Infrastruktur erfordert umfassenden Schutz

Mit der zunehmenden Bedeutung von Photovoltaik-Anlagen wächst jedoch auch das Risiko, dass diese zu potenziellen Zielen für Sabotage, Vandalismus oder Diebstahl werden. Der jüngste Verfassungsschutzbericht und Warnungen des BSI vor hybriden Bedrohungsszenarien machen deutlich: Digitale Sicherheit allein reicht nicht mehr aus.

Für Betreiber von Photovoltaik-Anlagen bedeutet dies die Notwendigkeit, neben der Cybersicherheit auch für umfassenden physischen Schutz vor unerlaubtem Zutritt und Manipulation zu sorgen. Die großflächigen und oft abgelegenen Solarparks stellen dabei besondere Anforderungen. Nicht zuletzt erfordern die Betriebsabläufe mit unterschiedlichen Serviceteams und Wartungsfirmen differenzierte Zugangsberechtigungen zu unterschiedlichen Anlagenbereichen.

Dezentrale Anlagen, zentrale Verwaltung

Auf der Suche nach einer geeigneten Schließlösung für diese Anforderungen, fiel die Wahl auf die Cliq-Technologie von Assa Abloy. Das System lässt sich flexibel erweitern, kombinieren oder nachrüsten und ist damit wie gemacht für den Anwendungsfall. Ein entscheidender Vorteil liegt in der wartungsarmen Konzeption. Anders als herkömmliche elektronische Schließzylinder benötigt eCliq keine regelmäßigen Batteriewechsel vor Ort. Energieversorgung und Datenübertragung erfolgen direkt über den Schlüssel beziehungsweise Programmierschlüssel. Dies bedeutet Kosteneinsparungen bei der Wartung.

Ebenso effizient gestaltet sich auch die Programmierung und Verwaltung des elektronischen Schließsystems. Zugangsrechte lassen sich individuell steuern und bei Bedarf zentral anpassen. Im Fall eines Schlüsselverlusts kann die betreffende Schließberechtigung gezielt aus dem System entfernt werden, ohne dass andere Zugänge betroffen sind. Diese Flexibilität ist entscheidend, wenn verschiedene Personen differenzierten Zugang zu unterschiedlichen Anlagenbereichen benötigen.

Partner für Beratung und Einbau

Bei der Umsetzung des Sicherheitskonzepts setzte Greentech auf die Expertise der Wilhelm Albers Hamburg. Das traditionsreiche Unternehmen übernahm nicht nur die umfassende Beratung zur Systemauswahl, sondern auch die fachgerechte Installation der eCliq-Komponenten. Mit jahrzehntelanger Erfahrung im Bereich professioneller Sicherheitslösungen und einem breiten Portfolio rund um elektronische Zutrittssysteme zählt Wilhelm Albers Hamburg zu den führenden Fachhändlern und Servicepartnern im norddeutschen Raum.

Die bislang gesammelten positiven Erfahrungen lassen die Verantwortlichen bei Greentech daher bereits über eine mögliche Ausweitung des Einsatzes nachdenken: „Die große Flexibilität, die hohe Sicherheit sowie die langfristig gut planbaren und vergleichsweise geringen Kosten des Systems haben uns überzeugt. Wir planen daher eCliq auch in weiteren Anlagen einzusetzen“, erklärt Max Langkabel, Team Lead Power Plant IT & ICS von Greentech. GIT

Assa Abloy Sicherheitstechnik GmbH
www.assaabloy.com/de

A&E Partnerprogramm von Dallmeier unterstützt Fachplaner

© Dallmeier electronic

Mit dem Architects & Engineers (A&E) Partnerprogramm bietet Dallmeier Architekten, Fachplanern und Ingenieuren umfassende Unterstützung bei der Planung und Umsetzung moderner Videosicherheitssysteme – durch fundiertes Know-how, spezialisierte Tools und exklusive digitale Ressourcen. Mit dem A&E Partnerprogramm erhalten Planer und Ingenieure direkten Zugang zu praxisbewährten Tools, Ressourcen und Fachkenntnissen, um belastbare und zukunftsorientierte Videosicherheitslösungen zu planen – gestützt auf jahrzehntelange Erfahrung. Ziel ist es, maximale Effizienz, Transparenz und Planungssicherheit bei der Spezifikation, Planung und Implementierung von Sicherheitsprojekten zu gewährleisten. Zu den Kernbausteinen des A&E Partnerprogramms zählen die professionelle Planungssoftware PlanD, die mobile Medienplattform PresentD sowie CalcD, um Projektkosten auf Knopfdruck visualisieren zu können. **www.dallmeier.com**

ZUTRITTSKONTROLLE

Das Beste aus zwei Welten

Zutrittsmanagement mit dem Smartphone

Mit dem Dom Tapkey-Portfolio bietet Dom1 Sicherheitstechnik eine große Auswahl an digitalen Zylindern, digitalen Beschlägen, Wandlesern, digitalen Möbelverschlüssen und einem digitalen Hangschloss, um jede Verschlusssituationen erfüllen zu können. Egal ob man Familie, Vermögenswerte oder die Firma schützen möchte – für Sicherheit ist gesorgt.

Alle Dom Produkte sind durch höchste Verschlüsselungsmechanismen gesichert. Zudem sorgt die hochwertige und starke Mechanik in Kombination mit innovativen Elektronikkomponenten für Sicherheit, Zuverlässigkeit und eine lange Lebensdauer. Innerhalb von wenigen Minuten kann man ein eigenes digitales Schließsystem in drei einfachen Schritten erstellen: Tapkey App im Google Playstore oder App-Store herunterladen, Aktivierung eines Accounts und Aufnahme eines Schließgerätes per BLE , z. B. ein digitaler Zylinder in der Eingangstür oder der Garage – und fertig.

In wenigen Schritten vergibt man Berechtigungen an Benutzer, die dann mit dem Smartphone Türen öffnen und schließen können. Alternativ nutzt man einfach die Dom Tapkey Transponder (Schlüsselanhänger-Transponder für digitale Schlüssel) oder die Apple Watch.

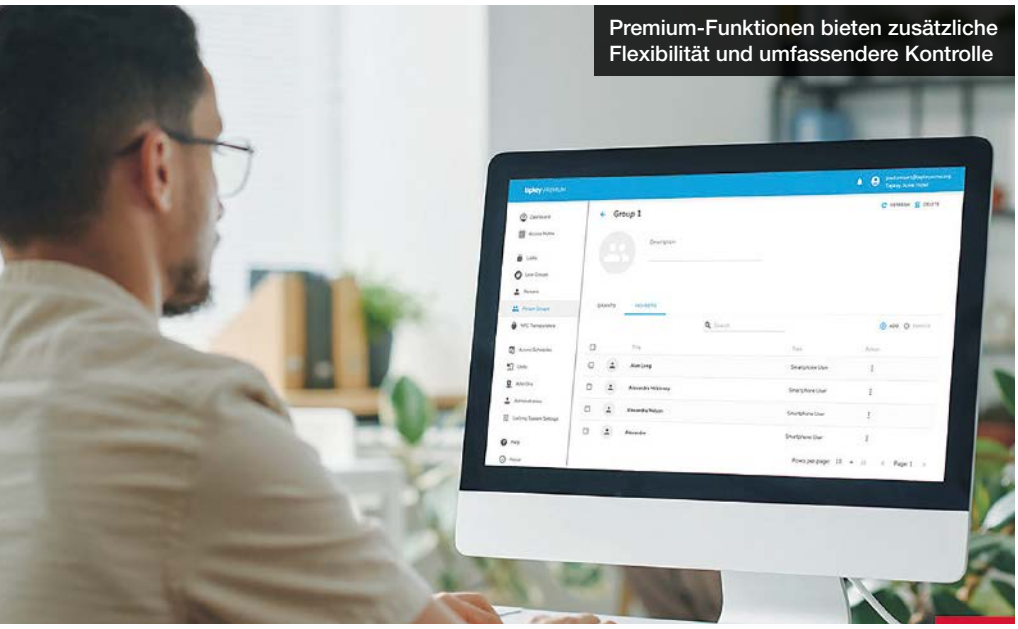
Basisfunktionen

Die wichtigsten Basisfunktionen für mobilen Zutritt sind sofort einsatzbereit. Mit der Tapkey-App erledigt man alle Schritte komfortabel und ohne technischen Aufwand: Von der schnellen Installation über die Registrierung bis hin zur laufenden Verwaltung und Wartung von smarten Geräten.

Das Erstellen, Vergeben und Löschen von elektronischen Schlüsseln – sogenannte Smartphone Keys – ist innerhalb weniger Sekunden erledigt. Auf Wunsch lassen sich zeitliche Beschränkungen festlegen, um den Zugang präzise zu steuern.

Auch das Beschreiben von Transpondern z.B. Zutrittskarten ist direkt mit dem Smartphone möglich. Die Tapkey App macht das Programmieren von physischen Zutrittsmedien schnell, sicher und unkompliziert. Das Zutrittsprotokoll zeigt alle Aktivitäten an und informiert, wer zu welchem Zeitpunkt welches elektronische Gerät geöffnet hat.

Mit dem „Office Mode“ bleiben Türen, beispielsweise während Bürozeiten, dauerhaft geöffnet. So haben etwa Besucher, Kunden oder Lieferdienste auch ohne digitale Schlüssel Zugang. Mehrere Geräte lassen sich zu Gruppen zusammenfassen, zur Strukturierung des Zutrittsmanagements – ideal, um verschiedene Bereiche oder Standorte effizient zu organisieren.



Premium-Funktionen bieten zusätzliche Flexibilität und umfassendere Kontrolle

Premium-Features

Die Premium-Funktionen, die im Rahmen eines Premium-Tarifs verfügbar sind, bieten zusätzliche Flexibilität und umfassendere Kontrolle – insbesondere für wachsende Unternehmen und komplexe Zutrittsanforderungen.

Individuelle Zeitfenster, in denen berechtigte Personen Zugang zu bestimmten Türen erhalten, lassen sich festlegen. Diese Zeitpläne können mehrfach genutzt werden

und vereinfachen die zentrale Verwaltung sowie Anpassung mehrerer Zugangsberechtigungen.

Außerdem möglich ist das Bündeln von Usern, Schließmedien oder Smartphone Keys mit identischen Zutrittsanforderungen in übersichtlichen Gruppen. So passt man Berechtigungen für viele Personen gleichzeitig mit nur wenigen Handgriffen an.

Um den Überblick zu behalten, lassen sich sämtliche Personen, Türen und Schließmedien über eine zentrale Zutrittsmatrix steuern. Das spart Verwaltungsaufwand und reduziert Fehler durch eine klar strukturierte Darstellung.

Das Schließsystem lässt sich zudem in separate Bereiche aufteilen – jede Einheit mit eigenen Administratorrechten und individuellen Datenschutzeinstellungen. Dies eignet sich insbesondere für großflächige Anlagen oder Gebäude mit mehreren Parteien. GIT

Mit Dom Tapkey kann man innerhalb von wenigen Minuten ein digitales Schließsystem erstellen

© Bilder: Dom Sicherheitstechnik

Dom Sicherheitstechnik
www.dom-security.com

Planet Absenkdichtungen für Glastüren

Die Assa Abloy (Schweiz) AG präsentiert im zweiten Halbjahr 2025 ein vollständiges Upgrade ihrer Absenkdichtungen aus der Planet KG-Produktfamilie für Glastüren. Die vielfältigen Absenkdichtungen der optimierten Glaslinie KG-A/S/F zeichnen sich vor allem durch ihre einfache Montage ohne Trocken- und Liegezeiten sowie den ungebrochen hohen Anspruch an Qualität und Funktionalität aus. Dank der vielen verfügbaren Farbvarianten werden sie außerdem jedem Design gerecht. Die Absenkdichtungen der Marke Planet schließen zuverlässig den Spalt zwischen Tür und Boden und eignen sich für alle Arten von Türen im Neubau sowie Bestand. Bei der Optimierung des Planet KG-Produktportfolios für ein- und zweiflügelige Ganzglastüren legten die Schweizer Türlösungsexperten einen besonderen Fokus auf eine clevere und zeitsparende Montage. Gleichzeitig bleibt der effektive Schallschutz für die Glassysteme sowie das ästhetische optische Erscheinungsbild in gewohnt hoher Qualität gewährleistet. **www.assaabloy.com**

© Assa Abloy (Schweiz) AG

DIGITALE SCHLIESSTECHNIK

Jede Menge Schotter

Digitale Schließtechnik bei Ernst Derfeser in Tirol

„Stillstand gibt es bei uns nicht“ – so ließe sich die Philosophie der Derfeser Firmengruppe in Vomp (Tirol) beschreiben. Sie spiegelt sich auch bei der eingesetzten Sicherheitstechnik: Das Unternehmen setzt auf modernste digitale Schließtechnik von SimonsVoss.

Die Firma Ernst Derfeser ist ein renommiertes Tiroler Familienunternehmen, das in dritter Generation geführt wird. Die kontinuierlich gewachsene Firmengruppe ist durch ihre breite Produkt- und Dienstleistungspalette (Erdbau, Sand- und Schottergewinnung, Erzeugung von Transportbeton, Containerdienst, Recycling & Entsorgung, Deponiebewirtschaftung, Transporte, Kranarbeiten, Mietpark und Straßendienst) seit mehr als 95 Jahren Partner am Bau. In mehreren Schritten wurde und wird im Unternehmen nun modernste digitale Schließtechnik von SimonsVoss installiert.

Dezentrale Unternehmensstruktur

Der Start ins digitale Zeitalter mit SimonsVoss als Lieferant begann 2018 mit der Montage der ersten Schließungen. Die Herausforderung bestand von Anfang an in der Tatsache, dass die Gebäude und Infrastruktureinrichtungen der Derfeser-Gruppe regional an verschiedenen Standorten liegen. Ein Teil davon verfügte zu diesem Zeitpunkt noch über eine mechanische Schließanlage, deren Verwaltung und Betrieb aber zusehends schwieriger wurden. Durch

Ernst Derfeser in Tirol: Seit mehr als 95 Jahren Partner am Bau

die dezentrale Gebäudestruktur konnte die digitale Schließtechnik nun bis heute einen ihrer größten Vorteile ausspielen, denn damit lassen sich die unterschiedlichen Einheiten und Schließungen zentral und sehr flexibel verwalten. Mitarbeiter mit großem Schlüsselbund sieht man bei Derfeser nicht mehr.

Blick auf das Verwaltungsgebäude auf dem Gelände von Ernst Derfeser

Funktionssicher trotz Staub und Feuchte

Weitere Eigenschaften der SimonsVoss-Technologie überzeugten die Verantwortlichen in der Firmengruppe: Die Stabilität der Komponenten erweist sich als äußerst hilfreich bei den oft widrigen Bedingungen auf dem regional verzweigten Betriebsgelände, zum Beispiel mit reichlich Staubentwicklung im Bereich der Schotterproduktion. Witterungseinflüsse wie Feuchtigkeit und Kälte sind ebenfalls kein Problem und es gibt keine Auswirkungen auf die im Vergleich zu Wettbewerbsprodukten sehr langen Batteriestandzeiten.

Transponder und SmartCards im Einsatz

Ausgestattet mit SimonsVoss-Komponenten sind derzeit das Gebäude der kaufmännischen Verwaltung in Vomp, das Schotterwerk Vomperbach, der Standort Recycling & Entsorgung in Pill und das Betonwerk in Ranggen.

Aktuell umfasst die digitale Zutrittssteuerungsanlage bei Derfeser fünf SmartRelais 3 (SREL 3) Steuerungseinheiten mit externem Leser zur Außenabsicherung an den Haupteingängen und Waschanlagen sowie 60 Digital Cylinder AX in verschiedensten Türen im Bestand und Garagentoren mit integrierten Gehtüren. Dazu kommen 65 Beschläge für Innentüren im Bürotrakt (Typ 3062 und SmartHandle AX) und in außenliegenden Containern (SmartHandle AX Advanced). Bei den Schließmedien werden sowohl Transponder wie auch SmartCards (Mifare Desfire) eingesetzt. Der Kreis der Zutrittsberechtigten umfasst inklusive der Fahrer rund 600 Personen.

Maßgeschneiderte Zutrittsberechtigungen

Verantwortlich für die Planung und Montage der digitalen Schließtechnik ist der SimonsVoss-Fachhandelspartner Schrack Seconet mit Sitz in Innsbruck. Das Unternehmen hat außerdem das zuständige Personal von Derfeser auf die Anlage geschult, so dass eine interne Betreuung und Verwaltung gesichert sind. Nachdem man zunächst mit einer Offline-Betriebsweise gestartet war, werden nun Schritt für Schritt alle Schließungen auf Online-Vernetzung umgestellt. So lassen sich die Programmierungen vereinfachen und beschleunigen. Die heterogene Unternehmensstruktur bei Derfeser bedingt viele verschiedene Berechtigungsebenen mit entsprechenden Öffnungsabläufen. Zum Teil sind bestimmte Zeitprofile programmiert mit festgelegten Uhrzeiten, in denen der Zugang möglich ist.

Dieses Procedere für alle transparent zu managen, ist mit der digitalen Schließtechnik ebenso wenig ein Problem wie die Vergabe von Zutrittsberechtigungen an Externe. So ist beispielsweise eine Reinigungsfirma für Derfeser tätig, deren Mitarbeitende mit jeweils zeitlichen Begrenzungen Gebäude und Räume betreten können. Sieben Jahre Erfahrung mit den digitalen Schließsystemen von SimonsVoss hat die Derfeser Unternehmensgruppe gesammelt. Erweiterungen der Anlage betrafen neben einzelnen Türen zuletzt das Schotterwerk. Und digital gesichert wird ebenso das im Bau befindliche neue Headquarter in Vomp. GIT

Einer der mit digitaler SimonsVoss-Schließtechnik ausgestatteten Eingänge im neuen Schotterwerk

SimonsVoss Technologies GmbH
www.simons-voss.com

ZUTRITT

Intelligent, individuell, barrierefrei

Wie digitale Zutrittslösungen kommunale Gebäude sicherer und effizienter machen

Das digitale Zutrittssystem eAccess von Glutz lässt sich nahtlos in den kommunalen Alltag integrieren

Traditionelle Schließsysteme stoßen zunehmend an ihre Grenzen. Der Verwaltungsaufwand ist hoch, Schlüsselverluste sind ein Sicherheitsrisiko und kurzfristige Änderungen nur schwer umsetzbar. Digitale Zutrittssysteme wie eAccess von Glutz bieten eine moderne und praxisnahe Lösung, die sich nahtlos in den kommunalen Alltag integrieren lässt. Ein Beitrag von Dietmar Vinke, Geschäftsführer Glutz Deutschland.

Die Anforderungen an moderne kommunale Gebäude haben sich in den letzten Jahren deutlich verändert. Sicherheit, Barrierefreiheit, Datenschutz und gleichzeitig flexible Nutzung – das alles muss heute unter einen Hut gebracht werden. Ob Verwaltungsgebäude, Pflegeeinrichtung, Schule oder Kulturzentrum: Die Vielfalt an Nutzergruppen, wechselnden Zutrittsrechten und organisatorischen Anforderungen stellt Betreiber vor komplexe Herausforderungen.

Das digitale Zutrittssystem eAccess von Glutz ist ein elektronisches, schlüsselloses Zutrittssystem, das berührungslosen, sicheren Zugang ermöglicht – gesteuert über RFID, Code oder App. Es eignet sich gleichermaßen für Neubauten wie für die einfache Nachrüstung im Bestand.

Zutritt intelligent verwalten

In der täglichen Praxis erfordert der Zugang zu öffentlichen Gebäuden differenzierte Lösungen: Angestellte im Rathaus benötigen andere Zugangsrechte als Reinigungspersonal, externe Dienstleister, Besucher oder Vereinsgruppen. Mit einem herkömmlichen Schließsystem lassen sich solche Anforderungen oft nur unzureichend abbilden – ganz abgesehen von den Risiken verlorener Schlüssel oder unbefugter Duplikate.

eAccess erlaubt die Vergabe individueller Zutrittsrechte, die räumlich und zeitlich genau definiert und bei Bedarf in Sekunden geändert oder gelöscht werden können. Die Verwaltung erfolgt zentral über eine benutzerfreundliche Software – lokal, serverbasiert oder über die Glutz-Cloud. Auch die Protokollierung von Zutritten ist möglich und trägt zur Transparenz und Sicherheit bei.

Das System ist dabei so konzipiert, dass es sich flexibel an das jeweilige Gebäude anpasst – vom einzelnen Büroraum über Sitzungssäle bis hin zu komplexen Verwaltungszentren mit mehreren Eingängen und Etagen.

Barrierefreier Zugang

Einrichtungen wie Seniorenresidenzen, Pflegezentren oder medizinische Versorgungszentren stellen besondere Anforderungen an den Zugang: Nutzer mit eingeschränkter Mobilität, wechselndes Personal, Notfallzugänge und gleichzeitig ein hohes Sicherheitsbedürfnis – hier ist ein System gefragt, das zuverlässig funktioniert, einfach bedienbar ist und individuelle Szenarien abbilden kann.

eAccess erfüllt diese Anforderungen durch seine berührungslose Zutrittsfunktion und die Möglichkeit, Zugangspunkte beispielsweise zeitgesteuert oder mit Liftsteuerung auf bestimmte Etagen zu beschränken. Auch digitale Gegensprechanlagen, Briefkastenlösungen oder Paketfächer lassen sich integrieren – für mehr Komfort im Alltag und klare Prozesse in sensiblen Bereichen.

Dank der Möglichkeit zur mobilen Öffnung via App kann das System zudem auch Pflegedienste, externe Therapeuten oder Lieferanten flexibel einbinden – ohne persönliche Schlüsselübergabe.

Kultur, Bildung und Freizeit

In Schulen, Kindergärten, Sporthallen oder Kultureinrichtungen begegnen sich täglich viele unterschiedliche Nutzergruppen. Die Anforderungen reichen von regelmäßigem Zugang für Lehrer oder Personal bis hin zu temporären Zutrittsrechten für Eltern, Vereine oder Veranstalter. Sicherheitsrelevante Bereiche wie Technikräume, Lagerräume oder Lehrerzimmer müssen besonders geschützt werden.

Hier überzeugt eAccess mit seiner Modularität: Zutrittsrechte lassen sich indi-

eAccess ermöglicht berührungslosen, sicheren Zugang– gesteuert über RFID, Code oder App

Glutz bietet nicht nur die Steuerungstechnik, sondern auch passende Beschläge, E-Zylinder, Schlösser und Designkomponenten

viduell definieren, bestimmte Bereiche können nur zu bestimmten Zeiten zugänglich gemacht werden. Auch eine zentrale Freigabe aller Ausgänge im Alarmfall oder bei Gefahrensituationen ist realisierbar. Die einfache Programmierung spart Zeit, senkt Kosten und gibt Verantwortlichen die notwendige Kontrolle.

Technologische Basis

Die Technik hinter eAccess ist ebenso ausgereift wie flexibel. Die Funklösung mit verschlüsselter Datenübertragung ermöglicht die einfache Installation ohne Verkabelung – ideal für Bestandsbauten. Die energieeffizienten Komponenten kommunizieren nur bei Bedarf und weisen extrem niedrige Emissionswerte auf. Der Betrieb ist auch in sensiblen Umgebungen wie Kliniken oder Bildungseinrichtungen unbedenklich.

Die Auswahl an Identifikationsmedien – vom RFID-Clip über die PIN-Eingabe bis hin zur mobilen App – ermöglicht eine nutzerfreundliche Anwendung für alle Alters- und Zielgruppen. Die Systemarchitektur erlaubt es, vom kleinen Objekt bis zum großflächigen Campus alles aus einer Hand zu steuern – mit Investitionssicherheit und zukunftsfähiger Skalierbarkeit.

Das System dahinter

eAccess ist Teil eines durchdachten Gesamtsystems. Glutz bietet nicht nur die Steuerungstechnik, sondern auch passende Beschläge, E-Zylinder, Schlösser und Designkomponenten – alles aufeinander abgestimmt und aus eigener Entwicklung und Fertigung in der Schweiz. Damit lassen sich sowohl sicherheitstechnische als auch gestalterische Anforderungen abdecken – von der robusten Außentür bis zum sensiblen Innenbereich.

Für öffentliche Auftraggeber ergibt sich daraus ein entscheidender Vorteil: eine ganzheitliche Lösung, bei der alle Komponenten zusammenpassen – technisch wie optisch. Beratung, Umsetzung und Betreuung erfolgen aus einer Hand, unterstützt durch zertifizierte Partner und objektbezogene Planung. GIT

Glutz AG
www.glutz.com

ALARMIERUNG

Sicherheit mit System

Funk-Alarmsysteme für Komfort, Flexibilität und Zuverlässigkeit

Ob in den eigenen vier Wänden, in Unternehmen oder öffentlichen Einrichtungen – das Sicherheitsbedürfnis wächst stetig. Gleichzeitig steigen die Ansprüche an Komfort, Flexibilität und Zuverlässigkeit. Daitem, seit über vier Jahrzehnten einer der führenden Hersteller von Funk-Sicherheitslösungen, bietet dafür bewährte Systeme, die sich durch hohe Qualität, einfache Installation und nachhaltige Produktion auszeichnen.

Funk-Alarmsysteme zählen heute zu den fortschrittlichsten Lösungen im Bereich der Sicherheitstechnik und bieten höchste Flexibilität bei Planung und Installation. Sie lassen sich ohne aufwendige Installationsarbeiten in nahezu jeder Umgebung einsetzen – etwa für Neubauten, Bestandsgebäude oder denkmalgeschützte Objekte. Daitem entwickelt und produziert seine Systeme vollständig in Europa und hat sich kompromissloser Sicherheit verpflichtet. Die Systeme sind unabhängig vom Stromnetz, arbeiten mit langlebigen Batterien und kommunizieren über speziell entwickelte, verschlüsselte Funkprotokolle.

Modulares Konzept

Bei der Entwicklung legt Daitem besonderen Wert auf eine einfache, intuitive Handhabung und den praktischen Nutzen für die Anwender. Das modulare Konzept ermöglicht Lösungen, die exakt auf den jeweiligen Bedarf zugeschnitten sind – vom Einfamilienhaus über Reihenhäuser bis hin zu großen Gewerbeobjekten. Komponenten wie Bewegungsmelder, Außensirenen oder Funk-Fenstergriff-Sensoren lassen sich flexibel kombinieren und später jederzeit erweitern. Damit wachsen die Anlagen mit den Anforderungen ihrer Nutzer.

Bedienkomfort per Smartphone

Über die Daitem Secure App können Nutzer ihr Alarmsystem bequem per Smartphone steuern, den Status abrufen oder Benachrichtigungen in Echtzeit erhalten. Der Hersteller setzt auf ein starkes Netzwerk qualifizierter Facherrichter, die Kunden von der Planung bis zur Inbetriebnahme kompetent begleiten. Diese enge Zusammenarbeit stellt sicher, dass jedes System optimal auf die jeweiligen Anforderungen abgestimmt ist und professionell installiert wird. GIT

Funk-Alarmsysteme bieten höchste Flexibilität bei Planung und Installation

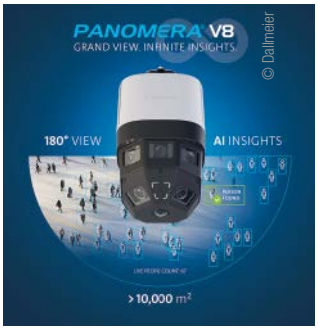
Daitem
www.daitem.com

e*Message und F24 als Partner auf der PMRExpo 2025


© e*Message

e*Message W.I.S Deutschland GmbH und die F24 AG, präsentierten erstmals gemeinsam ihre Lösungen für hoch redundante Alarmierung und Krisenmanagement auf der PMRExpo 2025. Im Mittelpunkt ihrer Zusammenarbeit steht die Integration des hochverfügbaren e*Message Sicherheitsfunknetzes in das Produktportfolio von F24. Diese Kooperation ermöglicht eine höhere Resilienz und zusätzliche Sicherheit durch redundante Alarmierung. Darüber hinaus stellte e*Message mit der Leitstellen-Lösung e*loquentia einen neuen Standard für mehrsprachige Notfallkommunikation vor. Ergänzt wurde das Portfolio durch die intelligente Lösung e*inzelarbeiter für den sicheren Schutz von Alleinarbeitenden sowie die leistungsstarken Multichannel-Lösungen e*rsthelfer und Alarm Manager. **www.emessage.de**

Panomera V8: 180°-Sicht für smarte Analysen auf großen Flächen



Mit der Panomera V8 präsentiert Dallmeier eine Kamera, die moderne Multifocal-Sensortechnologie und künstliche Intelligenz in einem System vereint – für eine lückenlose 180°-Sicht ohne toten Winkel und präzise Analysen auch auf weitläufigen Flächen. Die Panomera V8 erreicht ein Blickfeld von 180 Grad und ermöglicht es, mit acht Linsen, acht Sensoren und acht KI-Chips eine sehr große Fläche zu erfassen – mit nur einer Kamera. Durch ein komplexes Verfahren werden die acht Systeme zu einem großen Übersichtsbild verbunden und die neuronalen Netze logisch verknüpft. Das macht sowohl menschliche Operatoren als auch KI-Assistenz-Systeme deutlich effizienter, präziser und zuverlässiger. So lassen sich die unterschiedlichsten Areale, von Marktplätzen über Logistikflächen bis hin zu Flughafen-Vorfeldern, erfassen und auswerten.

www.dallmeier.com

Milestone Systems stellt Generative-AI-Plug-in für XProtect vor

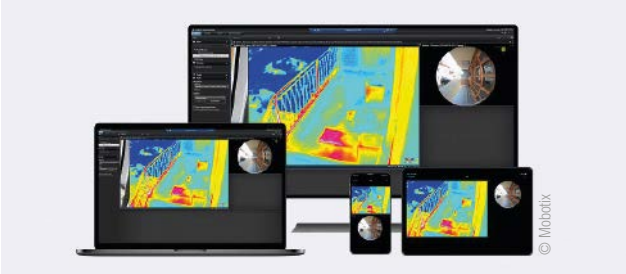
Milestone Systems stellt gemeinsam mit Nvidia ein generatives AI-Plug-in für sein Video-Management-System XProtect vor, das Videoanalysen beschleunigt und Fehlalarme reduziert. Grundlage ist das Vision Language Model „Hafnia“, einsetzbar on-premises oder in der Cloud. Das Plug-in unterstützt Leitstellen, Sicherheitsabteilungen und Verkehrsmanagementzentralen dabei, Videoereignisse schneller einzuordnen, Fehlalarme zu reduzieren und Maßnahmen zügiger einzuleiten. Erste Tests zeigen, dass das Tool die Alarmbelastung von Operatoren um bis zu 30 Prozent senken kann. Das XProtect-Plug-in fasst Videoinhalte automatisiert zusammen, priorisiert relevante Vorgänge und unterstützt so schnellere Lagebeurteilungen, beispielsweise bei: Verkehrsüberlastung und Unfällen, öffentlicher Sicherheit in Bahnhöfen und Innenstädten und Objektschutz in kritischer Infrastruktur. **www.milestonesys.com**

Gretsch-Unitas gewinnt bfb barrierefrei Award

© © Gretsch-Unitas

Die HS LiftUnit von Gretsch-Unitas wurde mit dem bfb barrierefrei Award 2025 als Produkt des Jahres ausgezeichnet. Nach 2019 und 2024 erhält Gretsch-Unitas bereits zum dritten Mal diese Auszeichnung – ein Beleg für die konsequente Weiterentwicklung praxisorientierter Lösungen innerhalb der GU-Gruppe. Das kompakte, wartungsfreie System HS LiftUnit unterstützt die Laufwagen beim Anheben schwerer Türflügel ab 100 kg und reduziert das notwendige Drehmoment am Griff um bis zu 50 %. Dadurch lassen sich Türflügel bis 400 kg mühelos bewegen. Die HS LiftUnit kann einfach in bestehende Systeme integriert werden.

www.g-u.com



Leistungsstarke Video-Management-Systeme

Mit MxManagementCenter (MxMC) und Mobotix Hub stehen zwei leistungsstarke Video-Management-Systeme (VMS) zur Verfügung, je nachdem, welche Anforderung gewünscht ist. Das MxManagementCenter zeichnet sich aus durch eine dezentrale Architektur, dadurch gibt es keine zentrale Ausfallstelle und keine Serverkosten. Die VMS-Lösung bietet eine hohe Datensicherheit, wobei die Aufzeichnung direkt in der Kamera vorgenommen wird. Die integrierte Kamera-Gruppenfunktion ermöglicht Zeit- und Kostenvorteile für den Admin. Für mehr Flexibilität bietet das Unternehmen die skalierbare Allround-Plattform Mobotix Hub an. Über 10.500 Geräte verschiedenster Hersteller können in das VMS integriert werden. Die zentrale Verwaltung ist ideal geeignet für hybride Systeme, mehrere Benutzer und große Netzwerke. **www.mobotix.com**

Schnellere Ermittlungen in Security Center SaaS

Neue, durch intelligente Automatisierung unterstützte Ermittlungsfunktionen helfen Nutzern von Genetec Security Center, Videobeweise schnell zu finden, den Kontext zu verstehen und Fälle in wenigen Minuten abzuschließen. Die neuen, durch Intelligent Automation (IA) unterstützte Ermittlungsfunktionen in Security Center SaaS helfen Nutzern, Videobeweise schnell zu finden, den Kontext rund um ein Ereignis zu verstehen und Fälle innerhalb weniger Minuten abzuschließen. Für viele Organisationen bestehen Ermittlungen noch immer darin, stundenlang Videos zu durchsuchen und zwischen verschiedenen Systemen zu wechseln. Die neuen Funktionen von Security Center SaaS zentralisieren diese Arbeitsabläufe in einer modernen, intuitiven Benutzeroberfläche. Dort können Nutzer Personen oder Fahrzeuge in Live- oder aufgezeichnetem Material mithilfe natürlicher Sprache und erweiterter Filter suchen. **www.genetec.de**

Schließt Sicherheitslücken über offenem Gelände: SecuriDrone Interceptor Iron Drone fliegt bis 180 km/h schnell und fängt fremde Flugobjekte ab

Mit Netz und Fallschirm gegen verdächtige Flugobjekte

Fremde Fluggeräte können mit dem Multilayer-System „SecuriDrone Fortress“ von Securiton Deutschland frühzeitig erkannt, eingeschätzt und kontrolliert gestört oder gelandet werden. Die neue autonome und leistungsstarke Abfangdrohne „SecuriDrone Interceptor Iron Drone“ ergänzt das bewährte Perimeterschutzkonzept von Securiton Deutschland: Sie verfolgt ihr fliegendes Ziel unabhängig von GPS oder Funkverbindungen und fängt es mit einem Netz sicher ein. Ein Fallschirm verhindert dabei Kollateralschäden und die Vernichtung von Beweismaterial. Rund um die Uhr und völlig autonom sichert das leistungsstarke Abfangsystem SecuriDrone Interceptor Iron Drone den Luftraum in einem Radius von bis zu 2.500 Metern. Es ist der neueste Bestandteil des Multilayer-Systems SecuriDrone Fortress von Securiton Deutschland, das mehrstufig verschiedene Sensor- und Wirkkomponenten kombiniert und damit ein unüberwindliches Schutzkonzept für den Luftraum bildet. **www.securiton.de**

Schwachstellen erkennen, bevor es Einbrecher tun

Die Kriminalstatistik zeigt: Die Einbrüche haben 2024 wieder zugenommen und nicht mal 20 Prozent werden aufgeklärt. Alle sechs Minuten findet irgendwo in Deutschland ein Einbruch statt. Der Schutz der eigenen vier Wände mit einfachen Maßnahmen und intelligenter Sicherheitstechnik lässt sich einfach und wirkungsvoll deutlich verbessern. Telenot-Sicherheitsexperte Frank Brucker gibt Tipps für mehr Sicherheit und ein besseres Lebensgefühl.

„Ein individuelles Sicherheitskonzept lässt sich mit wenig Aufwand umsetzen und erfordert keine hohen finanziellen Investitionen“, sagt Frank Brucker. Er leitet die Planungsabteilung bei Telenot und gibt ein paar grundsätzliche Tipps. So sollte man beim Verlassen des Hauses darauf achten, dass alle Fenster und Garagentore nicht gekippt, sondern geschlossen sowie die Haus-, Terrassen- oder Balkontüren verriegelt sind und keine Leitern rund ums Haus griffbereit liegen. „Man muss es potenziellen Einbrecher sichtbar schwer machen, ins Haus zu dringen“, betont Frank Brucker. „Dazu gehören sicher fixierte Gitter an den Lichtschächten zum Keller und eine stabile Kellertür.

Telenot bietet VdS-Zuverlässigkeit und Produkte, die es wert sind, für den Schutz von Leib und Leben und der Sachwerte zu sorgen. Alle Komponenten wie Bewegungsmelder, Magnetkontakte für Fenster und Türen, Außensignalgeber und natürlich das sie koordinierende „Gehirn“, die Gefahrenmelderzentrale, wie die Hiplex 8400H, spielen perfekt zusammen und sind vor Manipulation geschützt. „So entsteht echte Sicherheit, die, wie im Falle Telenot, alle von der unabhängigen VdS Schadenverhütung geprüft und zertifiziert sind“, so Frank Brucker.

www.telenot.com

VisionCore von Eizo

Eizo führt zur Erweiterung des Produktportfolios für industrielle Märkte eine neue Softwaremarke, VisionCore, ein. Die Marke VisionCore debütiert mit zwei Softwareprodukten: VisionCore FCS, eine Software zur Dateikonvertierung und Bildverarbeitung, und VisionCore FCS Viewer, eine Bildbetrachtungs- und Bearbeitungssoftware.

Die Software-Suite VisionCore wurde zur Nutzung von Videotechnologie in Verbindung mit den Hardware-Lösungen von Eizo, wie z. B. der DuraVision Industrie-Serie, entwickelt. Sie erweitert das Eizo Visual System (EVS)-Lösungsportfolio, indem sie auf die sich verändernden Herausforderungen des Marktes eingeht, die eine Kombination aus fortschrittlichen Technologien wie KI-gesteuerten Analysen und umfassender Datenerfassung und -analyse erfordern. VisionCore verbessert die Effizienz und verringert die Arbeitsbelastung des Personals bei der videobasierten Sichtprüfung.

Klare Sicht in aufgezeichneten Videos ist entscheidend für Anwendungen, die sich auf visuelle Inspektionen konzentrieren, wie z. B. die Überwachung von Infrastrukturen und die Untersuchung nach Unfällen. VisionCore FCS ist eine Softwarelösung zur Bildoptimierung, die schwer zu erkennende Bereiche in aufgezeichneten Videos verbessert, sodass sie klarer und visuell leichter zu interpretieren sind. Außerdem erhöht sie die Erkennungsraten in KI-gestützten Systemen und sorgt so für eine genauere und effizientere Videoanalyse. Die patentierte Bildverarbeitungstechnologie des Herstellers analysiert und korrigiert jedes einzelne Pixel in schlecht sichtbaren Bildern, z. B. in dunklen oder hellen Bereichen, bei Nebel, Dunst oder anderen Sichtbehinderungen. Das Ergebnis sind Bilder mit einer höheren Sichtbarkeit, als das bloße Auge wahrnehmen kann, was optimierte Inspektionsprozesse in Umgebungen ermöglicht, die eine hohe visuelle Klarheit erfordern. **www.eizo.de**

Auerswald kooperiert mit DoorBird

Höhere Sicherheit und Transparenz bei der Zutrittskontrolle: Auerswald, Spezialist für die Businesskommunikation, und die Bird Home Automation GmbH, Hersteller der DoorBird Türsprechanlagen, geben ihre Technologiepartnerschaft bekannt. Das erste gemeinsame Projekt ist die Integration einer DoorBird IP-Video-Türstation mit einem Telefongerät der Auerswald COMfortel D-Serie über einen Auerswald COMtrexx PBX-Server. Das System ist bereits bei ersten Anwendern im Einsatz. Weitere gemeinsame Lösungen folgen. Durch die Integration einer DoorBird IP-Video-Türstation mit einem COMfortel D-Endgerät werden Türrufe in Unternehmen auf dem verbundenen Telefon angezeigt. **www.doorbird.com**

All-in-One Sicherheitslösung DSS OneBox

Die leichtgewichtige Workstation für KMUs, die DSS OneBox, von Dahua Technology ist eine All-in-One-Workstation, die mit einer vorinstallierten Lizenz geliefert wird und sofort einsatzbereit ist – ohne Set-up und ohne zusätzlichen Server. Mit den Maßen von nur 117×117×42 mm und einem Gewicht von 0,52 kg bietet dieses Tischgerät ein platzsparendes und elegantes Erscheinungsbild, das sich nahtlos in jede Büro- oder Kontrollraumumgebung einfügt. Das System zeichnet sich durch die Abschaffung komplexer Konfigurationen aus: Auto-Start und Auto-Log-in für sofortigen Betrieb; vorkonfigurierte Software und Lizenzen, die Zeit bei der Installation sparen. Und integrierter Server und Client – kein zusätzlicher Server erforderlich. Ausgestattet mit einem Intel Core i7-Prozessor, 32 GB RAM und einem integrierten Grafikprozessor ist das Gerät sehr leistungsstark. **www.dahuatech.com**

© Fraunhofer SIT

Schritt halten

Wissen und Können: Kontinuierliche Cybersicherheits-Weiterbildung entscheidet

Rasanter technologischer Fortschritt, zunehmende Angriffsoberfläche, Aufrüstung bei Cyberkriminellen. Diesen Risiken kann man heute nicht mehr nur mit Technik allein begegnen. Menschen mit Fachwissen sind gefragt. Aber Wissen in Cybersicherheit evolviert so rasch wie in kaum einem anderen technischen Gebiet; Wissen, von dem sehr viel abhängen kann. Deshalb ist kontinuierliche Weiterbildung in Cybersicherheit wichtig. Ein Beitrag von Dr. Markus Schneider, Stv. Institutsleitung & Leitung Training Cybersicherheit, Fraunhofer SIT & Nationales Forschungszentrum für Angewandte Cybersicherheit Athene.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bezeichnet die Cybersicherheitslage in Deutschland als angespannt. Für Unternehmen und Behörden stellt sich in Bezug auf Angriffe weniger die Frage des Ob als vielmehr des Wann. Cyberangriffe gelten seit einigen Jahren als das größte Geschäftsrisiko mit Auswirkungen auf Wettbewerbsfähigkeit bis hin zur Existenz.

Die digitale Transformation führt immer wieder zu neuen Anwendungen und Funktionen; technologischer Fortschritt bringt viele Vorteile, z.B. Effizienzgewinne. Damit vergrößert sich jedoch auch die Angriffsfläche und es entstehen große Herausforderungen, sich zu wappnen.

Wappnen beinhaltet technische Maßnahmen zum Schutz, Prozesse und Wissen. Aufgrund seiner Tragweite wird Cybersicherheit ein Thema, das zunehmend mehr verschiedene Ebenen in Organisationen und Rollen betrifft, von operativen Aufgaben in der IT-Administration bis hin zu strategischen Belangen in der Führungsebene. Die hohe Technologieentwicklungsdynamik führt zwangsläufig zur schnellen Weiterentwicklung von relevantem Cybersicherheitswissen, einschlägige neue Rechtsakte verlangen Reaktionen.

Angesichts der immensen Professionalisierung der Cyberkriminalität und der sich daraus ergebenden Bedrohung ist es wichtig, das relevante Wissen in Organisationen immer auf dem aktuellen Stand zu halten. Jedoch: Auch eine sehr gute Ausbildung kann das erforderliche Wissen nicht mehr über längere Zeiträume abdecken; es kommt auf Weiterbildungen an, insbesondere auch aufgrund des immensen Fachkräftemangels für Cybersicherheit. Aufgrund des Querschnittscharakters von

Cybersicherheit differenzieren sich Weiterbildungen immer weiter aus.

Cybersicherheitswissen – Warum so besonders?

Die Rahmenbedingungen für Cybersicherheitswissen unterscheiden sich deutlich von anderen Gebieten. Sind in anderen IuK-Bereichen Marktanforderungen und neue Funktionen die Evolutionstreiber, so ist es in Cybersicherheit die Bedrohungslage. Die Vorhersehbarkeit ist hier meist deutlich geringer als in anderen Bereichen. Cybersicherheitswissen veraltet und wird durch neue Erkenntnisse abgelöst. Die Halbwertszeit des taktischen Wissens liegt bei wenigen Monaten, in anderen IuK-Bereichen bei wenigen Jahren; beim strategischen Wissen stehen wenige Jahre vielen Jahren gegenüber

Die geforderten Reaktionszeiten können sehr kurz sein, in anderen IuK-Bereichen akzeptiert man längere Zeiträume. Auch die Obsoleszenz ist unterschiedlich ausgeprägt: abruptes Aufgeben bei Cybersicherheit versus gradueller Übergänge bei anderen IuK-Bereichen. Darüber hinaus sind aufgrund der Notwendigkeiten zum kurzfristigen Handeln Dokumentationen mit Bezug zu Cybersicherheit oft unvollständig, in anderen IuK-Bereichen sind sie eher umfangreich und strukturiert.

Cybersicherheit ist heute eines der am schnellsten evolvierenden Felder in der IuK-Technologie. Dies hat enorme Implikationen für das, was Organisationen in Cybersicherheit wissen müssen, und wie sie dieses Wissen aktuell halten. Was gestern noch richtig war, kann morgen schon obsolet sein. Diese Diskrepanzen in Bezug auf Wissen in Cybersicherheit und anderen IuK-Bereichen ergeben sich aus verschiedenen Einflussfaktoren: Fachkräftemangel, Überlastung, technologische Komplexität, Vergrößerung der Angriffsfläche, Asymmetrie zwischen Angreifer- und Verteidigerseite, neue Angriffsmethoden, neue regulatorische Anforderungen, Ausdifferenzierung verschiedener Rollen und Aufgaben, Anwendungsorientierung versus Grundlagen.

Neben langfristigem Wissen (z.B. grundlegende Prinzipien, kryptographische Primitive) spielen in Cybersicherheit auch mittel- (z.B. Bedrohungen aus neuen Anwendungstechnologien, Werkzeuge) und kurzfristiges Wissen (z.B. neue Schwachstellen, Patches) eine wichtige Rolle. Kurzfristiges Wissen kann ad hoc relevant werden, aber auch schnell wieder veralten. Solides mittel- und langfristiges Wissen hilft bei der selbständigen Einordnung von aktuellen Meldungen.

Für Hochschulen ist es oft herausfordernd, mit ihren Curricula Schritt zu halten. Darüber hinaus braucht es seine Zeit, bis Studierende als Fachkräfte auf den Arbeitsmarkt kommen. Um sich besser zu schützen, müssen Unternehmen auf Weiterbildungen in Cybersicherheit setzen, am besten kontinuierlich. Nicht zuletzt helfen sie der Geschäftsführung auch zum Beleg der ihr obliegenden Risikovorsorge.

Verpflichtungen für Organisationen

Zur Wahrung der eigenen Interessen müssen Organisationen das Notwendige tun, um auf dem aktuellen Stand bzgl. Cybersicherheit zu bleiben. Tun sie dies nicht, und leiten sie nicht die erforderlichen Maßnahmen daraus ab, droht Organisationsversagen. Spätestens nach erfolgten Angriffen wird dies transparent.

Weiterbildungen in Cybersicherheit, z.B. als Schulungen oder Trainings, sind für Organisationen nach verschiedenen Rechtsakten verpflichtend. Dies gilt für Organisationen entweder direkt (z.B. DSGVO, IT-Sicherheitsgesetz) oder indirekt gemäß den Sorgfaltspflichten für Vorstände oder Geschäftsführungen (z.B. AktG, GmbHG). Diesen obliegt auch die Bereitstellung der erforderlichen Ressourcen (z.B. Zeit, Finanzen).

Bedarfe

Der Fachkräftemangel in Cybersicherheit ist nicht auf Deutschland beschränkt. Unternehmen und Behörden suchen weltweit nach geeigneten Fachkräften, deren Expertisen die anwendungsorientierten Anforderungen erfüllen. Hierfür sind gute Ausbildung und entsprechende Weiterbildung gefragt.

In einer Untersuchung in den USA hatte man vor einigen Jahren festgestellt, dass auch die Universitätsabsolventen der Ivy-League die inhaltlichen Anforderungen von Organisationen nicht mehr erfüllt haben. Da man auf staatlicher Seite im Fachkräftemangel und inhaltlichen Defiziten ein nationales Sicherheitsproblem gesehen hat, wurde die National Initiative for Cybersecurity Education (NICE) ins Leben gerufen; sie hat ein Kompetenzrahmenwerk für Aus- und Weiterbildung erarbeitet. Auch andere Länder, z.B. China, sehen in der Aus- und Weiterbildung in Cybersicherheit eine Säule ihrer nationalen Sicherheit. In Anlehnung an NICE hat man in Europa mit dem EU Cybersecurity Skills Framework (ECSF) reagiert.

Unternehmen brauchen Weiterbildungen, die sich inhaltlich und im Ablauf gut in die praktische Arbeitswelt integrieren lassen. Von praktischen Komponenten in der Wissensvermittlung erwartet man schnellere und effektivere Lernerfolge. Wichtige neue Erkenntnisse sind unverzüglich in Weiterbildungscurricula aufzunehmen.

Wissen auf kurzen Wegen

Das Fraunhofer SIT ist Mitwirkender im Nationalen Forschungszentrum für angewandte Cybersicherheit Athene, dem größten Forschungszentrum für Cybersicherheit in Europa. Neben F&E hat das Fraunhofer SIT ein umfangreiches Weiterbildungsangebot. Die Nähe zur angewandten Forschung ist sehr wertvoll, da neue Erkenntnisse zügig übernommen werden:

- TISP: Die Inhalte decken praxisrelevantes Wissen zu technischen, organisatorischen, rechtlichen, und wirtschaftlichen Themen ab, das sich an nationalen und internationalen Standards orientiert.
- Athene Cyber Range: Hier kann man die Erkennung und Verteidigung von echten Cyberangriffen trainieren.
- Lernlabor Cybersicherheit: Es werden Inhalte anhand praktischer Übungen und kompakter Theorie vermittelt. Die praktische Anwendung von neu erworbenem Wissen führt zu besseren Lernerfolgen.

Fazit

Zum Schutz gegen Cyberangriffe müssen Organisationen ihren Mitarbeitenden ermöglichen, sich kontinuierlich in der Cybersicherheit weiterzubilden. Lebenslanges Lernen ist wichtig, da Cybersicherheit rasant evolviert. Weil sich Inhalte und Angebote sehr stark ausdifferenzieren, ist es entscheidend, die für die eigenen Bedarfe relevanten Trainings und Schulungen auszuwählen. GIT

Weiterführende Information finden Sie hier:

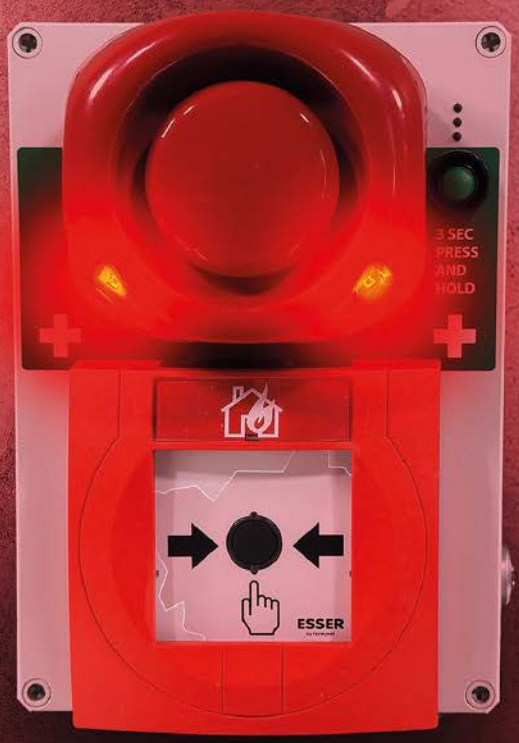
- **Weiterbildung:** www.sit.fraunhofer.de/weiterbildungen-allgemein
- **Teletrust Information Security Professional (T.I.S.P.):** www.sit.fraunhofer.de/de/tisp
- **Athene Cyber Range:** www.athene-center.de/cyber-range-trainings
- **Lernlabor Cybersicherheit:** www.sit.fraunhofer.de/de/llcyber

Fraunhofer SIT
www.sit.fraunhofer.de

ALARMIERUNG

Alarmierung in der Bauphase

Mobile Evakuierungseinheit für Logistikzentrum



© C.M. Heim/Boveda Fotodesign

Die Firma Häfele in Nagold steht für intelligente Beschlagtechnik, elektronische Schließsysteme, Beleuchtung und Gebäudevernetzung. In direkter Nachbarschaft zu den bestehenden Logistikgebäuden wird seit Juli 2023 das Dynamikzentrum mit etwa 11.900 m² Geschossfläche gebaut. Im Jahr 2026 sollen Büro-, Produktions- und Logistikflächen bezogen und genutzt werden. Bis zur Inbetriebnahme der fest installierten Brandschutz- und Evakuierungsanlage wurden 25 Mobile Evakuierungseinheiten MEU von C.M. Heim im weitläufigen Gebäudekomplex installiert.

„Die Interimsalarmierung bis zur Fertigstellung der Anlagentechnik ist vor allem zur Räumung des Gebäudes relevant. Dabei geht es darum, dass alle Personen das Gebäude verlassen und die Sammelplätze aufsuchen. Dazu ist eine mobile Alarmierungsanlage so auszulegen, dass diese händisch ausgelöst werden kann und akustisch die Personen im Gebäude warnt“, erklärt Joachim Maurer, Leitung Technisches Facility Management bei Häfele, die Anforderungen an die Mobilen Evakuierungseinheiten. In der Bauphase kommt es wegen der Brandlast der bereits eingelagerten Kunststoffbehälter zur Lagerung und Kommissionierung und der noch nicht funktionsfähigen Brandschutzeinrichtungen zu einer erhöhten Gefährdung.

In Abstimmung mit dem Fachverantwortlichen von Häfele haben die Experten von C.M. Heim nach der ASR A2.3 Fluchtwege und Notausgänge, dem bauzeitlichen Brandschutzkonzept, der Gefährdungsbeurteilung und der DIN VDE 0833-2 für Handfeuermelder in vier Geschossen 25 Mobile Evakuierungseinheiten (MEU) an Kreuzungspunkten im Abstand von 20 m bis 50 m zueinander und an den Zugängen zum Treppenraum oder in Treppenräumen temporär installiert.

© Heim/Boveda Fotodesign

In Abstimmung mit dem Fachverantwortlichen von Häfele haben die Experten von C.M. Heim 25 Mobile Evakuierungseinheiten (MEU) temporär installiert

Mobile Evakuierungseinheit MEU

Dämpfe, Flüssigkeiten, Panik, Rauch: Bei verschiedenen Gefahrenlagen erhöht eine mobile Evakuierungsanlage die Sicherheit. Auch bei Großbaustellen ohne eigene Stromversorgung, bei Großveranstaltungen, in Logistik- und Lagergebäuden, aber auch bei Umbau- und Sanierungsarbeiten in Bestandsgebäuden und in Werften sind laut der Technischen Regel für Arbeitsstätten (ASR) A2.2. die Einrichtung und der Betrieb von Feuerlöscheinrichtungen und weiteren Maßnahmen zur Erkennung, Alarmierung sowie Bekämpfung von Entstehungsbränden erforderlich. In Anlehnung an die EN 54 entspricht die mobile Evakuierungseinheit MEU von C.M. Heim diesen Anforderungen und dem Stand der Technik.

Die Evakuierungseinheit wird regulatorisch als Funkprodukt und nicht als Bauprodukt in den Verkehr gebracht. Dies erleichtert die Planung und Inbetriebnahme erheblich und reduziert die Kosten. So ist beispielsweise keine Abnahme durch einen Sachverständigen erforderlich.

Die Basiseinheit MEU besteht aus einer Sirene, einer Blitzleuchte, einem Handfeuermelder und einem Erste-Hilfe-Rufknopf. Die Einheiten sind batteriebetrieben und werden mit geringem Montageaufwand kabellos installiert. Die MEU kommuniziert über ein Mesh-Netzwerk selbstständig untereinander. Über den MEUadapter wird die Verbindung zur Zentrale OAMplus hergestellt. Im Notfall wird über ein Telefonwählgerät automatisch mit einem zertifizierten Protokoll die Verbindung zur Leitstelle hergestellt. Alternativ mit einer überwachten IP-Verbindung zu MyMOBS mit einer präzisen Ortsangabe mit Lageplan und notwendiger Quittierung.

Wie bei einer mobilen Brandmeldeanlage sind auch bei der mobilen Evakuierungseinheit die Alarmierungsqualität und die Betriebssicherheit unter ungünstigen Bedingungen für die Sicherheit entscheidend. Das Mesh-Netzwerk kommuniziert auf mehreren Frequenzen in verschiedenen Gruppen. Damit können somit auch größere Gebäude schnell und effizient evakuiert werden. Die Funkstreckenüberwachung stellt sicher, dass die Evakuierungsanlage gegen Sabotage geschützt ist – bis zu einer Reichweite von 1.500 m im freien Feld. GIT

Eine transparente Verbindungsbrücke verbindet das Versandzentrum Nord mit dem Dynamikzentrum und dient dem Personen- und Warenverkehr

© C.M. Heim/Boveda Fotodesign

C.M. Heim
www.cmheim.com

© C.H. Heim / Mark Heim

an Mark Heim, Geschäftsführer C.M. Heim GmbH

Wie schätzen Sie derzeit die wirtschaftliche Lage insgesamt und die Ihrer Branche insbesondere ein - und welche Rückschlüsse ziehen Sie daraus für Ihre strategischen Entscheidungen?

Mark Heim: Die deutsche Wirtschaft investiert trotz der schwachen Konjunktur in die Zukunft. Batteriewerke werden gebaut, KI-Unternehmen boomen, die Automobilwirtschaft ist allerdings auf der Bremse und strukturiert sich um. Daher ist die Baubranche im Moment eher im Stand-by-Betrieb. Wir sind ein agiles Unternehmen und können uns schnell an die sich ändernde Gegebenheiten anpassen.

Welches sind Ihrer Einschätzung nach derzeit die drängendsten Herausforderungen Ihrer Kunden - und welche besonderen Anforderungen stellen diese wiederum an Sie als deren Partner, Lieferant oder Dienstleister?

Mark Heim: Die Unternehmen sind gegenwärtig in vielen Bereichen gefordert. Die Herausforderung ist es, den Fokus auszurichten, Prioritäten zu definieren. Wir sind mit den Mobilen Brandmelde- und Evakuierungsanlagen klar aufgestellt. Die Kunden erwarten vor allem eines: Lösungen, die Sicherheit bieten. Das bedeutet qualifizierte Mitarbeiter, klare Prozesse von der Beratung bis Inbetriebnahme und hervorragende Produkte.

Neue Produkte, Lösungen, Dienstleistungen: Woran arbeiten Sie gerade am intensivsten? Und was können wir demnächst an Neuigkeiten aus Ihrem Hause erwarten?

Mark Heim: Wir haben nun von der Entwicklung bis zum Versand alles an einem Standort – mit der Option zu wachsen. Nicht erst seit KI ist Schnelligkeit und Effizienz unser Thema. Wir haben vergangenes Jahr die Förderung „Spitze auf dem Land“ als eines von acht Unternehmen in Baden-Württemberg erhalten. Das ist Ansporn, unser Lösungen noch schneller zu entwickeln und marktreif als andere zu sein.

BRANDMELDEZENTRALEN

Gehobener Anspruch

Brandschutz in der Gastronomie: Ein Konzept für das Amtshaus in Iggingen

Die Sanierung historischer Bausubstanz stellt Planer, Architekten und Brandschutzexperten gleichermaßen vor komplexe Herausforderungen. Wie das gelingen kann, zeigt das Beispiel des Amtshauses in Iggingen bei Schwäbisch Gmünd. Dort wurde ein innovatives Brandschutzsystem von Telenot installiert, das mit modernster Sensortechnik und intelligentem Loop-System nicht nur den gesetzlichen Vorgaben, sondern auch den sensiblen Anforderungen des Denkmalschutzes gerecht wird – und dabei ein Stück regionaler Baugeschichte bewahrt.

Das Amtshaus ist eines der ältesten Gebäude der Gemeinde

© Iggingen

Das Amtshaus in Iggingen, eines der ersten Gebäude, die nach den Verwüstungen des Dreißigjährigen Kriegs errichtet wurden, führte über Jahre ein Schattendasein. Nach 1900 wurde das historische Bauwerk vielfältig genutzt: als Stall, Bauhof, Geräteschuppen der Feuerwehr und später als Sozialwohnung sowie Obdachlosenunterkunft. Schließlich stand es lange Zeit leer und war trotz Denkmalschutz vom Abriss bedroht. Im Jahr 2015 gelang der Wendepunkt: Die Gemeinde Iggingen, unweit von Schwäbisch Gmünd, erhielt Fördermittel für die Sanierung des Gebäudes. Nach zahlreichen Diskussionen überzeugte das Stuttgarter Architekturbüro Kohn und Kohn den Gemeinderat mit seiner Vision eines modernen Dorfgasthauses. Im Sommer 2023 wurde das neue Lokal eröffnet und erfreut sich seither großer Beliebtheit. Hier werden schwäbische Klassiker zeitgemäß interpretiert und weitestgehend mit regionalen Zutaten zubereitet. „Wir wollten das klassische Dorfgasthaus moderner denken“, erklärt Johannes Zweig, der heutige Betreiber.

Historisches Ambiente – moderne Technik

Ein wesentlicher Erfolgsfaktor des neuen Dorfgasthauses ist das besondere Ambiente des sanierten Amtshauses: Viele historische Elemente wurden bewahrt, darunter auch Details aus dem 17. Jahrhundert. Um den Denkmalschutzauflagen gerecht zu werden, legte das Planungsteam großen Wert auf ein umfassendes Brandschutzkonzept. „Für uns kam von Anfang an nur TSO Sicherheitssysteme als Partner in Frage“, sagt Architektin Melanie Handloser von Kohn und Kohn, die den Umbau plante.

43 Rauchmelder

Jan Wieland von der TSO Sicherheitssysteme, der das Projekt verantwortete, erklärt: „Seit 2018 kann für den Brandschutz in Gaststätten die Norm DIN VDE V 0826-2 angewendet werden. Das Brandmeldesystem Hifire 4000 BMT von Telenot erfüllt diese Anforderungen vollständig.“ Die besondere Herausforderung lag darin, den Brandschutz mit den Vorgaben des Denkmalschutzes in Einklang zu bringen.

In der Telenot Brandmelderzentrale hifire 4400 im Keller laufen alle Fäden des Brandschutzsystems zusammen.

Bei der Sanierung konnte ein großer Teil der ursprünglichen Architektur erhalten werden

Insgesamt wurden 43 Rauchmelder des Anbieters im gesamten Gebäude installiert, das neben dem Restaurant auch Veranstaltungs- und Praxisräume beherbergt.

Die Rauchmelder reagieren zuverlässig auf Rauchentwicklung und sorgen so für maximale Sicherheit. In Bereichen mit starker Wärmeentwicklung, wie der Küche und über der Theke, kommen zudem drei Mehrsensormelder von Telenot zum Einsatz. Diese kombinieren optische sowie thermische Sensorik und arbeiten mit Loop-Technik. Dank intelligenter Auswertungsalgorithmen minimieren sie das Risiko von Falschalarmen und gewährleisten schnelle Reaktionen auf echte Gefahren. Zusätzlich wurden sechs Handfeuermelder im Gebäude installiert. Im Brandfall fährt der neu eingebaute Aufzug automatisch ins Erdgeschoss und öffnet dort seine Türen, um eine schnelle Evakuierung zu ermöglichen.

Im Bereich der Küche kommt ein Mehrsensormelder zum Einsatz

Funk-Handfeuermelder von Telenot melden dank Manipulationsüberwachung auch schon jede unerlaubte Öffnung der Gehäusetür.

Loop-System als Herzstück der Sicherheit

Das Herzstück des Brandschutzsystems befindet sich in einem Brandschutzgehäuse im Keller des Gebäudes. Hier laufen alle Komponenten zusammen, die per Loop-Technik miteinander verbunden sind. Diese Ringleitungsstruktur reduziert den Verkabelungsaufwand erheblich, da lediglich eine Zweidrahtleitung benötigt wird. Gleichzeitig bleibt das System bei Leitungsunterbrechungen funktionsfähig, da die Kommunikation über den anderen Teil des Rings sichergestellt wird. Die Loop-Technologie ermöglicht zudem die präzise Adressierung der Melder und eine einfache Erweiterung des Systems.

Ein weiterer zentraler Bestandteil ist die Feuerwehr-Informationszentrale (FIZ), die im Bereich der Erstanlaufstelle der Feuerwehr untergebracht ist. Sie enthält Laufkarten, die den Einsatzkräften im Ernstfall eine schnelle Orientierung und einen gezielten Zugriff auf den Gefahrenherd ermöglichen. GIT

Telenot Electronic GmbH
www.telenot.com

Baur Hermes Fulfilment erhält Sprinkler Protected Award

Das Logistikunternehmen Baur Hermes Fulfilment wurde mit dem Bvfa-Gütesiegel „Sprinkler Protected“ ausgezeichnet. Damit würdigt der Bvfa – Bundesverband Technischer Brandschutz den vorbildlichen Industriebrandschutz im neugebauten und vollautomatisierten Shuttlelager am Unternehmensstandort, das die Zeitspanne zwischen Auftragseingang und Versand auf durchschnittlich vier Stunden verkürzt hat. Das zur Otto Group gehörende Unternehmen hatte insgesamt rund 150 Millionen Euro in den Neubau und die Erweiterung des Logistikcampus investiert. Bvfa-Geschäftsführer Dr. Wolfram Krause übergab die Auszeichnung an Peter Volk, Geschäftsführer bei Baur Hermes Fulfilment. „Für unser Shuttlelager haben unsere Bau- und Brandschutzexperten ein eigenes Konzept entwickelt: Es vereint Brandschutz und Wirtschaftlichkeit auf sehr hohem Niveau“, so Peter Volk. **www.bvfa.de**

Bvfa-Geschäftsführer Dr. Wolfram Krause (l.) übergab die Auszeichnung an Peter Volk, Geschäftsführer bei Baur Hermes Fulfilment

Brandschutztechnik von Securiton auf den VdS BrandSchutzTagen

Securiton zeigte auf den VdS BrandSchutzTagen in Köln, dem zentralen Treffpunkt für Experten des vorbeugenden Brandschutzes, seine praxisbewährten Brandschutzlösungen mit den Schwerpunkten Sonderbrandmeldetechnik und Sprachalarmierung. Systeme, die perfekt zusammenspielen und in anspruchsvollen Umgebungen zuverlässigen Schutz gewährleisten. Neu in diesem Jahr: SecuriGAS, Ansaugrauchmelder mit hochsensibler Gassensorik zur frühzeitigen Detektion von Li-Ionen-Akku-Entstehungsbränden. Diese Technologie erkennt kritische Entwicklungen in Lithium-Ionen-Energiespeichern bereits in ihrer Entstehung und leistet damit einen wichtigen Beitrag zur Sicherheit nachhaltiger Energiesysteme. Darüber hinaus war der Stand des Unternehmens Teil des offiziellen Messerundgangs. Dort zeigte der Hersteller SecuriGAS live in Aktion und gab Einblicke in die Praxisanwendung dieser innovativen Technologie. **www.securiton.de**

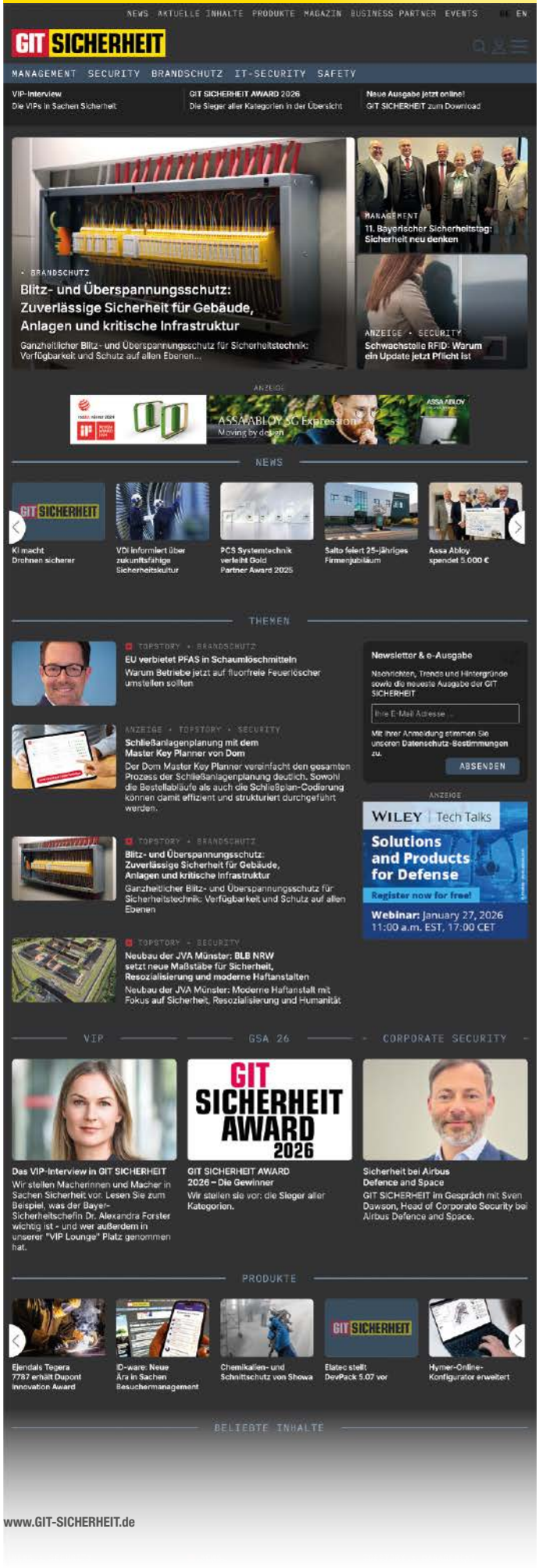
Wagner auf der Buildinx

Die Wagner Group GmbH zeigte auf der Buildinx in Dortmund zukunftsweisende Lösungen für den Brandschutz in modernen Logistikimmobilien. Im Zentrum des Messeauftritts standen die Themen Digitalisierung und CO_2-neutrale Brandvermeidung – zwei Schlüsselbereiche für mehr Sicherheit, Effizienz und Nachhaltigkeit in der Immobilienwirtschaft. Darüber hinaus zeigte das Unternehmen, wie Risiken in sensiblen Technikbereichen wirksam reduziert werden und sich diese Bereiche resilient gegenüber Störungen schützen lassen: mit einem speziell für Schalt- und Serverschränke entwickelten Ansaugrauchmeldesystem. Der Ansaugrauchmelder Titanus Rack·Sens eignet sich für den Einsatz in der IT-Infrastruktur automatisierter Logistikzentren. Das kompakte System erkennt selbst geringste Rauchpartikel frühzeitig und ermöglicht ein schnelles Eingreifen, bevor es zu Betriebsunterbrechungen oder Sachschäden kommt. **www.wagnergroup.com**

Planerdialog 2025: Sonderbrandmeldetechnik im Fokus

Hekatron bietet eine Online-Veranstaltung für Elektrofachplaner und Brandschutzplaner an. Sie beleuchtet das Thema „Sonderbrandmeldetechnik“ aus rechtlicher und praxisorientierter Sicht. Extrembedingungen, wie sie in Rechen- und Logistikzentren oder Recyclinganlagen oft herrschen, stellen auch extreme Anforderungen an die Meldetechnik. Sonderbrandmeldetechnik für Einsatzbereiche, in denen klassische Melder an ihre Grenzen stoßen, sind dieses Jahr Thema bei der Veranstaltung „Planerdialog“. Sie findet am 9. und 10. Dezember online statt und ist von Architekten- und Ingenieurkammern als Fortbildung anerkannt. Mit Vorträgen und Diskussionen zu rechtlichen und praktischen Aspekten bietet die Veranstaltung des Brandschutzanbieters Hekatron seit 2019 Teilnehmern fundiertes Wissen, aufschlussreiche Praxisbeispiele und die Möglichkeit zum Austausch mit Fachexperten.
www.hekatron.de

Diesen Monat auf GIT-SICHERHEIT.de



IMPRESSUM

Herausgeber
Wiley-VCH GmbH

Geschäftsführer
Dr. Guido F. Herrmann

Senior Director, Publishing and Content Services
Dr. Katja Habermüller

Publishing Director
Dipl.-Betriebswirt Steffen Ebert

Product Manager Safety & Security
Dr. Timo Gimbel
+49 6201 606 049

Wissenschaftliche Schriftleitung
Dipl.-Verw. Heiner Jerofsky
(1991–2019) †

Anzeigenleitung
Miryam Reubold
+49 6201 606 127

Sales Director
Jörg Wüllner
+49 6201 606 748

Redaktion
Dipl.-Betrw. Steffen Ebert
+49 6201 606 709

Matthias Erler ass. iur.
+49 160 72 101 21

Cinzia Adorno
+49 6201 606 114

Tina Renner
+49 6201 606 021

Textchef
Matthias Erler ass. iur.
+49 160 72 101 21

Herstellung
Jörg Stenger
+49 6201 606 742

Claudia Vogel (Anzeigen)
+49 6201 606 758

Satz + Layout
Andreas Kettenbach

Lithografie
Elke Palzer

Sonderdrucke
Miryam Reubold
+49 6201 606 172

Wiley GIT Leserservice (Abo und Versand)
65341 Eltville
Tel.: +49 6123 9238 246
Fax: +49 6123 9238 244
E-Mail: WileyGIT@vuservice.de
Unser Service ist für Sie da von Montag - Freitag zwischen 8:00 und 17:00 Uhr

Verlag
Wiley-VCH GmbH
Boschstr. 12, 69469 Weinheim
Telefon +49 6201 606 0

Verlagsvertretung
Dr. Michael Leising
+49 36 03 89 42 800

Bankkonten
J.P. Morgan AG, Frankfurt
Konto-Nr. 6161517443
BLZ: 501 108 00
BIC: CHAS DE FX
IBAN: DE55501108006161517443

GIT SICHERHEIT
Auflage: s. ivw.de
inkl. GIT Sonderausgabe PRO-4-PRO

Abonnement 2025
10 Ausgaben (inkl. Sonderausgaben)
122,30 €, zzgl. MwSt.
Einzelheft 17 € zzgl. Porto + MwSt.

Schüler und Studenten erhalten unter Vorlage einer gültigen Bescheinigung einen Rabatt von 50 %. Abonnement-Bestellungen gelten bis auf Widerruf; Kündigungen 6 Wochen vor Jahresende. Abonnementbestellungen können innerhalb einer Woche schriftlich widerrufen werden, Versandreklamationen sind nur innerhalb von 4 Wochen nach Erscheinen möglich. Alle Mitglieder der Verbände BHE, BID, BDSW, BDGW, BDLS, PMeV, Safety Network International, vfdb, VfS, VSW-Bundesverband sowie seiner Regionalverbände sind im Rahmen ihrer Mitgliedschaft Abonnenten der GIT SICHERHEIT sowie der GIT Sonderausgabe PRO-4-PRO. Der Bezug der Zeitschriften ist für die Mitglieder durch Zahlung des Mitgliedsbeitrags abgegolten.

Druck
westermann DRUCK | pva

Printed in Germany, ISSN 2751-4536

PEFC-zertifiziert
Dieses Produkt stammt aus nachhaltig bewirtschafteten Wäldern und kontrollierten Quellen
PEFC/04-31-0714
www.pefc.de

WILEY

OT-SECURITY

Security-by-Design in der Automatisierungstechnik

Worauf es für Produkthersteller wirklich ankommt – die 8 Practices der IEC 62443-4-1

Im Beitrag mit dem Titel „Strukturierte OT Security“ (Mai-Ausgabe der GIT SICHERHEIT 2023) wurde ein einführender Überblick zu Aufbau und Struktur der Normreihe IEC 62443 „IT-Sicherheit für industrielle Automatisierungssysteme“ gegeben. In diesem weiterführenden Beitrag geht es nun um die sogenannten 8 Practices, um einen sicheren Entwicklungsprozess (Security Development Lifecycle) aus Herstellersicht zu etablieren: Welche Anforderungen gibt es? Wie sind diese konkret zu verstehen? Worauf muss ein Produkthersteller achten, um OT Security für seine Abnehmer gewährleisten zu können?

Bis auf Practice 1 („Security Management“) und Practice 8 („Security Guidelines“) folgen Practice 2 bis 7 in der Aufteilung einem klassischen Entwicklungsmodell ausgehend von den Anforderungen, über das Design, die Implementierung, das Testing und Fehler Management, bis zum Umgang mit Updates. In diesem Sinne beginnt auch dieser Beitrag mit Practice 2, um am Ende mit Practice 1 zu schließen.

Practice 2: Specification of Security Requirements

Zu Beginn von Entwicklungsprojekten werden Anforderungen an das Produkt definiert. Im Rahmen dieser Practice geht es nicht um funktionale Anforderungen, sondern explizit nur um die Anforderungen, welche die Security-Eigenschaften des Produktes betreffen. Hier gibt die Norm vor, dass ein Bedrohungsmodell (Threat Model) erstellt werden muss. Im Rahmen der Bewertung möglicher Bedrohungen müssen Strategien entwickelt werden, diese Bedrohungen zu mitigieren. Aus diesen Strategien folgen dann wiederum Anforderungen.

Als Beispiel betrachten wir eine Webanwendung mit Anmeldemaske. Eine mögliche Bedrohung wäre, dass Angreifer so lange verschiedene Kombinationen aus Benutzername und Passwort ausprobieren, bis sie eine valide Kombination gefunden haben (Brute-Force-Angriff). Eine mögliche Mitigation dieser Bedrohung wäre das Sperren eines Accounts für 10 Minuten nach 3 erfolglosen Anmeldeversuchen. Diese Mitigation wäre dann als eine Security-Anforderung zu definieren.

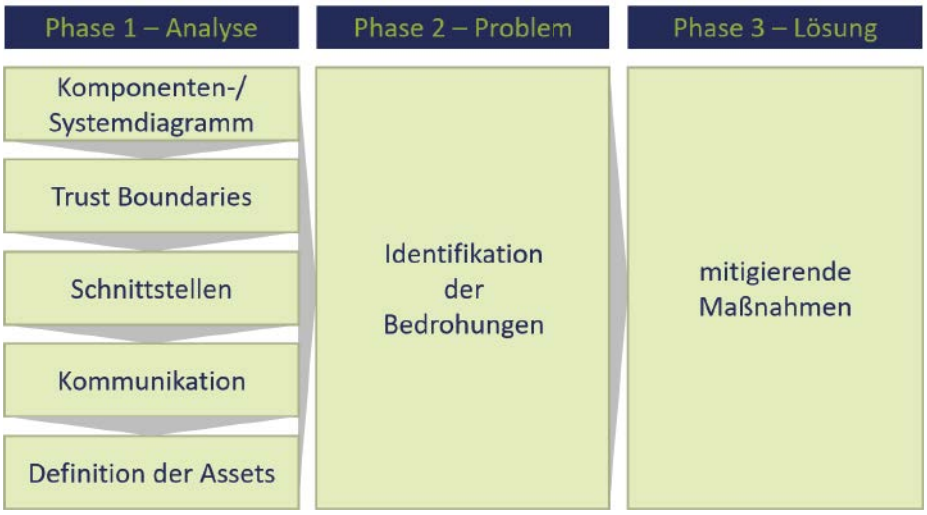
Practice 3: Secure by Design

Die Anforderungen dieser Practice haben zum Ziel, ein sicheres Komponentendesign zu entwickeln. Dadurch wird sichergestellt, dass Security fest im Produkt verankert ist. Ein zentrales Konzept der IEC 62443 ist das Defense-in-Depth-Konzept. Hierbei müssen – wie bei Zwiebelschalen – mehrere Schichten entwickelt werden, von denen jede Schicht eine bestimmte Verteidigungsfunktion übernimmt. Als äußere Zwiebelschale kann beispielsweise eine Firewall Angreifer abwehren. Falls Angreifer diese Firewall überwinden, können Angriffe durch ein Intrusion Detection System erkannt und gegebenenfalls abgewehrt werden.

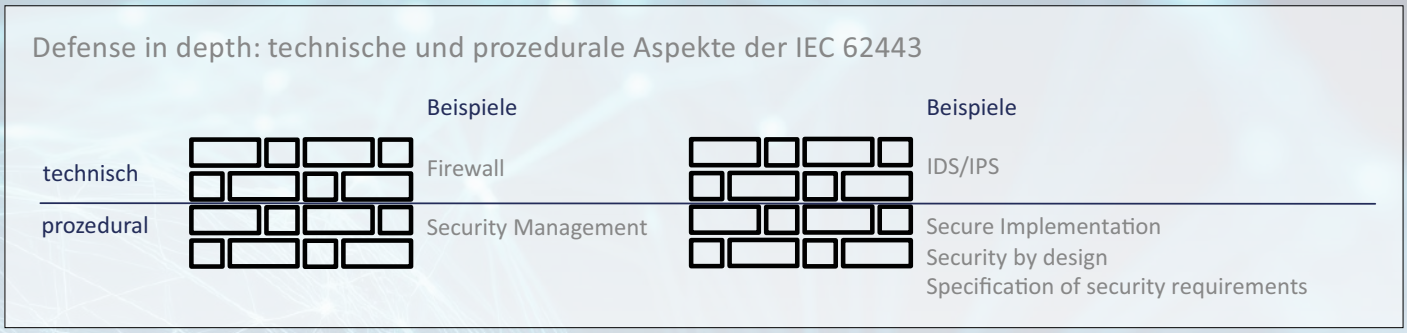
Einen Freiheitsgrad, den die Norm bezüglich eines Defense-in-Depth-Konzepts erlaubt, ist das Auslagern von Funktionen bzw. Verteidigungsschichten in die Systemumgebung. Wird ein Teil der Verteidigungsfunktionen von der Umgebung sichergestellt, spricht man auch von met-by-integration. Werden Funktionen von der Komponente selbst sichergestellt, spricht man von met-by-component.

Practice 4: Secure Implementation

Practice 4 fordert, das sichere Design auch sicher in Soft- und/oder Hardware umzusetzen. Zum einen muss dazu ein 4-Augen-System eingeführt werden. Weiterhin müssen Secure-Coding-Guidelines aufgestellt und befolgt werden. Diese Guidelines müssen sich auf mehrere Abstraktionsschichten beziehen. Je nach verwendeter Programmiersprache sollten Funktionen verboten werden, sodass diese vom Entwickler nicht verwendet werden. Darüber hinaus dürfen keine Code-Konstrukte verwendet werden, die ein mögliches Sicherheitsrisiko zur Folge haben. Auch Design-Konstrukte mit möglichen Sicherheitsrisiken dürfen nicht verwendet werden, z. B. die fehlende Überprüfung von Input-Werten.



Im Rahmen von Practice 2 geht es um die Anforderungen, die die Security-Eigenschaften des Produktes betreffen. Hier gibt die Norm vor, dass ein Bedrohungsmodell (Threat Model) erstellt werden muss



Ein zentrales Konzept der IEC 62443 ist das Defense-in-depth-Konzept

Practice 5: Security Verification and Validation Testing

Practice 5 stellt sicher, dass erstellte Software adäquat getestet und somit einer umfangreichen Qualitätssicherung unterworfen wird, bevor sie veröffentlicht wird. Dies geschieht durch die Verpflichtung zu verschiedenen Tests, wie z. B. funktionale Tests von Security-Anforderungen, Penetrationtests oder Robustnesstests. Um sicherzustellen, dass kein Interessenskonflikt zwischen Testern und Entwicklern auftritt, gibt die Norm für verschiedene Tests verschiedene Grade der Unabhängigkeit vor. Beispielsweise müssen Penetrationtests unabhängig vom Entwicklungsteam durchgeführt werden.

Practice 6: Management of Security Related Issues

Für Kolleginnen und Kollegen stellt es immer wieder eine äußerst frustrierende Situation dar, wenn sie in Produkten Schwachstellen finden, diese den Verantwortlichen melden wollen, und dort auf taube Ohren stoßen. Die Umsetzung dieser Practice sorgt dafür, dass genau dies nicht geschieht. Die zentrale Anforderung hierbei ist, dass es eine dedizierte Meldekette von Schwachstellen geben muss. Diese muss allen potentiellen Anlaufstellen bekannt sein und sowohl die Möglichkeit berücksichtigen, dass eine Schwachstelle von intern, als auch von extern gemeldet wird.

Weiterhin werden hier Anforderungen an den darauffolgenden Prozess definiert. Dies beinhaltet die Bewertung von potenziellen Sicherheitslücken sowie der Umgang mit deren Veröffentlichung. Die Norm gibt hier keine harten Vorgaben an den Prozess. Wie vorgegangen wird, dies kann innerhalb der Organisation geregelt werden.

Practice 7: Security Update Management

Logische Folge der Behandlung einer Sicherheitslücke ist das Ausrollen eines Updates, um diese Sicherheitslücke zu schließen. In Practice 7 werden nun die Anforderungen an Updates beschrieben. Hier muss unter anderem sichergestellt werden, dass ein Update die Sicherheitslücke auch wirklich schließt. Um den Stillstand einer Anlage zu verhindern, muss ein Update im Rahmen seiner geplanten Betriebsumgebung funktionsfähig sein. Die Norm verbietet daher das Deaktivieren einer fehlerhaften Funktion und erzwingt die Korrektur selbiger.

Practice 8: Security Guidelines

Nachdem in den Practices 2 bis 7 nun alle Schritte eines klassischen Entwicklungs- bzw. Produktlebenszyklus, von der Definition der Anforderungen bis hin zur Updatefähigkeit abdeckt, werden in dieser Practice abschließend Anforderungen an Handbücher formuliert. Hier werden keine Anforderungen an die Handbücher zur Bedienung gestellt, sondern lediglich zur sicheren Bedienung. Mit anderen Worten: Die Handbücher müssen die Frage beantworten, was ein Kunde machen muss, um Angriffe auf das Produkt möglichst schwierig zu gestalten. Hier muss die komplette Lebensdauer von der In- bis zur Außerbetriebnahme betrachtet werden. Beispielsweise kann der Kunde dazu aufgefordert werden, bei der Inbetriebnahme ein neues Passwort zu vergeben und bei der Außerbetriebnahme alle Daten zu überschreiben.

Practice 1: Security Management

Practice 1 beinhaltet nun einige Punkte, die sich nur schwer thematisch gruppieren lassen und außerhalb eines klassischen Entwicklungszyklus stehen. Stellvertretend soll hier auf einige Punkte gezielt verwiesen werden. So fordert die Norm sowohl Konsistenz mit, als auch die Eingliederung in einen übergeordneten Entwicklungsprozess. Hierdurch kann sichergestellt werden, dass die Prozessschritte, die die Norm vorgibt, auch konsequent angewendet werden. Die Norm lässt aber ganz explizit die Freiheit nur auf einzelne Produkte oder Produktlinien angewandt zu werden.

Weiterhin wird hier wie auch in fast allen anderen Practices eine ständige Verbesserung durch Feedbackschleifen gefordert. Die jeweiligen Prozesse müssen also ständig überprüft und bei Bedarf verbessert werden. Hinsichtlich der Security in der Entwicklungsumgebung selbst gibt es punktuell eine gewisse Redundanz zu Informationssicherheitsmanagementsystemen (ISMS) wie nach ISO/IEC 27001. Hier werden Anforderungen an die IT Security im Entwicklungsprozess auf verschiedenen Abstraktionsebenen gestellt. Zum einen gibt es Anforderungen auf der Systemebene (z. B. an die Entwicklungsrechner) und zum anderen gibt es Anforderungen auf der Prozessebene (z. B. an den Umgang mit Signing-Keys).

In dieser Practice wird weiterhin auch auf die Lieferkette Bezug genommen. Es muss sichergestellt werden, dass Subkomponenten keine Sicherheitslücken verursachen. Die Norm differenziert hier zwischen 3rd-Party-Komponenten (z. B. Open-Source Programmbibliotheken) und Komponenten, die explizit für den Anwender der Norm entwickelt wurden. Ebenso muss der Anwender sicherstellen, dass eine gewisse Security-Expertise im Unternehmen vorhanden ist. Dies geschieht typischerweise durch Weiterbildungen.

Bis hierher wurde die IEC 62443-4-1 inhaltlich vorgestellt. Die Menge der Themen erfordert aber auch einen pragmatischen Umgang mit den knapp 50 Detailanforderungen der Practices. Hierzu bietet die Norm ein Reifegradmodell an, welches vier Stufen definiert, die Maturity-Level ML-1 bis ML-4. Über diesen Ansatz ist es möglich festzustellen, wo ein Anwender der Norm in Bezug auf eine Anforderung steht. Des Weiteren kann so über die acht Practices sowie über die gesamte Norm ein zusammengefasster Reifegrad ermittelt werden. Die Norm definiert dies zwar nicht explizit, in der praktischen Anwendung findet dies aber statt. Will man die Norm nun umsetzen, bietet es sich an, ML-2 über alle Anforderungen als Meilenstein zu definieren. Dies stellt sicher, dass alle Prozesse korrekt aufgesetzt und beschrieben sind. Durch die Anwendung im Rahmen einer Produktentwicklung wird dann quasi automatisch ML-3 als nächste Stufe erreicht. GIT

Secuvera GmbH
www.secuvera.de

ELEKTRIFIZIERUNG

AC-DC-Reloaded

Gleichstrom und seine neuen Chancen für nachhaltige Verbindungslösungen

Die Nutzung von Gleichstrom (DC) in automatisierten Produktions- und Logistikprozessen birgt ein großes Potential für die Zukunft: Komplette Nutzung der Bremsenergie von Antrieben, direkte Einspeisung von Photovoltaik und Speichersystemen, Wegfall einzelner Wandlungsstufen, weniger Aufwand für Material und Installation, Einsparung von Kupfer, höhere Verfügbarkeit von Anlagen und das auch bei sukzessivem Umbau von Bestandsanlagen (Retrofit). Entsprechend intensiv wurde und wird die Entwicklung der Gleichstromtechnik in Deutschland vorangetrieben. Letzter Meilenstein in dieser Entwicklung war die Gründung der Open Direct Current Alliance (ODCA) am 03. November 2022, eine Arbeitsgemeinschaft des ZVEI und 33 Unternehmen aus der Industrie bzw. Hochschulen und Forschungsstätten. Zu den Gründungsmitgliedern der ODCA gehört u. a. auch Lapp, ein führender Anbieter von Verbindungslösungen, insbesondere Kabel und Leitungen, sowie Steckverbinder und Lösungen zur Ladetechnologie. Da Gleichstrom genau wie Wechsel- bzw. Drehstrom (AC) zur Übertragung Kabel, Leitungen und Stecker benötigt, hat das Stuttgarter Unternehmen eine Reihe neuer Produkte für DC-Anwendungen entwickelt. Welche Herausforderungen die Entwickler nicht zuletzt in Punkto Sicherheit bei dieser zukunftsweisenden Technologie zu bewältigen hatten, wollte GIT SICHERHEIT wissen und hat bei Dr. Karsten Fuchs, Research Engineer Advanced Technology bei Lapp, nachgehakt.

GIT SICHERHEIT: Herr Dr. Fuchs, die Nutzung von Gleichstrom in Produktion und Logistik könnte sich zukünftig als ein zentraler Baustein der Industrie 4.0 erweisen. DC-Netze warten gleich mit einer ganzen Reihe potenzieller Vorteile gegenüber AC-Netzen auf. Was sind aus Ihrer Sicht als Forscher und Entwickler die entscheidenden Vorzüge von Gleichstrom? Worin besteht Ihrer Ansicht nach das größte Potential dieser Technologie?

Dr. Karsten Fuchs: Das größte Potential steckt in der höheren Energieeffizienz, aber auch in der Materialeffizienz durch die Einsparung von Gleichrichterstufen innerhalb von Frequenzumrichtern und der Reduzierung von Kupfer in Kabeln und Leitungen. Durch die Gleichstromversorgung in einer Produktionshalle ist unter anderem eine einfachere und effizientere Integration erneuerbarer Energien (z. B. einer Photovoltaikanlage auf der Fabrikhalle) möglich, die eine geringere Leistungsentnahme aus dem öffentlichen Netz bewirkt. Zudem wird in DC-Netzen durch eine höhere Spannung und den Wegfall von Blindleistung eine Senkung des Energieverbrauchs sowie eine reduzierte Einspeiseleistung (bei gleicher Wirkleistung

Dr. Karsten Fuchs, Research Engineer Advanced Technology bei Lapp

Schematische Darstellung eines Ölflex DC Grid 100 im Querschnitt mit normgerechter Farbkodierung der Aderisolation: rot und weiß für die Phasen, grün-gelb für den Schutzleiter ▼

◀ Speziell für mechanisch beanspruchte Anschlussleitungen bietet Lapp seinen Kunden im Bereich DC neben Ölflex Servo 700 auch Ölflex Chain 800 und Ölflex Robot 900

wie im AC-Netz) erreicht. Je nach Querschnitt resultiert in den Kabeln eine geringere Verlustleistung von etwa 40 % und eine Kupfereinsparnis von bis zu 55 %.

Mal angenommen ich möchte den Teil einer Produktion auf Gleichstrom umstellen: Welche Teile einer Anlage müsste ich dann gegen spezielle DC-Komponenten austauschen und sind diese gegenwärtig überhaupt schon erhältlich?

Dr. Karsten Fuchs: Grundsätzlich besteht eine solche Gleichstromversorgung aus einem DC Bus, an dem die einzelnen Verbraucher angeschlossen sind. Sie kennen den Begriff Bus auch aus der industriellen Kommunikationstechnik, bei der es sich um ein System zur Datenübertragung zwischen mehreren Teilnehmern über einen gemeinsamen Übertragungsweg handelt. Bei DC ist es ähnlich und bedeutet die gemeinsame Versorgung der Verbraucher über eine gemeinsame DC-Strecke.

Dafür wird eingangsseitig ein zentraler bidirektionaler Gleichrichter (Active Infeed Converter, AIC) benötigt, der die vielen dezentralen Wandlungsstufen von AC zu DC ersetzt. Der eigentliche DC Bus wird entweder über Stromschienen (aus Kupfer oder Aluminium) oder DC-Kabel realisiert. Je nach Verbraucher können weitere Stromrichter (DC/AC oder DC/DC) notwendig sein. Für eine zuverlässige Abschaltung im Betriebs- und Kurzschlussfall sind DC-Schalter notwendig (Stichwort: Lichtbogenlöschung). Hier gibt es verschiedene Technologien, die sich zur AC-Technik grundlegend unterscheiden. Aber auch der Einsatz von Schmelz-Sicherungen wäre denkbar. Einige Komponenten sind bereits auf dem Markt verfügbar.

Welche DC-Komponenten bietet Lapp selbst seinen Kunden an?

Dr. Karsten Fuchs: Unser aktuelles DC-Portfolio umfasst Kabel und Leitungen im Niederspannungsbereich bis 1500 VDC. Dieses beinhaltet unsere erdverlegbare Ölflex DC Grid 100 als Energie- und Infrastrukturkabel sowie unsere Ölflex DC 100 als eine Standard-Anschlussleitung. Zudem bieten wir spezielle und mechanisch beanspruchbare Anschlussleitungen (Ölflex Servo 700, Ölflex Chain 800 und Ölflex Robot 900) mit einer normgerechten Farbkodierung der Aderisolation an: rot und weiß für die Phasen, grün-gelb für den Schutzleiter. Bei Netzen mit Mittelpunktleiter ist ein zusätzlicher Leiter mit blauer Kodierung enthalten. Außerdem sind einadrige Solarleitungen für PV-Anlagen sowie einadrige Leitungen für den Anschluss von Energiespeichern in unserem DC-Portfolio enthalten.

An dieser Stelle wollen wir mal etwas näher auf Ihre eigene Rolle beim Thema Gleichstrom eingehen. Welche Aufgaben fielen bei der Entwicklungsarbeit in Ihrem Bereich an und mit welchen Herausforderungen wurden Sie dabei konfrontiert?

Dr. Karsten Fuchs: Am Anfang unserer DC-Reise vor 5 Jahren und im Rahmen der Arbeit im Forschungsprojekt DC Industrie 2 (Start 2019) bewegte uns vor allem die Frage: Wie kann für DC eine beschleunigte Alterung von Kabeln unter Laborbedingungen realisiert werden. Ziel war es zu verstehen, ob wir DC-Kabel anders als bei AC entwickeln müssen.

Was bedeutet „beschleunigte Alterung“?

Dr. Karsten Fuchs: Wir möchten ein Kabel, das typischerweise mehr als 10 Jahre im Betriebseinsatz mit einer bestimmten Spannung, einem bestimmten Leiterstrom und unter speziellen Umgebungsbedingungen beansprucht wird, unter verkürzten Laborbedingungen so belasten, dass diese Beanspruchung der eigentlichen Betriebsbean-

Bitte umblättern ▶

Ölflex DC Grid 100 mit teilweise entferntem Mantel: Anders als bei AC-Netzen gibt es in DC-Netzen keine vierte Ader, was unter anderem die Einsparung von Kupfer von bis 55 % ermöglicht

spruchung entspricht. Dafür gibt es in der Fachwelt bereits einige Verfahren, u. a. das Verfahren nach Arrhenius. Durch die Beanspruchung mit einer höheren Temperatur über 5.000 Stunden ist es möglich, eine Aussage über die tatsächliche Lebensdauer der Isolierung für den späteren Betrieb zu treffen. Für unsere Betrachtungen bei DC ist zusätzlich die Beanspruchung mit einer Gleichspannung notwendig.

Die Alterung von Einzeladern mit diversen Isolierstoffen, die wir u. a. für unsere AC-Leitungen bereits verwenden, musste mit der richtigen Prüfmethodik im Labor nachgestellt werden können. Da hinsichtlich der Alterung noch keine Normen für DC existieren, lehnten wir uns an bereits existierende Normen aus der AC-Welt an. Wir entschieden uns für die Alterung im Wasserbad mit einer Temperatur von 70 °C und einer Spannung von 1 kV für eine Zeitdauer von 2.500 Stunden. Auch, wenn die Methode im Wasser den Stand der Technik darstellt, stellten wir uns die Frage, welchen Einfluss das Wasser auf die Spannungsfestigkeit der Isolierstoffe haben wird. Deshalb realisierten wir parallel weitere Untersuchungen in Wärmeschränken mit den gleichen Parametern für Temperatur und Spannung. Alle Untersuchungen wurden auch für AC durchgeführt, um (mögliche) Einflüsse des Prüfverfahrens bewerten zu können. Parallel wurden in unserem Labor umfangreich mechanische Kenngrößen (z. B. Zugfestigkeit) der Einzeladern bestimmt und das Wasser wurde regelmäßig auf seine Bestandteile analysiert.

Da uns das Thema Sicherheit besonders am Herzen liegt, wollen wir hier natürlich noch einmal etwas tiefer bohren: Müssen beispielsweise die Isolierstoffe bei DC-Kabeln anders beschaffen sein als bei Wechselstromnetzen, um die nötige Sicherheit zu gewährleisten? Und sind diese in Hinblick auf ihre Eigenschaften genauso belastbar?

Dr. Karsten Fuchs: Von Hochspannungskabeln ist bekannt, dass nicht gleichermaßen die Isolierstoffzusammensetzungen von AC auch für DC verwendet werden können. Aufgrund der physikalischen Effekte ist bei DC ein sehr viel größerer Aufwand bei der Fertigung der Isolation notwendig. Diese Frage stellte sich auch für uns im Niederspannungsbereich.

Last but not least, wäre ihre persönliche Einschätzung noch einmal gefragt. Welches Potential sehen Sie zukünftig bei der Verbreitung von DC-Netzen und gibt es Pläne bei Lapp, das eigene Portfolio weiter auszubauen?

Dr. Karsten Fuchs: Ich bin davon überzeugt, dass der Umstieg auf DC in den nächsten Jahren noch stärker voranschreiten wird. Auch durch die intensivierte Auseinandersetzung mit dem Thema Nachhaltigkeit und Klimaneutralität. Durch die aktive Mitarbeit in der ODCA und ein starkes Netzwerk an engagierten und überzeugten Firmen, nicht nur aus der Automatisierungstechnik, werden wir Anlagen Schritt für Schritt umbauen und das auch bei uns im eigenen Umfeld umsetzen. GIT

Lapp Holding AG
www.lappkabel.de

Euchner auf der SPS 2025

Euchner stellte auf der SPS in Nürnberg innovative Safety-Produkte für die automatisierte Fertigung vor. Die Lösungen erfüllen moderne Kommunikationsanforderungen in vernetzten Prozessen. Sie lassen sich nahtlos integrieren und schützen so Menschen, Maschinen und Anlagen optimal.

Steigende Anforderungen an Flexibilität, Produktivität und Verfügbarkeit treffen auf komplexere Sicherheitstechnik – Anlagen- und Maschinenbauer stehen heute unter enormem Druck. Eine durchgängige, sichere Kommunikation von der Steuerung bis zum Sensor ermöglicht das Unternehmen mit robusten Komponenten und IO-Link Safety. Mit dieser standardisierten herstellerunabhängigen Schnittstelle lassen sich Schalter, Zuhaltungen und Türsysteme effizient anbinden. Das reduziert den Planungs- und Installationsaufwand erheblich. Umfassende Diagnosefunktionen erleichtern zudem die Fehlersuche, senken Wartungskosten und steigern die Verfügbarkeit der Anlagen.

Auf seinem Stand zeigte der Anbieter auch das Schutztürsystem MGB2 Modular, das sich flexibel an wechselnde Anforderungen anpasst. Es kann nahtlos in Profinet, EtherCAT (P) und EtherNet/IP eingebunden werden. Ausgelegt ist das System für alle gängigen Steuerungsarchitekturen. Ein integrierter Ethernet-Switch reduziert die Verdrahtung und vereinfacht die Netzwerktopologie. Die MGB2 Modular ermöglicht neben der Zutrittskontrolle unter anderem auch die Maschinenbedienung und Signalisierung. Das Gerät ist robust (bis -30 °C, IP65) und erfüllt die Sicherheitslevel PL e/SIL3.

Mit dem Electronic-Key-System EKS2 bietet das Unternehmen eine zentrale, manipulationssichere Lösung für die Zugriffsverwaltung in vernetzten Produktionsumgebungen mit variablen Rollen und Schichtmodellen. Wird der Zugriff nicht aktiv gesteuert, verhindert das System Fehlbedienungen, Stillstände und Sicherheitslücken. Zusammen mit dem Electronic-Key-Manager EKM2 und der integrierten Datenbank lassen sich die elektronischen Schlüssel flexibel am PC verwalten. Vordefinierte Templates, Datenverschlüsselung, hygienisches IP69-Design und die direkte Profinet-Anbindung erleichtern die Integration in bestehende Automatisierungslösungen.

Besucher konnten sich zudem über den kompakten Sicherheitsschalter CTS informieren. Dieser hat eine hohe Zuhaltekraft von bis zu 5.000 Newton und bietet flexible Einbaumöglichkeiten für Schwenk- und Schiebetüren. Sein schwimmend gelagerter Betätiger toleriert Vibrationen und Versatz. Die FlexFunction ermöglicht mit nur einem Gerät vielfältige Anwendungen, für die bisher mehrere Schaltervarianten nötig waren. Dazu kommt umfangreiches Zubehör wie die verlängerbare Fluchtentriegelung, ein Sperreinsatz oder Montageplatten, um den CTS und den Betätiger flexibel installieren zu können.

www.euchner.de

Seminare & Tagungen

Brandschutz

Ausbildung zum Brandschutzbeauftragten nach vfdb-Richtlinie 12-09-01, DGUV Information 205-003 sowie VdS 3111
19. - 28.01.26 in Essen
16. - 25.03.26 in Essen
04. - 13.05.26 in Essen
29. - 08.07.26 in Travemünde

Fachkunde zur Freigabe von Feuer- und Schweißarbeiten
20. - 21.01.26 in Essen

Weiterbildung von Brandschutzbeauftragten Schalke
Mit Begehung der VELTINS-Arena auf Schalke
27. - 28.01.26 in Essen
14. - 15.04.26 in Essen

Fahrzeugbrände – Entstehung durch Fehler bei Konstruktion, Herstellung oder Instruktion
24. - 25.02.26 in Essen

Befähigte Person Flucht- und Rettungspläne sowie Feuerwehrpläne
04. - 05.03.26 in Essen

Brandursachenermittlung
18. - 20.03.26 in Essen

Ausbildung zum Brandschutz-Manager
18. - 20.03.26 in Essen

Tagung Brände von Hochenergie-Batterien vorbeugen, erkennen, kontrollieren, löschen und entsorgen
25. - 26.03.26 in Essen

Weiterbildung von Brandschutzbeauftragten Hamburg
Mit Führung Miniatur-Wunderland
26. - 27.03.26 in Hamburg

Weiterbildung von Brandschutzbeauftragten Trier
Fortbildung nach vfdb-Richtlinie 12-09/01
16. - 17.04.26 in Trier

Gefährdungsbeurteilung im Brandschutz
27. - 28.04.26 in Essen

Prüfung von Brandschutztüren und Fachkraft für Feststellanlagen gemäß DIN 14677
07. - 08.05.26 in Essen

Brandschutz in der Gebäudetechnik
23. - 24.06.26 in Essen

Tagung Brandschutz im Tank- und Gefahrgutlager
25.06.26 in Essen

IHR ANSPRECHPARTNER:
Dipl.-Ing. Kai Brommann
Leiter Fachbereich Chemie –
Brandschutz – Verfahrenstechnik
Telefon: +49 (0)201 1803-251
E-Mail: fb5@hdt.de

hdt

hdt.de/brandschutz

Das HMI kommt an zentralen Stellen der Maschinen zum Einsatz, um die Werkstückbeladung zu steuern oder für die Steuerung der Werkzeugbeladeeinrichtung

Schwäbische Werkzeugmaschinen (SW) setzt in ihren neu gestalteten Bearbeitungszentren der A5-Serie eine modulare Profinet-/IO-Link-Bedieneinheit von Schlegel ein. Ziel war die Standardisierung der Bedienoberflächen, die Reduktion des Verdrahtungsaufwands und eine erhöhte Prozesssicherheit. Das Ergebnis: ein flexibles, robustes Bedienkonzept, das sich leicht in verschiedene Maschinentypen integrieren lässt.

MASCHINEN- UND ANLAGENSICHERHEIT

Bedienung standardisieren – Effizienz steigern

Modulare Bedienlösungen zur Vereinheitlichung von Produktionsprozessen

Schwäbische Werkzeugmaschinen mit Hauptsitz in Schramberg-Waldmössingen zählt zu den international führenden Anbietern von smarten Fertigungslösungen. Weltweit beschäftigt das Unternehmen rund 1700 Mitarbeiter und ist Weltmarktführer im Bereich der mehrspindligen CNC-Bearbeitungszentren für die Zerspanung verschiedener Materialien. Diese kommen in unterschiedlichsten Branchen zum Einsatz: von der Automobilindustrie über Elektromobilität und Medizintechnik bis hin zur Luft- und Raumfahrt. Neben den Werken in Deutschland hat SW Produktionsstandorte in den USA und China sowie in Frankreich, Italien, Polen, Ungarn, Mexiko, Korea und Indien.

SW liefert nicht nur Maschinen, sondern Komplettlösungen: modulare Bearbeitungszentren, autarke Fertigungszellen, integrierte Softwarelösungen und ganzheitliche Automationskonzepte. Bei allen Lösungen stehen Präzision, Rückverfolgbarkeit und Effizienz im Mittelpunkt. So verfolgt SW konsequent das Ziel, Fertigungssysteme skalierbar und zukunftsfähig zu gestalten.

Einheitliche Bedienung bei hoher Variantenvielfalt

Bei den modular aufgebauten Maschinenbaureihen im Serienstand A5 (z. B. BA W06, BA7x1 oder BA W08) war es ein Ziel, eine einheitliche Bedienlogik zu realisieren – trotz unterschiedlicher Konfigurationen und kundenspezifischer Anforderungen. Bei der Realisierung setzt SW auf eine Profinet- oder IO-Link-fähige Bedieneinheit von Schlegel.

Das Human-Machine-Interface (HMI) kommt an zentralen Zugriffsstellen der Maschinen zum Einsatz, um die Werkstückbeladung zu steuern oder für die Steuerung der Werkzeugbeladeeinrichtung. Um unterschiedlichen Funktionsanforderungen an der Maschine zu ermöglichen, wurden entsprechend die Bedieneinheiten konfiguriert. Wichtig war dabei nicht nur die technische Funktionalität, sondern auch die einheitliche Gestaltung, ein attraktives Design sowie eine einfache Integration in bestehende Systeme. Auch auf eine robuste Ausführung, hochwertige Qualität sowie eine integrierte Tastenbeschriftung wurde bei SW großen Wert gelegt. „Die Schlegel-Produktserie ermöglicht die Konfiguration individueller Bedientafeln mit standardisierten und zertifizierten Busschnittstellen

in attraktivem Design“, sagt René Hermle, Leiter Entwicklung Hardware.

Modular, standardisiert, anschlussfertig

Die HMI basieren auf dem Modulare Bussystem (MBS) von Schlegel und lassen sich bei SW für Profinet und IO-Link direkt in die Maschinensteuerung einbinden. Das MBS ermöglicht eine standardisierte und effiziente Integration der Bedientafeln. Durch die standardisierte Kommunikationsarchitektur reduziert sich der Verdrahtungsaufwand erheblich, gleichzeitig sinkt das Risiko von Verdrahtungsfehlern.

Die Bedientafeln werden vorkonfiguriert und mit integrierter Beschriftung ausgeliefert. Über IO-Link lassen sich die Bedienelemente parametrieren, sodass beispielsweise Fehlfunktionen erkannt oder der Austausch von Verschleißteilen rechtzeitig veranlasst werden kann. Zusätzlich können Schaltzustände ausgelesen, Statusanzeigen überwacht, Betriebsstunden gezählt und Leuchtanzeigen kontrolliert werden – Funktionen, die Wartung und Prozessüberwachung erheblich vereinfachen.

Weitere Features des MBS sind ein Analog-Eingang mit 8-Bit-A/D-Wandlung sowie die Möglichkeit, das System unkompliziert um ein RFID-Modul zu erweitern. Auch die Helligkeit der Leuchtanzeigen lässt sich flexibel anpassen – etwa durch Dimmfunktion oder ein Nachtdesign.

Positiv bewertet werden im Betrieb die hochwertige Haptik der Taster sowie die eindeutige Zuordnung der Funktionen. In der Instandhaltung profitieren die Teams von der einheitlichen Bestückung und den reduzierten Lagerbedarfen für Ersatzteile.

Standardisiert, aber anpassbar

Die modulare Gestaltung erlaubt serienspezifische oder kundenspezifische Anpassungen – ohne die Gesamtarchitektur zu verändern. So bleibt der Maschinenpark standardisiert, aber anpassbar. Die eingesetzten HMI haben sich sowohl in der Kleinserie als auch im Serienmaßstab bewährt.

SW und Schlegel verbindet eine langjährige Partnerschaft. Bereits seit über 20 Jahren arbeiten die Unternehmen zusammen, seit rund zehn Jahren auch im Bereich der Bedienlösungen. Besonders geschätzt wird bei SW die hohe Flexibilität von Schlegel bei individuellen Kundenanfragen, die gute Erreichbarkeit und die Innovationsfähigkeit bei neuen Anforderungen. „Durch die Innovationskraft von Schlegel konnte – auch dank der seit vielen Jahren professionellen und zuverlässigen Zusammenarbeit – eine hervorragende Lösung für die SW-Bedientafeln erarbeitet werden“, so Hermle. Das umfassende Produktportfolio – von Tastern über Not-Halt bis zu Anschlusskomponenten – ermögliche SW individuelle Lösungen und biete dabei dennoch eine durchgängig hohe Design- und Qualitätslinie.

Mit der erfolgreichen Einführung der Profinet-/IO-Link-Bedieneinheit ist die Entwicklung nicht abgeschlossen. Ziel bleibt es, die Mensch-Maschine-Schnittstelle noch intelligenter, vernetzter und wartungsfreundlicher zu gestalten. GIT

Bei den modular aufgebauten Maschinenbaureihen im Serienstand A5 wie z. B. BA W06 oder BA7x1 gelang es mit der modularen Profinet-/IO-Link-Bedieneinheit von Schlegel eine einheitliche Bedienlogik zu realisieren

Georg Schlegel GmbH & Co. KG
www.schlegel.biz

IO-Link Safety – Sicherheitslösungen für die Smart Factory

Mit dem IO-Link Safety-System bietet Schmersal eine intelligente Verbindung von funktionaler Sicherheit und Datentransparenz. Die nahtlose Kommunikation zwischen Maschine und Steuerung reduziert Stillstandszeiten und steigert die Effizienz. Mit der geplanten Markteinführung der Sicherheitszuhaltung AZM42 und des Sicherheitssensors RSS362 gegen Ende des ersten Halbjahres 2026 wird ein wichtiger Meilenstein für IO-Link-Safety-Anwendungen gesetzt. Damit zählt das Unternehmen zu den Pionieren der IO-Link-Safety-Integration und unterstreicht seine führende Rolle in der funktionalen Sicherheit. Beide Geräte erweitern das IO-Link-Safety-Installationssystem von Schmersal für industrielle Sicherheitsanwendungen und bieten eine bidirektionale, sichere Kommunikation über eine 3-adrige Leitung. Damit lassen sich sichere Anwendungen bis Performance Level e, Kategorie 4 bzw. SIL 3 realisieren – bei zugleich hoher Flexibilität und einfacher Integration in bestehende Anlagen. **www.schmersal.com**

Hymer-Online-Konfigurator erweitert

Hymer-Steigtechnik hat den bewährten Online-Konfigurator erweitert und bietet mehr Komponenten für individuelle und sichere Steigtechniklösungen. Die neuen Ausstattungsoptionen umfassen selbstschließende Salontüren für besonders kurze Plattformen, Durchgangssperren mit Fußleiste und Führungsrolle sowie zusätzliche Bremssysteme für fahrbare Plattformtreppen. Der Online-Konfigurator ermöglicht es Kunden aus Handwerk, Industrie und Logistik, Steigleiteranlagen, Treppen, Wartungsbühnen und Plattformen individuell und effizient zu konfigurieren. Aus dem Hymer-Baukastensystem wählen sie eine Grundlösung, die im Konfigurator flexibel an projektspezifische Anforderungen angepasst werden kann. Nach Eingabe aller Parameter erzeugt das System ein 3D-Modell in Echtzeit – für eine sofortige visuelle Prüfung und passgenaue Umsetzung. **www.hymer-alu.de**

Die Alleskönner unter den Schutzjacken

© Blåkläder

Ausführliche Beschreibung Seite 73

Effizienter Schutz vor Hitze, Flammen, Chemikalien und elektrischen Gefahren – Multinormjacken im Vergleich

Egal ob Flamm-, Hitze-, Chemikalien- und Störlichtbogenschutz oder Warnschutz – moderne Multinormschutzkleidung vereint verschiedene Schutzfunktionen in einem Kleidungsstück. Die Branche setzt dabei zunehmend auf nachhaltige, recycelte Materialien, smarte Gewebe mit erhöhter Ergonomie und Komfort sowie innovative Designs, die Bewegungsfreiheit und Langlebigkeit vereinen. Auch die Individualisierung gewinnt zunehmend an Bedeutung. Diese Trends sorgen für mehr Akzeptanz unter den Beschäftigen, was zugleich für mehr Sicherheit sorgt, denn nur Schutzkleidung die getragen wird, kann ihre Funktion erfüllen. Auf Seiten der Unternehmen reichen die Vorteile von einer Verringerung der Beschaffungskosten, über eine verbesserte Anerkennung von Versicherungsleistungen, bis hin zu einer Reduzierung von Ausfallzeiten und Folgekosten bei Arbeitsunfällen. Bei der Auswahl der Multinormschutzkleidung sind die Gefährdungsbeurteilung, der konkrete Einsatzbereich sowie Passform, Tragekomfort und Zertifizierungen entscheidend. Für eine dauerhaft hohe Schutzwirkung ist zudem die fachgerechte Pflege nach Herstellerangaben sowie eine regelmäßige Kontrolle und sachgerechte Reparatur unerlässlich. Die folgende Produktübersicht bietet einen aktuellen, herstellerübergreifenden Vergleich führender Multinormjacken und unterstützt Sie dabei, die passende Schutzkleidung für Ihre Anforderungen schnell und fundiert auszuwählen.

Firma	Blåkläder
Produktname	4446 Shell Jacke Inhärent
Normen	Oeko-Tex std 100, SE 23-302, RISE EN 1149-5 EN ISO 11611, Klasse 1 A1+A2 EN 13034 PB [6], Max. 20 Waschgänge EN ISO 11612 A1, A2, B1, C1, E3, F1 EN 343, Klasse 4, 1 EN 61482-2, APC 2, ELIM - 19, 4cal/cm², ATPV - 19, 4cal/cm²"
Materialzusammensetzung	39% Modacryl 27% Baumwolle 18% Polyamid 10% Polyurethan 5% Aramid 1% antistatisch Faser
Gewicht des Materials (g/m²)	290 g/m²
Verfügbare Größen	XS - 4XL
Farbe(n)	Schwarz, Marineblau
Taschenanzahl und -position	Brusttasche mit Reißverschluss und D-Ring Vordertaschen mit Reißverschlüssen Innentasche mit Klettverschluss"
Verschlusssystem	Verdeckter 2-Wege-Reißverschluss aus Kunststoff
Zertifizierungen	siehe Normen
Pflegehinweise	Normalwaschgang 60 °C Nicht bleichen Nicht chemisch reinigen Nicht bügeln Nicht im Trockner trocknen
Tragekomfort	Hoher Tragekomfort dank inhärenter Flammhemmung in der Faser
Besonderheiten	Metallfrei und ATEX-konform, wind- und wasserdicht, öl- und schmutzabweisend, mit Befestigungspunkten für Messgeräte; Kapuze separat erhältlich
Preis (UVP)	449,- €
Lieferzeit	sofort verfügbar
Nachhaltigkeitsaspekte	Oeko-Tex std 100, SE 23-302, RISE
Herstellungsland	Myanmar
Link zum Shop	https://shorturl.at/Es8rF

© HB Protective Wear


© Fristads


© Paul H. Kübler


© uvex

HB Protective Wear	Fristads	Paul H. Kübler	uvex
HB MultiPro FR Fleecejacke 4kA und 7kA	Flamestat High Vis Airtech Winterparka Kl.3 4086 ATHR	Kübler Protectiq High Vis Jacke ARC1	Softshelljacke
EN ISO 20471 Klasse 3 IEC 61482-2 / 1-lagig APC 1; 2-lagig APC 2 EN ISO 11612 A1, B1, C1, F1 EN 14058 Klasse 1	EN 342 Kälteschutz EN 343 Regenschutz EN ISO 11611 Klasse 1 Schweißer-Schutz EN 13034 Schutz (begrenzt) vor flüssigen Chemikalien EN ISO 11612 Schutz vor Hitze und Flammen EN 1149 Schutz vor elektrostatischer Entladung EN 61482-2 Störlichtbogen, Box test APC 2 Co-Zertifizierung High vis U6 EN ISO 20471 Klasse 3 Warnschutz	EN 11611, Klasse 1-A1 EN 11612 Code A1 B1 C1 F1 EN 61482-2 APC=1 EN 1149-5 EN 20471 +A1, Klasse 2 EN 15797	EN ISO 11611 Klasse 2 A1 EN ISO 11612 A1, B1, C2, F2 EN 61482-2 Klasse 1 EN 1149-5 EN 20471 Klasse 2
48% Modacryl 32% Baumwolle 18% Polyester 2% Carbon	Außenmaterial Airtech: 50% Modacryl 41% Baumwolle 7% Polyurethan 2% antistatische Faser, 2-Lagen-Laminat Futter: 40% Modacryl 37% Viskose FR 22% Viskose 1% antistatische Faser Gesteppte Wattierung: 100% Polyester	6% Modacryl 33% Polyester 30% Aramid 1% antistatische Faser	Softshell außen: 42 % Modacryl 37 % Polyester 20 % Baumwolle 1 % antistatische Faser Softshell innen: 100 % Modacryl-Fleece Futter: 50 % Aramid 50 % Viskose
ca. 360 g/m² (2-lagig / 7kA-Ausführung: + ca. 195 g/m²)	Oberstoff 260 g/m², Futter 195 g/m², Wattierung 170 g/m², Ärmel 120 g/m²	ca. 260 g/m²	350g/m²
3XS - 5XL	2XS - 4XL	2XS - 6XL	S - 6XL
Fluoreszierend Gelb	Warnschutz-Gelb/Marine - 171	Warngelb/Anthrazit, Warnorange/Anthrazit	warngelb/schwarz
2 Seitentaschen	Verdeckter Zwei-Wege-Reißverschluss vorne unter einer Patte mit Klettverschluss / Innentasche mit Reißverschluss und Handytasche, zugänglich bei geschlossenem Kleidungsstück / Innentasche mit Reißverschluss	2 Brusttaschen 2 Seitentaschen 2 Innentaschen	2 Seitentaschen eine Brusttasche mit verdecktem Reißverschluss
Frontleiste und Taschen mit verdeckten Reißverschlüssen gearbeitet	Reißverschluss	Abgedeckter Frontreißverschluss, Blende mit Druckknöpfen, Klette, Taschen mit Patte und Klette	Reißverschluss
s.o. Normen + OEKO-TEX Standard 100	OEKO-TEX®	siehe Normen, OEKO-TEX	
Normalwaschgang bei 60 °C Trocknen bei niedriger thermischer Beanspruchung	Normalwaschgang bei 60°C Nicht bleichen Trocknen im Wäschetrockner möglich, bis 60 °C Nicht bügeln Nicht chemisch reinigen	Schonwaschgang 60 °C Nicht bleichen Trocknen mit normaler thermischer Beanspruchung Bügeln mit geringer Temperatur Chemische Reinigung (P)	Pflegeleicht 40 °C Nicht bleichen Trocknen bei niedriger thermischer Beanspruchung Bügeln mit geringer Temperatur Nicht im Trockner Trocknen
Bequeme Strickbündchen an den Ärmeln, weicher Stehkragen	Funktionelle Multinorm-Arbeitsjacke mit hohem Lichtbogenschutz aus einem weichen und bequemen Material mit inhärentem Flammschutz	Angenehmer Tragekomfort, Comfort-Fit	Hoher Tragekomfort durch Materialeinsatz und suXXeed Passform (Stretchelemente)
Saum mit Kordelzug; hochsichtbar durch Reflexanbringung im Bodylanguage Prinzip; einzippbar in Multinormen Parkas und zusätzliche Befestigungslaschen	Wasserdicht, winddicht und atmungsaktiv Multinorm inhärenter Schutz Extra hoher Störlichtichtbogenschutz ELIM 26 cal, APC 2	Bekleidungssystem (auch ohne Warnschutz erhältlich, mit verschiedenen Schutzklassen, auch als Schweißerschutzvariante, Damenprodukte, Wetterprodukte	Materialmix, Tragekomfort, Passform, Design
4kA 190,30€ / 7kA 229,60€	599,90 €	337,60 €	289€ Listenpreis
lagerhaltig verfügbar	sofort verfügbar	sofort verfügbar	sofort verfügbar
Oeko-Tex zertifiziert	Frei von PFAS	Reparaturfreundlich verarbeitet, OEKO-TEX Standard 100	-
Bulgarien	Ukraine	Nord-Mazedonien	Bosnien und Herzegowina
https://shorturl.at/jGZIS			

SICHERHEITSSCHUHE

Dauerhaft leicht und robust

Sicherheitsschuhe mit Gore-Tex Extraguard-Technologie von Atlas und Elten

Die neue Extraguard-Obermaterialtechnologie von Gore-Tex Professional vereint die Vorteile von robusten Materialien mit der Leichtigkeit textiler Oberflächen. Sie wurde insbesondere für den Einsatz unter extremen Arbeitsbedingungen entwickelt und bietet nicht nur Schutz und Komfort, sondern reduziert auch den Pflegeaufwand erheblich. Die ersten Modelle von Atlas und Elten sind bereits im Handel erhältlich.

© Gore-Tex Professional

Die Extraguard-Technologie richtet sich an Branchen, in denen Arbeitnehmer extremen Bedingungen ausgesetzt sind. Dazu gehören das Baugewerbe, der Schienenbau, die Versorgungsindustrie sowie der Garten- und Landschaftsbau. In diesen Bereichen ist es entscheidend, dass Sicherheitsschuhe nicht nur Schutz bieten, sondern auch leicht und bequem sind. Lutz Hentrey, Leiter der Abteilung Produktmanagement bei Elten, betont: „Extraguard richtet sich an Branchen, in denen Arbeitnehmer täglich extremen Bedingungen ausgesetzt sind, die aber dennoch nicht auf Komfort bei ihren Sicherheitsschuhen verzichten möchten. Dazu gehören das Baugewerbe, das Abbruchgewerbe, der Schienenbau, die Versorgungsindustrie sowie der Garten- und Landschaftsbau."

Vorteile der Extraguard-Obermaterialtechnologie

Die Extraguard-Obermaterialtechnologie besteht aus drei Lagen: Die äußere Lage ist hoch abriebfest und robust, die zweite Lage schützt den Fuß vor Stoß- und Schlagbelastungen, und die dritte Lage verhindert das Eindringen von Feuchtigkeit, wodurch im Ergebnis auch der Wärmeverlust reduziert wird. Diese Konstruktion sorgt dafür, dass die Schuhe auch bei starker Nutzung leicht und komfortabel bleiben. „Die Vorteile von Extraguard für den Endkunden liegen in der Kombination aus Leichtigkeit, Langlebigkeit und hohem Tragekomfort. Im Vergleich zu herkömmlichem Leder ist das Extraguard-Obermaterial rund 40 Prozent leichter und behält diese Leichtigkeit selbst bei starker Nässe", erklärt Lutz Hentrey weiter. Zudem ermöglicht das neue Obermaterial eine wesentlich schnellere Rücktrocknungszeit im Vergleich zu Sicherheitsschuhen mit konventionellen Obermaterialien.

Einblicke in die Entwicklung und Produktion

Die Entwicklung der Extraguard-Technologie war ein intensiver Prozess, der umfangreiche Forschung und Tests erforderte. „Die Materialien von Gore-Tex werden erst dann marktreif, wenn sie in intensiven Tests unter extremsten Bedingungen ihre Leistung und Haltbarkeit unter Beweis gestellt haben. Diese gehen weit über die Anforderungen aus Nomen hinaus. Dazu gehören Material- und Systemtests, Leistungstests mit Testpersonen und Praxistests im Feld." erklärt Helmut Klug von Gore-Tex Professional Fabrics.

Das Unternehmen arbeitete eng mit verschiedenen Partnern zusammen, um sicherzustellen, dass die Technologie den hohen Anforderungen der Zielbranchen gerecht wird. Dabei wurden zahlreiche Prototypen erstellt und unter extremen Bedingungen getestet, um die optimale Kombination aus Schutz, Komfort und Langlebigkeit zu erreichen.

Lutz Hentrey erläutert: „Wir legen bei Elten größten Wert auf den Tragekomfort unserer Schuhe. Denn wer den ganzen Tag in seinen Sicherheitsschuhen auf den Beinen ist, merkt am Ende des Tages, ob sie relativ schwer oder leicht sind. Gerade in Branchen, in denen besonders robuste Lederschuhe getragen werden, kann die neue Extraguard-Obermaterialtechnologie eine gute Alternative sein."

Insbesondere bei Nässe und Kälte kann Extraguard als Obermaterial gegenüber Leder punkten

© Gore/www.paulrossfilm.com

Nachhaltigkeit und Umweltfreundlichkeit: Modelle von Atlas und Elten

Ein weiterer wichtiger Aspekt der Extraguard-Technologie ist ihre Umweltfreundlichkeit. Die Materialien sind so konzipiert, dass sie langlebig und pflegeleicht sind, was den Ressourcenverbrauch reduziert. Zudem wird bei der Produktion auf umweltfreundliche Verfahren geachtet, um den ökologischen Fußabdruck zu minimieren.

„Alle Gore-Tex Produkte sind auf dauerhafte Performance und eine lange Lebensdauer ausgelegt. Das Extraguard Obermaterial ist aufgrund seiner robusten und dauerhaften Performance ein hervorragendes Beispiel dafür, da es die Produktlebensdauer verlängert. Dies belegen zahlreiche unter Labor- und Praxisbedingungen durchgeführte Tests. Durch den geringen Ressourcenverbrauch und minimierte CO_2 -Emissionen setzt das Material zudem neue Maßstäbe in Bezug auf die geringen Umweltauswirkungen bei der Herstellung“, so Helmut Klug.

Des Weiteren ist die Reinigung extrem einfach und erfordert im Gegensatz zu konventionellen Obermaterialien wie Leder keine speziellen Pflegeprodukte, was ebenfalls Kosten reduziert und zugleich die Umwelt schont.

Die ersten Modelle, die mit der Extraguard-Technologie ausgestattet wurden, stammen von den Herstellern Atlas und Elten. Es handelt sich um die Modelle der Atlas XT-Serie und das Modell Antonio XXSG GTX Mid ESD S3S WR CI von Elten. Die Schuhe sind nicht nur funktional, sondern auch ästhetisch ansprechend gestaltet, was sie zu einer attraktiven Wahl für Arbeitnehmer in verschiedenen Branchen macht.

Lutz Hentrey betont: „Die Einführung der Extraguard-Obermaterialtechnologie markiert einen wichtigen Schritt in der Weiterentwicklung von Sicherheitsschuhen. Durch die Kombination von Robustheit und Leichtigkeit bietet sie einen erheblichen Mehrwert für Arbeitnehmer in verschiedenen Branchen.“ GIT

Gore-Tex Professional
www.goretexprofessional.com/de

PSA

Gut sichtbar auch im Dunkeln

Erhöhte Sicherheit für mittlere Risikosituationen durch lichtreflektierende Workwear

Zusätzlich aufgenähte Reflexstreifen erhöhen bei Dunkelheit die Sichtbarkeit der Trägerinnen und Träger

Die DIN EN 17353:2020 ersetzt seit 2020 die EN 1150 für Wanderbekleidung und die EN 13356 für Warnzubehör, wie zum Beispiel Reflexanhänger- und Bänder sowie Warnkrägen und Rucksackabdeckungen. Im Unterschied zu den beiden Vorgängernormen regelt sie die Anforderungen an Warnschutzbekleidung und Warnzubehör für den Einsatz in mittleren Risikobereichen sowohl im Freizeit- als neuerdings auch im professionellen Bereich.

Die DIN EN 17353 unterscheidet drei Typen. Wenn das Risiko, übersehen zu werden, nur bei Tageslicht besteht, kommt Kleidung vom Typ A mit fluoreszierendem Material zum Einsatz. Zulässig sind hier mehr fluorisierende Farben als bei der für Hochrisikobereiche geltenden EN ISO 20471, so beispielweise fluoreszierendes Gelb-Grün oder fluoreszierendes Rosa. Besteht das Risiko, übersehen zu werden, ausschließlich bei Dunkelheit, erhöht Kleidung vom Typ B die Sichtbarkeit durch Verwendung von retrofluoreszierendem Material (siehe Tabelle) .

Laufen Anwender Gefahr, bei Tageslicht, bei Dämmerung und in Dunkelheit übersehen zu werden, ist die Kleidung vom Typ AB vorgeschrieben. Diese ist mit reflektierenden und fluoreszierenden und/oder Materialien mit kombinierten Eigenschaften ausgestattet.

Der Typ AB setzt voraus, dass die Anforderungen an Typ A und B2 bzw. B3 erfüllt sind. Bei Typ AB2 muss die Kleidung im Bereich der Gliedmaßen reflektierende und fluoreszierende und/oder Materialien mit kombinierten Eigenschaften aufweisen. Bei Typ AB3 gilt es dies für Gliedmaßen und Torso.

Relevanz der DIN EN 17353 und PSA-Kategorie 2

Die DIN EN 17353 ist mit ihrer Veröffentlichung im Jahr 2020 noch eine recht junge Norm und spielt im direkten Vergleich mit der DIN EN ISO 20471 eine eher untergeordnete Rolle. Allerdings ist zu beobachten, dass das Sicherheitsbewusstsein, was die Sichtbarkeit anbelangt, in den letzten Jahren deutlich zugenommen hat. Folglich wird findet auch Kleidung, welche die DIN EN 17353 erfüllt, mehr Beachtung.

Wie die DIN EN ISO 20471 fällt die DIN EN 17353 in die PSA-Kategorie 2 mit allen

Rechten und Verpflichtungen im professionellen Bereich. Dazu zählen Tragepflicht in den Gefahrenbereichen, kostenlose Bereitstellung, hygienisch einwandfreie Wiederaufbereitung und jährliche Unterweisung. Relevant für die Auswahl von Schutzkleidung und damit auch für die nach der DIN EN 17353 zertifizierte Bekleidung ist die im Rahmen einer Gefährdungsanalyse erstellte Gefahrenstellenbeschreibung. Sowohl der Arbeitgeber als Bereitsteller der PSA als auch der Arbeitnehmer als Anwender sind zur Einhaltung verpflichtet. Zuwiderhandlungen können arbeitsrechtliche Konsequenzen und Haftungsrisiken nach sich ziehen.

Tab.: Übersicht über die Typen und Stufen der DIN EN 17353

	Tageslicht (Fluoreszierend)	Dunkelheit (Retroreflektierend)	Kombinierte Eigenschaften
Baumelnd / frei beweglich		**Typ B1** Baumelnde hängende Reflexelemente	
Gliedmaßen		**Typ B2** Langarm Shirts mit Reflexelemente Bein- und Armbänder	**TYP AB2** Shirts, Jacken, Westen Ponchos
Gliedmaßen und Körper	**Typ A** Shirts, Jacken, Westen Hosen	**Typ B3** Shirts, Hosen, Westen, Jacken	**TYP AB3** Shirts, Hosen, Westen, Jacken

Erweiterte Sicherheitsstandards und neue Produktlinien

Für die erfolgreichen Workwearkollektionen Kübler Activiq und Kübler Bodyforce, die Multinormkleidung Kübler Protectiq sowie die Schweißerkleidung Kübler Protectiq Welding bietet der renommierte Hersteller ab sofort zusätzlich nach DIN EN 17353 Typ B2 zertifizierte Modelle an. Diese werden auf Kundenwunsch mit hochwertigem Reflexmaterial versehen, um die Sichtbarkeit von Trägerinnen und Trägern in der Dämmerung und bei Dunkelheit zu erhöhen. Die nachträgliche Ausstattung erfolgt in der Produktion am Stammsitz in Plüderhausen. Kübler wird außerdem neue Produktlinien mit Eignung für Zielgruppen, die einem mittleren Risiko des Übersehen-Werdens ausgesetzt sind, nach der einschlägigen Norm zertifizieren. So kann die Norm auf Anfrage auch bei diesen Produkten kurzfristig umgesetzt werden. GIT

Paul H. Kübler Bekleidungswerk GmbH & Co. KG
www.kuebler.eu

Liebe Leserinnen und Leser,

In BusinessPartner, dem „Who is who in Sachen Sicherheit", präsentieren sich Ihnen die kompetentesten Anbieter aus allen Sicherheitsbereichen. Die hier vertretenen Firmen legen Wert auf den Kontakt mit Ihnen. Alle Einträge finden Sie auch in www.git-sicherheit.de/buyers-guide mit Links zu den Unternehmen!

Sie gehören selbst zu den wichtigen Anbietern und wollen mit jeder Ausgabe 30.000 Entscheider direkt erreichen? Dann kontaktieren Sie uns für eine Aufnahme.

SICHERHEITS MANAGEMENT

Sicherheitsmanagement

barox
Switche für Video

barox Kommunikation GmbH · 79540 Lörrach
Tel.: +49 7621 1593 100
www.barox.de · mail@barox.de
Cybersecurity, Videoswitch, PoE Power-over-Ethernet, Medienkonverter, Extender

Sicherheitsmanagement

GU BKS SERVICE

GU BKS SERVICE GmbH
Heidestr. 71 · 42549 Velbert
Tel. 0800/2051001
office@gu-bks.de · www.gu-bks.de

Service mit System

Sicherheitsmanagement

BOSCH

Bosch Building Technologies
Fritz-Schäffer-Straße 9 · 81737 München
Tel.: 0800/7000444 · Fax: 0800/7000888
Info.service@de.bosch.com
www.boschbuildingtechnologies.de
Produkte und Systemlösungen für Einbruchmelde-, Brandmelde-, Sprachalarm- und Managementsysteme, professionelle Audio- und Konferenzsysteme. In ausgewählten Ländern bietet Bosch Lösungen und Dienstleistungen für Gebäudesicherheit, Energieeffizienz und Gebäudeautomation an.

Sicherheitsmanagement

idware
Identity · Access · Control

ID-ware Deutschland GmbH
Walther-von-Cronberg-Platz 2-18, Haus 6
60594 Frankfurt am Main
Tel. 069-210 855 60
info@id-ware.com, www.id-ware.com
Physical Identity & Access Management (PIAM)-Lösungen für große Organisationen, Software sowie Dienstleistungen für smarte Identifikations- und Authentifizierungsprozesse: PIAM-Suite, Credential Management, Access Management, Visitor Management, Contractor Management, SDK zur Kartenpersonalisierung, Photo Capture Tool, Hardware, Secure Credential Consultancy, Credentials as a Service

Sicherheitsmanagement

ABUS
Security Tech Germany

ABUS Security-Center GmbH & Co. KG
Linker Kreuthweg 5 · D-86444 Affing
Tel.: +49(0)8207/95990-0
Fax: +49(0)8207/95990-100
info.de@abus-sc.com · www.abus.com
ABUS Security-Center ist Hersteller innovativer Alarmanlagen, Videoüberwachungssysteme und Zutrittskontrollsysteme. Als Teil der ABUS Gruppe ist das Unternehmen sowohl auf branchenspezifische Sicherheitsbedürfnisse, als auch auf die Anforderungen von Privatanwendern spezialisiert.

Sicherheitsmanagement

DAITEM

Daitem / Atral Security Deutschland GmbH
Eisleber Str. 4 · D-69469 Weinheim
Tel.: +49(0)6201 94 330-40
info.de@daitem.com · www.daitem.com
Funk-Einbruch- und Brandschutzlösungen vom Technologieführer. Vertrieb über qualifizierte Sicherheitsfacherrichter.

Sicherheitsmanagement

nsc
Sicherheitstechnik GmbH

NSC Sicherheitstechnik GmbH
Grete-Hermann-Str. 6
33758 Schloß Holte-Stukenbrock
Tel.: +49 (0) 5257 97799-0
Fax: +49 (0) 5257 97799-29
info@nsc-sicherheit.de · www.nsc-sicherheit.de
Brandmeldetechnik, Videotechnik, Sprach-Alarm-Anlagen

Sicherheitsmanagement

ASSA ABLOY
Opening Solutions

ASSA ABLOY Sicherheitstechnik GmbH
Bildstockstraße. 20 · 72458 Albstadt
www.assaabloy.com/de · albstadt@assaabloy.com
Das Unternehmen entwickelt, produziert und vertreibt unter den traditionsreichen und zukunftsweisenden Marken IKON, effeff und KESO hochwertige Produkte und vielseitige Systeme für den privaten, gewerblichen und öffentlichen Bereich.

Sicherheitsmanagement

deister electronic

deister electronic GmbH
Hermann-Bahlsen-Str. 11
D-30890 Barsinghausen
Tel.: +49(0)5105/516-111 · Fax: +49(0)5105/516-217
info.de@deister.com · www.deister.com
Zutritts- und Zufahrtskontrollsysteme; biometrische Verifikation; Wächterkontrollsysteme; Verwahrung und Management von Schlüsseln und Wertgegenständen

Sicherheitsmanagement

Security Robotics

Security Robotics Development & Solutions GmbH
Mühlweg 44 · 04319 Leipzig
Tel.: 0341-2569 3369
info@security-robotics.de · www.security-robotics.de
Robotics, Sicherheitstechnik, Autonomie, Qualitätssteigerung, Künstliche Intelligenz, Vernetzte Zusammenarbeit, SMA Unterstützung

Sicherheitsmanagement

Vereinigung für die Sicherheit der Wirtschaft e.V.
Lise-Meitner-Straße 1 · 55129 Mainz
Tel.: +49 (0) 6131 - 57 607 0
info@vsw.de · www.vsw.de
Als Schnittstelle zwischen den Sicherheitsbehörden und der Wirtschaft in allen Fragen der Unternehmenssicherheit steht die gemeinnützige Vereinigung seit 1968 der Wirtschaft als unabhängige Organisation zur Verfügung.

Gebäudesicherheit

SimonsVoss Technologies GmbH
Feringastr. 4 · 85774 Unterföhring
Tel.: 089 992280
marketing-simonsvoss@allegion.com
www.simons-voss.com
Digitale Schließanlagen mit Zutrittskontrolle, kabellose und bohrungsfreie Montage, batteriebetrieben, keine Probleme bei Schlüsselverlust.
Digital Schließen ist neu für Sie? Rufen Sie an: 089 99228-555

VIDEO ÜBERWACHUNG

GEBÄUDE SICHERHEIT

Gebäudesicherheit

Süd-Metall Beschläge GmbH
Sägewerkstraße 5 · D - 83404 Ainring/Hammerau
Tel.: +49 (0) 8654 4675-50 · Fax: +49 (0) 8654 4675-70
info@suedmetall.com · www.suedmetall.com
Funk-Sicherheitsschlösser made in Germany, Mechanische & elektronische Schließsysteme mit Panikfunktion und Feuerschutzprüfung, Zutrittskontrollsysteme modular und individuell erweiterbar, Systemlösungen, Fluchttürsteuerung

Videoüberwachung

ABUS Security-Center GmbH & Co. KG
Linker Kreuthweg 5 · D-86444 Affing
Tel.: +49(0)8207/95990-0
Fax: +49(0)8207/95990-100
info.de@abus-sc.com · www.abus.com
ABUS Security-Center ist Hersteller innovativer Alarmanlagen, Videoüberwachungssysteme und Zutrittskontrollsysteme. Als Teil der ABUS Gruppe ist das Unternehmen sowohl auf branchenspezifische Sicherheitsbedürfnisse, als auch auf die Anforderungen von Privatanwendern spezialisiert.

Gebäudesicherheit

deister electronic GmbH
Hermann-Bahlsen-Str. 11
D-30890 Barsinghausen
Tel.: +49(0)5105/516-111 · Fax: +49(0)5105/516-217
info.de@deister.com · www.deister.com
Zutritts- und Zufahrtskontrollsysteme; biometrische Verifikation; Wächterkontrollsysteme; Verwahrung und Management von Schlüsseln und Wertgegenständen

Gebäudesicherheit

TAS Sicherheits- und Kommunikationstechnik
Telefonbau Arthur Schwabe GmbH & Co. KG
Langmaar 25 · D-41238 Mönchengladbach
Tel.: +49 (0) 2166 858 0 · Fax: +49 (0) 2166 858 150
info@tas.de · www.tas.de
Übertragungsgeräte, Alarmierungs- und Konferenzsysteme, Remote Services für sicherheitstechnische Anlagen, vernetzte Sicherheitslösungen

Videoüberwachung

Ihr Value Added Distributor für Videosicherheitstechnik „Made in Germany“

Dallmeier Components GmbH
Hoheluftchaussee 108 | 20253 Hamburg
Tel. +49 40 47 11 213-0 | Fax +49 40 47 11 213-33
info@d-components.com | www.d-components.com

Gebäudesicherheit

Dictator Technik GmbH
Gutenbergstr. 9 · 86356 Neusäß
Tel.: 0821/24673-0 · Fax: 0821/24673-90
info@dictator.de · www.dictator.de
Antriebstechnik, Sicherheitstechnik, Tür- und Tortechnik

Gebäudesicherheit

Uhlmann & Zacher GmbH
Gutenbergstraße 2-4 · 97297 Waldbüttelbrunn
Tel.: +49(0)931/40672-0 · Fax: +49(0)931/40672-99
contact@UundZ.de · www.UundZ.de
Elektronische Schließsysteme, modular aufgebaut und individuell erweiterbar

Videoüberwachung

Dallmeier electronic GmbH & Co. KG
Bahnhofstraße 16 · 93047 Regensburg
Tel.: 0941/8700-0 · Fax: 0941/8700-180
info@dallmeier.com · www.dallmeier.com
Videosicherheitstechnik made in Germany: Multifocal-Sensortechnologie Panomera®, IP-Kameras, Aufzeichnungsserver, intelligente Videoanalyse, Videomanagementsoftware

Gebäudesicherheit

DOM Sicherheitstechnik GmbH & Co. KG
Wesselinger Straße 10-16 · D-50321 Brühl / Köln
Tel.: + 49 2232 704-0 · Fax: + 49 2232 704-375
dom@dom-group.eu · www.dom-security.com
Mechanische und digitale Schließsysteme

PERIMETER SCHUTZ

Videoüberwachung

EIZO Europe GmbH
Belgrader Straße 2 · 41069 Mönchengladbach
Tel.: +49 2161 8210 0
info@eizo.de · www.eizo.de/ip-decoding
Professionelle Monitore und Lösungen für den 24/7-Einsatz in der Videoüberwachung, IP-Decoder-Lösungen mit einfacher Installation und computerlosem Betrieb.

Gebäudesicherheit

frogblue · Smart Building Technology
Luxemburger Straße 6 · 67657 Kaiserslautern
Tel: +49-631-520829-0
info@frogblue.com · www.frogblue.com/de/
Frogblue ist führend in der Entwicklung von drahtlosen, auf Bluetooth® basierenden Elektroinstallationslösungen für den professionellen Einsatz, die vollständig in Deutschland produziert werden. (Sicherheit, SmartHome, energieeffiziente Gebäudetechnik, Zutrittskontrolle)

Perimeterschutz

Berlemann Torbau GmbH
Ulmenstraße 3 · 48485 Neuenkirchen
Tel.: +49 5973 9481-0 · Fax: +49 5973 9481-50
info@berlemann.de · www.berlemann.de
INOVA ist die Marke für alle Komponenten der Freigeländesicherung aus einer Hand! Als Qualitätshersteller für Schiebetore, Drehflügeltore, Zaun-, Zugangs- und Detektionssysteme haben Sie mit INOVA auf alle Fragen des Perimeterschutzes die passende Antwort.

Videoüberwachung

Hanwha Techwin Europe Limited
Kölner Strasse 10
65760 Eschborn
Tel.: +49 (0)6196 7700 490
hte.dach@hanwha.com · www.hanwha-security.eu/de
Hersteller von Videoüberwachungsprodukten wie Kameras, Videorekorder und weiteren IP-Netzwerkgeräten. Sowie Anbieter von Software-Lösungen wie beispielsweise Videoanalyse, Lösungen für den Vertical-Market und Videomanagementsoftware (VMS).

Videoüberwachung

HIKVISION

HIKVISION Deutschland GmbH
Flughafenstr. 21 · D-63263 Neu-Isenburg
Tel.: +49 (0) 69/40150 7290
sales.dach@hikvision.com · www.hikvision.com/de
Datenschutzkonforme Videoüberwachung, Panorama-Kameras, Wärmebild-Kameras, PKW-Kennzeichenerkennung

Zeit + Zutritt

DoorBird
Technology meets Design.

Bird Home Automation GmbH
Uhlandstr. 165 • 10719 Berlin
Tel. +49 30 12084824 • pr@doorbird.com
Zutrittskontrolle; Tür- und Tortechnik; Türkommunikation; Gebäudetechnik; IP Video Türsprechanlage; RFID; Biometrie; Fingerabdruck; Made in Germany

www.doorbird.com

Zeit + Zutritt

FEIG

FEIG ELECTRONIC GMBH
Industriestr. 1a · 35781 Weilburg
Tel.: +49(0)6471/3109-375 · Fax: +49(0)6471/3109-99
sales@feig.de · www.feig.de
RFID-Leser (LF, HF, UHF) für Zutritts- und Zufahrtskontrolle, Geländeabsicherung, Bezahlsysteme u.v.m.

Videoüberwachung

i-PRO

i-PRO EMEA B.V.
Laarderhoogtweg 25 · 1101 EB Amsterdam
Netherlands
https://i-pro.com/eu/en
Hochwertige CCTV-Lösungen (IP & analog), Video-Automatisierung und KI, Technologien für hohe Ansprüche (FacePro, Personen-Maskierung), Schutz vor Cyber-Attacken im Einklang mit DSGVO, VMS: Video Insight

Zeit + Zutritt

cryptin
CICHON STOLBERG

Cichon+Stolberg GmbH
Wankelstraße 47-49 · 50996 Köln
Tel.: 02236/397-200 · Fax: 02236/61144
info@cryptin.de · www.cryptin.de
Betriebsdatenerfassung, Zeiterfassung, cryptologisch verschlüsselte Zutrittskontrolle

Zeit + Zutritt

gantner
INSPIRED ACCESS

GANTNER Electronic GmbH
Bundesstraße 12 · 6714 Nüziders · Österreich
Tel.: +43 5552 33944
info@gantner.com · www.gantner.com
Systemlösungen in Zutrittskontrolle/Biometrie, Zeiterfassung, Betriebsdatenerfassung, Schließsysteme, Zugriffsschutz, Schrankschließsysteme

Videoüberwachung

Zeit + Zutritt

deister electronic

deister electronic GmbH
Hermann-Bahlsen-Str. 11
D-30890 Barsinghausen
Tel.: +49(0)5105/516-111 · Fax: +49(0)5105/516-217
info.de@deister.com · www.deister.com
Zutritts- und Zufahrtskontrollsysteme; biometrische Verifikation; Wächterkontrollsysteme; Verwahrung und Management von Schlüsseln und Wertgegenständen

Zeit + Zutritt

GUNNEBO

Gunnebo Deutschland GmbH
Carl-Zeiss-Str. 8 · 85748 Garching
Tel.: +49 89 244163500
info@gunnebo.de · www.gunnebo.de
Tresore und Schränke, Tresorräume, Tresortüren, Hochsicherheitsschlösser, Elektronische Schlösser

ZEIT
ZUTRITT

Zeit + Zutritt

DNAKE

DNAKE (Xiamen) Intelligent Technology Co., Ltd.
No.8, Haijing North 2nd Rd., Xiamen, Fujian, China
Tel.: +86 592-5705812
sales01@dnake.com, www.dnake-global.com
Intercom System, IP Video Intercom, 2-Wire IP Intercom, Cloud Intercom Service, Access Control

Zeit + Zutritt

pcs

PCS Systemtechnik GmbH
Pfälzer-Wald-Straße 36 · 81539 München
Tel.: 089/68004-0 · Fax: 089/68004-555
intus@pcs.com · www.pcs.com
Zeiterfassung, Gebäudesicherheit, Zutritts- und Zufahrtskontrolle, Biometrie, Video, Besuchermanagement, SAP, Handvenenerkennung

Zeit + Zutritt

AceProx
Identifikationssysteme GmbH

AceProx Identifikationssysteme GmbH
Bahnhofstr. 73 · 31691 Helpsen
Tel.: +49(0)5724-98360
info@aceprox.de · www.aceprox.de
RFID-Leser für Zeiterfassung, Zutrittskontrolle und Identifikation

Zeit + Zutritt

dormakaba

dormakaba Deutschland GmbH
DORMA Platz 1 · 58256 Ennepetal
T: +49 (0) 2333/793-0
info.de@dormakaba.com · www.dormakaba.de
Umfassendes Portfolio an Produkten, Lösungen und Services rund um die Tür sowie den sicheren Zutritt zu Gebäuden und Räumen aus einer Hand. Dies umfasst Schließsysteme, voll vernetzte elektronische Zutrittslösungen, physische Zugangs- und automatische Türsysteme, Türbänder, Beschläge, Türschließer, Zeiterfassung inkl. ERP-Anbindungen, Hotelschließsysteme und Hochsicherheitsschlösser.

Zeit + Zutritt

phg
Die richtige Verbindung

phg
Peter Hengstler GmbH + Co. KG
D-78652 Deißlingen · Tel.: +49(0)7420/89-0
datentechnik@phg.de · www.phg.de
RFID und Mobile Access: Leser für Zutrittskontrolle, Zeiterfassung, BDE, Türkommunikation, Besuchermanagement, Parksysteme, Zufahrtskontrolle, Vending, ... Terminals, Einbaumodule, Kartenspender, Tischlesegeräte, Leser für Markenschalterpogramme, Identifikationsmedien, ... einfach und komfortabel zu integrieren.

Zeit + Zutritt

AZS
SYSTEM AG

AZS System AG
Mühlendamm 84 a · 22087 Hamburg
Tel.: 040/226611 · Fax: 040/2276753
www.azs.de · anfrage@azs.de
Hard- und Softwarelösungen zu Biometrie, Schließ-, Video-, Zeiterfassungs- und Zutrittskontrollsysteme, Fluchtwegsicherung, Vereinzelungs- und Schrankenanlagen, OPC-Server

Zeit + Zutritt

ELATEC
RFID Systems

ELATEC GmbH
Zeppelinstr. 1 · 82178 Puchheim
Tel.: +49 89 552 9961 0
info-rfid@elatec.com · www.elatec.com
Anbieter von Benutzerauthentifizierungs- und Identifikationslösungen. Unterstützung der digitalen Transformation von Kunden und Partnern durch das Zusammenspiel von universellen Multifrequenz-Lesegeräten und fortschrittlicher Authentifizierungssoftware, Service und Support.

Zeit + Zutritt

primion
AZKOYEN Time & Security Division

primion Technology GmbH
Steinbeisstraße 2-4 · 72510 Stetten a.K.M.
Tel.: 07573/952-0 · Fax: 07573/92034
info@primion.de · www.primion.de
Arbeitszeitmanagement, Zugangsmanagement, Personaleinsatzplanung, grafisches Alarmmanagement, SAP-Kommunikationslösungen, Ausweiserstellung, Biometrie

Zeit + Zutritt

ASSA ABLOY
Entrance Systems

Record Türautomation GmbH | Part of ASSA ABLOY
Otto-Wels-Straße 9 · 42111 Wuppertal
Tel: +49 202 60901 130 · Fax: +49 202 60901 11
sec.de@assaabloy.com · www.assaabloyentrance.de
Speedgates, Durchgangs- und Sicherheitsschleusen, Drehkreuze, Schwenktüren, Sicherheits-Karussell-türen und -Portale für die Sicherheits-Zutritts-kontrolle und Personenvereinzelung.

BRAND SCHUTZ

ARBEITS SICHERHEIT

Zeit + Zutritt

salto
INSPIRED ACCESS

SALTO Systems GmbH
Schwelmer Str. 245 · 42389 Wuppertal
Tel.: +49 202 769579-0 · Fax: +49 202 769579-99
info.de@saltosystems.com · www.saltosystems.de
Vielseitige und maßgeschneiderte Zutrittslösungen – online, offline, funkvernetzt, Cloud-basiert und mobil.

Brandschutz

DENIOS
UMWELTSCHUTZ & SICHERHEIT

DENIOS SE
Dehmer Straße 54-66
32549 Bad Oeynhausen
Fachberatung: 0800 753-000-3
Gefahrstofflagerung, Brandschutzlager, Brandschutz für Lithium-Akkus, Wärme- und Kälte-kammern, Containment, Auffangwannen, Arbeits-schutz, sicherheitsrelevante Betriebsausstattung, Gefahrstoff-Leckage-Warnsystem

Arbeitssicherheit

ELTEN

ELTEN GmbH
Ostwall 7–13 · 47589 Uedem
Tel.: 02825/8068
www.elten.com · service@elten.com
Sicherheitsschuhe, Berufsschuhe, PSA, ELTEN, Berufsbekleidung, Sicherheit

Zeit + Zutritt

TKH SECURITY

TKH Security GmbH
Heinrich-Hertz-Straße 40 | D-40699 Erkrath
Tel.: +49 211 247016-0 | Fax: +49 211 247016-11
info.de@tkhsecurity.com | https://tkhsecurity.com/de/
Zugangskontrolle, Zutrittssteuerung, Cloudlösungen, Schließanlagen, Videoüberwachung, Sicherheitsmanagement

Brandschutz

Hertek
Brandschutzsysteme

Hertek GmbH
Landsberger Straße 240
12623 Berlin
Tel.: +49 (0)30 93 66 88 950
info@hertek.de · www.hertek.de
Hertek: ein Unternehmen im Bereich Brandschutz-lösungen. Branchenspezifisches Fachwissen mit hoch-wertigen Brandschutzkomponenten vereint zu einem sicheren und verlässlichen Brandschutz. Flankiert wird dies mit Fachschulungen und einem umfangreichen, lösungsorientierten Kundenservice.

Arbeitssicherheit

Hailo

Hailo-Werk
Rudolf Loh GmbH & Co. KG
Daimlerstraße 8 · 35708 Haiger
www.hailo-professional.de
professional@hailo.de
Steig-/Schachtleitern, Steigschutzsysteme, Schachtabdeckungen, Servicelifte, Schulungsangebote

NOTRUF SERVICE LEITSTELLE

Ihr Eintrag in der Rubrik

GIT BusinessPartner
Die Einkaufsrubrik für den direkten Kontakt

Schicken Sie einfach eine E-Mail an miryam.reubold@wiley.com

Wir beraten Sie gerne!

GEFAHRSTOFF MANAGEMENT

Notruf- und Service-Leitstelle

HWS

HWS Wachdienst Hobeling GmbH
Am Sportpark 75 · D-58097 Hagen
Tel.: (0 23 31) 47 30 -0 · Fax: -130
hobeling@hobeling.com · www.hws-wachdienst.de
VdS-Notruf- und Service-Leitstelle, Alarmempfangs-stelle DIN EN 50518, Alarmprovider, Mobile Einsatz- und Interventionskräfte, Objekt- und Werkschutz

Brandschutz

seTec

Securitas Technology GmbH
SeTec Sicherheitstechnik
Haupstr. 40 a · 82229 Seefeld
Tel.: +49(0)8152/9913-0 · Fax: +49(0)8152/9913-20
info@setec-security.de · www.setec-security.de
Handfeuermelder, Lineare Wärmemelder, Feuerwehr Schlüsseldepots, Feuerwehr, Schlüsselmanager, Feuerwehrperipherie, Feststellanlagen, Störmeldezentralen

Gefahrstoffmanagement

asecos

asecos GmbH
Sicherheit und Umweltschutz
Weiherfeldsiedlung 16–18 · 63584 Gründau
Tel.: +49 6051 9220-0 · Fax: +49 6051 9220-10
info@asecos.com · www.asecos.com
Gefahrstofflagerung, Umwelt- unad Arbeitsschutz, Sicherheitsschränke, Chemikalien- und Umluft-schränke, Druckgasflaschenschränke, Gefahrstoffar-beitsplätze, Absauganlagen, Raumluftreiniger uvm.

Notruf- und Service-Leitstelle

Fernwirk-Sicherheitssysteme Oldenburg
FSO
Ihr Security-Provider

FSO Fernwirk-Sicherheitssysteme Oldenburg GmbH
Am Patentbusch 6a · 26125 Oldenburg
Tel.: 0441-69066 · info@fso.de · www.fso.de
Alarmempfangsstelle nach DIN EN 50518
Alarmprovider und Notruf- und Service Leitstelle nach VdS 3138, zertifiziertes Unternehmen für die Störungsannahme in der Energieversorgung.

Brandschutz

WAGNER
DIE BESSERE LÖSUNG IM BRANDSCHUTZ

WAGNER Group GmbH
Schleswigstraße 1–5 · 30853 Langenhagen
Tel.: +49 (0)511 97383 0
info@wagnergroup.com · www.wagnergroup.com
Brandfrüherkennung und Brandmeldeanlagen, Brandvermeidung, Brandbekämpfung, Gefahrenmanagement

Gefahrstoffmanagement

BAUER
SÜDLOHN

BAUER GmbH
Eichendorffstraße 62 · 46354 Südlohn
Tel.: + 49 (0)2862 709-0 · Fax: + 49 (0)2862 709-156
info@bauer-suedlohn.com · www.bauer-suedlohn.com
Auffangwannen, Brandschutz-Container, Fassregale, Gefahrstofflagerung, Regalcontainer, Wärmekammern, individuelle Konstruktionen

Gefahrstoffmanagement

DENIOS
UMWELTSCHUTZ & SICHERHEIT

DENIOS SE
Dehmer Straße 54-66
32549 Bad Oeynhausen
Fachberatung: 0800 753-000-3
Gefahrstofflagerung, Brandschutzlager, Brandschutz für Lithium-Akkus, Wärme- und Kältekammern, Containment, Auffangwannen, Arbeitsschutz, sicherheitsrelevante Betriebsausstattung, Gefahrstoff-Leckage-Warnsystem

MASCHINEN ANLAGEN SICHERHEIT

Maschinen + Anlagen

Leuze

Leuze electronic GmbH & Co. KG
In der Braike 1 · D-73277 Owen
Tel.: +49(0)7021/573-0 · Fax: +49(0)7021/573-199
info@leuze.com · www.leuze.com
Optoelektronische Sensoren, Identifikations- und Datenübertragungssysteme, Distanzmessung, Sicherheits-Sensoren, Sicherheits-Systeme, Sicherheits-Dienstleistungen

Gefahrstoffmanagement

SÄBU
BAUEN MIT SYSTEM

SÄBU Morsbach GmbH
Zum Systembau 1 · 51597 Morsbach
Tel.: 02294 694-23 · Fax: 02294 694-38
fladafi@saebu.de · www.fladafi.de
Gefahrstofflagerung, Gefahrstoffcontainer, Arbeits- & Umweltschutz, Auffangwannen, Gasflaschenlagerung, Gasflaschencontainer, Gasflaschenbox, Kleingebinderegale
Besuchen Sie unseren Online-Shop: www.fladafi.de

Maschinen + Anlagen

EUCHNER
More than safety.

EUCHNER GmbH + Co. KG
Kohlhammerstraße 16
D-70771 Leinfelden-Echterdingen
Tel.: 0711/7597-0 · Fax: 0711/753316
www.euchner.de · info@euchner.de
Automation, MenschMaschine, Sicherheit

Maschinen + Anlagen

PEPPERL+FUCHS

Pepperl+Fuchs SE
Lilienthalstraße 200 · 68307 Mannheim
Tel.: 0621/776-1111 · Fax: 0621/776-27-1111
fa-info@de.pepperl-fuchs.com
www.pepperl-fuchs.com
Sicherheits-Sensoren, Induktive-, Kapazitive-, Optoelektronische und Ultraschall-Sensoren, Vision-Sensoren, Ident-Systeme, Interface-Bausteine

GASMESS TECHNIK

Maschinen + Anlagen

IBF

IBF Solutions GmbH
Bahnhofstr. 8 · 6682 Vils - AT
Tel. +43 (0) 5677 53 53 - 30
sales@ibf-solutions.com · www.ibf-solutions.com
Führender Anbieter von Softwaresystemen und Consulting-Leistungen im Bereich Maschinensicherheit. Unser Fokus liegt auf der Unterstützung nationaler und internationaler Kunden bei der CE-Kennzeichnung und Risikobeurteilung von Maschinen, Anlagen und elektrischen Geräten.

Maschinen + Anlagen

pizzato

Pizzato Deutschland GmbH
Brienner Straße 55 · 80333 München
Tel.: 01522/5634596 · 0173/2936227
info@pizzato.com · www.pizzato.com
Automatisierung, Maschinen- und Anlagensicherheit: Sensorik, Schalter, Zuhaltungen, Module, Steuerungen, Mensch-Maschine-Schnittstelle, Positions- und Mikroschalter, Komponenten für die Aufzugsindustrie, u.v.m.

Gasmesstechnik

smart GasDetection Technologies

GfG Gesellschaft für Gerätebau mbH
Klönnestraße 99 · D-44143 Dortmund
Tel.: +49 (0)231/56400-0 · Fax: +49 (0)231/56400-895
info@gfg-mbh.com · GfGsafety.com
Gaswarntechnik, Sensoren, tragbare und stationäre Gasmesstechnik

Maschinen + Anlagen

SCHMERSAL
THE DNA OF SAFETY

K.A. Schmersal GmbH & Co. KG
Möddinghofe 30 · 42279 Wuppertal
Tel.: 0202/6474-0 · Fax: 0202/6474-100
info@schmersal.com · www.schmersal.com
Sicherheitszuhaltungen und Sicherheitssensoren, optoelektronische Sicherheitseinrichtungen wie Sicherheitslichtschranken sowie Sicherheitsrelaisbausteine, programmierbare Sicherheitssteuerungen und die Safety Services des Geschäftsbereichs tec.nicum

Maschinen + Anlagen

SSP
Safety System Products

SSP Safety System Products GmbH & Co. KG
Max-Planck-Straße 21 · DE-78549 Spaichingen
Tel.: +49 7424 980 490 · Fax: +49 7424 98049 99
info@ssp.de.com · www.safety-products.de
Dienstleistungen & Produkte rund um die Maschinensicherheit: Risikobeurteilung, Sicherheitssensoren, -Lichtvorhänge, - Zuhaltungen, -Steuerungen sowie Schutzumhausungen, Zustimmtaster uvm.

Sicherheit komplett

aus dem Wiley Verlag

NEWSLETTER
GIT-SICHERHEIT.de
Jetzt kostenfrei registrieren

www.git-sicherheit.de/newsletter

WILEY
Industry Talks

Mit **Profis, Macherinnen und Entscheidern** in Sachen Sicherheit

Ausgabe ONLINE lesen

Mit unseren digitalen und gedruckten Medien sind Sie immer bestens informiert – über alle Themen der Sicherheit.

Probeabos, Mediadaten, Kontakt: GIT-GS@wiley.com

WILEY

DIE VIP LOUNGE

Marco Mille

Global Head of Security, Siemens AG

- geb. in Luxemburg, verheiratet und Vater zweier erwachsener Töchter
- Studium Politikwissenschaften an der Universität Freiburg im Breisgau sowie an der Brock University in St. Catharines, Kanada.
- Berufliche Stationen: Westeuropäischen Union, Auswärtiges Amt in Luxemburg, Luxemburgischer Staatlicher Nachrichtendienstdienst.
- Seit 2010 Chief Security Officer der Siemens AG in München.

Was hat Sie dazu bewogen, eine Aufgabe im Bereich Sicherheit zu übernehmen? Sicherheit hat mich schon immer fasziniert, weil Sicherheit und Frieden die Grundlagen für unser Zusammenleben sind. Bereits während meines Studiums der Politikwissenschaft bemerkte ich die enge Verbindung zwischen Sicherheit, internationalen Beziehungen und Geschichte.

Welche sicherheitspolitische Entscheidung oder welches Projekt sollte Ihrer Meinung nach schon längst umgesetzt sein? Wir brauchen eine gesamtgesellschaftliche, integrierte Sicherheitspolitik, die über sektorale Interessen hinausgeht und verschiedene Akteure – von Politik und Behörden über die Wirtschaft und Zivilgesellschaft bis hin zur Wissenschaft – miteinander verbindet.

Die beste Erfindung im Bereich Sicherheit ist Ihrer Meinung nach: Technologien wie KI und Quantentechnik haben in der Sicherheitsbranche Potenzial haben, aber sie sind gleichzeitig auch Werkzeuge, die von Angreifern genutzt werden können. Dieses Paradox macht die Branche so herausfordernd. Etwas Unscheinbares, aber brillant Einfaches: die elektrostatisch haftende Flipchart-Folie. Mit ihr lässt sich in Sekundenschnelle ein beliebiger Raum in einen voll funktionsfähigen Krisenraum verwandeln.

Ein Erfolg, den Sie kürzlich errungen haben, war: Ich hatte kürzlich das Privileg, an der Young Security Professionals Academy (YSPA) teilzunehmen – einer Initiative, die sich der Förderung von Nachwuchstalenten in der Sicherheitsbranche widmet. Was mich besonders beeindruckt hat, war die Energie und der frische Blick, den die Nachwuchsprofessionals mitgebracht haben. Diese Gespräche waren nicht nur lehrreich, sondern haben mir auch neue Perspektiven eröffnet.

Wer hat Ihrer Meinung nach eine Auszeichnung verdient? Ohne jede Frage: Meine Ehefrau. Seit 35 Jahren schafft sie es nicht nur, mich mit bewundernswerter Geduld und Liebe zu begleiten, sondern auch aktiv zu managen und zu motivieren.

Wobei entspannen Sie? Ich entspanne beim Lesen und in der Natur – am liebsten mit Frau und Hund, oder im Garten. Reisen mit meiner Frau gehört auch dazu, genauso wie ein guter Film, eine spannende Serie oder, wenn ich allein bin, eine Runde Football – nur auf der Couch, versteht sich.

Welchen Urlaubsort können Sie empfehlen? Mich persönlich zieht es regelmäßig ins Burgund. Die Region bietet eine wunderbare Mischung aus malerischer Natur, erstklassigem Wein, köstlichem Essen und einer wunderschönen, historischen Kulisse.

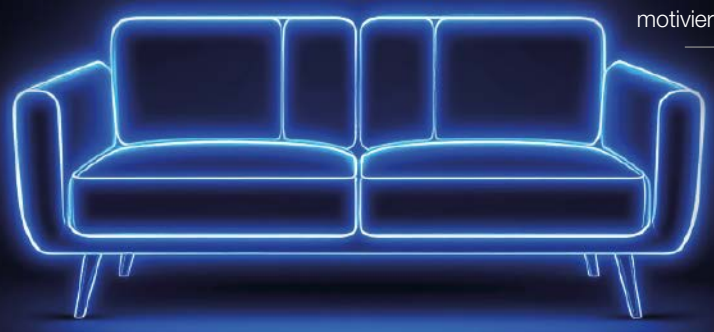
Welche Zeitschriften lesen Sie regelmäßig? Ich muss zugeben, ich bin kein großer Zeitschriftenkonsument – zumindest nicht, was Printmedien betrifft. Fach- und Nachrichtenliteratur konsumiere ich mittlerweile fast ausschließlich online.

Die GIT SICHERHEIT ist für mich wichtig, weil… Die GIT SICHERHEIT bietet ein umfassendes Informationsangebot für Fachleute und Entscheidungsträger in verschiedenen Bereichen der Unternehmenssicherheit. Sie verbindet aktuelle, fundierte Inhalte mit einem modernen digitalen Format und schlägt eine wichtige Brücke zwischen Anbietern und Nutzern von Sicherheitslösungen. Gleichzeitig ermöglicht sie es den unterschiedlichen Gewerken, stets auf dem neuesten Stand der Entwicklungen zu bleiben – ein wichtiges Medium, um den Überblick in diesem dynamischen Umfeld zu behalten.

Welches Buch haben Sie zuletzt gelesen? Ich lese gerade Sebastian Haffners „Geschichte eines Deutschen. Die Erinnerungen 1914–1933“. Das Buch zeigt, wie politische Umbrüche und extremistische Bewegungen das Leben und Denken einzelner Menschen prägen können.

Welche Musik hören Sie am liebsten? Ich höre am liebsten gitarrenlastige Rock- und Bluesmusik der alten Schule – von Led Zeppelin, Deep Purple, Lynyrd Skynyrd und Eric Clapton bis hin zu Joe Bonamassa und Greta van Fleet. Aber auch Größen wie B.B. King und Stevie Ray Vaughan stehen ganz oben auf meiner Liste.

Was motiviert Sie? Das Morgen.



Unser VIP-Lounge-Gespräch mit Marco Mille war besonders inspirierend und sprengt den vertrauten Rahmen dieser Rubrik. Sie möchten das ganze Gespräch lesen? Schauen Sie unter:

Wir denken Sicherheit neu.

Risiken verändern sich. Bedrohungen wie Cyberangriffe, technische Ausfälle, Lieferkettenunterbrechungen oder auch Extremwetterereignisse stellen Unternehmen, Institutionen und Anlagenbetreiber vor Herausforderungen.

Wir bündeln die verschiedenen Systeme auf einer herstellerneutralen Plattform. Qualifiziertes Personal überwacht rund um die Uhr aus unserer intelligenten Leitstelle sämtliche sicherheitsrelevanten Prozesse in Ihrem Unternehmen.

www.klueh.de

KI-generiert durch Frank Maagh, NT-Medien GmbH

DIE NÄCHSTE GENERATION SMARTER GEBÄUDEAUTOMATION

Zukunftssicher. Innovativ. Energieeffizient.

MADE IN GERMANY

OHNE KABEL.
OHNE LIMITS.
MAXIMAL SICHER.

Für Projekte jeder Größe!

frogblue™
SMART BUILDING TECHNOLOGY GERMANY

Luxemburger Straße 6
67657 Kaiserslautern
frogblue.de
info@frogblue.com
+49 631 520829-0