35. JAHRGANG | Januar/Februar 2026 | AUSGABE 1–2 | 17 €

GIT SICHERHEIT

30 926

MAGAZIN FÜR SAFETY UND SECURITY

Ausgabe ONLINE lesen:

Titelthema Seite 28:

Kritis im Griff

Ganzheitliche Sicherheitslösung von Interflex für die Stadtwerke München

HEFT IM HEFT

ROBOTIK I DROHNEN
ab S. 22

WILEY


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

Das Recht des Stärkeren

Die jüngsten Schritte der USA gegenüber Venezuela und die erneute Diskussion um den Erwerb Grönlands sind ein Beleg für die drohende Auflösung der regelbasierten Weltordnung. Macht ersetzt Diplomatie – wie in den dunkelsten Tagen der Kanonenbootpolitik des 19. Jahrhunderts. Die damit einhergehenden geopolitischen Verschiebungen betreffen längst nicht mehr nur Staaten, sondern wirken tief in unsere Gesellschaften und Infrastrukturen hinein. Sie verdeutlichen, wie fragil Sicherheit geworden ist und wie sehr hybride Bedrohungen, Einflussoperationen und digitale wie physische Angriffe ineinandergreifen.

Vor diesem Hintergrund gewinnt die Debatte um nationale Resilienz an Dringlichkeit. Der Beitrag „Kritik rund ums Kritis Dachgesetz“ (ab Seite 8) zeigt eindrucksvoll, wie kontrovers die Einschätzungen im Bundestag ausfallen: Zwischen Überregulierung und notwendigem Schutz gilt es, jene Balance zu finden, die kritische Anlagen wirklich widerstandsfähiger macht. Gleichzeitig verschwimmen die Linien zwischen militärischen und zivilen Gefahren, wie unser exklusives Interview mit Professor Dennis-Kenji Kipker (ab Seite 10) verdeutlicht. Drohnen, Cyberoperationen und verdeckte Einflussnahmen sind längst Teil des Alltags und verlangen nach integrierten Antworten, die Technik, Organisation und strategisches Denken verbinden.

Dass dies besonders Energieversorger betrifft, verdeutlicht ein weiteres Interview mit Andreas Sauerwald von Bosch Building Technologies ab Seite 12. Die Energiewende schafft neue Abhängigkeiten und Angriffsflächen, die nur mit ganzheitlichen Konzepten beherrschbar sind. Doch Resilienz endet nicht am Werktor. Unternehmen müssen in Netzwerken denken, wie wir mit Daniel Fai, Sicherheitschef bei Procter & Gamble und Vorstand im VSW-Mainz, ab Seite 14 aufzeigen.

Wie diese Anforderungen in der Praxis aussehen, verdeutlicht unser Titelthema ab Seite 28 am Beispiel der Stadtwerke München, realisiert mit Lösungen von Interflex: Die Vielzahl verteilter Standorte, unterschiedliche Sicherheitsniveaus und der hohe regulatorische Druck verlangen skalierbare, integrative Systeme, die Zutritt, Besucherströme und betriebliche Abläufe sicher zusammenführen. Ergänzend dazu widmet sich ein weiterer Schwerpunkt der Robotik und Drohnentechnologie (ab Seite 20) – einem Feld, das Sicherheits- und Inspektionsprozesse revolutioniert. Während Robotik hilft, Personalengpässe und gefährliche Einsatzorte abzufedern, entwickeln sich Drohnenabwehr und sensorbasierte Erkennung zu unverzichtbaren Bausteinen moderner Sicherheitsarchitekturen.

All unsere Themen machen deutlich: Sicherheit ist 2026 keine statische Disziplin mehr. Sie ist ein permanenter Transformationsprozess – von Resilienz über Robotik bis hin zu neuen Sicherheitslösungen.

Bleiben Sie neugierig,
bleiben Sie sicher.

Herzlichst,
Ihr

Dr. Timo Gimbel
für das Team GIT SICHERHEIT

TITELTHEMA

Kritis im Griff

Ganzheitliche Sicherheitslösung von Interflex für die Stadtwerke München

ab Seite 28

PRO-4-PRO für 2025/2026

Dennis-Kenji Kipker

Andreas Sauerwald

Daniel Fai

Erik Liegle

MANAGEMENT

HEFT IM HEFT
ROBOTIK I DROHNEN

SECURITY

Martin Kaller

Hendrik Tarek Dehne

Alexander Bogocz

Marion Heidrich

CYBER-SECURITY

BRANDSCHUTZ

KULTUR-/DENKMALSCHUTZ

FEUERLÖSCHER

RUBRIKEN

SAFETY

MASCHINEN- UND ANLAGENSICHERHEIT

SCHUTZKLEIDUNG

SICHERHEITSHANDSCHUHE

EVENTS

INDEX

QUICK-FINDER

ORGANISATIONEN, INSTITUTIONEN UND UNTERNEHMEN IM HEFT

NEWS

VDMA meldet Auftragsplus

Die Elektrische Automation verzeichnete in den ersten neun Monaten des laufenden Jahres ein reales Auftragsplus von 5 Prozent, doch der Umsatz blieb im Vergleich zum Vorjahreszeitraum unverändert. Das teilt der VDMA mit. Auf Kundenseite geht der Abbau der Lagerbestände auf Komponentenebene voran, aber es fehlen im Maschinen- und Anlagenbau weiterhin Aufträge, um die Auftragslage wieder auf eine stabile Basis zu heben.

Die zuletzt unberechenbare Zollpolitik der USA hat hier für weitere Zurückhaltungen gesorgt. Neue Investitionen seitens der Kundenbranchen werden wegen der Unwägbarkeiten am Markt zurückgestellt und Investitionsentscheidungen verschoben. Insgesamt rechnet die Elektrische Automation für dieses Jahr mit einem Plus von 1 Prozent beim Umsatz gegenüber dem Vorjahr.

„Aufgrund der geopolitischen Herausforderungen erwartet die Branche für die erste Jahreshälfte 2026 eine weiterhin angespannte Auftragslage gegenüber 2025. Bei verbesserten politischen Rahmenbedingungen ist in der zweiten Jahreshälfte mit einem Aufwärtstrend zu rechnen“, prognostiziert Jörg Freitag, Vorstandsvorsitzender VDMA Elektrische Automation. „Die fortschreitende Digitalisierung, Künstliche Intelligenz und technologischen Innovationen im Produktionsbereich bieten die Chance zum Wachstum für die Elektrische Automation“, so Jörg Freitag. Deshalb engagiert sich der VDMA Elektrische Automation in Digitalisierungsthemen wie Datenökonomie, Cyber Resilienz und Tools aus einer anwendungsorientierten Perspektive. **www.vdma.org**

ZVEI Onlineseminar „Fachkraft für Rufanlagen nach DIN VDE 0834“

Die ZVEI-Akademie bietet am 25.2.2026 das Onlineseminar „Fachkraft für Rufanlagen nach DIN VDE 0834“ an. Der Teilnehmer erhält eine Einführung in die DIN VDE 0834 und das notwendige Know-how zur Inspektion, Wartung und Instandsetzung von Rufanlagen, um sich optimal auf die Fachkraftprüfung vorzubereiten. Rufanlagen dienen in Krankenhäusern, Altenpflegeheimen und Justizvollzugsanstalten dazu, Pflege- oder Aufsichtspersonal in Notfällen herbeizurufen. Die Anlagen werden auch als Lichtruf, Schwesternruf, Personen- oder Patientenruf bezeichnet. Sie dürfen nach DIN VDE 0834 nur von geschulten Fachkräften geplant, errichtet, betrieben und instandgehalten werden. **www.zvei-services.de**

Jens Kronenberg übernimmt Vertriebsleitung bei GU BKS Service GmbH


© GU BKS Service GmbH

Jens Kronenberg

Die GU BKS Service GmbH verstärkt ihre Vertriebsorganisation: Jens Kronenberg hat die Vertriebsleitung des Unternehmens übernommen. Er wechselt von Dormakaba Deutschland, wo er zuletzt als Leiter Objektmanagement die Architekten- und Objektberatung verantwortete. Mit mehr als zwei Jahrzehnten Erfahrung im Projektgeschäft der Bau- und Gebäudetechnikbranche bringt Jens Kronenberg ein breites Kompetenzspektrum in den Bereichen Objektvertrieb, Projektakquise sowie digitale Planungs- und Umsetzungsprozesse mit. Durch seine langjährige Zusammenarbeit mit Investoren, Projektentwicklern, Architekten und Fachplanern hat er tiefgreifendes Know-how zu sicherheitsrelevanten Anforderungen im Gebäudeumfeld – ein Themenfeld, das durch KRITIS- und NIS2-Anforderungen weiter an Relevanz gewinnt. **www.g-u.de**

Flughafen BER: Kötter Aviation Security gewinnt Ausschreibung


© Kötter Services

Andreas Kaus, Geschäftsführender Direktor der Kötter Aviation Security SE & Co. KG

Wichtiger Erfolg und nachhaltige Qualitätsbestätigung für Kötter Aviation Security: Das Unternehmen hat von der Flughafen Berlin Brandenburg GmbH im Zuge einer europaweiten Ausschreibung den Zuschlag für umfangreiche Sicherheits- und Serviceaufgaben am drittgrößten Flughafenstandort in Deutschland erhalten. Diese umfassen die Personal- und Warenkontrollen (von Flughafen-Mitarbeitern, Zulieferern/Handwerkern, Crews etc.) sowie die Bordkartenkontrolle (aller Fluggäste), Zugangskontrollen und Streifengänge. Der Neuauftrag startet am 1. Juni 2026.

Mit der jetzt erfolgten Vergabe setzt die Flughafen Berlin Brandenburg GmbH die seit Sommer 2024 bestehende Partnerschaft mit Kötter Aviation Security fort. „Wir freuen uns sehr über das positive Votum unseres Auftraggebers sowie auf die weitere Zusammenarbeit und bedanken uns bei der Flughafen Berlin Brandenburg GmbH für das damit verbundene Vertrauen“, erklärt Andreas Kaus, Geschäftsführender Direktor der Kötter Aviation Security SE & Co. KG.

„Gleichzeitig sind wir stolz darauf, dass unser Familienunternehmen sowohl im Rahmen der aktuellen Ausschreibung als auch durch die bisherige Leistung auf ganzer Linie als Qualitätsgarant überzeugen konnte. Damit unterstreichen wir erneut unsere Kompetenz im Bereich der Flughafensicherheit und beim Schutz kritischer Infrastrukturen. Meine besondere Anerkennung und mein ausdrücklicher Dank gelten daher unserem Aviation Security-Team am BER.“ **www.koetter.de**

FORSI-Tagungsband 5 ist erschienen

© FORSI

Wie die Hochschule der Akademie der Polizei Hamburg, Forschungsinstitut für Unternehmenssicherheit und Sicherheitswirtschaft (FORSI), mitteilt, ist der 5. FORSI-Tagungsband erschienen. Die 5. FORSI-Sicherheitstagung befasste sich mit dem Thema „Schutz Kritischer Infrastrukturen (KRITIS) am Beispiel des Sektors Verkehr". Die Veranstaltung wurde von der Hochschule der Akademie der Polizei Hamburg, Forschungsinstitut für Unternehmenssicherheit und Sicherheitswirtschaft (FORSI), in Kooperation mit der Handelskammer Hamburg durchgeführt. Gegenstand der Tagung waren die Cybergefahren wie auch die physischen Gefahren für KRITIS unter Berücksichtigung des Sektors Verkehrs. **https://akademie-der-polizei.hamburg.de**

Sicherheit im Fokus: BHE-Fachsymposium „Einbruchschutz" 2026

Am 9./10. Februar 2026 lädt der BHE Bundesverband Sicherheitstechnik e. V. zum fünften Fachsymposium „Einbruchschutz" nach Fulda ein. Die Veranstaltung bietet Sicherheitsfachfirmen und NSL-Betreibern sowie Anwendern, Versicherern und Behördenmitarbeitern eine ausgezeichnete Plattform, um sich über aktuelle Entwicklungen und innovative Lösungen im Einbruchschutz auszutauschen.

Die Teilnehmer erwartet ein abwechslungsreiches Vortragsprogramm mit praxisnahen Beiträgen renommierter Sicherheitsexperten. So widmet sich Harald Schmidt, Kriminaldirektor der Stiftung Deutsches Forum für Kriminalprävention (DFK), der neuen Zertifizierung von Fachfirmen für Überfall-/Einbruchmelde- sowie Gefahrenwarnanlagen nach DIN VDE V 0827-41. Dabei geht er unter anderem auf den bundeseinheitlichen Pflichtenkatalog der Polizei und die Arbeit der neu gegründeten Arbeitsgemeinschaft EMA-Fachfirmen-Zertifizierung ein.

Mit den Auswirkungen aktueller rechtlicher Vorgaben befasst sich Achim Winter, Telenot Electronic GmbH. In seinem Vortrag „Sicherheitstechnik in Zeiten von KRITIS, NIS-2 & Co." erläutert er, welche Anforderungen moderne Sicherheitslösungen erfüllen müssen und wie diese erfolgreich in der Praxis umgesetzt werden können.

Frank Wahr, ABI-Sicherheitssysteme GmbH, stellt in seinem Vortrag „Von der Insellösung zum integrierten System" die Vorteile und Chancen offener Schnittstellen für die Vernetzung von Gebäuden heraus. Ergänzt wird das Vortragsprogramm durch eine begleitende Fachausstellung, auf der führende Anbieter ihre Produkte und Lösungen präsentieren. Hier bietet sich den Teilnehmern die Gelegenheit, sich mit Experten auszutauschen und wertvolle Impulse für die eigene Praxis zu gewinnen. Der abendliche Branchentreff am ersten Veranstaltungstag lädt zudem zum entspannten Networking und persönlichen Austausch. **www.bhe.de**


© Prosero Security

(v. l.:) Jürgen Stein, Goldfunk Sicherheitstechnik, Johan Martinsson, M&A Prosero Security, Michael Ackert, Goldfunk Sicherheitstechnik

Goldfunk Sicherheitstechnik wird Teil von Prosero Security

Prosero Security akquiriert Goldfunk Sicherheitstechnik, ein namhaftes Sicherheitsunternehmen mit Sitz in Erfurt in Mitteldeutschland. Mit dieser Akquisition stärkt Prosero die eigene Position auf dem deutschen Markt und erweitert das eigene Know-how im Bereich fortschrittlicher Sicherheitslösungen für Verkehrstunnel sowie für kritische und öffentliche Einrichtungen. Goldfunk plant, installiert und wartet ein breites Spektrum von Sicherheitstechnologien, darunter CCTV, Zutrittskontrollsysteme, Sprechanlagen, Brandmeldeanlagen und Einbruchmeldeanlagen. Darüber hinaus bietet Goldfunk fortschrittliche Kommunikations- und Funksysteme sowie Komplettlösungen für öffentliche, industrielle und gewerbliche Gebäude an. Mit langjähriger Erfahrung, hoher Kundenzufriedenheit und einer starken Innovationskraft ist Goldfunk hervorragend aufgestellt, um sich auf dem schnell wachsenden Markt für technische Sicherheitslösungen weiterzuentwickeln. **www.prosero.com**

Startschuss für Mitteldeutschlands Sicherheitsindustrie

Chancen für mitteldeutsche Unternehmen: Nach seiner Gründung im September geht das Mitteldeutsche Institut für Sicherheitsindustrie (MISI) nun in die Umsetzung. Eine hochrangig besetzte Gründungsveranstaltung markiert den operativen Start. Rund 120 Vertreter aus Bundeswehr, Forschung, Industrie und Politik diskutierten in Leipzig, welche Rolle Mitteldeutschlands Unternehmen in der sicherheitspolitischen Zeitenwende übernehmen können. Die Konferenz wurde gemeinsam mit Sachsenmetall, dem Unternehmensverband der Metall- und Elektroindustrie Sachsen, organisiert.

Ziel des MISI ist es, Mitteldeutschland als leistungsfähigen Standort der Sicherheits- und Verteidigungswirtschaft sichtbar zu machen – national und europäisch. Die Region soll künftig stärker auf der Karte der deutschen und europäischen Verteidigungswirtschaft erscheinen. Gleichzeitig will das Institut regionale Wertschöpfung erhöhen und Unternehmen den Marktzugang erleichtern. Die Veranstaltung sendet ein klares Signal: Mitteldeutschland will sich als verlässlicher Partner für Bundesregierung, Bundeswehr und große Systemhersteller positionieren. Schon bis Ende dieses Jahres will das MISI zahlreiche Zulieferer, technologieorientierte Mittelständler, Verbände und Forschungseinrichtungen unter einem gemeinsamen institutionellen Dach bündeln. **https://misi-ev.de**

KRITIS

Kritik rund ums Kritis-Dachgesetz

Expertenkritik am aktuellen Entwurf im Innenausschuss des Deutschen Bundestages

Bei einer Anhörung im Innenausschuss des Deutschen Bundestages Anfang Dezember erhoben sich kritische Expertenstimmen zum Gesetzesvorhaben der Bundesregierung zur Stärkung der physischen Sicherheit kritischer Anlagen. Dies berichtete die Pressestelle des Deutschen Bundestages. Bei der Anhörung ging es um einen Gesetzentwurf der Bundesregierung „zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz kritischer Anlagen“ (21/2510) sowie um einen Antrag der Fraktion Bündnis 90/Die Grünen mit dem Titel „Deutschland resilient machen – Für einen ganzheitlichen Schutz unserer kritischen Infrastruktur“ (21/2725).

Alexander Averhoff, Deutscher Städte- und Gemeindebund, erklärte, Resilienzstrategien, umfassende Prävention und effektiver Bevölkerungsschutz seien große Herausforderungen für die Kommunen und die Betreiber kritischer Infrastruktur. Er sehe kritisch, dass im Gesetzentwurf aber „die Kommunen komplett raus“ seien. Die vorgesehenen Umsetzungsfristen seien den Kommunen zu kurz. Sie wünschten sich eine Verlängerung auf 24 Monate. Bund und Länder müssten den Kommunen angemessene finanzielle Mittel bereitstellen.

Betreiber nicht alleine lassen

Mathias Böswetter, BDEW-Bundesverband der Energie- und Wasserwirtschaft, befand, der Gesetzentwurf schaffe erstmals einen sektorenübergreifenden Rechtsrahmen für den physischen Schutz kritischer Anlagen und ergänze damit das bestehende IT-Sicherheitsrecht für die kritischen Infrastrukturen. Dieses Ziel begrüße sein Verband ausdrücklich.

Insbesondere die wirtschaftliche Umsetzung der Maßnahmen sei entscheidend für eine nachhaltige Resilienzsteigerung bei den kritischen Infrastrukturen und eine gesamtgesellschaftliche Aufgabe. Wirtschaft und Gesellschaft seien auf eine wirtschaftliche Versorgung mit Energie und Wasser sowie eine gesicherte Abwasserentsorgung

angewiesen. Der Bund dürfe die Betreiber bei der akuten Drohnenbedrohung nicht allein lassen. Drohnenabwehr müsse hoheitliche Aufgabe bleiben.

Sylvia Borcherding, 50Hertz Transmission, wies darauf hin, dass der aktuelle Rechtsrahmen die Betreiber kritischer Infrastruktur in zahlreichen Verfahren zur umfassenden Offenlegung von Planungs- und Infrastrukturunterlagen verpflichte. Häufig müssten detaillierte Karten, technische Parameter, Standortinformationen, Leitungs- und Trassenverläufe sowie Infrastrukturen öffentlich zugänglich gemacht werden. Hier bestehe ein dringender gesetzgeberischer Handlungsbedarf, der durch das Kritis-Gesetzgebungsvorhaben nicht angegangen werde. Die bestehenden Transparenzpflichten seien im Lichte der aktuellen Bedrohungslage neu zu bewerten und anzupassen. Sie wünsche sich klare Regelungen für Finanzierung und Kosten, so Borcherding. Sie forderte einen bundesweit einheitlichen Rahmen zur Anerkennung und Refinanzierung von Resilienzkosten.

Ein Kraftakt für KMU

Professor Clemens Gause, Verband für Sicherheitstechnik, legte dar, für große Konzerne sei die Umsetzung des Kritis-Dachgesetzes ein Kraftakt, für viele kleine und mittlere Unternehmen indes nicht umsetzbar, weil es an finanziellen Mitteln mangele. Diese Unternehmen bildeten aber das Rückgrat der deutschen Wirtschaft und seien zunehmend ein Schlüssel zur Inneren Sicherheit, auch im Operationsplan Deutschland der Bundeswehr. Sein Verband fordere Bundesregierung und Abgeordnete auf, klare Maßnahmen zur Unterstützung der Industrie und des Mittelstands zu ergreifen. Dazu zählte er neben zinsgünstigen KfW-Krediten gezielte Steuerentlastungen sowie direkte Förderprogramme. Er regte an, die Sicherheitswirtschaft als Wirtschaftsfaktor in Deutschland nach vorne zu bringen.

Jürgen Harrer, Universität der Bundeswehr München, erklärte, der Gesetzentwurf sei mit den gesetzten Schwerpunkten grundsätzlich auf dem richtigen Weg. Neben den bereits vorhandenen Mindeststandards im Bereich der digitalen Sicherheit würden nun endlich auch Mindeststandards für den Bereich der physischen Sicherheit kritischer Infrastrukturen formuliert. Der Gesetzentwurf könne dazu beitragen, die Resilienz der Kritis-Betriebe und damit auch die Resilienz der Wertschöpfungs- und Lieferketten der deutschen Wirtschaft zu stärken. Harrer warf einen Blick auf die Kosten. Kleine und mittlere Betriebe dürften nicht überlastet werden. Unterstützungen etwa durch Sonderkredite oder Sonderabschreibungen hielt er für sinnvoll.

Wichtig, aber noch unvollständig

Professor Dennis-Kenji Kipker, Universität Bremen, Cyberintelligence Institute, Frankfurt am Main, nannte den Entwurf des Kritis-Dachgesetzes einen wichtigen, aber bislang unvollständigen Schritt hin zu einem kohärenten Schutz kritischer Infrastruktur (siehe dazu auch unser GIT SICHERHEIT-Interview mit Prof. Kipker auf Seite 10). So sei eine einheitliche und integrierte Kritis- und IT-Sicherheitsarchitektur vonnöten. Das nationale IT-Sicherheitsrecht sei bislang fragmentiert und vielfach nicht hinreichend aufeinander abgestimmt. Die Einbeziehung der öffentlichen Verwaltung in den Schutzbereich müsse konsequent fortgeführt werden. Die bisherige Ausklammerung weiter Teile der Bundesverwaltung sowie der Landes- und Kommunalverwaltungen führe zu systematischen Schutzlücken und einem uneinheitlichen Resilienzniveau. Er machte sich stark für ein Kritis-Dachgesetz, das digitale und physische Sicherheit bündele. Dadurch sollten Doppelstrukturen vermieden werden.

Unklare Rollenverteilung

Kerstin Petretto, BDI Bundesverband der Deutschen Industrie, monierte, dass es keine Abgrenzung der Zuständigkeiten zwischen den beteiligten Aufsichtsbehörden gebe. Insbesondere die Rolle der Bundesländer bleibe unklar. Da sie auch abseits des Kritis-Dachgesetzes über Regelungskompetenzen verfügten, drohten Schnittstellenprobleme und Doppelstrukturen. Sie kritisierte, dass ein erheblicher Teil der Bundesverwaltung vom Gesetz ausgenommen und Landesverwaltungen erst gar nicht adressiert worden seien. Infrastrukturen im Kritis-Sektor Staat und Verwaltung unterlägen damit keinen Anforderungen. Sie seien jedoch wie Unternehmen physischen Risiken ausgesetzt. Petretto beanstandete, dass die neuen Bedrohungen nicht adressiert würden. Im Zusammenhang mit Drohnenüberflügen sprach sie von einer Rechtslücke.

Ohne Staat und Verwaltung

Christian Stuffrein, Deutscher Landkreistag, der auch für den Deutschen Städtetag sprach, begrüßte, dass verbindliche nationale Regeln für Betreiber kritischer Infrastrukturen geschaffen werden sollen. Problematisch sei, dass im Gesetzentwurf der Bundesregierung der Bereich Staat und Verwaltung im Geltungsbereich fehle. Er müsse in die Auflistung der Kritis-Sektoren aufgenommen werden. Die Städte und Landkreise forderten eine angemessene kommunale Finanzausstattung und laufende Finanzierung zur Stärkung der Resilienz. Eine Finanzierung durch Anhebung der Kommunalabgaben sei nicht sachgerecht. Der Schwellenwert von 500.000 versorgten Einwohnern sei viel zu hoch. Damit würde das Gesetz keine Anwendung für Einrichtungen in der deutlichen Mehrheit der Kommunen enthalten. Denkbar sei der vom Bundesrat eingebrachte Schwellenwert von 150.000 versorgten Einwohnern.

Nach Einschätzung von Manuel Atug, Gründer und Sprecher der AG KRITIS, bleibt Deutschland auch mit dem aktuellen Entwurf zum Kritis-Dachgesetz „peinlich“ hinter dem Ziel zurück, das sich aus den EU-Vorgaben zu defensiver physischer Resilienz und Cyberresilienz ergebe. Die Verantwortlichen für die Sicherheit in Deutschland scheinen nach seiner Ansicht mit Vorsatz keine Handlungen aus den hybriden Gefährdungen der letzten Monate ableiten zu wollen. Dem Bundesinnenministerium warf er vorsätzliche Arbeitsverweigerung und damit vorsätzliche Gefährdung von Menschenleben vor. GIT

Deutscher Bundestag
www.bundestag.de


© Cyberintelligence institute

KRITIS

Zwischen Krieg und Frieden

Hybride Angriffe und die Folgen für Kritische Infrastrukturen

Drohnenüberflüge über Flughäfen und Bundeswehrstandorte, digitale Spionage, verdeckte Einflussoperationen und „Wegwerf-Agenten“: Militärische Konflikte werden durch subtile, vielschichtige Bedrohungen ersetzt. Deutschland sieht sich seit Beginn des russischen Angriffskrieges gegen die Ukraine mit einer wachsenden Zahl solcher Vorfälle konfrontiert. Unternehmen und Betreiber Kritischer Infrastrukturen stehen vor der Herausforderung, ihre Sicherheitsarchitekturen grundlegend zu transformieren. GIT SICHERHEIT sprach mit Prof. Dennis-Kenji Kipker, Gründer und Research Director des Cyberintelligence institute.

GIT SICHERHEIT: Herr Prof. Kipker, in letzter Zeit ist öfters von einem Verschwimmen der Grenzen zwischen Frieden und Krieg die Rede. Was halten Sie davon?

Dennis-Kenji Kipker: Es beschreibt die zunehmende Auflösung traditioneller Unterscheidungen zwischen klar definierten militärischen Konflikten und Phasen formeller Friedenszeiten. Gemeint ist, dass Staaten und nichtstaatliche Akteure Maßnahmen einsetzen, die zwar konfliktorientiert sind, jedoch bewusst unterhalb der Schwelle eines offenen militärischen Angriffs bleiben. Dies umfasst verdeckte, asymmetrische, digitale und psychologisch wirkende Methoden, die flexibel kombiniert werden. Diese Vorgehensweise schafft eine Grauzone, in der sich zivile und militärische Sphären überlagern und die Betroffenen einem permanenten Zustand latenter Bedrohung ausgesetzt sind.

Es gab in jüngster Zeit einige besorgniserregende Fälle von Drohneneinsätzen – etwa an den Flughäfen Kopenhagen und München. Geben Sie uns einmal ein Lagebild?

Dennis-Kenji Kipker: In Deutschland ist seit Beginn des russischen Angriffskrieges gegen die Ukraine ein deutlicher Anstieg unerlaubter Drohnenüberflüge zu beobachten. Die dokumentierten Zahlen übersteigen bereits mehrere hundert Vorfälle, wobei allein über Bundeswehrstandorten im Jahr 2023 mehr als 440 Überflüge registriert wurden. Die Spannbreite reicht von großformatigen, hochleistungsfähigen Militärdrohnen, die mutmaßlich aus größeren Entfernungen – etwa von Schiffen in Nord- und Ostsee – gesteuert werden, bis hin zu handelsüblichen Quadrocoptern, die im Nahbereich durch Einzelpersonen betrieben werden.

Was genau sind hybride Angriffe?

Dennis-Kenji Kipker: Hybride Angriffe bezeichnen die strategische Verknüpfung unterschiedlicher physischer, digitaler, geheimdienstlicher und psychologischer Mittel, die darauf abzielen, Staaten, Gesellschaften oder Unternehmen zu destabilisieren, ohne eine offene militärische Eskalation herbeizuführen. Diese Angriffe umfassen Sabotageakte, Cyberoperationen, klassische Spionage sowie Informations- und Einflussoperationen. Die Kombination verschiedener Angriffsvektoren erschwert die Identifikation des Urhebers und erschwert angemessene politische oder völkerrechtliche Reaktionen. Stellvertretergruppen, Tarnidentitäten oder nichtstaatliche Organisationen dienen häufig zur Verschleierung. Durch diese Vielschichtigkeit wirken hybride Angriffe zugleich auf operative, strukturelle und psychologische Ebenen und schaffen ein Umfeld anhaltender Unsicherheit.

Wie sind denn deutsche Unternehmen und Kritische Infrastrukturen auf all das vorbereitet?

Dennis-Kenji Kipker: Die Vorbereitung deutscher Unternehmen und Betreiber Kritischer Infrastrukturen unterliegt derzeit erheblichen Transformationsprozessen. Mit dem geplanten KRITIS-Dachgesetz und den europäischen Vorgaben der NIS-2-Richtlinie wird ein umfassender Rahmen geschaffen, der Sicherheitsanforderungen vereinheitlichen und das Schutzniveau deutlich anheben soll. Zahlreiche Organisationen haben bereits mit der Implementierung erweiterter Risikomanagement-, Melde- und Sicherheitsanforderungen begonnen. Gleichwohl bestehen in vielen Bereichen noch Lücken, insbesondere im physischen Schutz, im Umgang mit menschlichen Angriffsvektoren und bei der Integration hybrider Bedrohungsszenarien in Sicherheitsarchitekturen. Der Reifegrad variiert stark nach Branche,

Ressourcenzugang und bereits etablierter Sicherheitskultur.

Dass man sich auf Cyberangriffe vorbereiten muss, ist inzwischen sicher weitgehend etabliert?

Dennis-Kenji Kipker: Der Handlungsbedarf im Bereich der Cybersicherheit ist im Unternehmenssektor weitgehend anerkannt. Dennoch bleibt die Bedrohungslage dynamisch und erfordert stetige Anpassung. Die NIS-2-Richtlinie verpflichtet betroffene Einrichtungen, umfassende technische, organisatorische und prozessuale Schutzmaßnahmen einzuführen und kontinuierlich weiterzuentwickeln. Dazu gehören unter anderem Risikomanagement sowie Meldepflichten. In vielen Branchen haben sich entsprechende Standards etabliert, wobei vor allem von NIS-2 betroffene Einrichtungen wie z.B. große Unternehmen und KRITIS-Betreiber bereits über relativ ausgeprägte Cyberabwehrstrukturen verfügen. Im Falle von KMUs, kommunalen Verwaltungen oder Bildungseinrichtungen hingegen besteht jedoch angesichts der Bedrohungen oftmals noch Nachholbedarf.

Wie ist das mit Drohnenangriffen?

Dennis-Kenji Kipker: Im Bereich der Drohnensicherheit bestehen im Vergleich zu Cyberangriffen deutlich größere Unsicherheiten. Ein einheitlicher regulatorischer Rahmen fehlt bislang, und das geplante KRITIS-Dachgesetz wird hierzu erst über eine ergänzende Rechtsverordnung konkrete Vorgaben schaffen. Die technische Erkennung und Abwehr von Drohnen ist komplex, rechtlich sensibel und häufig mit hohen Kosten verbunden. Viele Unternehmen und Kritische Infrastrukturen verfügen daher bislang nur über begrenzte Fähigkeiten, um Drohnenaktivitäten systematisch zu detektieren, zu klassifizieren oder wirksam zu unterbinden. Die Lücke zwischen Bedrohungslage und vorhandenen Schutzmaßnahmen ist in diesem Feld besonders ausgeprägt.

Was können Betreiber Kritischer Infrastrukturen erreichen, wenn sie alles richtig machen?

Dennis-Kenji Kipker: Eine ideale Sicherheitsaufstellung basiert auf einem integrierten, mehrschichtigen Ansatz, der sowohl technische als auch organisatorische und personelle Maßnahmen umfasst. Zu den zentralen Elementen gehören ein systematisches Verständnis der Bedrohungslage auf der Führungsebene, regelmäßige Sensibilisierungs- und Trainingsprogramme für Mitarbeitende sowie eine umfassende Risikoanalyse, die hybride Angriffsvektoren einschließt. Darauf aufbauend sollten ganzheitliche Sicherheitskonzepte etabliert werden, die robuste Frühwarnsysteme, klare Meldeketten, definierte Reaktionsmechanismen und wiederkehrende Übungen beinhalten. Unternehmen, die dies konsequent umsetzen, erreichen eine deutlich erhöhte Reaktionsfähigkeit im Krisenfall und reduzieren die Wirksamkeit psychologischer Effekte hybrider Angriffe. Zudem können sie Betriebsunterbrechungen minimieren, Angriffsflächen verringern und im besten Fall Schwachstellen identifizieren, bevor sie ausgenutzt werden.

Sie schlagen einen dreifachen Ansatz vor, mit denen wir in Deutschland auf Drohnenüberflüge reagieren sollen...

Dennis-Kenji Kipker: Ein tragfähiges Konzept für den Umgang mit Drohnenüberflügen in Deutschland muss aus drei miteinander verzahnten Säulen bestehen: einer aktiven, technisch robusten Abwehr, einer Stärkung der baulichen und organisatorischen Resilienz kritischer Anlagen und einer deutlichen Professionalisierung der Detektion, Analyse und Entscheidungslogik.

Die aktive Abwehr umfasst sowohl Hard-kill-Methoden wie Abschuss, Laser oder Mikrowellenwaffen als auch Soft-kill-Instrumente wie Jamming, Spoofing oder kinetisches Einfangen. Obwohl diese Technologien weltweit rasch voranschreiten und viele Systeme bereits im militärischen Bereich einsatzreif sind, bleibt ihr Einsatz im zivilen Umfeld in Deutschland rechtlich stark begrenzt und abhängig von staatlichen Stellen.

Die zweite Säule besteht aus Resilienzmaßnahmen, also der Frage, wie sich kritische Infrastruktur gegen Aufklärung, Sabotage und physische Schäden schützen lässt, selbst wenn Drohnen in ihren Luftraum eindringen. Bauliche Eingriffe wie Netze, verstärkte Dachkonstruktionen oder Abschirmungen können verhindern, dass Drohnen sensible Bereiche ausspähen oder beschädigen. Sichtschutz, Tarnung und Täuschung reduzieren den Informationsgewinn des Angreifers, während Nebel, Blendmaßnahmen oder kurzfristige Verhüllungstechniken als taktische Reaktion dienen können.

Die dritte Säule – Detektion, Informationslage und organisatorische Reaktionsfähigkeit – ist der kritische Engpass. Ohne frühzeitige Identifikation der Drohne, ihres Typs, ihrer Steuerungsart und ihres Verhaltens bleiben sowohl aktive als auch passive Abwehrmaßnahmen weitgehend wirkungslos. Moderne Systeme kombinieren Radar, Funkpeilung, optische und akustische Sensorik, doch sind diese teuer und benötigen geschultes Personal. Zugleich dauern Drohnenüberflüge oft nur wenige Minuten, was extrem kurze Reaktionsfristen mit sich bringt.

Insgesamt liegt Deutschland damit in einem Zwischenstadium. Die technischen Instrumente existieren weitgehend, doch ihr Einsatz ist rechtlich eingeschränkt und organisatorisch nicht durchgängig vorbereitet. Resilienzmaßnahmen sind grundsätzlich umsetzbar, werden aber in der Breite noch kaum genutzt. Und die wichtigste Voraussetzung – eine integrierte Detektions- und Entscheidungsfähigkeit – ist bislang nur ansatzweise realisiert. GIT

Das vollständige Gespräch mit Prof. Dennis-Kenji Kipker finden Sie auf www.git-sicherheit.de

Cyberintelligence.institute
www.cyberintelligence.institute

KRITIS

„Safety first" für Energieversorger

Sicherheitskonzepte für Kritische Infrastrukturen

Andreas Sauerwald, Key Account-Manger für Energieversorgungsunternehmen bei Bosch Building Technologies

Der Ausbau erneuerbarer Energien verpflichtet Versorger, den Schutz ihrer Infrastrukturen neu zu denken. In einem Gespräch mit GIT SICHERHEIT erkärt Andreas Sauerwald, Key Account-Manager für Energieversorgungsunternehmen bei Bosch Building Technologies, worauf es dabei ankommt.

Herr Sauerwald, Deutschland arbeitet an der Energiewende. Was bedeutet das für die Energieversorger?

Andreas Sauerwald: Der Wandel bringt enorme Chancen, aber eben auch ein ganzes Bündel neuer Herausforderungen mit sich. Es gibt immer mehr dezentrale Anlagen – Solarfelder, Windparks, Batteriespeicher – die alle ans Netz angebunden sind. Das heißt: Erzeugung und Verbrauch schwanken viel stärker als früher. Das erhöht den Druck auf die Netzstabilität. Die Versorger müssen sich damit beschäftigen, wie man die Grundlast absichert, wie man den Energieüberschuss speichert und all das muss intelligent gesteuert sein. Diese Dezentralität bedeutet zudem: Es gibt unzählige neue Schnittstellen und Anlagen, die potenziell angreifbar sind, ob digital oder physisch. Energieversorger müssen also nicht nur ihre klassischen Kraftwerke besser schützen, sondern auch ihre Umspannwerke auf der grünen Wiese oder Trafostationen am Ortsrand. Die Komplexität steigt enorm an.

Tatsächlich ist immer wieder von Cyberangriffen oder Sabotageakten auf Energieanlagen zu lesen, das Risiko für solche Attacken steigt. Wie können sich die Versorger dagegen wappnen?

Andreas Sauerwald: Zunächst einmal braucht es ein Sicherheitskonzept, das wirklich ganzheitlich gedacht ist. Das darf sich nicht nur auf IT-Themen konzentrieren, sondern muss auch den physischen Schutz der Anlagen einbeziehen – Stichwort Perimeterschutz. Früher galt der Brand eines Kraftwerks als größte Gefahr, heute gehören auch der Diebstahl von Kupferkabeln und gezielte Sabotageakte zu den Risiken. Ein wirksamer Schutz fängt deshalb bei stabilen Zäunen, intelligenten Zutrittskontrollen sowie einer zuverlässigen Videosicherheitslösung an und hört bei Cyberabwehr und Notfallplänen noch lange nicht auf.

Nun haben viele Energieversorger aber intern nur begrenzte Ressourcen für diese Themen. Oder es geht erfahrenes Personal in Rente, sodass die erforderliche Expertise im Haus fehlt. Was raten Sie?

Andreas Sauerwald: Ja, das erleben wir immer wieder. Gerade kleinere und mittlere Unternehmen stoßen dann bei komplexen Sicherheitsfragen schnell an ihre Grenzen. Mein Rat ist: Holen Sie sich einen erfahrenen Partner ins Boot, der das Thema Sicherheit von A bis Z ganzheitlich begleiten kann – Bosch Building Technologies ist spezialisiert auf integrierte und vernetzte Sicherheitslösungen für Gebäude und Infrastrukturen. Wir decken von der Risikoanalyse über die Planung bis hin zur Umsetzung und regelmäßigen Wartung alles ab. Das entlastet das eigene Team und spart unterm Strich Zeit, Nerven und oft auch Kosten, weil man teure Fehler vermeidet.

Sie haben einen ganzheitlichen Ansatz angesprochen. Wie darf man sich das vorstellen und welche Rolle spielt Bosch Building Technologies dabei?

Andreas Sauerwald: Wenn wir Lösungen entwickeln, sprechen wir oft von `Co-Creation´: Gemeinsam mit dem Kunden schauen wir uns genau an, wo die größten Risiken liegen und welche Anforderungen der jeweilige Standort mitbringt. Darauf aufbauend entwickeln wir ein individuelles Konzept, das nicht nur modernste Technik integriert, sondern auch Prozesse und Notfallpläne mitdenkt. Idealerweise werden alle sicherheitsrelevanten Ebenen dann nahtlos miteinander verknüpft, beispielsweise Zutrittskontrolle, Videosicherheit, Perimeterschutz, Brandschutztechnik und Cyber Security. Alternativ dazu können auch gezielte Einzelmaßnahmen sinnvoll sein, die sich in vorhandene Konzepte integrieren lassen. Beispielsweise eine lückenlose 24/7-Videosicherheitslösung für das gesamte Firmenareal, Sensorik, um austretenden Wasserstoff zu detektieren, oder eine Lösung zur Drohnendetektion zum Schutz gegen Spionage. Das hängt vom konkreten Fall ab.

Planung ist das eine – Installation, Inbetriebnahme und Service das andere. Hier stellt sich ja oft die Frage, wie sich das effizient organisieren lässt.

Andreas Sauerwald: Absolut. Deshalb kümmern wir uns als Komplettanbieter auch um die gesamte Umsetzung, wenn dies gewünscht ist. Wir sind der Partner der Energieversorger in sämtlichen Sicherheitsbelangen! Das heißt konkret: Bosch Building Technologies liefert die passenden Produkte und Lösungen aus einer Hand, abgestimmt auf die jeweilige Infrastruktur. Und wir decken Installation, Service und Wartung gleich mit ab. Wir haben ein deutschlandweites Servicenetz, damit unsere Techniker regelmäßig vor Ort sein können. Zusätzlich lassen sich praktische Remote-Lösungen installieren, das erspart oft Serviceeinsätze vor Ort. All das stellt sicher, dass die Anlagen dauerhaft zuverlässig arbeiten, ohne dass der Betreiber mit vielen verschiedenen Dienstleistern jonglieren muss. Nicht zu vergessen: Unsere Expertinnen und Experten begleiten Energieversorger und deren Anlagen seit Jahrzehnten, erfüllen die Anforderungen an sicherheitsüberprüftes Personal und können so optimal in jeder Phase der Energiewende unterstützen. GIT

Bosch Sicherheitssysteme GmbH
Info.Service@bosch.com

VDI informiert über zukunftsfähige Sicherheitskultur

Die oft widersprüchlichen Anforderungen an Safety- und Security-Funktionen waren Anlass, im Fachbereich Sicherheit und Zuverlässigkeit des VDI den Fachausschuss Safety & Security einzurichten. Das Expertengremium aus Industrie, Forschung und sicherheitsrelevanten Organisationen waren sich schnell einig: Safety und Security sind zwei Perspektiven auf ein gemeinsames Ziel – den Schutz von Menschen, Technik und Gesellschaft. Als zentrales Ergebnis seiner Arbeit präsentiert der Fachausschuss das neue VDI-Wiki Safety & Security unter www.vdi.de/safety-security.

Mit der fortschreitenden Digitalisierung, der zunehmenden Vernetzung und der steigenden Bedrohungslage wächst die Notwendigkeit, beide Disziplinen gemeinsam zu betrachten. Um die bestehenden Herausforderungen und Lösungsansätze sichtbar zu machen, hat der Fachausschuss eine interaktive Wiki-Plattform aufgebaut. Sie dokumentiert den Stand des Wissens zu Safety und Security in verschiedenen technischen Disziplinen – von Automotive über Industrieanlagen und Luftfahrt bis hin zu Kritischen Infrastrukturen – und macht ihn erstmals systematisch zugänglich. **www.vdi.de**


© Monty Rakusen via GettyImages

Daniel Fai, Vorstand VSW Mainz

Auf dem Weg zur „Cross Company Resilience“

Sicherheit in Zeiten geopolitischer Spannungen und hybrider Bedrohungen

Daniel Fai, Vorstand des VSW-Mainz und Leiter Informationssicherheit bei Procter & Gamble, unterstützt mit seiner Expertise im Bereich Cybersecurity u.a. das VSW-Forum „Cybercrime & Wirtschaftskriminalität“, das Führungskräften und Sicherheitsverantwortlichen aktuelle Entwicklungen und praxisnahe Lösungsansätze bietet. Angesichts geopolitischer Spannungen, hybrider Bedrohungen und wachsender Cyberrisiken fordert Daniel Fai mehr Resilienz und Anpassungsfähigkeit von Unternehmen. Sein eigener Ansatz der „Cross Company Resilience“ betont die gemeinsame Verantwortung entlang der Lieferkette, um Sicherheit als entscheidenden Erfolgsfaktor zu verankern.

Herr Fai, Sie sind Vorstand im VSW-Mainz und Leiter Informationssicherheit bei Procter & Gamble. Das Thema Cybersecurity ist damit auch Ihr zentrales Feld im Rahmen Ihrer Verbandstätigkeit?

Daniel Fai: Ja, hier bringe ich zusätzliche Cybersecurity-Expertise aus Sicht der Wirtschaft in die Verbandsarbeit. Neben der Hauptfunktion eines Vorstandsmitgliedes unterstütze und betreue ich gemeinsam mit dem VSW, und einem weiteren Vorstandsmitglied, das VSW-Forum Cybercrime & Wirtschaftskriminalität. In Foren werden spezifische Themen der Sicherheitsbranche behandelt, von Cybersicherheit bis Risiko-Management. Experten und auch Vertreter der Behörden präsentieren aktuelle Entwicklungen und Best Practices. Wir richten uns an Führungskräfte, Sicherheitsverantwortliche und Fachleute aus verschiedenen Sektoren. Teilnehmende können sich mit anderen Fachleuten vernetzen und von den neuesten Trends und Lösungen profitieren.

Procter & Gamble gehört ja zu den Urgesteinen unter der Mitgliedschaft im VSW. Worin sehen Sie die wichtigsten Beiträge, den der VSW den Mitgliedsunternehmen bietet?

Daniel Fai: Eine Mitgliedschaft im VSW bietet einen vielfältigen Mehrwert. Neben immateriellen Vorteilen durch das Kompetenznetzwerk des VSW – der VSW ist die Schnittstelle zwischen Wirtschaft und Behörden – gibt es eine Vielzahl von direkt messbaren, auch finanziellen Vorteilen. Der VSW setzt insbesondere auf den steten Ausbau des VSW-Netzwerkes und Informationsaustausch, sowie Kompetenzbündelung zwischen den Sicherheitsbehörden, Wirtschaftsorganisationen wie den IHKs, Sicherheitsverbänden, Forschungsinstituten, Universitäten etc., sowie unter den Mitgliedern. Es gibt eine große Zahl an Kooperationen und Partnerschaften. Darüber hinaus werden noch Schulungen zu den unterschiedlichsten Sicherheitsthemen angeboten.

Zu den wichtigsten Veranstaltungen im Jahr gehört ja der VSW-Sicherheitstag. Im Jahr 2026 wird er im September stattfinden?

Daniel Fai: Ja, der nächste VSW-Sicherheitstag am 30.09.2026 steht unter dem Motto „Gemeinsam die Sicherheit in der Wirtschaft stärken“. Unser jährlicher Sicherheitstag ist eine hervorragende Plattform, um sich umfassend über Unternehmenssicherheit auszutauschen und wertvolle Netzwerke zu knüpfen. Dabei kommen Experten und Fachkräfte aus unterschiedlichen Bereichen – vom staatlichen Sicherheitssektor bis hin zur privaten Wirtschaft – zusammen, um aktuelle Sicherheits- und Gefährdungslagen zu diskutieren. Die Planungen, Referenten und Themen für 2026 haben erst begonnen.

In der Regel haben wir Vorträge von hochrangigen Sicherheitsverantwortlichen, von den Innenministern unserer drei Bundesländer (Hessen, Rheinland-Pfalz, Saarland) und von Sicherheitsexperten, die Einblicke in die aktuellen Gefährdungslagen geben und über präventive Sicherheitsmaßnahmen sprechen. Themen wie Cybersicherheit, Schutz vor Wirtschaftsspionage und Terrorabwehr spielen ebenfalls eine große Rolle. Auch spezifische Themen wie Zugangskontrollen, IT-Sicherheitsstrategien, Risikomanagement oder Krisenkommunikation bieten praxisnahe Lösungsansätze.

Die jüngsten weltpolitischen Ereignisse lassen die Sicherheit von Unternehmen jeder Größe in einem neuen, durchaus dramatischeren Licht erscheinen. Wie schätzen Sie das ein?

Daniel Fai: Geopolitische Spannungen, Handelskonflikte, Cyberangriffe, Liefer-

kettenrisiken und die Auswirkungen von Klimawandel und Pandemien, haben die Sicherheitslage für Unternehmen erheblich verschärft. Hybride-Bedrohungen sind ebenso Teil unserer Realität. Alle diese Bedrohungen nehmen in der Quantität, aber auch in der Qualität immer weiter zu.

Unternehmen sehen sich entsprechend zunehmend mit immer komplexeren Herausforderungen konfrontiert, die sowohl physische als auch digitale Sicherheitsaspekte betreffen.

Dazu kommen noch regulatorische Anforderungen die zwar die angesprochenen Risiken mitigieren und für mehr Resilienz sorgen sollen, was im Einzelfall sogar das Überleben eines Unternehmens sichern oder auch eine ganze Lieferkette schützen kann – Stichwort: Cyberangriff –, auf der anderen Seite aber auch Unternehmen teils überfordert, weil Ressourcen nicht zur Verfügung stehen, oder schlichtweg keine Expertise im Unternehmen vorhanden ist. Das gilt gerade im KMU-Bereich. Es ist eine schwierige Balance zwischen Wirtschaftlichkeit und Grad an Sicherheit.

Was sind die größten Herausforderungen?

Daniel Fai: Ich denke die größten Herausforderungen heutzutage sind, dass Unternehmen einen hohen Grad an Flexibilität, Anpassungsfähigkeit und Resilienz bezüglich aktueller Bedrohungsszenarien mitbringen müssen. Unternehmen sollten sich mit ihrem eigenen Sicherheits-Reifegrad beschäftigen, selbstreflektierend sein. Sie sollten wissen, wo sie derzeit stehen und was der eigene Reifegrad auch bezüglich Resilienz bedeutet. So kann auch eine gute Balance wie oben angesprochen ermittelt werden. Das können auch kleinere Unternehmen umsetzen. Resilienz, bzw. daraus resultierend u.a. auch Sicherheit, sollte nicht mehr als reiner Kostenfaktor betrachtet werden, sondern ist in unserer heutigen Welt ein ultimativer Faktor um den Geschäftserfolg zu sichern. Womöglich sogar ein Überlebensfaktor. Es ist ein Investment. Geschäftsleitungen sollten dies auch so organisatorisch reflektieren. Im Fall von Cyberrisiko ist Cyberrisiko Geschäftsrisiko Nummer 1.

Dies bedingt ein effektives Risikomanagement inklusive realistischer und erprobter Geschäftskontinuitätspläne, ein proaktives und integriertes, im Optimalfall ein adaptives Sicherheitsmanagement um potenzielle Bedrohungen frühzeitig zu erkennen und entsprechende Maßnahmen zu ergreifen. Wie viele Übungen und Prozesse werden nur am Tisch erprobt. Funktionieren die Prozesse wenn man diese praxisnah testet? Resilient bedeutet auch, gegenüber Angriffen gewappnet zu sein, so dass auch ein erfolgreicher Angriff massiv abgemildert werden kann. Dies umfasst sowohl physische als auch digitale Risiken.

Auch wenn dies häufig in Foren und Diskussionen gefordert wird: die Umsetzung richtet sich nicht immer nur nach dem Sicherheitsbudget. Vieles kann auch relativ kosteneffizient umgesetzt werden. Am Ende muss die Umsetzung, individuell auf ein Unternehmen, auf das Geschäftsmodell und die Unternehmensstrategie abgestimmt werden.

Sie sprechen selbst von Cross Company Resilience, also die Einbeziehung von Unternehmen die innerhalb der Lieferkette zusammenarbeiten – statt nur auf das eigene Unternehmen zu schauen. Könnten Sie das etwas näher erläutern?

Daniel Fai: Wie wir alle wissen, ist betriebliche Resilienz die Fähigkeit, betriebliche Störungen zu erkennen, zu vermeiden, abzuwehren, sich davon zu erholen, Schäden abzumildern und –wichtig – daraus zu lernen. Mein Ansatz geht aber darüber hinaus. In unserer heutigen vernetzten Welt mit teils komplexen Lieferketten und vielen Geschäftspartner die beteiligt sind, sei es digital oder physisch, reicht eine isolierte Betrachtungsweise nicht mehr aus.

Mein neuer Ansatz ist: „Cross Company Resilience“, eine gemeinsame, partnerschaftliche und kooperative Verzahnung, mit zumindest den wichtigsten Geschäftspartner in Bereichen mit hohem Schadenspotential, mit dem Ziel über die gesamte Lieferkette einen Resilienzbogen zu spannen. Abgestimmte, im Optimalfall gemeinsam erprobte Geschäftskontinuitäts- und Sicherheitsprozesse.

Ein Unternehmen mit einem hohen Grad an Resilienz mag resistent gegenüber Angriffen sein, wenn es aber abhängig von einer Lieferkette ist, sei es z.B. bei der Rohstoffbeschaffung bis zur Lieferung eines Produktes an einen Geschäftspartner – und einer der beiden Partner fällt aus, dann schadet dies womöglich allen Unternehmen in der Lieferkette. „Cross Company Resilience“ kann helfen, dass die Lieferkette dennoch lückenlos weiterbetrieben werden kann.

Lassen Sie uns noch einen Ausblick auf das neue Jahr vornehmen: Was werden die wichtigsten sicherheitsrelevanten Themen sein?

Daniel Fai: Ich sehe folgende wichtige Top-Themen für 2026: Regulatorisch werden uns die Themen NIS2, aber auch der EU Cyber Resilience Act (CRA) weiter beschäftigen. Hybride-Bedrohungen werden weiter zunehmen. KI im Sicherheitsbereich wird sowohl im defensiven als auch offensiven Bereich einen weiteren Schritt nach vorne machen. Gerade im offensiven Bereich, denke ich, wird der Fortschritt schneller vonstatten gehen. „Responsible AI“ und eine verbesserte Messbarkeit und Überwachung sehe ich als sehr wichtigen Aspekt.

Die sichere Anwendungsentwicklung im Bereich „Secure Software Development Lifecycle“, vom Threat Modelling über statischer Code Analyse bis zum Pentest muss weiter vorangetrieben werden. Gerade im SaaS-Bereich, auch um die Lieferkette noch weiter zu stärken. Es gab global zu viele Vorfälle bei denen SaaS-Software der „Single-Point of Failure“ ist. Ich erhoffe mir, dass das „Cross Company Resilience“-Konzept von vielen Unternehmen aufgegriffen wird: Für eine stärkere und resilientere Gemeinschaft und der Lieferkette.

Außerdem wichtig sind die Themen Quantumsicherheit, also u.a. quantensicherere Verschlüsselungstechnologien – Stichwort: Post-Quantum. Dann: Sicherheit im OT- und IoT- Bereich durch die auch hier stetig wachsende Vernetzung und Vergrößerung der Angriffsfläche. Schließlich die Themen Cloud und auch API-Sicherheit. GIT

Hier finden Sie weitere Informationen zu Veranstaltungen des VSW-Mainz:

Zum VSW-Sicherheitstag 2026

Die nächsten Termine des Forum Cybercrime & Wirtschaftskriminalität sind der 14. April 2026 und der 10. November 2026

Zum Lehrgang IT-Sicherheit & Wirtschaftsspionage (IHK)

VSW-Mainz
Verband für Sicherheit in der Wirtschaft
Hessen – Rheinland Pfalz – Saarland e.V.
www.vsw.de

Erik Liegle berät Unternehmen in den Bereichen Corporate Security, Risiko- und Krisenmanagement, Forensik, Compliance sowie Cyber- und Logistikschutz

Resilienz-dividende

Warum sich modernes Krisenmanagement doppelt auszahlt. Ein Beitrag von Erik Liegle

Investitionen in Resilienz zahlen sich nicht erst im Notfall aus. Sie stärken die Handlungsfähigkeit einer Organisation im Alltag, erhöhen ihre Anpassungsfähigkeit und schaffen einen messbaren Mehrwert – die Resilienzdividende. Wer seine Widerstandsfähigkeit systematisch entwickelt, legt damit einen entscheidenden Grundstein, um die heutige Verdichtung von Krisen und Störungen zu bewältigen. Erik Liegle, der Autor des nachfolgenden Beitrags, war in führenden Sicherheitsfunktionen bei Polizei, Europol sowie in internationalen Konzernen tätig. Heute berät er Unternehmen in den Bereichen Corporate Security, Risiko- und Krisenmanagement, Forensik, Compliance sowie Cyber- und Logistikschutz.

Unternehmen sehen sich längst nicht mehr einzelnen Vorfällen gegenüber, sondern einer Überlagerung geopolitischer Spannungen, Energie- und Lieferkettenrisiken, Cyberangriffe, Fachkräftemangel, Klimaextreme und eines enorm dynamischen Informationsraums. Diese Polykrise trifft auf hochgradig vernetzte Wertschöpfungsstrukturen: Ein Ausfall in einer Software-Schnittstelle oder bei einem kritischen Dienstleister kann heute ganze Produktionsverbünde binnen Minuten lahmlegen.

Von der Ereignislogik zur Fähigkeitslogik

Lange dominierte im Krisenmanagement die Logik einzelner Szenarien. Man plante für Brand, IT-Ausfall, Lieferantenschaden oder Reputationskrise und archivierte die Dokumente ordentlich – in der Hoffnung, das Richtige vorbereitet zu haben. Doch diese Logik greift zu kurz. Die entscheidende Frage lautet heute nicht: „Haben wir einen Plan für Ereignis X?“, sondern: „Verfügen wir über die Fähigkeiten, auch mit mehreren, unvorhersehbaren Ereignissen gleichzeitig umzugehen – unter Zeitdruck und mit unvollständigen Informationen?“

Resilienz wird damit zur Fähigkeitenfrage: der Fähigkeit, Lagebilder schnell zu entwickeln, funktionsübergreifend zu entscheiden und Prioritäten so zu setzen, dass das Unternehmen auch unter Stress handlungsfähig bleibt. Diese Fähigkeit entsteht nicht durch Papier, sondern durch geübte Zusammenarbeit, klare Rollen und eine Kultur, in der Risiken und Schwachstellen offen angesprochen werden.

Verwundbarkeiten einer vernetzten Welt

Moderne Verwundbarkeit entsteht an der Schnittstelle zwischen äußeren Risiken und inneren Strukturen. Globalisierung und Digitalisierung schaffen Effizienz – aber auch Abhängigkeiten, die oft unterschätzt werden. Wer seine kritischen Lieferanten, Dienstleister oder technischen Ressourcen nicht kennt, erlebt Störungen häufig als überraschend, obwohl sie systemisch erklärbar sind.

Zugleich haben viele Organisationen Puffer und Redundanzen zugunsten maximaler Effizienz abgebaut. Was im Normalbetrieb schlank wirkt, erweist sich in der Krise als spröde. Besonders deutlich wird das bei Schlüsselpersonen: In vielen Unternehmen gibt es Einzelne, die komplexe Systeme oder Verfahren als Einzige wirklich verstehen. Fällt diese Expertise aus, steht ein ganzer Prozess.

Eine oft unterschätzte Dimension ist die Kultur. Wo schlechte Nachrichten unerwünscht sind oder Warnhinweise ignoriert werden, verliert die Organisation ihre Sensorik. Technische Sicherheitsarchitekturen helfen wenig, wenn Mitarbeitende Auffälligkeiten nicht melden oder Fehler nicht offen ansprechen.

Was resiliente Organisationen auszeichnet

Resilienz zeigt sich nicht in der Anzahl der Pläne, sondern in der Art, wie eine Organisation mit Störungen umgeht – und was sie daraus macht. Resiliente Unternehmen nutzen Abweichungen und Beinahe-Schäden konsequent als Lernanlässe, entwickeln daraus konkrete Verbesserungen und vermeiden die Illusion eines „Resilienz-Theaters“, das auf Ordnern statt auf Fähigkeiten beruht.

Sie erkennen schwache Signale früh und verfügen über eine eingeübte Krisenorganisation, die im Ernstfall ohne Verzögerung in einen priorisierten Modus wechseln kann: Welche Produkte und Services haben Vorrang? Welche Ressourcen werden umgesteuert? Welche Maßnahmen können zurückgestellt werden?

Die Resilienzdividende

Im Mittelpunkt eines modernen Verständnisses von Resilienz steht die Resilienzdividende – der doppelte Mehrwert, der aus Investitionen in Sicherheit und Widerstandsfähigkeit entsteht.

Die erste Ebene ist der Schutz des Bestehenden: geringere Ausfallzeiten, weniger Vertragsstrafen, stabilere Lieferfähigkeit, geringere Reputationsrisiken. Durch Szenarioanalysen und Stresstests lässt sich quantifizieren, welche Schäden ohne Maßnahmen drohen und wie stark die Restexponierung nach Umsetzung geeigneter Maßnahmen sinkt.

Die zweite Ebene – und die strategisch bedeutsamere – ist die Schaffung neuer Möglichkeiten. Unternehmen, die in die Kompetenzen ihrer Mitarbeitenden investieren, erhöhen nicht nur die Ausfallsicherheit, sondern auch die Flexibilität im Alltag. Cross-Training, resilienzorientierte Qualifizierung oder klare Vertretungslogiken verbessern die Personaleinsatzplanung und erhöhen die Reaktionsfähigkeit bei Nachfrageschwankungen.

Resilient gestaltete Lieferketten sichern Lieferfähigkeit, wenn Wettbewerber bereits in der Krise stecken. Und die Transparenz, die im Rahmen von Resilienzanalyse entsteht, deckt häufig Ineffizienzen auf, die jenseits des Krisenkontexts behoben werden können.

Diese Effekte lassen sich konkret beobachten: in verkürzten Wiederanlaufzeiten, stabileren Kernprozessen unter Stress, verbesserten Auditergebnissen, günstigeren Versicherungsbedingungen und einem höheren Maß an Vertrauen seitens Kunden, Aufsichtsbehörden und Mitarbeitenden. Die Resilienzdividende ist messbar – und sie wirkt im Krisenfall ebenso wie im täglichen Geschäft.

Wachstum, Krise, Wandel

Der BVSW bietet in Kooperation mit Compleneo Consulting, einem renommierten Organisationsentwickler sowie Berater für Krisenmanagement und Resilienz („Wachstum, Krise, Wandel“) aus Potsdam zwei Seminare: Am 3. März vermittelt der Kurs „Krisenmanagement und Resilienzdividende“ kompakt die Grundlagen und rechtlichen Rahmenbedingungen für eine resiliente Organisation. Darüber hinaus zeigt das ergänzende fünftägige Präsenzseminar „Professionelles Krisenmanagement mit Organisationsentwicklungsfokus“, konkrete Werkzeuge und Strategien, damit Unternehmen dauerhaft widerstandsfähig bleiben.

Normen pragmatisch nutzen

Standards wie ISO 27001, ISO 22301, die neuen Normen zum Krisenmanagement oder regulatorische Anforderungen wie NIS2 und KRITIS schaffen wertvolle Orientierungsrahmen. Doch sie sind kein Selbstzweck. Entscheidend ist ein pragmatischer Umgang: Standards dienen als Landkarte, nicht als bürokratische Agenda. Zuerst sollten jene Maßnahmen umgesetzt werden, die die größten Verwundbarkeiten adressieren. Ein iteratives Vorgehen sichert Nutzen und verhindert Überforderung.

Der Mensch als Hauptverstärker der Resilienz

Bei aller Technik entscheidet in der Krise der Mensch. Führung, Kommunikation und Kultur sind die entscheidenden Verstärker: Sie bestimmen, ob ein Team im Stress zusammenhält oder zerfällt. Zwei Unternehmen mit ähnlicher technischer Ausstattung können sich im Ernstfall dramatisch unterscheiden – je nachdem, wie ihre Führungs- und Fehlerkultur ausgeprägt ist. Die Resilienzdividende ist daher immer auch eine Kulturdividende.

Eine einfache Routine mit großer Wirkung

Resilienz ist keine Maßnahme, sondern eine Führungsroutine. Eine der wirksamsten Methoden ist die monatliche „Waswäre-wenn“-Stunde: Die ersten Stunden eines realen Szenarios werden gemeinsam durchgespielt, ohne Inszenierung, aber mit Konsequenz. Solche Übungen schärfen das gemeinsame Lageverständnis, decken Lücken auf und verankern das Resilienzdenken dort, wo es am stärksten wirkt: in den Köpfen der Führungskräfte.

Wer Resilienz als Investition mit Dividende versteht, erkennt schnell: dieselben Maßnahmen, die im Krisenfall schützen, steigern im Alltag Leistungsfähigkeit, Attraktivität und Zukunftsfähigkeit einer Organisation. GIT

BVSW
www.bvsw.de

Dr. Martin Kaller ist Leiter der neu gegründeten Einheit Emergency Response & Site Security am BASF-Standort Ludwigshafen. Er ist verantwortlich für die Werkfeuerwehr sowie die operative Standortsicherheit am Hauptsitz des Unternehmens

Meilenstein für die Sicherheit

Das neue Gefahrenabwehrzentrum der BASF

BASF in Ludwigshafen hat vor kurzem dem Grundstein für ein neues Gefahrenabwehrzentrum (GAZ) gelegt. Hier werden künftig rund 130 Personen aus den Einheiten Werkfeuerwehr, Umweltüberwachung und Standortsicherheit sowie die integrierte Leitstelle aktiv sein. GIT SICHERHEIT sprach darüber mit Dr. Martin Kaller, der am dem 1. November 2025 die Leitung der neu gegründeten Einheit Emergency Response & Site Security am BASF-Standort Ludwigshafen übernommen hat. In seiner neuen Funktion verantwortet er die Werkfeuerwehr sowie die operative Standortsicherheit am Hauptsitz des Unternehmens.

GIT SICHERHEIT: Herr Dr. Kaller, das neue BASF-Gefahrenabwehrzentrum (GAZ) soll 2028 in Betrieb gehen. Wie wichtig ist die Entscheidung für ein solches Projekt für die Standort- und Unternehmenssicherheit bei BASF?

Dr. Martin Kaller: Die Entscheidung für das Gefahrenabwehrzentrum ist ein strategischer Meilenstein für die Sicherheit der BASF. Ludwigshafen ist komplexer Standort mit rund 200 Produktionsanlagen, 33.000 Mitarbeitenden und einer Lage im Herzen der Metropolregion Rhein-Neckar. Mit dem GAZ schaffen wir eine zentrale Plattform, die alle nicht-medizinischen Gefahrenabwehrkräfte unter einem Dach vereint. Wir investieren hier in die Zukunftsfähigkeit des Standorts und in die Sicherheit unserer Kolleginnen und Kollegen, Nachbarn und Partner.

Wie wird die Verzahnung von Werkfeuerwehr, Umweltzentrale und Standortsicherheit im neuen Zentrum konkret aussehen?

Dr. Martin Kaller: Die Zusammenarbeit zwischen Werkfeuerwehr, Umweltzentrale und Standortsicherheit läuft bereits erfolgreich und wird im neuen Gefahrenabwehrzentrum noch enger verzahnt. Im GAZ ziehen rund 130 Spezialistinnen und Spezialisten aus den drei Kernbereichen sowie die integrierte Leitstelle zusammen. Diese Leitstelle bildet das Herzstück des Zentrums: Sie bündelt alle relevanten Informationen und koordiniert Einsätze in Echtzeit.

Welche Szenarien für Großschadenslagen wurden bei der Planung berücksichtigt?

Dr. Martin Kaller: Von Ludwigshafen aus werden die Einsatzmaßnahmen bei allen Lagen und Großschadensfällen bei BASF konzernweit gesteuert bzw. unterstützt. Entsprechend werden die zentralen Funktionsräume im neuen GAZ abgebildet. Die integrierte Leitstelle sowie der Lenkungsausschuss Gefahrenabwehr, die Technische Einsatzleitung und weitere Gefahrenabwehrfunktionen erhalten neu ausgestattete Krisenstabsräume und Labore.

Können Sie Beispiele dafür geben, mit welchen Technologien und Systemen das GAZ ausgestattet werden soll, um den steigenden Anforderungen an Gefahrenabwehr und Prävention gerecht zu werden? Wird es beispielsweise KI-gestützte Systeme geben?

Dr. Martin Kaller: Das neue Gefahrenabwehrzentrum (GAZ) wird mit modernster Technik ausgestattet, um den wachsenden Anforderungen an Gefahrenabwehr und Prävention gerecht zu werden. Die Leitstelle entsteht nach den neuesten Erkenntnissen und technischen Standards und wird damit nicht nur den aktuellen Anforderungen entsprechen, sondern auch zukunftsweisende Technologien integrieren, um vernetztes Arbeiten und schnelle Reaktionsfähigkeit im Standard- und Krisenfall sicherzustellen.

Wichtig ist für uns auch der Einsatz von KI-gestützten Systemen. Bereits heute nutzt die Umweltzentrale künstliche Intelligenz, um Bilddaten von Überwachungskameras auszuwerten und Fackeltätigkeiten sowie Emissionen automatisch zu erkennen. Ebenso kommen Assistenzsysteme zum Einsatz, die helfen, Ursachen von Emissionen im Abwasserbereich schnell zu lokalisieren und zu beheben. Auch die Standortsicherheit nutzt KI-unterstützte Systeme zum Perimeterschutz. Darüber hinaus arbeiten wir kontinuierlich an weiteren KI-Anwendungen, die unsere Effizienz steigern und die Sicherheitsarbeit verbessern sollen.

Inwieweit profitieren die Stadt Ludwigshafen und die Anwohner von der neuen Infrastruktur – etwa durch schnellere Informationswege oder erweiterte Schutzmaßnahmen?

Dr. Martin Kaller: Unser Ziel ist klar: Die Sicherheit unserer Mitarbeitenden sowie der Menschen in Ludwigshafen und der Region hat höchste Priorität. Mit dem GAZ schaffen wir die Voraussetzungen für eine noch engere Verzahnung aller relevanten Funktionen, kürzere Informationswege und erweiterte Schutzmaßnahmen – für das Werk und für die Nachbarschaft.

Ein weiterer Vorteil des neuen Gefahrenabwehrzentrums liegt in der optimierten Infrastruktur für unsere Einsatzfahrzeuge. Größere Stellplätze und Ausfahrtstore ermöglichen ein noch sichereres Ausrücken. Zudem sorgt die Lage des Zentrums dafür, dass die Fahrzeuge im Einsatzfall nicht mehr über öffentliche Straßen fahren, sondern direkt vom Werksgelände starten können. Das reduziert nicht nur die Anmarschzeit, sondern auch potenzielle Risiken im öffentlichen Verkehrsraum. GIT

BASF SE
www.basf.com

© Bilder: BASF SE

So wird das neue Gefahrenabwehrzentrum der BASF aussehen – 2028 soll es in Betrieb gehen

Private Sicherheit – öffentliche Aufgabe?

Die Rolle der privaten Sicherheitswirtschaft für die innere Sicherheit Deutschlands

Siegfried Hüsgen, Co-Autor des Buches „Führung und Personalmanagement für die Sicherheitswirtschaft“, Boorberg 2024

Die Innere Sicherheit zu gewährleisten, ist Aufgabe des Staates. Dazu gehört der Schutz des Staates und der Gesellschaft vor Kriminalität, Extremismus, Terrorismus und den damit verbundenen Bedrohungen. Die Innenministerkonferenz (IMK) betrachtet die private Sicherheitswirtschaft schon seit einigen Jahren als festen Bestandteil der Sicherheitsarchitektur in Deutschland. Angesichts dieser Bewertung und der allgemeinen Sicherheitslage ist die Frage nach der zukünftigen Rolle der privaten Sicherheitswirtschaft zur Aufrechterhaltung der Inneren Sicherheit berechtigt. Der Buchautor, Unternehmens- und Sicherheitsberater Siegfried Hüsgen geht ihr in seinem Beitrag für GIT SICHERHEIT nach.

Seit August 2023 liegt ein Referentenentwurf zum Sicherheitsgewerbegesetz (SiGG) vor, bei dem es im Kern um die Formulierung und Definition von verbindlichen Qualitäts-anforderungen für Sicherheitsunternehmen und deren Beschäftige geht. Die ebenfalls im Jahr 2023 veröffentlichte Nationale Sicherheitsstrategie der damaligen Bundesregierung trägt den Titel: „Integrierte Sicherheit für Deutschland/Nationale Sicherheitsstrategie. Wehrhaft. Resilient. Nachhaltig.“ In dieser Sicherheitsstrategie, dem damaligen Koalitionsvertrag und auch dem aktuellen Koalitionsvertrag hat die private Sicherheitswirtschaft als Branche keine Relevanz und findet keine Erwähnung.

Bedeutung der privaten Sicherheitswirtschaft

Nach Angaben des BDSW hat die Branche in der Wirtschaftsklasse 80 zurzeit fast 294.000 Beschäftigte in fast 6.000 Unternehmen, die einen Umsatz im Jahr 2024 von 14,13 Mrd. Euro erwirtschaftet haben. Mit Stand vom 30.9.2024 sind die wesentlichen Einsatzgebiete der Werk- und Objektschutz (26%), der Empfangsdienst (12%), Schutz von Flüchtlingsunterkünften (10%), Luftsicherheit (9%), Einzelhandel (6%), Verwaltung (5%), Veranstaltungs- und Ordnungsdienst (5%), Geld- und Wertdienst (4%), Revier- und Streifendienst (4%), Notruf- und Serviceleitstellen (4%), Öffentlicher Personennahverkehr (3%), Militärische Einrichtungen (3%), Detekteien (3%), Sicherungsposten bei Gleisarbeiten (2%), mit jeweils 1 % folgende die Kerntechnischen Anlagen, die Citystreifen mit Personenschutz, der Arbeits-, Gesundheit- und Umweltschutz sowie die Werkfeuerwehren.

Auch die private Sicherheitswirtschaft unterliegt, wie alle anderen Wirtschaftsbereiche, einem Struktur- und Demografiewandel sowie fortschreitenden technischen Innovationen. Die Megatrends und Markttreiber der Sicherheitswirtschaft beinhalten sowohl Chancen als auch Risiken.

In den letzten Jahren hat es einen Paradigmenwechsel von der reinen Bewachung mittels überwiegend personeller Ressourcen (Mannstunden) hin zu einem zunehmenden Einsatz von Sicherheitstechnik und digitalen Systemen sowie der Kombination aus beiden Geschäfts-feldern, zur sogenannten „Solution“, gegeben.

Zu den Aufgaben und Einsatzgebieten der Branche gehören u. a. Sicherheitsdienstleistungen zum Schutz von Objekten und Unternehmen der kritischen Infrastrukturen (KRITIS), von Veranstaltungen und Events, im Öffentlichen Personenverkehr (ÖPV), in Aufnahme-einrichtungen und Gemeinschaftsunterkünften für Asylbewerber und Flüchtlinge.

Obgleich die private Sicherheitswirtschaft zahlreiche Dienstleistungen innerhalb kritischer Anlagen ausübt, wird sie selbst als Wirtschaftszweig bzw. Branche nicht als solche eingestuft.

Da die private Sicherheitswirtschaft aus Sicht der Innenministerkonferenz schon seit Jahren ein fester Bestandteil der Sicherheitsarchitektur der Inneren Sicherheit ist, strebt die Branche eine ganzheitliche Zugehörigkeit zur kritischen Infrastruktur an.

Zurzeit wird der sogenannte Operationsplan Deutschland (Oplan Deu) innerhalb der Sicherheitsbehörden und der Bundeswehr erarbeitet. Das darin formulierte Ziel, Deutschland gemeinsam zu verteidigen, wird als gesamtstaatliche und gesamtgesellschaftliche Aufgabe betrachtet. Der Wirtschaft wird ein entsprechend eigenverantwortliches Handeln nahegelegt, eine möglicherweise besondere Rolle der privaten Sicherheitswirtschaft ist wohl noch nicht bedacht.

Rechtliche Grundlagen und Einsatzmöglichkeiten

Sicherheit ist heute ein Querschnittsthema, was bereits durch die Begriffe Safety und Security deutlich wird. Die klassischen Tätigkeitsfelder der privaten Sicherheitsdienstleister sowie weitere Bereiche, wie Wirtschafts- und Umweltschutz, Unternehmens- und Arbeitssicherheit, Risiko- und Krisenmanagement, nicht zuletzt Business Continuity Management und Katastrophen-

schutz, zählen mittlerweile dazu, um nur einige zu nennen.

Entscheidend für alle einsatztaktischen und personalentwicklungsrelevanten Maßnahmen ist die unterschiedliche Rechtsgrundlage der öffentlichen und der privaten Sicherheit.

Wesentliches Unterscheidungsmerkmal ist die Wahrnehmung „hoheitlicher Aufgaben" durch behördliche und militärische Einsatzkräfte.

Gemäß § 17 der Bewachungsverordnung (BewachV) muss jede Dienstanweisung den Hinweis enthalten, dass „die Wachperson nicht die Eigenschaften und nicht die Befugnisse von Polizeivollzugsbeamten oder eines sonstigen Bediensteten einer Behörde besitzt." Angehörige privater Sicherheitsdienstleister können sich, wie jeder Bürger, also lediglich im Rahmen sog. „Jedermannsrechte" bewegen. Da diese Rechte jedoch nur dann in Anspruch genommen werden dürfen, wenn obrigkeitliche, also staatliche Hilfe nicht rechtzeitig zu erlangen ist, werden sie auch als „Ausnahmerechte" zum Gewaltmonopol des Staates bezeichnet.

Dies hat einen unmittelbaren Einfluss auf die Arbeitsweise, die Einsatzplanung sowie die taktische und strategische Struktur der privaten Sicherheitsdienstleistungen. Diese klare Abgrenzung schließt eine Zusammenarbeit zwischen Sicherheitsunternehmen und den Polizeien und Behörden ausdrücklich im Rahmen von Maßnahmen des „Public Private Partnership" (PPP) mit ein.

Private Public Partnership & Beleihung

Im Rahmen der Beleihung werden hoheitliche Befugnisse auf Private übertragen. Eine Beleihung darf nur durch Gesetz oder aufgrund eines Gesetzes erfolgen. Die „Beliehenen" sind entweder Einzelpersonen oder juristische Personen des Privatrechts, die mit der hoheitlichen Wahrnehmung bestimmter Verwaltungsaufgaben betraut sind. Beliehene treten infolge der konstitutiven Übertragung von Hoheitsrechten selbständig und im eigenen Namen handelnd auf.

Laut Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung bestehen „Public Private Partnerships" (Öffentlich-private Partnerschaften, ÖPP) in Kooperationen zwischen öffentlicher Hand und privater Wirtschaft beim Entwerfen, bei der Planung, Erstellung, Finanzierung, dem Management, dem Betreiben und dem Verwerten von zuvor allein in staatlicher Verantwortung erbrachten öffentlichen Leistungen.

In Abgrenzung zur herkömmlichen Beschaffung einzelner Sachmittel oder Dienstleistungen durch Private bzw. Privatisierungen zeichnet sich die ÖPP/PPP dadurch aus, dass die öffentliche Hand als Auftraggeber und die privaten Dienstleister als Auftragnehmer langfristig und vertraglich geregelt zum Zwecke der Erfüllung öffentlicher Aufgaben zusammenarbeiten.

Könnte sich hier mittel- oder langfristig ein neues Geschäftsfeld für die private Sicherheitswirtschaft herausbilden? Vielleicht in den Bereichen des Personen- oder Einsatz-Begleitschutzes als Unterstützung der Beschäftigten von Behörden und Organisationen mit Sicher-heitsaufgaben (BOS) bei deren Einsätzen?

Entwurf Sicherheitsgewerbegesetz

Seit dem 31.07.2023 liegt seitens des Bundesministeriums des Innern und für Heimat (BMI) ein Entwurf eines Gesetzes zur Regelung des Sicherheitsgewerbes (Sicherheitsgewerbegesetz / SiGG) vor. Obgleich ein solches Gesetz einst von einer Vielzahl der Unternehmen der privaten Sicherheitswirtschaft mit der Zielstellung der Marktkonsolidierung und Qualitätsoptimierung gefordert und diese Forderung mit Eckpunkte- bzw. Positionspapieren untermauert wurde, wird der vorliegende Entwurf nunmehr innerhalb der Branche kontrovers diskutiert.


© gesrey - stock.adobe.com

Als Ziel des Gesetzes ist formuliert: „Das Sicherheitsgewerbegesetz soll als neues Stamm-gesetz verbindliche Standards für das Sicherheitsgewerbe festlegen." Ferner heißt es:

§ 1 Anwendungsbereich

(1) Dieses Gesetz regelt das Betreiben eines Sicherheitsgewerbes und die Ausübung einer Tätigkeit als Sicherheitsmitarbeiter. Es dient dazu, die Auftraggeber sowie die Allgemeinheit vor der unsachgemäßen Erbringung von Bewachungstätigkeiten zu schützen.

(2) Auf die den Vorschriften dieses Gesetzes unterliegenden Gewerbebetriebe und Personen finden die Vorschriften der Gewerbeordnung Anwendung, soweit nicht in diesem Gesetz besondere Bestimmungen getroffen worden sind. § 1 des Sicherheitsüberprüfungsgesetzes bleibt unberührt.

Aufgabe der privaten Sicherheitswirtschaft

Die Beschaffung von geeignetem und zuverlässigen Personal ist Kernaufgabe des Personal-managements. Die Branche steht trotz positiver Entwicklung der Tariflöhne noch immer im Wettbewerb mit dem Niedriglohnsektor. Nachwuchskräfte haben zudem ein vielfältiges Angebot an Berufen in der öffentlichen Sicherheit.

Aus Mangel an geeigneten Fachkräften bedienen sich Unternehmen oftmals fachfremdem Personal. Die Defizite bei den Kompetenzen der Führungskräfte sind regelmäßig in den sozialen und den Fachmedien sowie bei den Personalentwicklern präsent und werden entsprechend thematisiert. Die Einstellung von branchenfremden Quereinsteigern ist betriebswirtschaftlich oftmals günstiger als die Qualifizierung von Bestandspersonal und nicht selten die scheinbar letzte Alternative, um offene Stellen zu besetzen.

Zu einem funktionalen und modernen Personalentwicklungskonzept gehören Anforderungs-profile, Stellenbeschreibungen, Vertretungsregeln und Nachfolgeplanungen. Schulungen für Führungskräfte sollten nicht nur angeboten, sondern verpflichtend durchgeführt werden.

Mittel- und langfristig müssen Konzepte entwickelt werden, wie sie bereits in anderen europäischen Ländern etabliert sind, bei denen das Image der privaten Sicherheitswirtschaft positiver und wertschätzender zu sein scheint. GIT

Siegfried Hüsgen
www.sh-consulting.org

Schlüsselfaktor für Wettbewerbsfähigkeit und Sicherheit

Lünendonk-Whitepaper: Einsatz von Robotik für technische Inspektionen

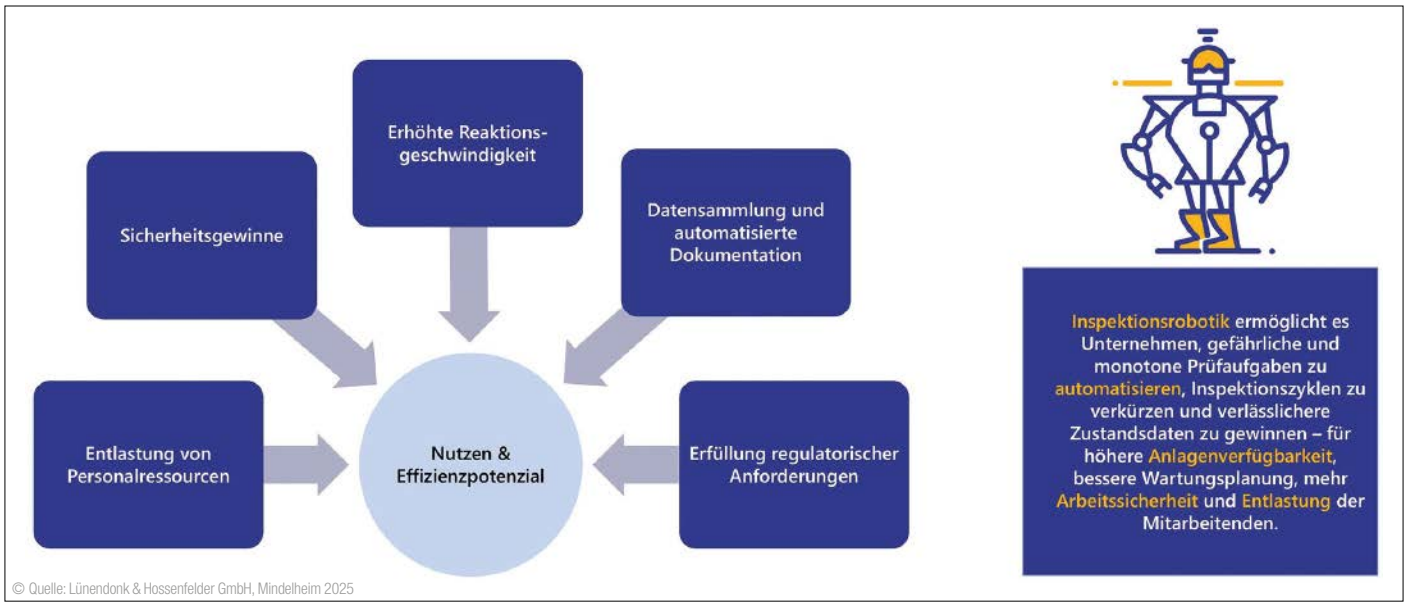
Das von Lünendonk zusammen mit CBRE GWS Schweiz erarbeitete Whitepaper „Robotik für die technische Anlageninspektion“ zeigt, wie Inspektionsroboter Unternehmen helfen, den Fachkräftemangel abzufedern und gleichzeitig steigende Sicherheitsanforderungen zu erfüllen. Sensorik, künstliche Intelligenz und Vernetzung ermöglichen präzise Zustandsüberwachung, sichere Prüfaufgaben und eine verlässliche Datenbasis. Demnach wird Robotik zum Effizienztreiber und zu einem Garanten für Arbeitssicherheit und regulatorische Konformität.

Industrieparks und Betreiber technischer Anlagen stehen vor der Herausforderung, Prozesse kontinuierlich zu überprüfen und gleichzeitig die Sicherheit von Mitarbeitenden zu gewährleisten. Der demografische Wandel verschärft die Situation: Millionen Beschäftigte der Babyboomer-Generation scheiden bis 2036 aus dem Erwerbsleben aus, während deutlich weniger junge Fachkräfte nachrücken. Parallel steigen regulatorische Anforderungen an Arbeitssicherheit und den Schutz sensibler Infrastrukturen.

Unternehmen müssen Wege finden, Effizienz, Sicherheit und Verfügbarkeit von Personal in Einklang zu bringen. Inspektionsroboter übernehmen Aufgaben, die für Menschen gefährlich, körperlich belastend oder monoton sind. Dazu zählen der Zugang zu schwer erreichbaren Anlagenteilen, die kontinuierliche Zustandsüberwachung oder die Dokumentation großer Datenmengen. Der Einsatz solcher Systeme entlastet Mitarbeiter, verbessert die Datenqualität und ermöglicht eine verlässliche Planung von Wartungsmaßnahmen.

Die International Federation of Robotics meldet für 2024 einen weltweiten Bestand von 4,7 Millionen Robotern – ein klares Zeichen für den Trend zur Automatisierung. Deutschland und die Schweiz zählen zu den führenden Ländern bei der Roboterdichte, dennoch besteht Handlungsbedarf, um das

Aus dem Whitepaper „Robotik für die technische Anlageninspektion“ – Automatisierte Anlageninspektion im Facility Management entlastet Industrieunternehmen und erhöht die Anlagenverfügbarkeit



Potenzial voll auszuschöpfen. Fortschritte in Sensorik, Bildgebung und KI eröffnen neue Einsatzfelder, insbesondere in sicherheitskritischen Umgebungen.

Mobile Roboter als Sicherheitsgaranten

Mobile Inspektionsroboter gelten als wirtschaftlich attraktive Alternative zu stationären Sensoren, da sie flexibel eingesetzt werden können und präzise Daten liefern. Der globale Markt für robotergestützte Inspektionen wächst stark: Von 3,5 Milliarden US-Dollar im Jahr 2024 soll er bis 2033 auf über 10 Milliarden US-Dollar steigen. Besonders die Öl- und Gasindustrie sowie die Wasserwirtschaft treiben diese Entwicklung voran. Sicherheit ist dabei ein zentrales Argument für Investitionen.

Das Whitepaper beschreibt drei zentrale Anwendungsbereiche: Erstens die sensorische Zustandsüberwachung, bei der Roboter Temperatur, Strahlung, Stoffe, Geräusche und Vibrationen erfassen. Zweitens physische Prüf- und Kontrollaufgaben, etwa die Vermessung mechanischer Strukturen oder die Kontrolle von Druckanzeigen. Drittens die digitale Erfassung und Systemintelligenz, die lernende Systeme ermöglicht und vorausschauende Instandhaltung unterstützt.

Sicherheit durch Sensorik und KI

Besonders in kerntechnischen Anlagen oder Chemieparks zeigt sich der Sicherheitsgewinn: Roboter erstellen Strahlenkarten, spüren Leckagen auf oder erkennen ungewöhnliche Geräusche, die auf Defekte hinweisen. Damit reduzieren sie Unfallrisiken und sichern die kontinuierliche Kontrolle kritischer Betriebsparameter. In Kombination mit KI entsteht eine neue Qualität der Inspektion, die nicht nur Daten sammelt, sondern auch interpretiert.

Das Whitepaper betont, dass Inspektionsrobotik nicht allein der Effizienzsteigerung dient. Vielmehr sind die Sicherheitsgewinne entscheidend: Roboter reduzieren Unfallrisiken, verbessern die Datenqualität und unterstützen die Einhaltung regulatorischer Vorgaben. Gleichzeitig entlasten sie das Personal und tragen zur Planbarkeit von Ressourcen bei.

Praxisbeispiel

Für den erfolgreichen Einsatz sind Systemdesign, Bedienbarkeit, Wartung und IT-Sicherheit zentrale Faktoren. Das Whitepaper liefert eine Checkliste für Unternehmen, die den Einstieg in die Robotik planen. Eine Fallstudie aus dem Getec-Park Muttenz zeigt, wie Inspektionsroboter bereits heute in der Praxis eingesetzt werden, um Sicherheit und Effizienz zu steigern.

Fazit: Robotik für die technische Anlageninspektion ist kein Zukunftsthema mehr, sondern bereits Realität. Angesichts des Fachkräftemangels und steigender Sicherheitsanforderungen entwickeln sich Inspektionsroboter zu einem unverzichtbaren Bestandteil moderner Instandhaltung. Sie erhöhen die Betriebssicherheit, reduzieren Risiken für Mitarbeitende und schaffen die Grundlage für nachhaltige, effiziente Prozesse. Damit wird Robotik zu einem Schlüsselfaktor für Wettbewerbsfähigkeit und Sicherheit in der Industrie. GIT

Das Lünendonk-Whitepaper „Robotik für die technische Anlageninspektion“ steht kostenfrei auf der Unternehmens-Website zur Verfügung.

Lünendonk & Hossenfelder GmbH
www.luenendonk.de

Salto feiert 25-jähriges Firmenjubiläum

Seit dem Jahr 2000 bietet Salto Lösungen an, wie Menschen Türen öffnen und Räume weltweit sichern. Aus einem kleinen Start-up in Spanien ist ein globaler Technologieführer geworden, der mit seinem intelligenten Zutrittsökosystem Türen öffnet.

Salto feiert 2025 sein 25-jähriges Bestehen. Gegründet im Jahr 2000 mit der Vision, universell einsetzbare, kabellose und vernetzte Zutrittslösungen zu schaffen, entwickelte sich das Unternehmen von einem kleinen Start-up im Norden Spaniens zu Salto Wecosystem – einer globalen Unternehmensgruppe, die die Branchenführer Gantner, Salto und Vintia vereint. Gemeinsam bieten sie moderne Lösungen für smarte Zutrittskontrolle, Ticketing, Identitätsmanagement und elektronische Schließtechnik.

Heute finden sich Salto Technologien in über 100.000 Installationen, an 10 Millionen Zutrittspunkten und ermöglichen mehr als 40 Millionen Menschen täglich einen sicheren Zutritt. Mit über 1.850 Mitarbeitern weltweit steht das Unternehmen für kontinuierliche Innovationskraft und nutzerzentriertes Design und ist so ein verlässlicher Partner für zahlreiche Branchen.

Die Erfindung des Salto Virtual Network (SVN) im Jahr 2002 war der erste entscheidende technologische Meilenstein, durch den eine sichere und hochfunktionale virtuelle Vernetzung von Zutrittspunkten möglich wurde. Bereits 2008 präsentierte das Unternehmen mit Salto Wireless eine Funkvernetzung für kabellose Echtzeit-Zutrittskontrolle. 2014 folgte mit Clay by Salto (heute Salto KS) der Schritt in die Cloud und nur ein Jahr später mit JustIN Mobile eine Technologie für Mobile Access. Die jüngsten Innovationen stellen die 2025 auf den Markt gekommenen Lösungen XS4 Face für hochsichere und

komfortable Gesichtserkennung mit mobiler Nutzererfassung und das umfassende ID-Managementsystem Salto IDM dar. Parallel wurden dem Hardwareportfolio laufend neue Produktserien und funktionale Upgrades hinzugefügt.

„Unser Jubiläum ist sowohl eine Feier unserer bemerkenswerten Reise als auch ein Bekenntnis zu einer ambitionierten Zukunft. Wir werden weiterhin mit modernsten Technologien intelligente Zutrittslösungen vorantreiben, um unseren Anwendern weltweit sichere und smarte Erlebnisse zu ermöglichen“, sagt Marc Gomez, CEO von Salto Wecosystem. **www.saltosystems.de**

Hör mal wer da fliegt!

Wie man Drohnen akustisch erkennt

Das Fraunhofer IDMT in Oldenburg hat eine intelligente Sensorlösung entwickelt, die Drohnen auch außerhalb der Sichtlinie erkennt. Die akustische Erkennertechnologie kann als Ergänzung mit Radar, Kamera und Lidar zu einem System kombiniert werden.

Wenn sich eine Drohne (auch „Unmanned Aerial System", kurz: UAS) unerlaubt einem sicherheitskritischen Bereich nähert, stellt sie eine Gefahr dar. Optische Sensoren, Funk und Radar sind in einigen Fällen durch Gelände, Wetter, oder technische Maßnahmen gestört und können eine Drohne nicht zuverlässig erfassen.

Das Fraunhofer-Institut für Digitale Medientechnologie IDMT in Oldenburg hat zur Drohnendetektion und -lokalisation eine integrierte akustische Sensorlösung entwickelt. Angesichts der zunehmenden Bedrohung durch unbemannte Luftfahrzeuge in sicherheitskritischen Bereichen füllt das System eine entscheidende Lücke: Es hört sozusagen um die Ecke. Die Akustik kann in Ergänzung zu Radar, Kamera und Lidar zu einem robusten Sensordatenverbund fusioniert werden. Anders als rein optische und radarbasierten Verfahren, die etwa auf die Sichtverbindung angewiesen sind, ermöglicht die Technologie, dass selbst in bebauten oder bewaldeten Gebieten Drohnenoperationen aufgespürt werden können.

Christian Rollwage, Gruppenleiter „Akustische Signalverbesserung", forscht mit seinem Team an den Algorithmen zur Drohnendetektion

Langjährige Forschungsarbeiten

Seit 2016 hat der Institutsteil Hör- Sprach- und Audiotechnologie in den öffentlich geförderten Verbundprojekten Ambos (BMBF) und Aladdin (H2020) die akustische Erkennung von Drohnen vorangetrieben. Am Projekt Ambos waren zwölf Partner unter der Leitung des Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie FKIE an der Forschung beteiligt. Für Aladdin haben sich 18 Verbundpartner aus neun europäischen Ländern zusammengeschlossen, darunter die CS Group als Projektleitung. In zahlreichen internen Vorhaben wurden die Algorithmen und Systemkomponenten kontinuierlich verfeinert. Heute können die Forschenden neben den leicht integrierbaren Algorithmen zur Erkennung und Lokalisation der UAS auch auf eine vollintegrierbare Systemlösung zurückgreifen.

Glasfasergelenkte Drohnen oder autonome Flugobjekte bleiben der Funkaufklärung häufig verborgen, während hochauflösende Radar- und Kamerasysteme hohe Kosten und energieintensive Rechenleistung erfordern. Die akustische Lösung des Fraunhofer IDMT dagegen arbeitet mit geringem Energiebedarf, sodass ein autonomer Betrieb mit Akkus möglich ist.

Auch das Aufwecken weiterer Sensorkomponenten nach einem akustischen Kontakt, bietet Vorteile. Die Technologie kann eine 360°-Abdeckung erreichen. Die Detektions- und Lokalisierungsreichweiten liegen je nach Störgeräuschumfeld zwischen 50 und 200 Metern, bei einer zeitlichen Auflösung von einer Sekunde. Eine Ausweitung auf weitere akustische Ereignisse, von Fahrzeugen bis hin zu Schussgeräuschen, ist denkbar. Durch die gute Verfügbarkeit können die akustischen Sensoren flächendeckend ausgebracht werden.

Preiswert und wartungsarm

„Mit unserer akustischen Technologie bieten wir eine preiswerte und wartungsarme Ergänzung zu bestehenden Drohnendetektionssystemen", erklärt Christian Rollwage, Gruppenleiter Audiosignalverbesserung am Fraunhofer IDMT. Insbesondere Unternehmen im Wehr- und Sicherheitsbereich, die bereits Drohnenerkennungssysteme – basierend auf Radar, Optik oder Lidar – entwickeln, sowie Systemintegratoren mit dem Wunsch nach eigener Sensorik und Drohnenhersteller, die Signale aus der Luft detektieren möchten, sind die adressierten Zielkunden der neuen Technologie. GIT

Hier finden Sie ein Video von Fraunhofer IDMT zur Detektion und Lokalisation von Drohnen

Fraunhofer-Institute for Digital Media Technology IDMT
www.idmt.fraunhofer.de/hsa

BVSW

BVSW Wintertagung

11. - 13. März 2026

Arabella Alpenhotel am Spitzingsee

Die Wintertagung des BVSW ist die zentrale Plattform für Sicherheitsverantwortliche aus Wirtschaft und Behörden. In Zeiten geopolitischer und technologischer Umbrüche bietet sie topaktuelle Vorträge, spannende Diskussionen und beste Möglichkeiten zum Networking – mitten in den Alpen.

Highlights

- Keynote: Prof. Dr. Günther Schmid
- Resüme MSC: Dr. Benedikt Franke
- Sicherheitslage Bayern: LPP Michael Schwald
- Aktuelle geopolitische Lage im Fokus
- Best Practices aus der Unterneh-menssicherheit
- Bayerischer Abend & Networking im Alpenhotel

JETZT ANMELDEN

www.bvsw.de

SICHERHEITSGIPFEL DER DEUTSCHEN WIRTSCHAFT

Kamikaze-Drohne „Hornet“ von Rheinmetall

Autonome Technologien und Robotik

Die Messe Düsseldorf lädt zum zweiten Mal zur Xponential Europe

Vom 24. bis 26. März 2026 findet wieder die Xponential Europe auf dem Messegelände Düsseldorf statt. Sie soll als Zentrum für die Branche der autonomen Technologien und Robotik in Europa bilden. Mit einer Kombination aus internationaler Fachausstellung und Konferenzprogramm wird die gesamte Wertschöpfungskette abgebildet – in Form von Live-Demonstrationen, Präsentation visionärer Start-ups bis hin zu Konferenzen und Keynotes.

Verletzungen des Luftraums, feindliche Drohnenüberflüge, Störmanöver an Flughäfen im In- und Ausland – das ist heute die Realität, vor dem die Sicherheits- und Verteidigungspolitik in Europa steht. Das zeigt auch die Xponential Europe in Düsseldorf. Die Messe für autonome Systeme und Robotik steht im Zeichen von „Dual use“, womit die sowohl zivile als auch militärische Nutzung von Technologien gemeint ist. Im Bereich Defense liegt der Fokus auf autonomen Systemen, die zur Verteidigung eingesetzt werden – etwa in der Luftaufklärung, der Abwehr von Angriffen, der Versorgung oder der Steuerung von Einheiten im Einsatz.

Neben großen Rüstungsunternehmen prägen Start-ups das Bild. Präsent sein werden u.a. Quantum Systems aus Gilching, MBDA Deutschland aus Schrobenhausen und Aaronia aus Strickscheid. Aaronia ist auf Mess-, Ortungs- und Überwachungstechnik spezialisiert und hat das weltweit erste Drohnenerkennungssystem Aartos entwickelt. Mehr als 600 dieser Systeme sind derzeit weltweit in Betrieb. Wo sie zum Einsatz kommen, schützen sie Flughäfen, Kraftwerke oder NATO-Territorien und Tagungen – beispielsweise die Airports London Heathrow, Singapur und Oman oder das NATO-Gipfel Treffen in Den Haag.

Europaweite Drone Wall

„Die Schaffung einer europaweiten Drone Wall ist ein zentrales Thema der kommenden Xponential Europe“, sagt Messe-Director Malte Seifert. Angesichts der aktuellen Bedrohungslage fordern Experten die Schaffung einer nationalen Taskforce zur Detektion und Luftabwehr. Vor diesem Hintergrund, so Seifert, sei die Fachmesse die wichtigste Plattform der Branche in Europa.

Vor dem Hintergrund der vielen verdächtigen Drohnensichtungen im Luftraum hat die EU die diskutierte Initiative einer Drone Wall konkretisiert. Ziel ist es, damit ein abge-

stuftes Verteidigungssystem gegen unbemannte Bedrohungen zu schaffen. Dieses soll – analog zur European Sky Shield Initiative (ESSI) im Bereich der bodengebundenen Luftverteidigung – als gesamteuropäisches Programm aufgesetzt werden. Damit sollen bestehende nationale Kompetenzen vernetzt, stationäre und mobile Systeme einbezogen sowie die Zahl der C-UAS-Lösungen deutlich erhöht werden – in der Detektion, Identifikation und gezielten Abwehr in der Luftverteidigung und bodengestützten Flugabwehr.

Dynamische Bedrohungslage

„Die aktuelle (hybride) Bedrohung durch Drohnen ist dynamisch und hochgradig komplex. Entscheidend ist: Wir haben Systeme und Lösungen, die sofort einsatzfähig sind – gleichzeitig arbeiten wir mit Hochdruck daran, diese zu skalieren und entsprechend der spezifischen Bedrohungsszenarien kontinuierlich weiterzuentwickeln", sagt Daniela Hildenbrand, Expertin für Drohnenabwehr beim Sensorspezialisten und Systemintegrator Hensoldt. Das in Taufkirchen ansässige Unternehmen entstand vor acht Jahren durch die Ausgliederung der früheren Geschäftsbereiche von Airbus Defence and Space für Sensortechnologie in den Bereichen Verteidigung, Sicherheit, Luft- und Raumfahrt. Heute zählt sich Hensoldt zu den führenden europäischen Häusern für Verteidigungs- und Sicherheitselektronik. Auf dessen Radar- und optronischen Systeme setzen Bundeswehr und Polizei ebenso wie Armeen und Sicherheitsbehörden befreundeter Staaten.

Abfangdrohnen sollen Luftraum schützen

Quantum Systems hat mit der „Jäger"-Drohne eine Abfangdrohne mit Raketenantrieb und autonomer KI-Steuerung präsentiert. Sie wird von einem Feststoffraketenmotor angetrieben und kann innerhalb von nur 30 Sekunden auf 4.000 Meter Höhe katapultiert werden. Das System ist darauf ausgelegt, feindliche Drohnen zu neutralisieren. Durch störungsresistentem Datenlink und autonomer Steuerung ohne GPS-Abhängigkeit bleibt das System auch in elektronisch gestörten Einsatzumgebungen funktionsfähig.

Drohne A900 – ein vielseitig einsetzbares System für Aufklärungs- und Inspektionsmissionen

Auch Start-ups wie Argus Interception aus dem niedersächsischen Rotenburg an der Wümme, dessen Fluggeräte mit Fangnetzen ausgestattet sind, sowie das Münchner Unternehmen Tytan Technologies sollen die Abwehr sichern. Erst vor wenigen Wochen wurde das 2023 gegründete Unternehmen an der Isar von der Bundeswehr damit beauftragt, ein Konzept für den Schutz sämtlicher militärischer Liegenschaften der Bundeswehr zu erstellen. GIT

PCS Systemtechnik verleiht Gold Partner Award 2025

PCS Systemtechnik GmbH hat sechs langjährige Partnerunternehmen mit dem PCS Gold Partner Award 2025 ausgezeichnet. Prämiert wurden die Softwarehäuser Atoria – the people software GmbH, Atoss Software SE, Bosch Sicherheitssysteme GmbH, Fourtexx GmbH, GFOS mbH und RLDatix GmbH für ihre herausragende Zusammenarbeit im Bereich Workforce Management, Zeitwirtschaft, Personaleinsatzplanung und Zutrittskontrolle.

Die Auszeichnung würdigt die erfolgreiche und kontinuierliche Partnerschaft mit PCS sowie die zahlreichen gemeinsamen Installationen, die sich durch hohe Qualität und nachhaltige Kundenerfolge auszeichnen. Alexander Harbecke, Leiter Partnervertrieb bei PCS, betont: „Wir sind stolz darauf, sechs unserer Kooperationspartner mit dem PCS Gold Partner Award 2025 auszuzeichnen. Im zurückliegenden Geschäftsjahr haben wir gemeinsam erfolgreiche Projekte realisiert und erfreuliche Umsätze erzielt. Der Markt ist viel dynamischer und volatiler geworden – auf diese Veränderungen sind wir mit unserer Intus Hardware und den Intus Systemen bestens vorbereitet. Nun gilt es, gemeinsam mit unseren Partnern weiter an den Workforce-Management-Lösungen von morgen zu arbeiten, um unsere Kunden auch zukünftig bestmöglich bedienen zu können."

Die prämierten PCS Kooperationspartner setzen mit ihren modernen HR-Lösungen regelmäßig neue Impulse im Workforce-Management und in der Zeiterfassung. Insbesondere in den vergangenen Monaten hat ein Innovationsschub stattgefunden, der durch den Einsatz von KI-basierten Datenanalysen entscheidende Mehrwerte für die moderne, ausbalancierte Personaleinsatzplanung schafft. Grundlage für ein rechtskonformes und effizientes Workforce-Management ist eine verlässliche Erfassung der Arbeitszeiten mit Intus Terminals. Die langlebige und zukunftsorientierte Intus Hardware ist cloud-ready und arbeitet nach aktuellen Cybersecurity-Standards. **www.pcs.com**

© PSC Systemtechnik

PCS Systemtechnik konnte 2025 sechs Kooperationspartner mit einem Gold Partner Award für den stärksten Umsatz auszeichnen, und zwar die Softwarehäuser Atoria, Atoss, Bosch Sicherheitssysteme, Fourtexx, GFOS sowie RLDatix

© Stadtwerke München, Stefan Heigl

Verwaltungsgebäude der Stadtwerke München, am Stammsitz München

TITELTHEMA

Gut versorgt

KRITIS: Umfassende Systemlösung für Stadtwerke München

Die Stadtwerke München (SWM) sind eines der größten kommunalen Versorgungs- und Dienstleistungsunternehmen in Deutschland: Sie versorgen die bayerische Landeshauptstadt mit Energie und Trinkwasser, sind Betreiber des öffentlichen Nahverkehrs, betreuen Bäderbetriebe und Immobilien. Die besondere Herausforderung für eine effektive und robuste Zutrittskontrolle zu den Liegenschaften sind die Vielzahl der SWM-Standorte und die unterschiedlichen Sicherheitsanforderungen.

© Interflex

Die IF-6040 koordiniert die Zutrittskontrolle für alle angebundenen Zugänge mit Zutrittsterminals der Baureihe IF-800

„Weil die Stadtwerke München mit ihren Erzeugungs- und Versorgungsanlagen Teil der kritischen Infrastruktur sind, bestehen hohe Anforderungen an die Sicherheit sowie an die Einhaltung von regulatorischen und gesetzlichen Vorgaben“, sagt Mike Busse, verantwortlicher Produkt- und Systemmanager für Sicherheitstechnik im Bereich Konzernsecurity der SWM. Die Infrastruktur, die sein Team betreut, verteilt sich auf mehrere Hundert Standorte im Stadtgebiet und dem Umland von München. Dazu zählen Betriebshöfe, Erzeugungs- und Verteilungseinrichtungen, Bahn- und Netzanlagen sowie Verwaltungsgebäude mit Büros.

Diese Vielfalt erfordert eine umfassende Sicherheitslösung, die den Schutz kritischer Versorgungsanlagen, die Zutrittskontrolle und das Besuchermanagement zuverlässig sicherstellt. Neben den rund 11.000 SWM-Beschäftigten haben auch etwa 1.100 externe Firmen, Lieferanten und Dienstleister mit etwa 10.000 Fachkräften kontrollierten Zugang zu verschiedenen Gebäuden und technischen Anlagen, beispielsweise für Reparatur- und Wartungs-

Zwei Multifunktionsstelen von Friendlyway unterstützen die Besucherselbstanmeldung vor Ort

Ein integrierter Dokumentenscanner ermöglicht eine zuverlässige Überprüfung von Ausweisdokumenten (ID-Check)

Unter anderem Büroräume werden mit wirelessfähigen Opendor Schließkomponenten gesichert. Im Bild: ein IF-271 Door Handle

arbeiten. Hinzu kommt das Management von Besuchern ohne regelmäßigen Zutritt zu den SWM-Einrichtungen.

Vielzahl von Standorten mit unterschiedlichen Sicherheitsanforderungen

„Eine zuverlässige und flexibel erweiterbare Lösung ist für uns entscheidend, damit wir die Sicherheitsbedürfnisse und Anwendungsfälle der verschiedenen, sich dynamisch entwickelnden Standorte optimal sicherstellen können," erklärt Mike Busse. Neben biometrischer Zwei-Faktor-Authentifizierung gehören die Steuerung von Einbruchmeldeanlagen, die Raumzonenverfolgung sowie die Automatisierung und präzise Kontrolle des Besucherverkehrs zum Gesamtkonzept. Seit mittlerweile mehr als 25 Jahren arbeiten die Stadtwerke München im Bereich Sicherheitstechnik mit Interflex, Spezialist für ganzheitliche, innovative Lösungen für Zutrittskontrolle und Besuchermanagement, zusammen. Erstes gemeinsames Projekt war die Einführung der elektronischen Zeiterfassung für die Beschäftigten, heute unterstützt Interflex die SWM mit ganzheitlichen Sicherheitslösungen.

Softwareplattform als zentrale Datendrehscheibe

Herzstück der Interflex-Lösungen ist die steuernde Softwareplattform IF-6040, die als „Datendrehscheibe" fungiert. Wegen der hohen Sicherheitsanforderungen in vielen Gebäuden und technischen Anlagen der SWM benötigen alle Personen, die sie eigenständig betreten, einen Ausweis. Diese Zutrittsberechtigungen werden in der Plattform zentral vergeben, verwaltet und gesteuert. In Summe sind das 31.000 Ausweise für Beschäftigte und Lieferanten, inklusive 2.500 registrierter Fahrzeuge und etwa 800 vorangemeldeter Besucher. Darüber hinaus koordiniert die IF-6040 die Zutrittskontrolle für alle angebundenen Zugänge mit Zutrittsterminals der Baureihe IF-800 oder batteriebetriebenen, wirelessfähigen Schließkomponenten der Interflex-Produktserie Opendor. Die offenen Schnittstellen der Plattform ermöglichen es außerdem, Drittsysteme anzubinden, beispielsweise Systeme mit Zwei-Faktor-Authentifizierung, Einbruchmeldeanlagen oder für das Parkhausmanagement.

Modernisiertes Besuchermanagement

Auch die Besucherverwaltung wurde mithilfe der Plattform IF-6040 modernisiert. Wurden bei der Vorgängerlösung die Besucher noch manuell angemeldet und erfasst, bietet die aktuelle Lösung die Möglichkeit, die Daten von Besuchern und deren Zugang automatisiert zu erfassen, zu verwalten und letztlich klar zwischen öffentlichzugänglichen und gesicherten Bereichen zu trennen. In einem Evakuierungsfall liefert das System darüber hinaus sichere Informationen, wie viele Personen sich im Gebäude oder auf dem Gelände befinden und evakuiert werden müssen.

In einem ersten Schritt entwickelte Interflex für das Gebäude der SWM-Hauptverwaltung das Konzept für eine kombinierte Lösung nach Kundenanforderung. Ziel war, den Self-Service so weit zu automatisieren, dass Besucher ihre An- und Abmeldung am Standort selbstständig durchführen können. „In der Hauptverwaltung haben wir große Besuchergruppen und auch Kundenverkehr," erklärt Mike Busse die Anforderungen. „Für unser Empfangspersonal ist es wichtig, diese unterschiedlichen Gruppen parallel zu steuern. Deshalb haben wir den Self-Service ausgelagert und die Anmeldung und Dokumentation der Besucher automatisiert." Eine weitere wichtige Anforderung war, dass die Lösung im Rahmen der Selbstanmeldung eine zuverlässige Überprüfung von Ausweisdokumenten (ID-Check) mittels Dokumentenscanner sicherstellen konnte.

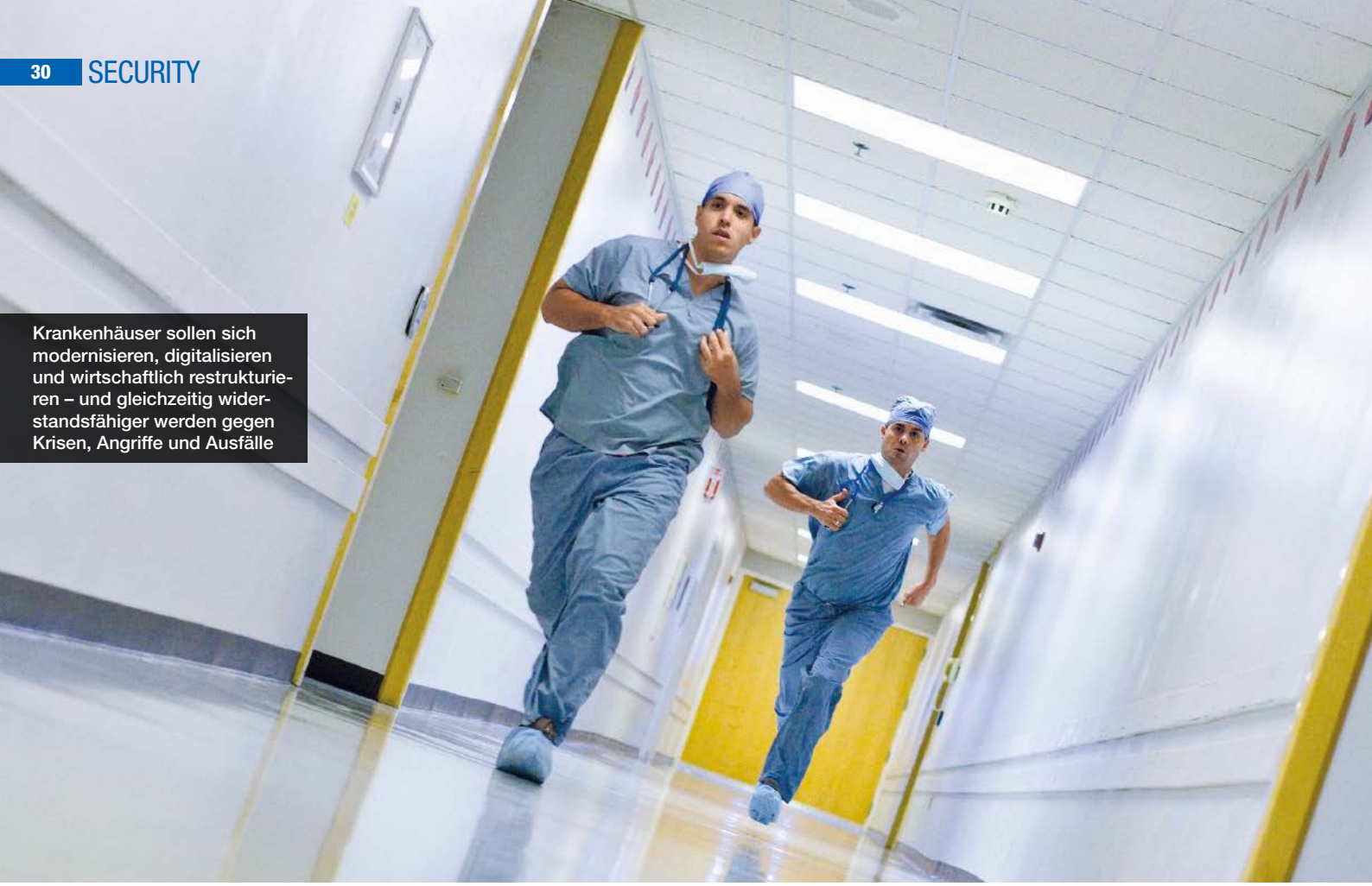
Multifunktionale Self-Service-Stelen

Für die Umsetzung der Besucherselbstanmeldung arbeitete Interflex mit dem Projektpartner Friendlyway Germany zusammen, der als Lösungsanbieter über jahrzehntelange Expertise mit Self-Service-Stelen verfügt. Daher sind heute im Eingangsbereich der Hauptverwaltung zwei Multifunktionsstelen mit Self-Service-Displays im Einsatz, die den An- und Abmeldeprozess automatisieren. Zu den installierten technischen Lösungen zählen unter anderem Pass-, RFID- und QR-Code-Leser. Im Ergebnis erhalten Besucher der Stadtwerke einen professionellen An- und Abmeldeprozess, den sie ohne zusätzliche Anmeldung am Empfang und den damit verbundenen Wartezeiten durchlaufen.

„Eine Besonderheit des Konzepts war, dass wir neben der Selbstanmeldung von Besuchern auch die Unterweisungsprozesse der Stadtwerke in die Lösung integriert haben," beschreibt Christian Weiss, Projektverantwortlicher und Solution Architect von Interflex, die Umsetzung. So werden alle an der Multifunktionsstele oder vorab im Unterweisungsportal der SWM absolvierten Unterweisungen ebenfalls an das System IF-6040 übertragen und dort gespeichert. Für die Beschäftigten bietet die Multifunktionsstele zusätzlich die Möglichkeit eine echte Führerscheinprüfung durchzuführen, wobei diese ihre Zugehörigkeit mittels ID-Check am Kiosk nachweisen.

Für die Stadtwerke München hat sich die Optimierung von Zutrittskontrolle und Besuchermanagement ausgezahlt. Denn mit der neuen Lösung lassen sich jetzt die unterschiedlichen Use Cases an den verteilten Standorten der SWM flexibel und die jeweiligen Sicherheitsprotokolle zuverlässig umsetzen. GIT

Interflex Datensysteme GmbH
www.interflex.com



Krankenhäuser sollen sich modernisieren, digitalisieren und wirtschaftlich restrukturieren – und gleichzeitig widerstandsfähiger werden gegen Krisen, Angriffe und Ausfälle

GESUNDHEITSWESEN

Zwischen Reform und Risiko

Krankenhäuser: Warum Resilienz jetzt zur sicherheitspolitischen Pflicht wird

Krankenhäuser stehen heute unter einem doppelten Druck: Sie sollen sich modernisieren, digitalisieren und wirtschaftlich restrukturieren – und gleichzeitig widerstandsfähiger werden gegen Krisen, Angriffe und Ausfälle. Die Deutsche Krankenhausgesellschaft (DKG) hat dazu im Oktober 2025 eine Studie vorgestellt, die deutlich macht, wie weit Anspruch und Wirklichkeit auseinanderliegen. Ein Beitrag von Hendrik Tarek Dehne von Assa Abloy.

Hendrik Tarek Dehne von Assa Abloy befasst sich speziell mit Sicherheitslösungen für Krankenhäuser

Drei Szenarien haben das Institute for Health Care Business (hcb) und das Deutsche Krankenhausinstituts (DKI) im Sinne: Cyberangriffe und Sabotage, den Bündnisfall eines NATO-Mitgliedsstaats und den Verteidigungsfall im engeren Sinne. In allen Fällen zeigt sich: Die Einrichtungen sind weder technisch noch organisatorisch auf größere Krisen vorbereitet. Besonders eklatant sind die Schwächen in fünf zentralen Bereichen – Personal, Cybersicherheit, physische Sicherheit, Lagerhaltung medizinischer Vorräte sowie Vorbereitung auf biologische, chemische oder nukleare Bedrohungen.

NIS2 und KRITIS-Dachgesetz

Mit der Veröffentlichung der DKG-Studie wächst zugleich der Druck auf die deutsche Politik, nun endlich Ernst bei der nationalen Umsetzung der IT-Sicherheitsrichtlinie NIS2 und dem KRITIS-Dachgesetz zu machen. Beide Regelwerke sollen europaweit einheitliche Mindeststandards festlegen, um kritische Infrastrukturen widerstandsfähiger gegen digitale und phy-

sische Bedrohungen zu machen. Betreiber betroffener Einrichtungen sollen künftig umfassende Risikoanalysen durchführen, physische und organisatorische Schutzmaßnahmen umsetzen und ihre Resilienz gegenüber Cyberangriffen, Naturkatastrophen, Sabotage, Personalengpässen oder Ausfällen von Lieferketten verbessern.

Auch für das Gesundheitswesen stellt dies einen bedeutenden Paradigmenwechsel dar. Galten bislang nur Krankenhäuser und Universitätskliniken mit einer vollstationären Fallzahl oberhalb 30.000 als kritische Infrastruktur, erfasst NIS2 nun nahezu die gesamte Versorgungskette im Gesundheitswesen: Also auch Labore, Diagnostik- und Analytikbetriebe sowie den Pharma-Bereich mit Medizintechnik, Referenzlaboren und Forschungseinrichtungen.

Fehlende Zutrittskonzepte als Sicherheitsrisiko

Doch es müssen nicht gleich der militärische Spannungsfall oder spektakuläre Hackerangriffe sein, um den dringenden Handlungsbedarf bei der Absicherung von Gesundheitseinrichtungen zu verdeutlichen. Seit Jahren schon häufen sich Übergriffe auf das Personal in Kliniken und Praxen, Fälle von unbefugtem Zutritt zu Stationen oder sensiblen Bereichen und der Diebstahl von Medikamenten oder medizinischem Gerät. Eine Blitzumfrage des Deutschen Krankenhausinstituts ergab beispielsweise, dass 73 % der Häuser eine Zunahme von Übergriffen gegen Beschäftigte feststellen.

Das sagt einiges über unsere Gesellschaft aus, offenbart aber auch Defizite im strukturell-technischen Bereich. Oft fehlen neben Sicherheitspersonal auch klare Zutrittskonzepte, die regeln, wer wann bestimmte Bereiche betreten darf. Nicht selten basieren diese Vorkehrungen zudem auf veralteten mechanischen Schließanlagen, mit denen sich die eigentlich erforderliche Zuweisung individueller Zutrittsrechte kaum umsetzen lässt. Verschaffen sich Unbefugte Zutritt zu Technik- oder Serverräumen, stehen dann schnell nicht nur Sachwerte, sondern die Versorgungssicherheit der gesamten Einrichtung auf dem Spiel. Denn wer erst einmal Zugang ins Objekt erlangt hat, hat häufig auch allzu leichtes Spiel beim Zugriff auf digitale Systeme.

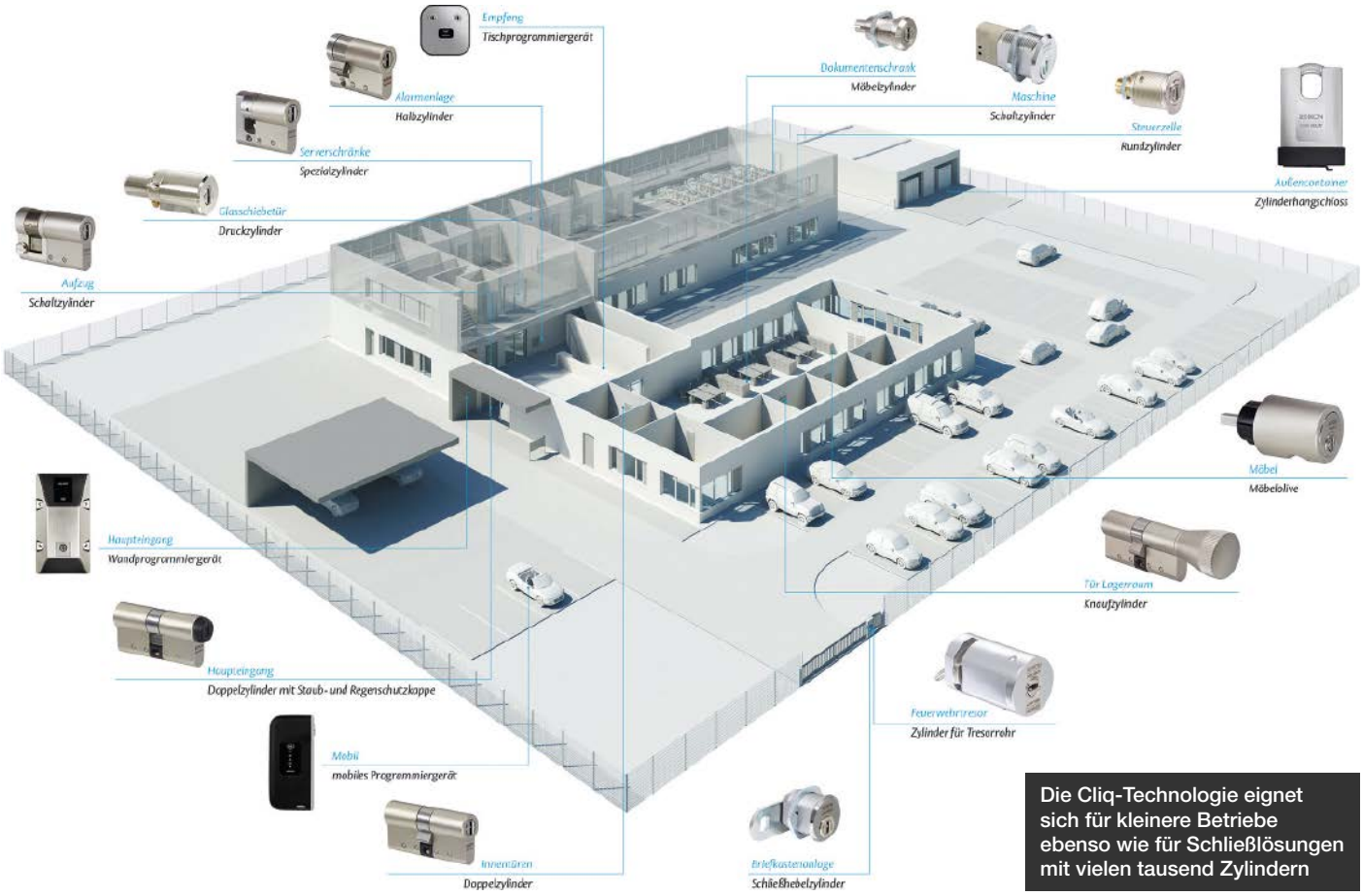
Zonenkonzepte: Fundament physischer Resilienz

Wenn Krankenhäuser künftig resilienter werden sollen, darf Sicherheit nicht erst an der Schwelle des Serverraums oder der telemedizinischen Einrichtungen beginnen. Sie muss das gesamte Gelände, die baulichen Strukturen und die internen Abläufe umfassen. Dabei bietet sich als Planungsprinzip das – sowohl in der Sicherheitsarchitektur von Rechenzentren als auch in forensischen Einrichtungen bewährte – Zonenkonzept an. Es teilt das

Bitte umblättern ▶

Krankenhaus-Transformationsfonds

Die Deutsche Krankenhausgesellschaft (DKG) beziffert den Finanzbedarf für mehr Resilienz in deutschen Krankenhäusern auf bis zu 15 Milliarden Euro. Der Verband schlägt vor, Mittel aus dem Sondervermögen für die Verteidigung teilweise in den Krankenhaus-Transformationsfonds (KHTF) umzulenken. Der Fonds soll den Strukturwandel im Gesundheitswesen fördern, bislang aber liegt der Schwerpunkt auf Digitalisierung und Effizienzsteigerung. Themen wie physische Sicherheit, Zutrittsorganisation oder Objektschutz werden in der Förderlogik bisher nur am Rande berücksichtigt. **Ein Support Paper zu Förderungsfragen von Assa Abloy finden Sie hier zum Download:**



Die Cliq-Technologie eignet sich für kleinere Betriebe ebenso wie für Schließlösungen mit vielen tausend Zylindern

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

Krankenhaus in verschiedene Sicherheitsbereiche – vom öffentlichen Eingangsbereich über Funktions- und Technikzonen bis hin zu Hochsicherheitsbereichen wie Intensivstationen, Laboren oder Medikamentenlagern.

Jeder Bereich erhält ein individuell abgestuftes Schutzniveau, das sowohl bauliche als auch elektronische Maßnahmen integriert. Darüber hinaus empfiehlt sich der Einsatz von Schleusenlösungen oder Vereinzelungsanlagen, die auch in Rechenzentren oder forensischen Kliniken als physische Schnittstelle zwischen Sicherheitszonen dienen. Durch Zwei-Faktor-Authentifizierung, biometrische Kontrolle und Anti-Passback-Funktion verhindern solche Systeme unkontrollierte Mehrpersonenzugänge oder unerlaubte Richtungswechsel. Auch Krankenhäuser erhalten damit ein wirksames Mittel, um sensible Bereiche wie Apotheken, Technikräume oder Datenzentren gezielt abzusichern.

Sicherheit bedeutet in diesem Kontext aber nicht Abschottung, sondern Steuerung: Wer das Haus betritt, soll sich sicher fühlen – egal ob als Patient, Besucher oder Beschäftigter. Zugleich muss gewährleistet sein, dass sensible Bereiche geschützt bleiben, ohne dass das System den Arbeitsfluss im Klinikalltag blockiert.

Diese Perimeter- und Zonensicherung ist die Grundlage für physische Resilienz: Ein Einbruch oder unbefugter Zutritt kann vielleicht nicht vollständig verhindert, seine Auswirkungen aber durch mehrschichtige Schutzbarrieren erheblich besser kontrolliert werden. So lassen sich Risiken frühzeitig erkennen und Schäden begrenzen. Besonders effektiv ist dieses Konzept, wenn es mit intelligenten Zutrittslösungen verknüpft wird – also mit Systemen, die bereichsbezogene Rechte vergeben und alle Zutrittsereignisse nachvollziehbar protokollieren.

Intelligente Zutrittssysteme

Hier kommen elektronische Schließ- und Zutrittskontrollsysteme ins Spiel. Lösungen wie das elektronische Schließsystem eCliq oder die drahtlosen Aperio-Komponenten von Assa Abloy ermöglichen eine fein abgestufte Steuerung von Zugangsrechten – von der äußeren Gebäudehülle bis hin zu einzelnen Räumen, Möbeln und Serverschränken. Mechanische Stabilität ergänzt sich dabei um digitale Flexibilität: Schlüssel und Zylinder lassen sich bei Personalwechsel oder temporären Zugängen einfach umprogrammieren, verlorene Schlüssel werden elektronisch gesperrt. Im Fall der Zutrittskontrolle sind alle Zutritte auch in Echtzeit nachvollziehbar. Das erhöht die Transparenz und erfüllt gleichzeitig die Anforderungen, die mit NIS2 und dem KRITIS-Dachgesetz an eine „nachweisbare physische Sicherheit“ gestellt werden.

Ein weiterer Vorteil: Solche Systeme lassen sich ohne großen baulichen Aufwand in bestehende Infrastrukturen integrieren – eine entscheidende Voraussetzung für Kliniken, die schrittweise modernisieren und gleichzeitig den Betrieb aufrechterhalten müssen. Die Verknüpfung mit Rettungswegtechnik oder Brandmeldeanlagen sorgt zudem dafür, dass Sicherheit nicht zu Einschränkungen führt, sondern den Betrieb unterstützt. GIT

Assa Abloy Sicherheitstechnik GmbH
www.assaabloy.com/de/de

Passkontrolle am Flughafen Zürich

Flughafen Zürich startet mit Secunet ins Einreise-/Ausreisesystem der EU

Schrittweise geht das Einreise-/Ausreisesystem der EU (Entry/Exit System, EES) in europäischen Ländern in Betrieb. Der Flughafen Zürich, der am stärksten frequentierte internationale Flughafen der Schweiz, startete nun unterstützt durch Grenzkontrolltechnologie von Secunet. Diese sorgt für eine reibungslose Anbindung an das EES, nimmt biometrische Gesichtsbilder auf und prüft automatisiert die Identität von Reisenden. Zudem verkürzt sie die Wartezeit am Schalter, indem die Reisenden ihre Daten vorab an Selbstbedienungskiosken eingeben können. Auf ähnliche Weise unterstützt Secunet die Grenzkontrollbehörden zahlreicher Schengen-Staaten beim EES-Rollout, darunter Deutschland, Österreich und Tschechien. Bei dem EES handelt es sich um die größte Neuerung in der europäischen Grenzkontrolle seit Einführung des Schengen-Raums. Sämtliche Grenzübertritte von Drittstaatsangehörigen werden künftig biometrisch registriert – das Stempelverfahren hat ausgedient.

www.secunet.com

BHE-Fachkongress

Die Sicherheits-Profis!

BHE Bundesverband
Sicherheitstechnik e.V.

Videosicherheit / Zutrittssteuerung

21./22. April 2026

Atrium Hotel Mainz

Ausstellung ◆ Vortragsprogramm ◆ Networking

Aktuelle Informationen und moderne Konzepte der Video- und Perimetersicherheit sowie Zutrittssteuerung für:

- Errichter, Planer- und Ingenieurbüros sowie Hersteller
- Sicherheitsbeauftragte von Anwendern, z.B. Banken, Logistik, Flughäfen, Krankenhäuser, KRITIS-Betreiber
- Versicherer
- Notruf- und Serviceleitstellen
- Behördenvertreter

Anmeldung und Programm beim BHE (Telefon 0 63 86 / 92 14-18)

… oder unter **www.bhe.de/kongress-video-zutritt**

SMART BUILDINGS

Unter einem Dach

Gewerkeübergreifende Kompetenz in Bad Kreuznach

Die Sicherheitsexperten von expertus sorgen für den Schutz des gemeinsam genutzten Gebäudes mit Technik von Telenot

Unter dem Namen Grete 12 haben sich im malerischen Bad Kreuznach drei Unternehmen der technischen Gebäudeausstattung unter einem Dach vereint. Zur Kooperation gehören auch die Sicherheitsexperten von Expertus. Diese sorgen für den Schutz des gemeinsam genutzten Gebäudes mit Technik von Telenot.

Schnelles Internet sowie eine sich immer weiter entwickelnde IT-Technologie haben dazu geführt, dass auch im Bereich der technischen Gebäudeausstattung die unterschiedlichen Gewerke immer enger aneinanderrücken. Beleuchtung, Klimatechnik, Energieversorgung, Unterhaltungselektronik und selbstverständlich auch die Bausteine der elektronischen Sicherheitstechnik sind in Gebäuden gleich welcher Nutzung heute keine alleinstehenden Systeme mehr. Vielmehr bilden sie ein smartes Netzwerk, mit dem sich ein gesamtes Haus steuern lässt – mit entsprechenden Synergie- und Einspareffekten.

Es liegt deshalb nahe, dass die damit befassten Fachbetriebe eng zusammenarbeiten, um für Bauherren und Planer optimale Lösungen zu erarbeiten. Die Firmen Enders & Zuhl, als Elektrohandwerksbetrieb für Planung und Installation von Smart-Home und KNX-Steuerung zuständig, Lichtlandschaften, Experte für Lichtdesign und Lichtkonzepte, sowie Media@home, Spezialist für Medien- und Konferenztechnik, gingen zusammen im Jahr 2022 einen Schritt weiter und residieren nun in Bad Kreuznach unter einem Dach in einem gemeinsamen Fachzentrum mit dem Namen „Grete 12". Der Name verweist auf die Adresse in der Grete-Schickedanz-Straße 12.

Sicherheits-Systemhaus im Verbund

Weiterer Partner dieser Kooperation, dessen Leistungen immer gefragter werden – auch aufgrund gesetzlicher Vorgaben, Normen und Regulierungen: das Sicherheits-Systemhaus Expertus. Der autorisierte Telenot-Stützpunkt ist in dem Verbund in erster Linie für alle Fragen der elektronischen Sicherheitstechnik zuständig. Expertus kooperiert bereits seit vielen Jahren mit Enders & Zuhl. Die rund 30 Mitarbeiter um Geschäftsführer Karsten Theis legen ihren Fokus auf Großprojekte. In den vergangenen zehn Jahren hat das VdS-zertifizierte Unternehmen Einbruchmeldetechnik, Brandmeldeanlagen und Videoüberwachungssysteme in verschiedenste Unternehmen, Kliniken oder Bürogebäude rund um Bad Kreuznach installiert.

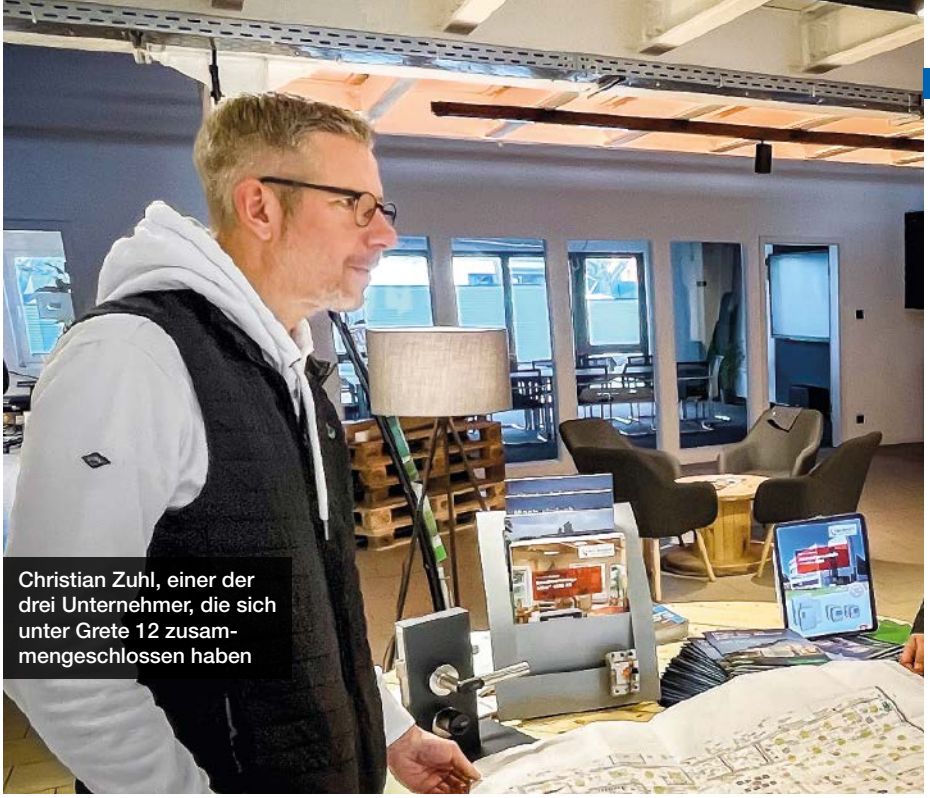
Durch die Grete-12-Kooperation konnte Expertus bereits neue Kunden gewinnen. „Wir spüren ganz deutlich, dass Projekte, bei denen gewerkeübergreifende Kompetenz gefragt ist, zunehmen", so Theis. Ein Erfolgsfaktor des Unternehmens ist das umfassende Know-how der Mitarbeiter. So besuchen auch alle Auszubildenden die Grund- und Weiterbildungslehrgänge von Telenot, um stets die neuste und modernste Technik zu kennen und so jederzeit fit für die Zukunft der Sicherheitstechnik zu sein.

Neugestaltung mit smarter Technik

Die Einzelunternehmen haben die Grete-12- Halle eines ehemaligen Motorradhändlers umfassend neugestaltet und ihren Bedürfnissen angepasst. Jeder Partner hat dabei eigene Räume erhalten, inklusive Ausstellungsfläche, Werkstatt und Büro.

Zudem gibt es einen gemeinsam genutzten Konferenzraum, den jede der drei Firmen individuell mit Elektro-, Audio- sowie Lichttechnik ausgerüstet hat. In komfortabler Atmosphäre können hier umfassende Haustechnik-Lösungen gemeinsam mit den Kunden geplant werden – zum Beispiel, wenn ein Architekt ein komplettes Gebäude mit smarter und vernetzter Technik ausrüsten will.

Durch die gemeinsame Planung sind solche Lösungen nicht nur zumeist deutlich günstiger, als wenn die Gewerke unabhängig voneinander arbeiten. Die Lösung über Grenzen hinweg schafft von Beginn an Synergien – beispielsweise, wie Lichter zu schalten oder Fenster zu schließen sind oder die Heizung herunterzufahren ist, sobald die Alarmanlage eines Gebäudes scharf geschaltet wird. Das macht die Bedienung komfortabler und kann helfen, den Energieverbrauch deutlich zu senken. „Nicht selten lassen sich Einsparungen im zweistelligen Prozentbereich erbringen“, weiß Theis.



Christian Zuhl, einer der drei Unternehmer, die sich unter Grete 12 zusammengeschlossen haben

Einbruch- und Überfallmelderzentrale

Expertus war auch für die Absicherung von Grete 12 mit hochwertiger Sicherheitstechnik von Telenot zuständig. Basis für das System ist die Einbruch- und Überfallmelderzentrale complex 400H, die alle Bestimmungen, Vorschriften und Richtlinien wie DIN EN 50131, VdS-Klasse C, VDE 0833 und die ÜEA-Richtlinie der Polizei erfüllt. Zum Sicherheitssystem gehören bei Grete 12 auch zahlreiche Rauch- und Bewegungsmelder. Diese sind meist per Kabel mit der Zentrale verbunden.

„In einigen Bereichen haben wir aber auch Funktechnik eingesetzt”, ergänzt Theis. Insgesamt ist die Lösung in drei Sicherheitsbereiche unterteilt. Die Außenhaut- und Flächenüberwachung wird von einer Zutrittskontrolle ergänzt, zu der auch die noch relativ neuen mechatronischen Schließelemente von Telenot an den Türen gehören. Im Gefahrenfall schlagen externe Signalgeber laut Alarm. Gleichzeitig wird ein Wachunternehmen benachrichtigt und die Mitarbeiter per App informiert. Über diese kann die Anlage übrigens auch extern gesteuert werden. Die Verbindung zwischen App und Sicherheitslösung ist maximal gegen Angriffe von außen geschützt. GIT

Telenot
www.telenot.com

Produkthighlights von Assa Abloy auf der Light + Building 2026

Die Light + Building 2026 macht unter dem Motto „Be Electrified – Electrifying Places. Illuminating Spaces.“ zukunftsweisende Trends erlebbar. Assa Abloy zeigt an ihrem Messestand, wie mit intelligenten, vernetzten und bedienfreundlichen Zugangslösungen und Rettungswegtechnik die Gebäude von heute zukunftssicher in eine neue Generation der Smart Buildings gewandelt werden.

Für höheren Nutzerkomfort erlaubt das neue Bedientableau 925-Touch die komfortable Anzeige und das intuitive Bedienen von bis zu 24 Fluchttüren oder Gruppenfunktionen

Mit der Produktlinie ePED (electrically controlled Panic Exit Device) zeigt das Unternehmen, dass hochfunktionale Rettungswegtechnik auch ästhetisch überzeugen kann. Mittelpunkt des Messeauftritts ist das kompakte ePED Display-Türterminal, das alle wesentlichen Steuerungsfunktionen – Schlüsselschalter, Not-Auf, beleuchtetes Fluchtrichtungspiktogramm und die Anzeige von Zeitverzögerungen – in einem übersichtlichen, handgroßen Display vereint.

Vernetzung, Sicherheit und digitale Gebäudesteuerung gehören zu den Kernthemen der Light + Building. Mit Scala präsentiert der Hersteller eine Lösung, die genau dafür entwickelt wurde und einfache Bedienbarkeit mit modularer Erweiterbarkeit verbindet. Für kleinere Objekte wie Büros, Praxen oder Kanzleien bietet die 1-Tür-Lösung Scala solo einen unkomplizierten Einstieg in die digitale Zutrittskontrolle ohne IT-Vorkenntnisse, während Scala offline die Verwaltung drahtloser Aperio-Beschläge und -Zylinder über eine intuitive Windows-Applikation ermöglicht – ganz ohne Verkabelung oder aufwendige Installation.

Mit der Zutrittskontrolllösung Scala net ist auch die Verwendung der drahtlosen Funk-Komponenten von Aperio möglich. Diese lassen sich unkompliziert anstelle mechanischer Schließlösungen einbauen und können anschließend per Funk-Hub oder offline in die Zutrittskontrollanlage integriert werden

Light + Building: Halle 12.1, Stand E80
www.assaabloy.com/de

Die Planung von Schließtechnikanlagen ist ein komplexer Vorgang, den Dom mit seinen digitalen Plattformen erleichtert und beschleunigt

Nima Hooshyar, Produktmanager für Zylindersysteme und Webtools bei Dom

Suraj Parmar, Group IT-Manager bei Dom

SCHLIESSTECHNIK

Meister der Schlüsselplanung

Digitale Plattform zur Planung komplexer Schließanlagen

Die digitalen Plattformen von Dom Security sollen die Interaktion von Schlüsseldiensten und Sicherheitsexperten mit Dom-Produkten verändern. Wie das aussieht, erläutern Group IT-Manager Suraj Parmar und Nima Hooshyar, Produktmanager für Zylindersysteme und Webtools bei Dom, im Interview.

Herr Parmar, Herr Hooshyar, für alle die eNet und den Master Key Planner nicht kennen: Worum geht es dabei?

Suraj Parmar: eNet ist unsere digitale Plattform, die als zentraler Kontaktpunkt für Kunden dient. Sie ist modular aufgebaut und kann an spezifische Marktanforderungen angepasst werden. Der Master Key Planner (MKS Planner) unterstützt Kunden bei der Planung und Bestellung komplexer Schließanlagen.

Nima Hooshyar: Der Master Key Planner vereinfacht den Bestellprozess. Er automatisiert viele Aufgaben, optimiert Abläufe und minimiert Fehler. Früher mussten Planungen per E-Mail oder Papier übermittelt werden, jetzt geben Kunden alles direkt im Planner ein und der Auftrag geht sofort in die Produktion.

Und das funktioniert über Ländergrenzen hinweg . . .

Nima Hooshyar: 85 Prozent unserer Kunden sind bereits registriert. Sie schätzen die einfache Anwendung und die zentrale Verwaltung.

Suraj Parmar: Jedes Land hat seine eigene Version, zugeschnitten auf lokale Bedürfnisse, während das Kernsystem gleich bleibt.

Wie kam es zur Entwicklung des Master Key Planners?

Nima Hooshyar: Kunden wünschten sich ein Onlinetool statt des Excel-Plans. Mit dem Planner können sie jederzeit bestellen – auch am Wochenende.
Suraj Parmar: Der Planner gibt den Kunden mehr Kontrolle, zeigt Konfiguration und Preis direkt an und beschleunigt die Prozesse.

Ist der Master Key Planner auch für technische Laien leicht anzuwenden?

Suraj Parmar: Ja, er ist für alle konzipiert, die Schließanlagen planen, ohne IT-Experten zu sein.
Nima Hooshyar: Das Design ist modern und einfach. Nutzer können zwischen klassischer Ansicht und neuer Oberfläche wählen.

Wie sieht der Bestellprozess aus?

Nima Hooshyar: Kunden richten Projekte ein, wählen Schlüsselprofile und fügen Zylinder hinzu. Das System führt sie Schritt für Schritt und zeigt den Preis sofort an.

Schließzylinder und Schlüssel von Dom

Suraj Parmar: Bestellungen werden direkt in die Produktion übermittelt. Fast-Lane-Bestellungen sind in Deutschland innerhalb von fünf Tagen ausgeliefert.

Ist der Master Key Planner im Fast-Lane-Service integriert?

Suraj Parmar: Ja, Bestellungen, die den Kriterien entsprechen, werden automatisch gekennzeichnet und direkt verarbeitet.
Nima Hooshyar: Kunden sehen sofort, welche Artikel verfügbar sind und wann die Lieferung erfolgt.

Was ist als Nächstes geplant?

Nima Hooshyar: Die Erweiterung bestehender Schließanlagen sowie die Bestellung von Ersatzzylindern soll ebenfalls über den DOM Master Key Planner möglich sein.
Suraj Parmar: Wir planen die Einführung in weiteren Ländern, Automatisierung von Schlüsselbestellungen und Integration von Tapkey-Lizenzen. GIT

Dom Sicherheitstechnik
www.dom-security.com

© Bilder: Dom Sicherheitstechnik

Intelligente Instandhaltung von Videosicherheitslösungen

Bosch Building Technologies bietet Kunden von Videosicherheitslösungen einen neuen digitalen Service, der die Systemverfügbarkeit deutlich steigert. Gleichzeitig profitieren Betreiber von Effizienzgewinnen im Betrieb. Hierfür vereint der Nexospace Video System Explorer, der in drei Service-Modulen erhältlich ist, intelligentes Monitoring mit Remote-Diagnosen und Cybersecurity-Funktionen.

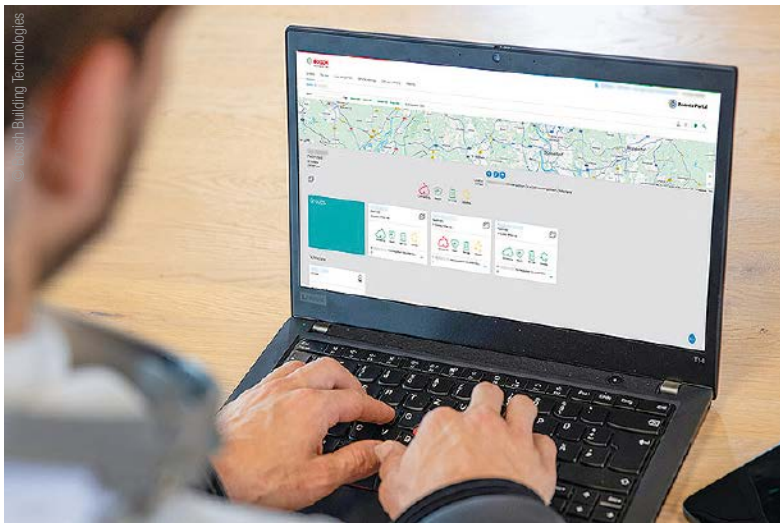
Kunden von Bosch Building Technologies können entsprechend ihren spezifischen Anforderungen zwischen den Service-Modulen Basic, Advanced und Premium wählen. Das Basic-Modul beinhaltet den sicheren Remote-Zugang zu einem zentralen Dashboard, das Mitarbeitern des Kunden Einblick in Kameras, Aufzeichnungen und Systemstatus bietet und über das Bosch Building Technologies remote unterstützen kann.

Auch im Basic-Modul enthalten ist ein Störungsmanagement durch die zertifizierte 24/7-Serviceleitstelle von Bosch. Das Advanced-Modul enthält ergänzend regelmäßige proaktive System- und Kamera-Funktionsprüfungen sowie Remote-Inspektionen durch Bosch Building Technologies. Hierdurch wird ein sicherer Betrieb der Videosystem-Infrastruktur gewährleistet. Das Premium-Modul schließt zusätzlich den Vor-Ort-Service für erforderliche Reparaturen mit ein.

Ein Systemausfall, eine unzureichende Systempflege oder Cyber-Schwachstelle können weitreichende Folgen haben: von Datenverlust über die Nichteinhaltung gesetzlicher Vorgaben bis hin zu erheblichen finanziellen Einbußen. Der Nexospace Video System Explorer begegnet diesen Herausforderungen mit einem umfassenden Schutzkonzept: Regelmäßige Updates sowie System- und Kamera-Funktionsprüfungen, die im Advanced- und Premium-Modul enthalten sind, minimieren IT-Risiken und schützen proaktiv vor Cyberangriffen und Datenlecks.

Diese integrierten Sicherheitsmaßnahmen tragen zur Robustheit der Infrastruktur bei und gewährleisten eine dauerhaft hohe Verfügbarkeit sowie die zukunftssichere Betriebsbereitschaft der Videosysteme. Die Lösung unterstützt vollständig die Anforderungen aus der DSGVO und dem Cyber Resilience Act (CRA). Besonders in kritischen Infrastrukturen, wo Ausfälle schwerwiegende Folgen haben können, sorgt das Monitoring für die Einhaltung von Normen wie DIN EN 62676 und VdS-Richtlinien. Der Nexospace Video System Explorer kann von Kunden genutzt werden, die ein Videosystem von Bosch mit DIVAR IP und installiertem Bosch-Videomanagementsystem (BVMS) haben.

www.bosch.com



© Bosch Building Technologies

PHYSISCHE SICHERHEIT

So geht es weiter

Genetec wirft einen Blick auf die physische Sicherheitsbranche im Jahr 2026

Unternehmen, so die Prognose des Softwareanbieters für physische Sicherheit Genetec, werden sich auf Flexibilität, verantwortungsbewusste KI und einheitliche, vernetzte Systeme konzentrieren, um die Sicherheit und die Betriebsleistung zu verbessern.

Im Jahr 2026 wird nach der Einschätzung von Genetec die Diskussion um die Einführung der Cloud weiter reifen. Unternehmen werden Lösungen priorisieren, die Flexibilität und Skalierbarkeit bei der Bereitstellung bieten. Anstatt sich auf ein einziges Bereitstellungsmodell festzulegen, werden sie jede Arbeitslast anhand der Anforderungen an Leistung, Kosten und Datenresidenz bewerten. Anschließend wählen sie die Umgebung, die ihre betrieblichen Anforderungen am besten unterstützt – sei es vor Ort, in der Cloud oder ein hybrider Ansatz.

Offene Architekturlösungen ermöglichen es Endnutzern, die Geräte und Anwendungen auszuwählen, die ihre Arbeitsabläufe am besten unterstützen. Dieser Ansatz verlängert die Lebensdauer der bestehenden Infrastruktur und ermöglicht es Teams, Cloud-Dienste dort einzusetzen, wo sie den größten Mehrwert bieten. Anbieter, die umfassende Bereitstellungsoptionen und eine starke Interoperabilität zwischen verschiedenen Umgebungen bieten, sind am besten positioniert, um diese Erwartungen zu erfüllen. Im Gegensatz zu proprietären Systemen, die die Auswahl einschränken und eine Bindung an einen Anbieter schaffen, bieten offene Lösungen einen anpassungsfähigeren Weg, der langfristige Flexibilität und Kontrolle ermöglicht.

KI: Vom Hype zur intelligenten Automatisierung

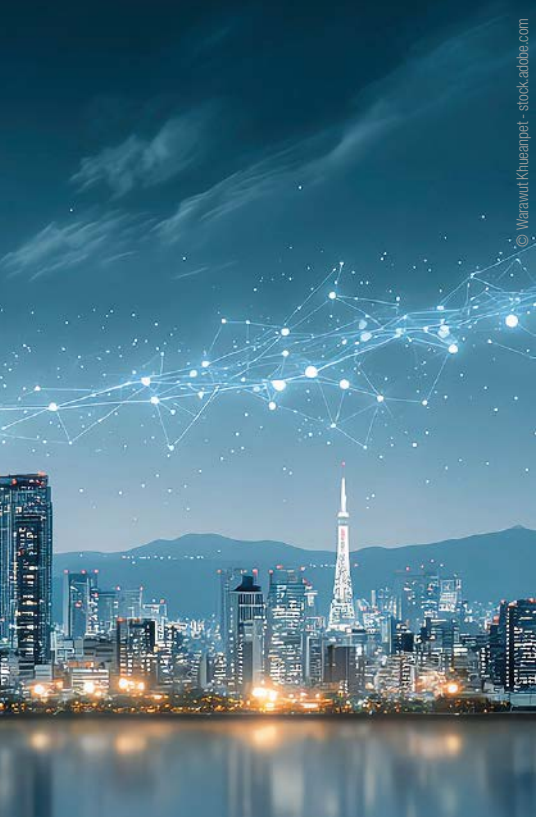
Die Diskussion werde vom Hype um KI und LLM zu praktischen, ergebnisorientierten Lösungen für intelligente Automatisierung (IA) übergehen. IA wird Arbeitsabläufe rationalisieren, die Genauigkeit verbessern und schnellere, intelligentere Entscheidungen ermöglichen. IA wird zunehmend repetitive Aufgaben automatisieren, die Überwachungsgenauigkeit verbessern, vorausschauende Wartung unterstützen und aussagekräftige Erkenntnisse aus wachsenden Datenmengen gewinnen.

Anstatt Technologie um ihrer selbst willen einzusetzen, werden sich die Nutzer auf Funktionen konzentrieren, die den täglichen Betrieb wirklich verbessern. Beispiele hierfür sind die intelligente Suche zur Beschleunigung von Untersuchungen, die Reduzierung von Fehlalarmen und die Stärkung des Situationsbewusstseins. Durch die Optimierung der Reaktionszeiten und die Reduzierung des manuellen Aufwands ermöglicht IA den Nutzern, ihre Zeit und Energie auf wichtige Arbeiten und Entscheidungen zu konzentrieren, die menschliches Urteilsvermögen erfordern.

Mit zunehmender Reife des Marktes werden die Erwartungen an Transparenz und verantwortungsvolle Umsetzung steigen. Die Nutzer werden Klarheit darüber verlangen, wie KI eingesetzt wird, wie Systeme aufgebaut sind und wie Daten gesammelt, verarbeitet und geschützt werden. Sie werden auch erwarten, dass Anbieter der Cybersicherheit Priorität einräumen und sicherstellen, dass KI-Funktionen auf sichere, kontrollierte und verantwortungsvolle Weise eingesetzt werden. Unternehmen werden sich von Innovationen um der Innovation willen abwenden und stattdessen messbare, vertrauenswürdige und sinnvolle Ergebnisse liefern, die durch intelligente Automatisierung ermöglicht werden.

Modernisierung der Zutrittskontrolle

Die Zutrittskontrolle wird nach der Prognose von Genetec auch weiterhin höchste



Priorität haben, da Unternehmen ihre veralteten Systeme modernisieren und sich auf die Maximierung des ROI konzentrieren. Der Wert der Zutrittskontrolle geht jedoch weit über das Ver- und Entriegeln von Türen hinaus. Er liefert messbare Geschäftsergebnisse in Form von Energieeffizienz, Belegungsmanagement und betrieblichen Erkenntnissen.

Die Einführung von Zutrittskontrolle-as-a-Service (ACaaS) wird sich beschleunigen, da Unternehmen Wert auf einfachere Wartung, größere Skalierbarkeit und vorhersehbare Betriebskosten legen. Unternehmen werden hybride Bereitstellungen bevorzugen, die lokale und Cloud-Funktionen kombinieren. Durch die Vereinheitlichung von ACaaS und Videomanagement-as-a-Service (VSaaS) wird sich die Transparenz weiter verbessern und die Verwaltung über Standorte hinweg optimieren lassen.

Vernetzte Systeme

Im Laufe des nächsten Jahres wird die Zahl der vernetzten Geräte weiter steigen, da Unternehmen IoT-Sensoren, Gebäudesysteme und intelligente Geräte in einheitliche Sicherheits- und Betriebsplattformen integrieren werden. Durch die Zusammenführung dieser Informationen an einem Ort erhalten Teams einen klareren Überblick über die Vorgänge in ihren Einrichtungen und können schneller und sicherer reagieren.

Die Konvergenz von IT, Betriebstechnik und physischer Sicherheit wird sich beschleunigen und den Austausch von Daten in Echtzeit sowie intelligentere Entscheidungen in allen Einrichtungen ermöglichen. Endnutzer werden offene, skalierbare Plattformen erwarten, die verschiedene Geräte sicher miteinander verbinden und einen betrieblichen sowie sicherheitstechnischen Mehrwert bieten.

Da die Landschaft immer komplexer wird, werden Unternehmen nach Anleitungen suchen, wie sie die richtigen Technologien einsetzen und effektiv verwalten können. In diesem Bereich werden diejenigen führend sein, die verschiedene Geräte sicher vereinen, Cloud-native und hybride Optionen anbieten sowie Cybersicherheit und Datenresidenz in ihr Design integrieren. GIT

Genetec
www.genetec.de

Domera Dome-Kameras mit Edge Analyse

Mit den Dome-Kameras der Serie RDF6100DN erweitert Dallmeier die erfolgreiche Domera Produktfamilie. Die neue Modellreihe zeichnet sich insbesondere durch ihre Edge Analyse-Fähigkeit, erweiterte Sicherheitsfunktionen und ein attraktives Preis-Leistungs-Verhältnis aus.

Die Kameras dieser Serie wurden speziell für Anwendungen entwickelt, bei denen es auf ein ausgewogenes Verhältnis von Funktionalität und Wirtschaftlichkeit ankommt. Als leistungsstarke Einstiegslösung innerhalb der Domera Produktfamilie bieten sie hohe Auflösung und Lichtempfindlichkeit. In Verbindung mit moderner Encoder-Technologie und ausgefeiltem Bild-Processing ermöglichen sie brillante Echtzeit-Aufnahmen mit hoher Farbtreue und exzellentem Kontrast. Die adaptive IR-Beleuchtung sorgt auch bei Dunkelheit für optimale Szenenausleuchtung, ohne störende Reflexionen.

Dank der PTRZ-Funktion, bei Dallmeier RPoD (Remote Positioning Dome) genannt, lassen sich die exakte Ausrichtung der Kamera sowie Zoom, Fokus und Blende bequem über das Netzwerk konfigurieren – ohne mechanische Eingriffe vor Ort. Das reduziert nicht nur den Aufwand bei der Erstinstallation, sondern vereinfacht auch spätere Anpassungen bei veränderten Anforderungen. Die Möglichkeit zur Fernjustierung senkt Personal- und Betriebskosten, verkürzt Projektlaufzeiten und entlastet Fachkräfte von zeitraubenden Routineaufgaben – ein weiterer Beitrag zur Gesamtwirtschaftlichkeit der Lösung.

Die Kameras bieten AI-Fähigkeit auf Basis eines neuronalen Netzes zur Objektklassifikation. Diese analysieren das Geschehen im Bild in Echtzeit und erkennen zuverlässig relevante Objekte wie Personen oder Fahrzeuge – selbst bei bewegtem Hintergrund (z. B. Grünanlagen, Wasserflächen) oder komplexen Szenen. Typische Einsatzmöglichkeiten sind etwa Intrusion, Counting, Parking oder Loitering. Die intelligenten Funktionen unterstützen Sicherheitsteams dabei, schneller zu reagieren, Ereignisse gezielter auszuwerten und Prozesse effizienter zu gestalten.

Das Unternehmen verfolgt bei der Entwicklung seiner KI-Technologien auch einen eigenen Ansatz: Die neuronalen Netze werden auf einem firmeneigenen Testgelände unter realen Bedingungen trainiert. Dadurch bleiben sowohl die Trainingsdaten als auch die Netzwerke selbst unter ständiger Kontrolle. Dieser Ansatz stellt sicher, dass die KI-Funktionen der Kameras zuverlässig, nachvollziehbar und praxisnah arbeiten – so schafft Dallmeier die Grundlage für vertrauenswürdige Technologien „Made in Germany“.

Mit der RDF6100-Serie unterstreicht Dallmeier seinen hohen Anspruch an IT- und Cybersecurity. Die Kameras bieten erweiterte Sicherheitsfunktionen, wie die Unterstützung von Secure Boot: Nur das signierte Domera OS-Betriebssystem kann gestartet werden, was Manipulationen durch Rootkits oder Malware effektiv verhindert. Zusätzlich sind die Kameras mit Trusted Platform Module (TPM 2.0) ausgestattet und erfüllen damit die Anforderungen an die FIPS 140-Konformität.

FIPS 140 ist ein vom National Institute of Standards and Technology (NIST) herausgegebener Standard, der insbesondere für US-amerikanische Behörden vorgeschrieben ist. Die strengen Vorgaben gewinnen aber auch international zunehmend an Bedeutung, insbesondere bei Ausschreibungen in sensiblen Bereichen.

Mit den RDF6100DN Dome-Kameras bietet das Unternehmen eine leistungsstarke Lösung für professionelle Anwendungen, bei denen Wirtschaftlichkeit, Bildqualität, KI-gestützte Analyse und höchste IT-Sicherheit gleichermaßen gefragt sind. **www.dallmeier.com**

Cybersicherheit strategisch angehen

Mit NIS-2-konformer Datenspeicherung

NIS-2 zwingt die betroffenen Unternehmen dazu, ihre Maßnahmen in puncto IT-Sicherheit auf den neusten Stand zu bringen und gegebenenfalls zu erweitern. Ein wichtiger Aspekt, den Verantwortliche dabei im Blick behalten sollten: Das Thema Datenspeicher und Backups.

Alles scheint normal zu laufen, doch plötzlich geht nichts mehr: Kein Zugriff mehr auf Ordner, fehlender Zugang zu verschlüsselten Daten – ein einfacher Angriff, aber die gesamte Infrastruktur steht still, als hätten die Hacker den Stecker gezogen. Szenen wie diese will niemand erleben – schon gar nicht im eigenen Unternehmen. Gleichzeitig steigt aber die Wahrscheinlichkeit, dass sich ein solcher Moment so oder so ähnlich ereignet – das zeigen unter anderem die Zahlen des aktuellen Bundeslagebild Cyberkriminalität. Um solchen Cyberangriffen auf kritische Infrastrukturen und dem auf sie folgenden Chaos vorzubeugen, hat die EU die NIS-2-Richtlinie zur Netz- und Informationssicherheit erlassen. Im Vergleich zur bisherigen NIS-Richtlinie erweitert NIS-2 den Anwendungsbereich und verschärft die Anforderungen. Unternehmen verschiedenster Branchen, insbesondere solche mit kritischen Dienstleistungen, müssen sicherstellen, dass ihre IT-Sicherheitsstrategien höchsten Standards entsprechen. Dies erfordert umfassende Investitionen in Cybersecurity-Lösungen und die Etablierung eines robusten Datenmanagements.

Die NIS-2-Richtlinie umfasst dabei wesentliche Neuerungen:

1. Erweiterter Anwendungsbereich: Neben den klassischen Sektoren wie Energie und Transport umfasst NIS-2 nun auch Gesundheitswesen, Banken und digitale Infrastruktur.

2. Strengere Meldepflichten und Reaktionszeiten: Sicherheitsvorfälle müssen schnellstmöglich gemeldet und entsprechende Maßnahmen ergriffen werden, um weitere Schäden zu verhindern.

3. Erhöhte Bußgelder und Haftung: Verfehlungen können für Unternehmen hohe Geldstrafen und für Führungskräfte persönliche Haftung bedeuten.

Die Richtlinie verfolgt das Ziel, die gesamte EU besser gegen Cyberangriffe zu wappnen und die Abwehrkraft durch gemeinsame Standards und eine engere Zusammenarbeit der Mitgliedsstaaten zu steigern. Für Unternehmen bedeutet das, dass ihre Cybersecurity-Strategien und -Infrastrukturen den Vorgaben entsprechen müssen und sie dafür Sorge tragen sollten, die neuen Regularien möglichst reibungslos in ihre bestehende Sicherheitsstrategie einzubetten. Dafür haben Verantwortliche nicht mehr unendlich Zeit. Zwar konnte der ursprüngliche Zeitplan für die Umsetzung der NIS-2-Richtlinie in nationales Recht nicht eingehalten werden, zum Frühjahr 2025 werden Betriebe aber voraussichtlich NIS-2-konform sein müssen.

Datenarchive als Angriffsziel: Regeln für NIS-2-konforme Cybersecurity

Daten sind das Herzstück moderner Unternehmen und das Hauptangriffsziel von Cyberkriminellen. Dabei geraten auch Datenarchive und Backups zunehmend mehr unter Beschuss – denn sie erhalten sensible und für den Geschäftsbetrieb kritische Informationen. Dabei dienen Datenarchive als wertvolle Ressourcen in Unternehmen nicht nur als Angriffsziel, sondern auch als Hebel für die Erpressung – in Form von Ransomware oder Datendiebstahl. Die Angreifer drohen dabei, die gestohlenen Daten zu

veröffentlichen oder Systeme lahmzulegen und bringen damit den Ruf und die finanziellen Strukturen von Unternehmen massiv in Gefahr. Wer also im Zuge der Vorbereitung auf NIS-2 die eigenen IT-Sicherheitsstrategien überprüft, sollte dabei auch auf Archive und Backups und deren Absicherung blicken und Backups als strategische Komponente von Cybersicherheit verstehen. Denn: Kommt es zum Cybervorfall, sorgt ein gesichertes Backup auch dafür, den Regelbetrieb zügig wiederherzustellen.

Zudem sieht auch NIS-2 vor, dass Unternehmen im Bereich Datenspeicherung und -management besondere Maßnahmen ergreifen. Dabei sollten diese Aspekte berücksichtigt werden:

- Daten schützen: Unternehmen müssen sicherstellen, dass ihre Maßnahmen zur Speicherung und Verarbeitung von Daten sowohl die Sicherheit als auch die Unversehrtheit der Daten gewährleisten.
- Daten archivieren: Organisationen sollten ihre Richtlinien zur Datenaufbewahrung regelmäßig überprüfen und gegebenenfalls anpassen, um sicherzustellen, dass Daten nur so lange wie nötig aufbewahrt werden und während dieser Zeit sicher gespeichert sind.
- Daten übertragen: Für Unternehmen mit globaler Präsenz umfasst die NIS2 auch die Anforderungen für grenzüberschreitende Datenübertragungen. Sie müssen sicherstellen, dass sie die Sicherheitsvorgaben aller relevanten Rechtsordnungen einhalten und ihre Datenmanagementpraktiken den internationalen Standards für Datensicherheit entsprechen.

Erfolgsfaktoren leistungsstarker Datenspeicherung

Wer also nun das Momentum nutzen und eine sichere und zugleich leicht zugängliche Archivlösung etablieren will, sollte darauf achten, dass die gewählte Softwarelösung im Bereich Datenspeicher unbedingt einige Kernaspekte erfüllt. Dazu gehören:

1. Robuste Speicherung und schnelle Wiederherstellung: Die gewählte Lösung sollte es erlauben, Daten sicher zu speichern und im Ernstfall schnell wiederherzustellen. So wird der Geschäftsbetrieb stabilisiert und die Verluste durch Ausfallzeiten minimiert. Möglich wird dies beispielsweise durch synchrone Mehrfachreplikation. Sie dient als Schutz gegen Hardware Defekte oder Elementarschäden mit nahtloser, aktiv-aktiv Bereitstellung an zwei oder mehr Standorten. Zusätzlich kann mittels asynchroner Replikation, aktiv-passiv über weite Distanzen an zusätzlichen Standorten gespeichert werden, die räumlich weiter voneinander entfernt sind. Fällt der primäre Standort aus, erfolgt entweder ein automatisches oder manuelles Failover zu einem weiteren Standort. Ist die Gefahr gebannt, können die Daten wieder synchronisiert werden. Außerdem sollten regelmäßige Backups, Snapshots und kontinuierliche Datenprotokollierung (CDP) Teil des Leistungsportfolios sein.

2. Regelmäßiges Testing, auch im laufenden Betrieb: Um Sicherheitslücken erst gar nicht entstehen zu lassen, sollte die Lösung Data-Recovery-Tests während des normalen Betriebes unterstützen.

3. Anomalieerkennung und Automatisierung: Die Lösung sollte in der Lage sein, verdächtige Aktivitäten frühzeitig zu erkennen und viele Prozesse der Wiederherstellung automatisiert durchzuführen. So können Cyberattacken effektiver abgewehrt werden.

4. Sicherheits- und Datenintegrität: Die gewählte Lösung sollte sicherstellen können, dass archivierte Daten unveränderlich und vor Manipulationen geschützt sind. Das gelingt beispielsweise durch Verschlüsselung der Daten im Ruhezustand und während der Übertragung über SSL. Hier besteht – je nach Angebotsumfang – auch die Chance, dass die gewählte Lösung gleichzeitig für die Einhaltung von FIPS 140-2 sorgen kann. Außerdem sollten Sicherheitsmaßnahmen wie rollenspezifische Zugangskontrollen und Authentifizierung oder Erfassung von Datenmanipulation durch Logging und Hashing für umfassende Sicherheit und Datenintegrität sorgen.

5. Nutzungsfreundlichkeit: Die beste Lösung nützt nichts, wenn sie nicht tagtäglich verwendet wird. Deshalb sollten Verantwortliche bei der Auswahl einer passenden Softwarelösung für ihre Datenarchive darauf achten, dass diese mit einer intuitiven Bedienoberfläche, hoher Kompatibilität mit anderen Systemen und einem übersichtlichen Dashboard punktet.

Unternehmen langfristig für die Zukunft wappnen

Mit der NIS-2-Richtlinie betritt die EU ein neues Zeitalter der Cybersicherheit. Diese ist dabei keineswegs ein Schönwettergesetz, sie ist ein Regelwerk, das IT-Sicherheitsstrategien zwingend aufrüstet, so als ob jedes Unternehmen permanent unter Beschuss stünde. Die passende Cybersecurity-Lösung bietet hier eine wertvolle Unterstützung, indem sie Datenarchive als integralen Bestandteil der Sicherheitsstrategie positioniert, eine schnelle Wiederherstellung nach Angriffen ermöglicht und durch eine benutzerfreundliche, zentrale Infrastruktur die kontinuierliche Einhaltung der NIS-2-Vorgaben gewährleistet. Unternehmen profitieren von einer sicheren Datenumgebung, die die Einhaltung gesetzlicher Vorgaben vereinfacht und dabei hilft, ihre kritischen Geschäftsprozesse gegen die zunehmenden Cyberbedrohungen abzusichern. GIT

Autor:
Alexander Best
Senior Director
Product Management

DataCore Software GmbH
www.datacore.com/de

Ein Strategiespiel

Die drei Säulen der Cyberresilienz

Cybersicherheit war gestern, heute brauchen Unternehmen Resilienz. Die baut auf den drei Säulen Sicherheit, Krisenmanagement und einer unbedingten Nachbearbeitung eines jeden Vorfalls auf. Ein Beitrag von Alexander Bogocz, Cyber-Incident-Experte bei Skaylink.

Alexander Bogocz,
Cyber-Incident-Experte bei Skaylink

Ein aktuelles Beispiel aus dem Gesundheitssektor Ende 2024 zeigt vorbildliches Verhalten: In einem deutschen Krankenhaus wurde an einem Sonntag ein IT-Sicherheitsvorfall bemerkt und es wurden sofort Maßnahmen ergriffen. Zunächst ging die klinikeigene IT ans Werk, die später einen externen Dienstleister an Bord geholt hat. Der Klinikbetrieb und vor allem die Patientenversorgung waren zu jedem Zeitpunkt gewährleistet. Das wurde bekannt, weil der Vorfall umgehend kommuniziert wurde. Aus ermittlungstaktischen Gründen erfolgte die Kommunikation kurz und knapp, weil die Klinik eng mit den zuständigen Behörden zusammengearbeitet hat.

Dieses Beispiel eines Cybervorfalls ist deshalb so positiv, weil es gleich eine ganze Reihe von Dingen zeigt. Erstens sind Angriffe auf die IT mittlerweile alltäglich, da sie jede Organisation unabhängig von der Branche oder ihrer Größe treffen können. Und da es keine hundertprozentige Sicherheit gibt, ist es für Unternehmen essenziell, sich auf einen möglichen Angriff vorzubereiten. Und genau das hat die betroffene Klinik gezeigt. Es gab offensichtlich einen Plan für den Ernstfall, externe Dienstleister, auf die die IT sofort zurückgreifen konnte, und auch eine Kommunikationsstrategie. Wenn die Frage ist, was mit dem Begriff Cyberresilienz gemeint ist, dann kann das Klinikum als positives Beispiel genannt werden.

Resilienz braucht eine Strategie

Wenn heute von Resilienz die Rede ist, geht es darum, Cybersicherheit ganzheitlich zu denken. Dazu gehört, das Sicherheitsniveau im Unternehmen permanent zu verbessern. Firewall, Multifaktorauthentifizierung, Verschlüsselungen, regelmäßige Patches und Updates sowie Detection- und Intrusion-Prevention-Systeme sind Schlagwörter, die auch jenseits der IT-Abteilung alle Verantwortlichen gehört haben sollten.

Neben dieser robusten Sicherheitsinfrastruktur gehören aber auch eine schnelle und gezielte Reaktionsfähigkeit zur Cyberresilienz. Und als dritte Säule: eine ehrliche und offene Reflexion nach einem Vorfall, um daraus zu lernen.

Genauso wichtig ist es, die eigene Belegschaft regelmäßig zu schulen und Angriffe zu simulieren, um für den Ernstfall zu trainieren. Wichtig ist hier: Es geht nicht darum, jemanden vorzuführen, sondern wirkliche Schwachstellen aufzudecken. Denn genauso wie Unternehmen Geld in die Cyberabwehr investieren, wird auch die Gegenseite stetig besser und effizienter. Deshalb sollten Unternehmen ihre Mitarbeiter über neue Social-Engineering-Taktiken oder Angriffsmethoden informieren. Denn nur wenn die Mitarbeitenden wissen, worauf sie achten oder wonach sie Ausschau halten müssen, können sie Angriffe verhindern oder zumindest rechtzeitig entdecken.

Neuralgische Punkte

Unser Compromise-Recovery-Team wird nicht nur von Kunden, sondern auch von Versicherungen oder Forensikern angefordert, um „zu retten, was zu retten ist“. Und das ist in der Regel deutlich mehr, als

man zunächst vermuten möchte. Wenn wir allerdings gerufen werden, war ein Angriff bereits erfolgreich. Müssten wir eine zentrale Gemeinsamkeit aus den diversen Einsätzen ziehen, dann die: Die wenigsten Unternehmen kennen ihre Schmerzpunkte.

Einerseits verständlich: Wer hört schon gerne von den eigenen Schwächen? Unangekündigte Angriffssimulationen oder Pentests können jedoch entscheidend dazu beitragen, Einfallstore zu schließen. Denn was die Verantwortlichen in den Unternehmen nicht außer Acht lassen dürfen: Letztendlich ist Cybersecurity immer auch ein Strategiespiel. Dabei dürfen sie nicht unterschätzen, wie hochprofessionell und gut ausgestattet die Angreifer sind. Deshalb ist es auch so wichtig, Bedrohungen möglichst früh zu erkennen. Hier können Unternehmen mittlerweile auf KI setzen, die mit einer Anomalie-Erkennung und Endpoint Detection and Response dabei unterstützt, verdächtige Aktivitäten zu finden.

Schnelle Handlungsfähigkeit entscheidend

Um noch einmal auf das genannte Beispiel aus dem Gesundheitssektor zurückzukommen: Die schnelle Handlungsfähigkeit ist das, was an diesem Beispiel positiv hervorsticht. Denn einen Notfallplan in der Schublade zu haben, ist das eine, handlungsfähig zu bleiben, etwas ganz anderes. Aber was zählt, wenn es doch ein Angreifer ins System schafft: Diesen schnellstmöglich auszuschließen und anschließend genauso schnell wieder handlungsfähig zu sein – oder noch besser: zu bleiben. Letzterer Aspekt ist eine der Kernkompetenzen von Compromised-Recovery-Teams und doch erleichtern Reaktions- und Krisenmanagementpläne im Unternehmen unsere Aufgabe immens.

Neben den technischen Maßnahmen ist auch die Kommunikation unabdingbar. Um Vertrauen zu erhalten und Reputationsschäden zu vermeiden, sollten Unternehmen ihre Kunden, Partner und Mitarbeiter zeitnah und transparent über den Vorfall sowie die Gegenmaßnahmen informieren. Und auch hier zeigt das Beispiel: Unternehmen, die schnell und professionell reagieren, können die Auswirkungen eines Cyberangriffs deutlich reduzieren und die Stabilität ihrer Geschäftsabläufe gewährleisten.

Nach dem Vorfall ist vor dem Vorfall

Wenn bei einem Cybervorfall die richtigen Experten miteinander arbeiten und schnell zum Einsatz kommen, ist es möglich, die Schäden einzugrenzen. Genauso wichtig wie eine solch gut ausgebildete, schnelle Einsatztruppe ist die Aufarbeitung eines Vorfalls. Jeder Cybervorfall darf als eine Art „Lerngeschenk" betrachtet werden, das dazu beiträgt, die eigene Cyberresilienz zu verbessern. Jede Ebene – von der Sicherheitsarchitektur über das Krisenmanagement bis hin zur Nachbereitung – baut auf der vorherigen auf und sorgt dafür, dass Unternehmen den Herausforderungen des digitalen Zeitalters gewachsen sind. Und auch wenn der „Cyberwar" nur wenig Regeln kennt. Eines ist definitiv nicht erlaubt: Stillstand. GIT

Skaylink
www.skaylink.com

Energieautarke Kommunikationsnetze für Krisengebiete

Wie kann Kommunikation im Katastrophenfall funktionieren, wenn der Mobilfunk überlastet ist? Eine Antwort auf diese immer aktuellere Frage geben Forscher des Fraunhofer-Instituts für Angewandte Informationstechnik FIT. Ein mobiles, selbstorganisierendes, auf Fraunhofer-Technologie basierendes Kommunikationsnetz verbindet die Einsatzkräfte untereinander, mit der Einsatzleitung und dem Internet. Private 5G-Netze ermöglichen eine schnelle Wiederherstellung der Kommunikation – und das ganz unabhängig von klassischen Infrastrukturen. Im Katastrophenfall kommt es häufig zu massiven Netzausfällen. So war etwa bei der Ahrtalflut im Juli 2021 schnell das komplette Telefon- und Mobilfunknetz zusammengebrochen, da die Wasser- und Schlammmassen viele Vermittlungsstellen weggerissen hatten. Für solche Ernstfälle bieten Forscher des Fraunhofer FIT smarte Kommunikationslösungen für den Zivil- und Katastrophenschutz, um der Überlastung der öffentlichen Netze zu begegnen. Im Projekt 5G Opportunity entwickelten und erprobten sie mit den Projektpartnern der Friedrich-Alexander-Universität Erlangen-Nürnberg und der Hochschule Bonn-Rhein-Sieg ein softwarebasiertes, drahtloses und ad-hoc-fähiges Kommunikationssystem für Behörden und Organisationen mit Sicherheitsaufgaben (BOS). **www.fit.fraunhofer.de**

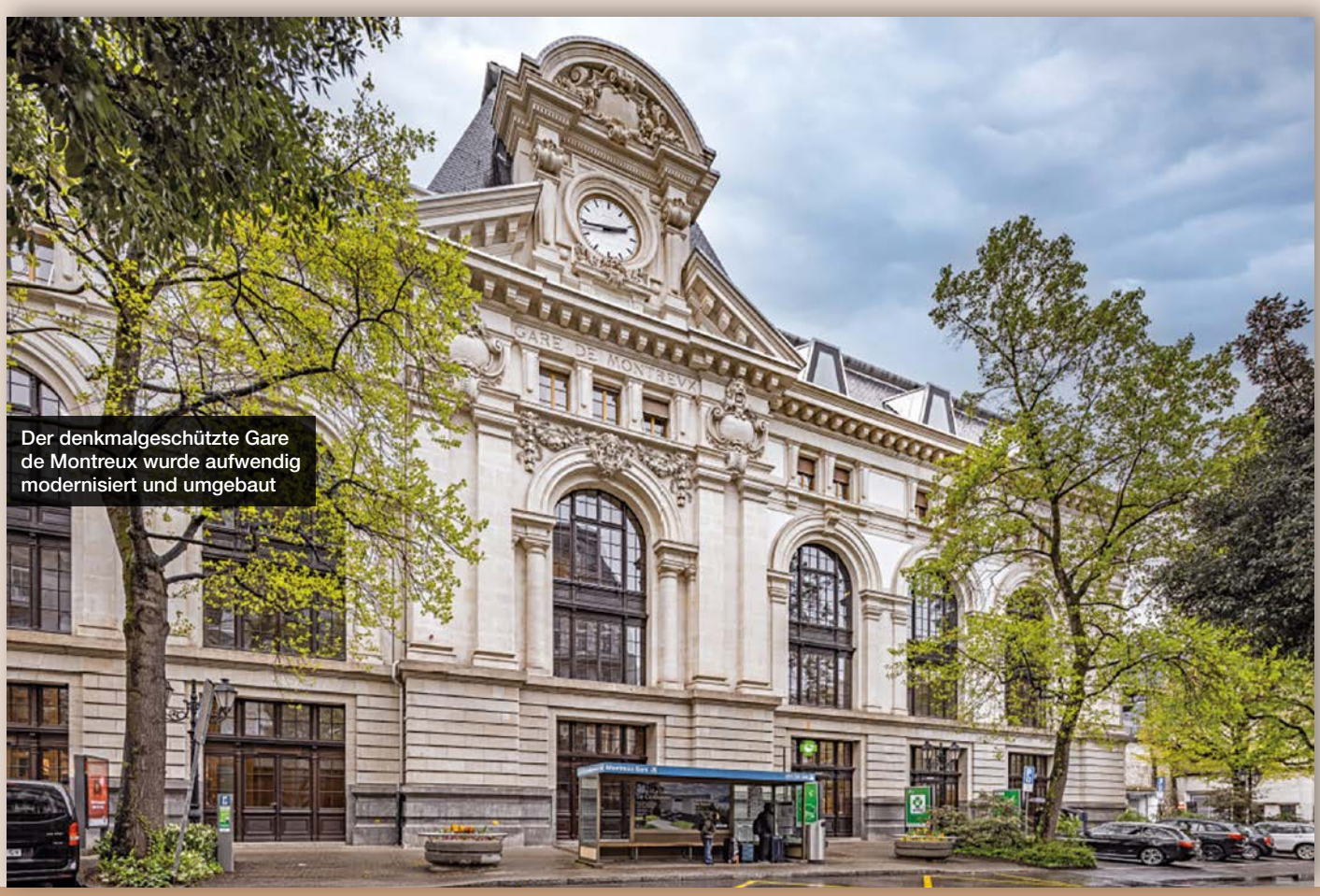
Portabler Antennenmast mit Wiback-Richtfunkantennen und 5G gNodeB

Cybersicherheit deutscher Universitäten verschlechtert sich

Das Nationale Forschungszentrum für angewandte Cybersicherheit Athene präsentierte die aktuellen Ergebnisse einer systematischen Langzeitanalyse zur Cybersicherheit deutscher Universitäten.

Im Forschungsausschuss des Bundestags fand ein Fachgespräch zur Forschungssicherheit statt. Laut BSI-Präsidentin Claudia Plattner befindet sich Deutschland in einer angespannten Bedrohungslage, in der die Forschungslandschaft ein hochattraktives Ziel darstellt. Die BSI-Präsidentin kritisierte, dass es derzeit kein gesamtstaatliches Lagebild über die Cybersicherheit im Forschungssektor gebe. Da der Hochschulsektor in die Zuständigkeit der Länder falle, sei eine einheitliche Erfassung erschwert.

Diese Lücke füllt der Athene-Forschungsbereich Science Shield, der unter Leitung von Athene-PI Prof. Dr. Haya Schulmann, Goethe-Universität Frankfurt, fortlaufend Daten zur Cybersicherheit im Forschungssektor erhebt und analysiert. Die konkret vorgestellte Studie betrifft 92 deutsche Universitäten. Analysiert wird, wie sich die von außen sichtbare IT dieser Universitäten seit 2023 veränderte und was diese Veränderungen für die Cybersicherheit der Universitäten bedeuten. Im Ergebnis zeigt sich eine teilweise dramatische Verschlechterung der Sicherheitslage. **www.sit.fraunhofer.de**



Der denkmalgeschützte Gare de Montreux wurde aufwendig modernisiert und umgebaut

KULTUR-/DENKMALSCHUTZ

Nächster Halt – Belle Époque

Brandschutzlösungen für den denkmalgeschützten Gare de Montreux

Der Schweizer Kur- und Ferienort Montreux am Genfer See begrüßt seine mondänen Gäste seit 1861 mit einem beeindruckenden, eleganten Bahnhofsgebäude im Stil des Historismus. 2017 wurde das denkmalgeschützte Bahnhofsgebäude umfassend modernisiert. Die Ausstattung des wichtigen Verkehrsknotenpunkts mit modernen Brandschutzlösungen war ein wichtiger Aspekt des Umbaus. Die Architekten des Büros Tempesta Tramparulo Architectes haben hier unter anderem auf Lösungen von Geze gesetzt.

Schon bei der Eröffnung galt der Gare de Montreux als technische und architektonische Meisterleistung: Weil der Bahnhof am Hang liegt, gelangen die Fahrgäste von der Empfangshalle über das zweite Obergeschoss zum Hausgleis, die anderen Gleise sind mittels Unterführung im ersten Obergeschoss erreichbar. Dadurch ist eine Architektur entstanden, die einige Herausforderungen an den Brandschutz stellt, sowohl technisch als auch im Design. Die Architekten von Tempesta Tramparulo Architectes entschieden sich für Fenstertechnik und Rauchwarnanlagen (RWA) von Geze, weil die sich einfach nachrüsten und installieren lassen und sich unauffällig in die denkmalgeschützte Architektur des Bahnhofs einpassen.

Natürliche Lüftung und RWA

Besonders beeindruckend sind die großzügigen Fensterfronten des Gare de Montreux: Ihr Lichteinfall ist prägend für Raumgefühl und Atmosphäre des Bahnhofs. Sie wurden mit dem „Powerchain“-Antrieb von Geze automatisiert. An besonders großen Fenstern wurde der Antrieb sogar bis zu 42-mal verbaut. Dieser sorgt dafür, dass die Fenster im Brandfall öffnen und überzeugt dabei besonders durch die Schnelligkeit, mit der er auch die großen und schweren Fenster bewegt. Für den Bahnhof von Montreux fertigte der Hersteller den Antrieb auch

Zahlreiche Fenster wurden mit Fenstertechnik von Geze ausgestattet

Der Kettenantrieb „Powerchain“ öffnet große und schwere Fensterelemente im Bahnhof

als Sonderausführung in der Farbe RAL 8014 Sepiabraun (Dunkelbronze).

Fenstersicherheit der höchsten Schutzklasse 4

Eine besondere Herausforderung im Gare de Montreux stellt nicht nur die Funktion der Fenster dar, sondern auch deren Positionierung. Da sich die automatisierten Fenster in für die Fahrgäste erreichbarer Höhe befinden, muss deren Sicherheit gewährleistet sein. Ohne zusätzliche Absicherung dürften diese kraftbetätigten Fenster sonst nicht betrieben werden.

In einer Immobilie mit Publikumsverkehr müssen die Fenster nach der Risikobewertung mit Fensterabsicherungen der höchsten Schutzklasse (Schutzklasse 4) ausgestattet werden. Die eingesetzte Technik muss sicherstellen, dass eine unsachgemäße Benutzung oder auch Unachtsamkeit nicht zu Verletzungen führt.

Alle automatisierten Fenster wurden deswegen mit einem Sicherheitsschaltmodul zur Absicherung der Gefahrenstellen an kraftbetätigten Fenstern ausgestattet. Die Geze IQ box Safety sichert die Haupt- und Nebenschließkanten ab. Die als Sicherheitssensoren eingesetzten Flatscans erkennen Fremdkörper und sorgen dafür, dass der Schließvorgang gestoppt oder die Bewegung umgekehrt wird. Der Mechanismus verhindert beispielsweise, dass Finger eingeklemmt werden.

Natürlicher Rauch- und Wärmeabzug

Neben der Systemlösung Powerchain-Flatscan-IQ box Safety wurden im Gare de Montreux auch neun Öffnungsantriebe RWA K 600 F sowie sechs Antriebe des Modells K 600 F+ Synchro installiert. Diese Klapphebelantriebe sorgen als Natürliches Rauch- und Wärmeabzugsgerät (NRWG) dafür, dass die Fenster im RWA-Fall in weniger als 60 Sekunden um 90° öffnen und einen schnellen Rauch- und Wärmeabzug gewährleisten. Dadurch werden Flucht- und Rettungswege rauchfrei gehalten. Auch hier konnte der Kundenwunsch nach einer Sonderanfertigung in der Farbe RAL 8014 Sepiabraun (Dunkelbronze) ermöglicht werden.

Hohe Beratungskompetenz

Neben den technischen und gestalterischen Möglichkeiten war auch die Erfahrung der Geze-Mitarbeiter im Bereich Modernisierung in historischen Gebäuden ein wichtiger Faktor für den Architekten Antonino Tramparulo, sich für den Anbieter aus Deutschland zu entscheiden: „Schon bei den ersten Entwürfen wurden wir über alle technischen Auswirkungen ihrer Produkte informiert. Es ist nicht einfach, mit technologischen Elementen an historischen Schreinerarbeiten aus dem Jahr 1909 zu arbeiten. Dank ihrer Erfahrung und Professionalität konnten wir diese Systeme unter den bestmöglichen Bedingungen integrieren und dabei die gesamte historische Substanz erhalten. Direkt nach Abschluss der Bauarbeiten wurden alle Geze-Produkte und Systeme bei mehreren Gelegenheiten gründlich getestet, sodass die Sicherheit der Nutzer gewährleistet ist.“ GIT

Geze GmbH
www.geze.de

Bilder: Lorenz Frey/Geze GmbH

Festliche Stimmung auf der 80-Jahr-Feier von Gloria

FEUERLÖSCHER

80 Jahre Gloria

Mit Pioniergeist in die Zukunft des Brandschutzes

In diesem Jahr blickt Gloria auf eine beeindruckende 80-jährige Erfolgsgeschichte zurück, die eng mit der Entwicklung des modernen Brandschutzes in Deutschland verknüpft ist. Was 1945 in der Nachkriegszeit unter schwierigen Bedingungen begann, hat sich zu einem international anerkannten Spezialisten für Brandschutzlösungen entwickelt.

Als Familienunternehmen gegründet, konzentrierte sich Gloria zunächst auf die Produktion und den Vertrieb von Feuerlöschern für den wachsenden Bedarf in der deutschen Nachkriegswirtschaft. Schon früh zeichnete sich das Unternehmen durch seinen Pioniergeist aus, der bis heute ein wesentliches Merkmal der Unternehmensphilosophie geblieben ist. Die konsequente Qualitätsorientierung und das technische Know-how führten dazu, dass das Unternehmen sich schnell als verlässlicher Partner für professionelle Brandschutzlösungen etablierte.

In den 1970er Jahren expandierte das Unternehmen deutlich und baute seine Marktposition aus, entwickelte neue Löschmittel und optimierte seine Produkte. Zum 50-jährigen Jubiläum 1995 hatte sich Gloria längst als einer der führenden Brandschutzexperten in Europa positioniert. Die damals veröffentlichte Jubiläumsbroschüre dokumentierte eindrucksvoll den Weg vom kleinen Familienunternehmen zum internationalen Akteur mit umfassendem Produktportfolio und innovativen Lösungsansätzen für komplexe Brandschutzherausforderungen. Damit korrespondierend, eröffnete kürzlich ein neuer Showroom im nordrhein-westfälischen Wadersloh, wo man die neuesten Entwicklungen im Brandschutz hautnah erleben kann.

Innovation als Treiber

Die Fähigkeit, technologische Entwicklungen zu antizipieren und in praxistaugliche

80 Jahre Gloria: Was 1945 in der Nachkriegszeit begann, hat sich zu einem international anerkannten Spezialisten für Brandschutzlösungen entwickelt

Lösungen zu überführen, spiegelt sich auch in den aktuellen Schwerpunkten des Unternehmens wider: der Fokus auf nachhaltige, PFAS-freie Feuerlöscher und die Entwicklung digitaler Trainingstools für die moderne Brandschutzausbildung. So repräsentieren die PFAS-freien Feuerlöscher das unternehmerische Engagement für umweltgerechte Brandschutzlösungen. PFAS (per- und polyfluorierte Alkylsubstanzen) standen lange Zeit als effektive Löschmittelzusätze im Einsatz, haben sich jedoch aufgrund ihrer Eigenschaften als Ewigkeits-Chemikalien, die sich in der Umwelt nicht abbauen und aufgrund potenzieller Gesundheitsrisiken als problematisch erwiesen. Gloria hat frühzeitig die Notwendigkeit erkannt, alternative Lösungen zu entwickeln, die gleiche Löschleistung bieten, aber ohne diese bedenklichen Substanzen auskommen.

Digitale Revolution im Feuerlöschtraining

Was zu Zeiten der Unternehmensgründung wie Science-Fiction angemutet hätte, gehört bei den Brandschutzexperten heute zum täglichen Geschäft: Mit dem „VR Fire Trainer" bietet Gloria ein Schulungstool an, das das Feuerlöschtraining völlig verändert. Das virtuelle Trainingsinstrument ermöglicht es Mitarbeitern verschiedenster Branchen, in realistischen virtuellen Szenarien den korrekten Umgang mit Feuerlöschern zu üben und die situationsgerechte Auswahl des passenden Löschmittels zu trainieren – ohne reale Gefahren oder Umweltbelastungen.

Auf diese Weise können Brandausbreitungen und Rauchentwicklungen in einer vollkommen sicheren, virtuellen Umgebung erlebt werden. Teilnehmer haben die Möglichkeit, Fehler zu machen und aus diesen zu lernen, ohne dass ernsthafte Konsequenzen drohen – ganz nach dem Prinzip des Learning-by-Doing. Die intuitive Bedienung sorgt dafür, dass auch technisch weniger versierte Personen schnell mit dem System vertraut werden.

Dank der Orts- und Zeitunabhängigkeit des VR Fire Trainers sind Unternehmen nicht mehr auf spezielle Übungsgelände oder aufwendige Vorbereitungen angewiesen. Dies spart Kosten und erhöht die Trainingsfrequenz und damit die Sicherheitskompetenz der Mitarbeiter. Die Kombination aus praxisnahem Training und spielerischen Elementen bringt zudem frischen Schwung in die Schulung.

Der Weg ins neunte Jahrzehnt

Für die Zukunft, so das Unternehmen, sollen weiter die Digitalisierung des Brandschutzes, die Entwicklung umweltverträglicher Produkte und die kontinuierliche Verbesserung der Benutzerfreundlichkeit im Mittelpunkt der aktuellen Unternehmensstrategie stehen. Gleichzeitig will Gloria seine ursprüngliche Mission unverändert beibehalten: Menschen und Sachwerte vor den verheerenden Auswirkungen von Bränden zu schützen. Während sich die technischen Möglichkeiten und regulatorischen Anforderungen weiterentwickeln, will das Unternehmen stets einen Schritt voraus sein und praktikable Lösungen für die Brandschutzherausforderungen unserer Zeit bieten. GIT

Technologie, Vernetzung und Nachhaltigkeit

GIT SICHERHEIT im Gespräch mit Marion Heidrich, Operations Director bei Gloria

Frau Heidrich, herzlichen Glückwunsch zu diesem beeindruckenden Firmenjubiläum! Welche Meilensteine sind Ihnen in den vielen Jahren Ihrer Betriebszugehörigkeit besonders in Erinnerung geblieben?

Marion Heidrich: Für mich persönlich war das sicher mein Start 1988 mit der Ausbildung zur Industriekauffrau. Zur damaligen Zeit war es ein Privileg einen Ausbildungsplatz bei Gloria zu erhalten. Mit Blick auf unsere Produkte sind mir zum einen die Einführung des elipsenförmigen Feuerlöschers F2000 und die Designserie F6 Mitte der 90er Jahre in Erinnerung geblieben, die sich von dem damaligen herkömmlichen Feuerlöscherdesign abhoben.

Im Jahre 2011 haben wir dann die Produktlinien Easy, Pro und Star auf den Markt gebracht und damit die Vielzahl von unterschiedlichsten Feuerlöschertypen durch Standardisierung, modulare Bauweisen und Wartungsfreundlichkeit abgelöst. Als weiterer Meilenstein ist dann noch der virtuelle Feuerlöschtrainer zu erwähnen, der 2021 auf den Markt kam. Diese innovative Lösung bereitet Unternehmen und deren Mitarbeiter mittels Virtual-Reality Headsets sowie einer Feuerlöscherattrappe unabhängig von Zeit, Ort oder PC-Anbindung auf den Ernstfall vor.

Als weiteres einschneidendes Erlebnis kann man sicher den Wechsel von einem privat geführten Familienunternehmen hin in eine Konzernstruktur nennen. Geprägt von einem familiären, traditionellen und eher konservativen Umfeld fanden wir uns nun in einer globalen Konzernwelt wieder.

Bitte umblättern ▶

Heute kann ich sagen, dass dieser Wechsel uns persönlich sowie geschäftlich und auch kulturell weiterentwickelt hat.

Wie hat sich der Brandschutz in den letzten 80 Jahrzehnten entwickelt? Haben sich die Bedürfnisse der Kunden verändert?

Marion Heidrich: Der Brandschutz hat sich stark verändert, ist fachübergreifender geworden bis hin zu komplexen Brandschutz- und Sicherheitskonzepten. Technischer Fortschritt, gesetzliche Regelungen und digitale Tools haben den baulichen, anlagentechnischen und organisatorischen Brandschutz deutlich verbessert. Die Bedürfnisse der Kunden haben sich ebenso gewandelt. Sie sind heute aufgeklärter und deutlich informierter. Nachhaltigkeit, Umwelt- und Klimaschutz und Digitalisierung sowie Smart Home gewinnen immer mehr an Bedeutung. Anstatt nur gesetzliche Mindestanforderungen zu erfüllen, erwarten sie heute maßgeschneiderte, effiziente und nachhaltige Lösungen.

Wenn Sie einen Vergleich ziehen müssten, wie bewerten Sie dann die Unterschiede im Sicherheitsdenken damals und heute?

Marion Heidrich: Heute besteht ein intensiveres Sicherheitsbewusstsein, da die Informationsbeschaffung allgemein, mediale Berichterstattungen über Brandkatastrophen sowie Regulierungen und gesetzliche Vorgaben öffentlich zugänglich sind. Im Vergleich zu früher hat sich das Sicherheitsdenken von reaktiv zu präventiv und ganzheitlich gewandelt. Während früher der Schutz vor Feuer oft erst nach einem Brand thematisiert wurde und sich auf das Löschen konzentrierte, stehen heute die Vermeidung von Bränden, die frühzeitige Erkennung und die sichere Evakuierung im Mittelpunkt. Zudem wird Sicherheit heute nicht mehr isoliert betrachtet, sondern als integraler Bestandteil von Planung, Betrieb und Nachhaltigkeit verstanden. Ziel ist es Menschen, Werte und Betriebsfähigkeit langfristig zu schützen.

Welche Errungenschaften waren im Laufe der Zeit besonders herausragend?

Marion Heidrich: Als Errungenschaften im Brandschutz würde ich die unterschiedlichen Zertifizierungen nennen, die heute für Qualität und Sicherheit sorgen. Auf Gloria bezogen, wurde mit der Entwicklung der Produktlinien F2000 und der F6 zudem erstmals Sicherheit mit Ästhetik vereinbart. Ganz aktuell und ein sehr wichtiger Schritt in die Zukunft ist die Umstellung auf PFAS-freie Feuerlöscher. Damit geht der Brandschutz den Weg in Richtung Nachhaltigkeit. Diese Umstellung hat uns und die gesamte Branche vor große Herausforderungen gestellt, da erst am 2. Oktober 2025 die EU-Verordnung verabschiedet wurde und nur 20 Tage nach Veröffentlichung in Kraft getreten ist. Last but not least halte ich unseren VR Fire Trainer für eine wichtige Errungenschaft, da er für eine neue Generation des Löschtrainings und die digitale Zukunft des Brandschutzes steht.

Wo sehen Sie den Brandschutz in Zukunft? Denken Sie, dass Produkte auch weiterhin merklich weiterentwickeln können? Oder ist hier irgendwann eine Grenze erreicht?

Marion Heidrich: In Zukunft wird der Brandschutz noch stärker von Technologie, Vernetzung und Individualisierung geprägt sein. Feuerlöscher-Entwicklungen sind begrenzt durch Bauartvorgaben und Normen. Die klassische Funktion des Feuerlöschers als manuell bedientes Gerät für den Erstangriff wird bestehen bleiben. Innovationen werden vermutlich im Bereich Vernetzung und Digitalisierung sowie hinsichtlich der Nachhaltigkeit, Bedienbarkeit und Anpassungen an neue Brandrisiken entstehen. Es bedarf teilweise neuer Lösungen und spezialisierter Löschmittel - z. B. für Lithium-Ionen-Batterien.

Viele Ihrer Mitarbeiter sind schon sehr lange bei Ihnen beschäftigt. Was ist das Geheimnis dieser engen Bindung zum Arbeitgeber?

Marion Heidrich: Wir sind ein Ausbildungsbetrieb und versuchen früh den Grundstein zu legen, um junge Menschen an unser Unternehmen zu binden. Die unsererseits gebotenen Entwicklungsmöglichkeiten, ein harmonisches Betriebsklima, eine gute Unternehmenskultur, ansprechende Sozialleistungen und Benefits, Wertschätzung durch den Arbeitgeber und Tarifbindung tragen ebenfalls dazu bei.

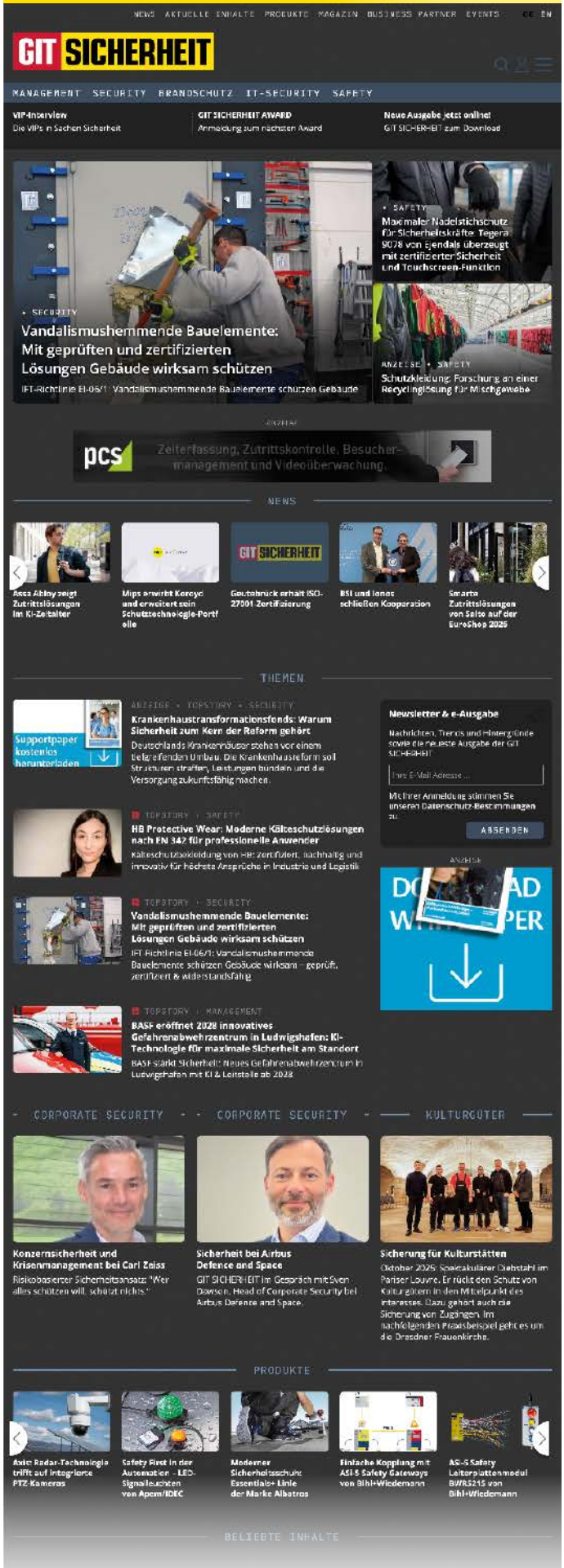
Welche konkreten Herausforderungen sehen Sie in der Brandschutzbranche in den kommenden Jahren?

Marion Heidrich: Zunächst ist die Transformation zu PFAS-freien Feuerlöschern im Markt umzusetzen – einhergehend mit der fachgerechten Entsorgung von PFAS-haltigen Feuerlöschern. Darüber hinaus wird der Bedarf an digitalen, vernetzten und individuellen Lösungen, die sich in smarte Gebäude integrieren lassen, eine große Rolle spielen. Auch der Fachkräftemangel bei der Wartung moderner Brandschutzsysteme und Feuerlöscher wird uns vor Herausforderungen stellen. GIT

Gloria GmbH
www.gloria.de

© Bilder: Gloria GmbH

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 2026
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, BDSW, BDGW, BDLS, PMeV, 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.

Originalarbeiten
Die namentlich gekennzeichneten Beiträge stehen in der Verantwortung des Autors. Nachdruck, auch auszugsweise, nur mit Genehmigung der Redaktion und mit Quellenangabe gestattet. Für unaufgefordert eingesandte Manuskripte und Abbildungen übernimmt der Verlag keine Haftung.
Dem Verlag ist das ausschließliche, räumlich, zeitlich und inhaltlich eingeschränkte Recht eingeräumt, das Werk/den redaktionellen Beitrag in unveränderter oder bearbeiteter Form für alle Zwecke beliebig oft selbst zu nutzen oder Unternehmen, zu denen gesellschaftsrechtliche Beteiligungen bestehen, sowie Dritten zur Nutzung zu übertragen. Dieses Nutzungsrecht bezieht sich sowohl auf Print- wie elektronische Medien unter Einschluss des Internet wie auch auf Datenbanken/Datenträger aller Art.
Alle etwaig in dieser Ausgabe genannten und/oder gezeigten Namen, Bezeichnungen oder Zeichen können Marken oder eingetragene Marken ihrer jeweiligen Eigentümer sein.

Gender-Hinweis
Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) sowie auf Sonderschreibweisen mit Doppelpunkt oder Genderstern verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

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

MASCHINEN- UND ANLAGENSICHERHEIT

Flexibilität und Effizienz in kompakter Form

Multifunktionales Sicherheitsrelais vereint hohe Sicherheit, schnelle Integration und minimiert den Platzbedarf

In der industriellen Automatisierung ist die funktionale Sicherheit ein integraler Bestandteil moderner Maschinen- und Anlagenkonzepte. Dabei geht es nicht nur um die Einhaltung gesetzlicher Vorgaben, sondern auch um Effizienz, Flexibilität und Wirtschaftlichkeit. Die multifunktionale Sicherheitsrelaisfamilie PSRuni von Phoenix Contact vereint diese Anforderungen in einem kompakten Gerät. Zudem bietet sie neben einem technischen ebenfalls einen wirtschaftlichen Mehrwert, wodurch sie zu einem Basisbaustein für zukunftsfähige Sicherheitslösungen wird.

Yasin Yasar, Produktmanager Safety, Automation Infrastructure, Phoenix Contact

Als erstes Mitglied der Produktfamilie überzeugt die L-Variante durch ihre technische Vielseitigkeit sowie die Fähigkeit, zwei sicherheitsrelevante Funktionen – zum Beispiel Not-Halt und Türüberwachung – parallel zu erfassen. Die beiden voneinander getrennten Schaltkreise ermöglichen eine unabhängige Auswertung und Aktivierung der jeweiligen Sicherheitsfunktionen. Daher lässt sich das Gerät in ein- ebenso wie zweikanaligen Betriebsarten einsetzen und stellt eine zuverlässige Lösung für unterschiedliche sicherheitstechnische Anforderungen zur Verfügung. Diese Besonderheit schafft die Grundlage für klassische als auch für anspruchsvollere Sicherheitsanwendungen, etwa die normgerechte Verkettung von Nothaltfunktionen über mehrere Maschinenmodule hinweg. Besonders in modular aufgebauten Produktionslinien, in denen einzelne Maschinenabschnitte miteinander vernetzt sind, eröffnet PSRuni L einen effizienten und übersichtlichen Ansatz zur sicheren Integration, sodass aufwendige Verdrahtungskonzepte der Vergangenheit angehören.

Vielseitige Integra- tion und platzsparende Sicherheit dank Push-in Technology

Ein weiterer Vorteil liegt in der Kompatibilität des Sicherheitsrelais mit einer Vielzahl sicherer Sensoren, sodass es sich nahtlos in bestehende Anlagenkonzepte einbinden lässt. Für eine effiziente Installation sorgt die moderne Push-in Technology, die eine werkzeuglose Verdrahtung gestattet. Ergänzt wird dies durch zwangsgeführte Kontakte und integrierte Diagnosefunktionen, die eine zuverlässige Fehlererkennung sowie eine sichere Abschaltung im Fehlerfall sicherstellen.

Besonders ressourcenschonend wirkt sich die kompakte Bauweise des Sicherheitsrelais aus. Da mehrere Funktionen in einem Gerät überwacht werden können, lassen

sich Steuerungseinheiten deutlich platzsparender realisieren. Dieser Vorteil ist gerade bei Retrofit-Projekten oder in räumlich begrenzten Schaltschränken von Bedeutung.

Optimierte Steuerung und platzsparende Integration

Auch die wirtschaftlichen Vorteile der L-Variante der Reihe PSRuni sind hervorzuheben. Aufgrund der universellen Einsetzbarkeit deckt das Sicherheitsrelais unterschiedliche Sicherheitsfunktionen mit nur einem Gerätetyp ab. Dadurch entfällt die Notwendigkeit, für jede Anwendung ein spezifisches Relaismodell vorzuhalten, was eine Standardisierung im Schaltschrankbau ermöglicht und die Komplexität in der Projektierung verringert. Das minimiert nicht nur den Planungsaufwand, sondern senkt auch die Fehleranfälligkeit bei der Auswahl und Einbindung der Komponenten.

Gleichzeitig profitieren Unternehmen von einer optimierten Lagerhaltung. Weil weniger Relaisvarianten bevorratet werden müssen, reduzieren sich die Lagerkosten spürbar.

Maßgeschneiderte Sicherheit durch softwaregestützte Flexibilität: Die nächste Generation Sicherheitsrelais

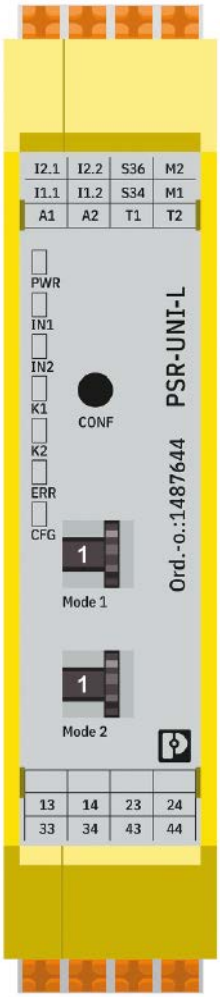
Die bisherigen Eigenschaften machen deutlich, wie facettenreich und ökonomisch PSRuni bereits mit seiner Einführungsvariante ist. Doch mit Blick auf die zunehmende Komplexität moderner Maschinen und die wachsenden Anforderungen an individuelle Sicherheitslösungen stellt sich die Frage, wie sich die Flexibilität noch weiter steigern lässt. Hier setzt die nächste Entwicklungsstufe an – mit einem erweiterten Funktionsumfang und softwaregestützter Parametrierung.

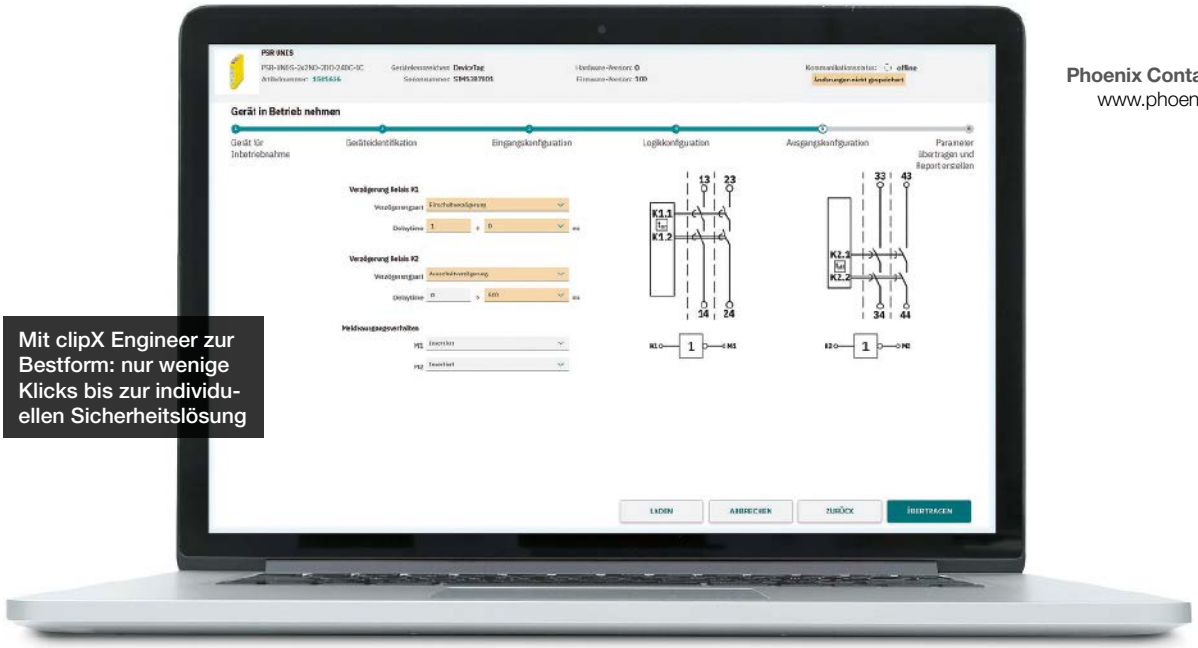
Mit der Variante PSRuni S ergänzt Phoenix Contact das Konzept des multifunktionalen Sicherheitsrelais um eine grafisch geführte Parametrierbarkeit, die dem Anwender ein hohes Maß an Anpassungsfähigkeit und Individualisierung eröffnet. Über die eigens entwickelte sowie intuitiv bedienbare Parametrierungs-Software clipX Engineer lässt sich das Sicherheitsrelais gezielt auf die jeweilige Anwendung abstimmen. Neben der Auswahl spezifischer Sicherheitsfunktionen können auch logische Verknüpfungen, Startverhalten, Meldeausgangsverhalten, Verzögerungsarten sowie Zeitparameter flexibel definiert werden. So entsteht ein modularer Baukasten für maßgeschneiderte Sicherheitskonzepte, der sich exakt an verschiedene Anforderungen und Einsatzszenarien adaptieren lässt. PSRuni S eignet sich somit für die Nutzung in der Serienfertigung, im Sondermaschinenbau sowie in modular aufgebauten Produktionssystemen.

Das Unternehmen setzt mit der Produktreihe PSRuni und im Besonderen der S-Variante neue Maßstäbe in der funktionalen Sicherheit. Die Verbindung aus technischer Leistungsfähigkeit, wirtschaftlicher Effizienz und softwaregestützter Individualisierbarkeit resultiert in einer zukunftssicheren Komponente für die sichere Automatisierung von morgen. GIT

Magnetschalter für die Positions- und Zustandsüberwachung

Die berührungslosen Magnetschalter von Phoenix Contact bieten eine robuste und präzise Lösung zur Positions- und Zustandsüberwachung in industriellen Automatisierungsprozessen. Durch die Verwendung von Reedkontakten in Kombination mit Permanentmagneten ermöglichen sie eine verschleißfreie Schaltfunktion mit großer Wiederholgenauigkeit. Die Geräte sind in kompakten Gehäusen mit hoher Schutzart bis IP67 verfügbar und eignen sich für den Einsatz in rauen Umgebungen. Aufgrund leichter Montage und flexibler Einbaulage lassen sie sich schnell in bestehende Anlagen integrieren. Die Magnetschalter, die kompatibel mit gängigen Steuerungssystemen sind, weisen zuverlässige Schaltabstände auf und sind mechanisch sehr langlebig. Sie erfüllen die Anforderungen gemäß EN 60947-5-3 und EN ISO 14119 und sind für Anwendungen in der Fördertechnik, im Maschinenbau sowie der Prozessautomatisierung geeignet.





Mit clipX Engineer zur Bestform: nur wenige Klicks bis zur individuellen Sicherheitslösung

Phoenix Contact GmbH & Co. KG
www.phoenixcontact.com/safety

MASCHINEN- UND ANLAGENSICHERHEIT

Warum bei Sonnenschein im Keller sitzen nicht die beste Lösung ist!

Wie Tailored Safety Solutions für mehr Effizienz und Produktivität sorgen

Der sicheren Einordnung eines Risikos geht die genaue Analyse der Gefährdung voraus. Das gilt immer und für alle Bereiche des menschlichen Lebens. So wäre bei der Risikobeurteilung von Sonneneinstrahlung auf die menschliche Haut das Sicherste, im Keller sitzend UV-Strahlung zu meiden. Doch da Menschen ohne Sonnenlicht erst recht Gefahr laufen ernsthaft zu erkranken, wägen sie das Risiko ab und haben eine Vielzahl von Lösungsstrategien entwickelt: Je nach Strahlungsstärke tragen sie wahlweise langärmlige helle Kleidung, halten sich im Schatten auf und/oder benutzen Sonnencreme mit passendem UV-Filter.

Eine solche Maßnahmen-Skalierung bei der Wahl des richtigen Schutzes in Abhängigkeit bestimmter Umgebungsfaktoren ist auch bei Safety-Lösungen in der industriellen und serviceorientierten Arbeitswelt erforderlich. Skalierbarkeit bedeutet beim Sensor- und Automatisierungsspezialisten Sick, dass die Sicherheitslösung exakt zur identifizierten Gefährdung passt und das Portfolio die vielfältigen Anwendungsfälle adäquat bedienen kann. Das Angebot der Waldkirchner reicht von Produkten und Systemen mit einem sehr hohen Risikominderungspotenzial von Performance Level e (PL e) (Sicherheitslichtvorhänge) und PL d (Sicherheitslaserscanner), bis hin zu Lösungen, die risikoärmere Gefährdungen mit einem PL c (sichere Mehrstrahlscanner) oder gar PL b (sichere Distanzsensoren) absichern können. Darüber hinaus lassen sich die einzelnen Komponenten auch in eine Systemlösung überführen, um kunden- und applikationsspezifische Anforderungen passend abzusichern (Objektdetektionssystem AOS).

Das vorausgehende Risk Assessment startet mit der Festlegung der Grenzen der Maschinenfunktionen und der Identifikation von Gefährdungen. Die anschließende Risikoeinschätzung und Risikobewertung folgt der Faustformel: Risiko ist gleich Schadensausmaß mal Eintrittswahrscheinlichkeit. Dabei ergibt sich je nach individueller Applikation entweder ein hohes oder niedriges Risiko und führt zur Einordnung in den erforderlichen Performance Level (PL r) gemäß ISO 13849-1.

Passgenaue Lösungen nach tiefgehender Analyse

Grundsätzlich empfiehlt Sick als Lösung für zuverlässigen Kollisions- und Personenschutz beim Einsatz schwerer mobiler Roboter mit PL d den nanoScan3 mit geringem Platzbedarf sowie den robusten microScan3. Doch ob in der Applikation mit einem AGV, einem AGC oder AMR wirklich immer eine Lösung für PL d notwendig ist, entscheidet erst die tiefergehende Analyse im individuellen Fall: Handelt es sich um einen zugangsbeschränkten automatisierten Bereich, in dem sich ausschließlich geschultes Personal aufhält? Wie schnell fährt das Fahrzeug, wie schwer (beladen) ist es und wie lange ist der Bremsweg? Neben der Beantwortung dieser Fragen wird das Expertenteam aus Anwender, AGV-Hersteller und Sick Safety-Experten zudem untersuchen, wie sich das Risiko auf die Schwere der Verletzung auswirken könnte, wie häufig oder wie lange das Risiko auftritt und welche Möglichkeiten es gibt, diese zu vermeiden.

Severity und Probability

Bei der Suche nach einer passgenauen, individuell ausreichenden und trotzdem sicheren Lösung muss zunächst die „Severity“, also der Schweregrad des Risikos ermittelt werden. Hier stehen AGCs mit wenig Ladung, die schmal, leicht und langsam sind, an einem Ende der Skala. Schnelle und große Fahrzeuge mit hohem Eigengewicht und schwerer Zuladung bilden das andere Extrem. Je nach Fahrzeugcharakteristik ergeben sich unterschiedliche Anforderungen an die Sicherheitsfunktionen.

So ist die Absicherung der Hauptfahrtrichtung von schweren Fahrzeugen mit einem microScan3 lösbar. Aber wie wird die Rückwärtsfahrt desselben Fahrzeuges adäquat abgesichert? In der Regel bewegen sich Fahrzeuge in dieser Fahrtrichtung langsamer, was sehr großen Einfluss auf den Schweregrad des Risikos hat. Eine Risikobeurteilung kann ergeben, dass die Sicherheitsfunktion für die Rückwärtsfahrt mit einem PL c oder gar PL b angemessen abgesichert ist.

Ähnlich verhält es sich bei stationären Applikationen für Zugangs- und Anwesenheitskontrolle, beispielsweise bei Pick-and-Place-Robotern. Niedrige Risiko-Schweregrade sind gegeben bei ungefährlichen Maschinenfunktionen, leichtgewichtigen Werkstücken und sehr niedrigen Krafteinwirkungen während der Prozesse.

Ein zweiter Aspekt betrifft die „Probability“, die Wahrscheinlichkeit, mit der Gefahrensituationen eintreten könnten. Niedriges Risiko besteht, wenn beispielsweise Reinigungsroboter in einer Shopping-Mall oder einem Flughafen nach Schließung ohne Kunden und Publikumsverkehr arbeiten und nur noch geschultes Reinigungspersonal anwesend ist. In diesen Fällen kann eine Tailored Safety Solution auf Basis des PL c die Applikation passgenau absichern.

Skalierbarkeit bedeutet bei Sick, dass die Sicherheitslösung exakt zur identifizierten Gefährdung passt und das Portfolio die vielfältigen Anwendungsfälle adäquat bedienen kann

Schon anhand weniger Beispiele wird klar, dass branchenübliche Standardlösungen nicht immer technologisch notwendig und wirtschaftlich sinnvoll sind. Erst die Bestimmung des tatsächlichen Risikos führt zu einer effizienten Lösung, die sicher, wirtschaftlich und produktiv zugleich ist.

Überwindung von Funktionseinschränkungen

Sick bietet mit seinem umfangreichen Sensorportfolio eine Skalierbarkeit, die auch Funktionseinschränkungen überwindet. So hat das Waldkirchner Unternehmen beispielsweise die 2D-LiDAR-Sensoren der TiM-Serie um sicherheitsgerichtete Sensoren ergänzt, die PL b erfüllen. Außerdem liefern die Varianten TiM7xxS als Safety-Sensoren erstmals sicherheitsgerichtete Messwerte und ermöglichen damit neue Wege abseits des bekannten Schutzfelds. So lässt sich nicht nur die Präsenz eines Menschen detektieren, sondern auch dessen Position bestimmen. Ein möglicher Use Case könnte die positionsabhängige Geschwindigkeitsreduktion sein, um den Mindestabstand einer sicherheitsgerichteten Abschaltung zu reduzieren und die Verfügbarkeit der mobilen Plattform zu optimieren. Anwender profitieren so von einem geringeren Invest und einem schnelleren Time-to-Market.

Risikominimierung für das primäre Ziel des Personenschutzes birgt aber noch zusätzliches Potential und kann einen willkommenen Zusatznutzen bieten. Schützt sich der Mensch wie im Fall der Maßnahmenskalierung bei UV-Strahlung mit einem Sonnenschirm vor übermäßiger UV-Strahlung, profitiert davon auch das umgebende Material, z. B. Terrassenmöbel und Baustoffe, mit einer längeren Lebensdauer. Ebenso können sichere Tailored Safety Solutions für die Zusammenarbeit von Mensch und Roboter zusätzlich der Vermeidung reiner Sachschäden dienen.

Der Schlüssel für die Produktivität jeder dieser Lösungen sind die individuelle, exakte Analyse und klare Einordnung der Risiken. Sick verfügt dafür über die komplette Bandbreite an Systemen und Produkten, berät individuell und vor Ort und bewahrt so Intralogistiker und AGV-Hersteller vor überdimensionierten und unnötigen „Kellerlösungen“. GIT

Sick verfügt über ein umfangreiches Produktportfolio an Systemen und Produkten die Ihre Anwendungen sicher und (wirtschaftlich) effizient absichern (v. l. n. r. TiM-S, DT35-S, WTT12S, scanGrid2)

Sick AG
www.sick.com

Multinormschutzkleidung fällt nach PSA-VO in die Kategorie III und muss somit Schutz vor Risiken bieten, die schwerwiegende Folgen wie irreversible Gesundheitsschäden oder gar den Tod haben können

Modul D bietet dem Hersteller die Möglichkeit, Schwerpunkte bei der Prüfung der Normkonformität auf die sicherheitsrelevanten Normen zu legen, wie z. B. bei dieser Jacke auf die EN 1149-5:2018, EN ISO 11612:2015 und EN ISO 11611:2015

SCHUTZKLEIDUNG

Mit Sicherheit sichere PSA

Welche Vorteile das Konformitätsbewertungsverfahren Modul D bietet

Ein unerlässlicher Baustein für die Sicherheit der Träger von PSA ist die Prüfung und Zertifizierung der Baumuster durch eine notifizierte Stelle. Zudem müssen später alle in der Serienfertigung produzierten Bekleidungsteile diesem Baumuster entsprechen sowie die Anforderungen der Verordnung über persönliche Schutzausrüstungen VO (EU) 2016/425 (PSA-VO) erfüllen. Diese so genannte Konformität wird per Konformitätsbewertungsverfahren sichergestellt. Im Folgenden werden die verschiedenen Verfahren der Konformitätsbewertung erläutert und warum Schutzbekleidungs-Hersteller HB Protective Wear sich bei seinen Kategorie III-Artikeln für das Verfahren nach Modul D entschieden hat.

In der PSA-VO wird persönliche Schutzausrüstung in drei Kategorien unterteilt. PSA der Kategorie I schützt ausschließlich vor geringfügigen Risiken, während Bekleidung der Kategorie III Schutz vor Risiken, die zu schwerwiegenden Folgen wie Tod oder irreversiblen Gesundheitsschäden führen können, bietet. PSA der Kategorie II beinhaltet Bekleidung, die weder in Kategorie I noch in Kategorie III fällt.

Baumusterprüfung und Fertigungskontrolle – Wie die Konformitätsbewertung für PSA erfolgt

Jedes Bekleidungsteil, dass unter der PSA-VO hergestellt wird, muss durch ein Konformitätsbewertungsverfahren überwacht werden. Dies wird über verschiedene Module gesteuert. Für Artikel der Kategorie I ist eine interne Fertigungskontrolle (Modul A) ausreichend. Hierbei erklärt der Hersteller selbstständig, dass die Anforderungen aus der PSA-VO erfüllt sind. Das beinhaltet die Erstellung technischer Unterlagen, die CE-

Kennzeichnung sowie der EU-Konformitätserklärung und natürlich die Herstellung selbst, die unter kontrollierten Bedingungen erfolgen soll.

Für alle Produkte, die in die Kategorien II und III fallen, wird eine EU-Baumusterprüfung (Modul B) obligatorisch. Das bedeutet, dass ein Baumuster durch eine notifizierte Stelle untersucht, geprüft und zum Schluss zertifiziert werden muss. Damit wird bestätigt, dass dieser Artikel die Anforderungen der PSA-VO erfüllt. Die hergestellte PSA muss im Anschluss durch interne Fertigungskontrollen (Modul C) beim Hersteller überprüft werden.

Die PSA-VO sieht für PSA Kategorie III weiterführend vor, dass die Konformität der Artikel durch eine jährliche Überwachung validiert werden muss. Dafür stehen zwei Verfahren zur Verfügung. Das ist zum einen das Modul C2, bei dem die Konformität mit dem Baumuster in internen Fertigungskontrollen überprüft wird und zusätzlich durch Produktprüfungen erfolgt. Für diese Produktprüfungen muss für jedes bestehende Zertifikat ein Vertrag mit einer notifizierten Stelle abgeschlossen werden, die mindestens einmal jährlich in unregelmäßigen Abständen stichprobenartig Lagerware auf Konformität mit dem Baumuster prüft. Als Gutachten wird am Ende der Prüfung ein Prüfbericht erstellt.

Daneben besteht die Möglichkeit, die Überwachung des Qualitätssicherungssystems entlang des Produktionsprozesses (Modul D) durchzuführen. Dieses muss ebenfalls durch eine notifizierte Stelle geprüft, bewertet und zugelassen werden. Durch diese aufwändige Validierung des gesamten Qualitätssicherungssystems wird aufgrund des Verfahrens sichergestellt, dass die hergestellte PSA dem Baumuster entspricht. Diese Überwachung wird ebenfalls jährlich durchgeführt, in diesem Falle jedoch in regelmäßigen Abständen. Als Gutachten werden ein Auditbericht sowie ein Zertifikat ausgestellt.

Portfoliogröße und Sicherstellung der Normkonformität sind entscheidend für den Konfektionär

Bei einem kleinen Produktportfolio von Bekleidung der Kategorie III ist es oft einfacher, diese nach dem Modul C2 überwachen zu lassen, weil Aufwand und Kosten, das gesamte Qualitätssicherungssystem entlang des Produktionsprozesses zu auditieren, unverhältnismäßig hoch wären. Je größer allerdings das Portfolio ist, desto mehr Ressourcen werden für die Überwachung der einzelnen Produkte benötigt. Dies ist bei dem Verfahren nach Modul D nicht der Fall, weswegen diese Variante als ressourcenschonender zu betrachten ist.

Die Menge der zu überwachenden Produkte ist aber nur eines der Kriterien bei der Auswahl des Konformitätsbewertungsverfahrens. Denn vor allem die Sicherstellung der Konformität der Produkte aus den laufenden Produktionen steht bei der Überwachung im Mittelpunkt. Dies geschieht bei Modul C2 durch die stichprobenartige Überprüfung der Produkte. Jedoch hat hier die notifizierte Stelle die Kontrolle und wählt die zu prüfenden Normen aus. Bei Modul D hat der Hersteller eine höhere Eigenverantwortung und muss die regelmäßige Überprüfung der Normkonformität eigenständig in sein Qualitätssicherungssystem integrieren. Mit der Zulassung durch eine notifizierte Stelle wird dies aber ebenfalls jährlich von einer externen Partei bestätigt. Außerdem hat der Hersteller eine bessere Steuerungsmöglichkeit für die Durchführung von Prüfungen, die die Normkonformität bestätigen. Es können individuell Schwerpunkte gelegt werden, zum Beispiel können Produkte mit besonderem Augenmerk auf die jeweiligen sicherheitsrelevanten Normen geprüft werden.

Konformitätsbewertungsverfahren nach Modul D bietet höhere Flexibilität und effizientere Abläufe

Auch der allgemeine organisatorische Aufwand und die Zeitachse können ein Entscheidungskriterium sein. Bei Modul C2, der Produktüberwachung, muss für jedes Zertifikat ein eigener Überwachungsvertrag mit einer notifizierten Stelle abgeschlossen werden. Dies kann auch bei verschiedenen notifizierten Stellen erfolgen. Die Überwachungszeiträume sowie der Termin zur Rezertifizierung können jedoch somit für jedes Zertifikat unterschiedlich sein. Wenn ein Produkt zum Zeitpunkt der Überwachung gerade nicht auf Lager liegt und auch nicht produziert wird, wird das Zertifikat ausgesetzt und muss zu Beginn einer neuen Produktion reaktiviert werden. Das bedeutet, dass beispielsweise die Produktion eines nicht lagerhaltigen Kundensonderartikels erst dann angestoßen werden kann, wenn zuvor ein Muster den oftmals langwierigen Prozess der Überwachungsprüfung durchlaufen hat. Für den Kunden führt dies teilweise zu langen Lieferzeiten.

Bei dem Konformitätsbewertungsverfahren nach Modul D hingegen arbeitet der Hersteller nur mit einer einzigen überwachenden Stelle zusammen. Jedes neue Zertifikat muss gemeldet und von der Stelle bearbeitet und dem Überwachungsvertrag hinzugefügt werden. Der entscheidende Vorteil hierbei ist aber, dass es nur eine notifizierte Stelle gibt, mit der kommuniziert wird und es nicht relevant ist, wann und wie oft der Artikel produziert wird. Der Hersteller kann unabhängiger agieren und seine Kunden schneller beliefern.

Auditierung aller Produktionsbetriebe – Nonkonformitäten frühzeitig entdecken und eliminieren

Unter dem Verfahren nach Modul C2 kann die Bekleidung in jedem beliebigen Produktionsbetrieb hergestellt werden. Dies bietet viel Flexibilität, jedoch können Nonkonformitäten dabei häufig erst spät im Prozess entdeckt werden, wenn unter Umständen bereits viele Teile in Verkehr gebracht wurden und gegebenenfalls ein Rückruf notwendig wird. Das resultiert daraus, dass unter Modul C2 jährlich nur stichprobenartige Prüfungen an den Fertigteilen durchgeführt werden. Unter Modul D werden im Gegensatz dazu alle Produktionsbetriebe auditiert und das Qualitätssicherungssystem von der Beschaffung bis hin zur Auslieferung geprüft und zertifiziert. Dies unterstützt den Hersteller dabei, Nonkonformitäten frühzeitig zu entdecken und zu eliminieren. Zudem ergeben sich oft geringere Prozesskosten und schnellere Produktionsabläufe.

Als Hersteller für qualitativ hochwertige Schutzbekleidung für eine Vielzahl von Gefahrenbereichen ist auch HB Protective Wear verpflichtet, für Produkte der Kategorie III die Konformität mit dem Baumuster durch eines der Konformitätsbewertungsverfahren sicherzustellen. Bis Ende 2022 ist dies bei allen betroffenen Artikeln über die Produktüberwachung mit Modul C2 erfolgt. Nachdem sich das Unternehmen entschieden hatte, auf Modul D umzustellen und die Konformität seiner PSA anhand der Qualitätssicherung sicherzustellen, wurde der erste Meilenstein hierzu bereits im Dezember 2021 mit der Zertifizierung nach ISO 9001 gelegt. Auf dieser Grundlage hat HB Protective Wear im Anschluss auch das Qualitätssicherungssystem in Bezug auf das Überwachungsverfahren nach Modul D erfolgreich auditieren und zertifizieren lassen. Hierzu wurde im April 2022 das erste Audit bei HB durchgeführt. In den nachfolgenden Monaten wurden dann ebenso die Produktionsbetriebe in Bulgarien, Nordmazedonien, Moldawien und Armenien erfolgreich auditiert. Die Zertifizierung nach Modul D bestätigt den hohen Anspruch von HB an die Qualität und an die Sicherheit seiner Produkte. GIT

HB Protective Wear GmbH & Co. KG
www.hb-online.com/de

Arbeiten, die sehr gute Haptik erfordern, die Kontrolle von Ausweisen oder der Durchsuchung von Gepäckstücken am Flughafen, können sicher ausgeführt werden, ohne dass der Handschuh als Fremdkörper empfunden wird

SICHERHEITSHANDSCHUHE

Nadelstichschutz für Profis

Zertifiziert, touchfähig und komfortabel – der Handschuh für Polizei und Sicherheitsdienste

Ob bei Polizei, Sicherheitsdiensten oder im Ordnungsdienst: Die Mitarbeiter sind im Einsatz immer wieder mit der Gefahr konfrontiert, sich durch unsachgemäß entsorgte oder im Umfeld auftretende Spritzen, Nadeln und andere spitze Gegenstände potenziell schwer zu verletzen. Gerade in urbanen Brennpunktbereichen, bei Großveranstaltungen oder im Kontrollalltag an Flughäfen und Bahnhöfen zählt der Schutz vor Nadelstichverletzungen daher zu den zentralen Herausforderungen und ist ein Schwerpunktthema moderner Arbeitssicherheit.

Der Tegera 9078 von Ejendals ist ein Handschuh, der in risikoreichen Arbeitsfeldern rundum zertifizierten Schutz bietet. Er kombiniert hohen Tragekomfort mit Alltagstauglichkeit inklusive Touchscreen-Bedienung. In der täglichen Praxis von Security-Teams an Flughäfen, Kontrollpersonal in öffentlichen Verkehrsmitteln, Rettungskräften, Polizeieinheiten und Mitarbeitern im Ordnungsdienst steht der zuverlässige Schutz vor Nadelstichverletzungen im Mittelpunkt. Diese Gefahr wird oft unterschätzt, kann aber schwerwiegende gesundheitliche Folgen haben. In diesen dynamischen und oft unübersichtlichen Einsatzumgebungen ist die Wahrscheinlichkeit hoch, spontan mit Spritzen oder anderen spitzen Gegenständen konfrontiert zu werden. Hier beweist der Handschuh seine zentrale Stärke.

Rundumschutz durch Para-Aramid-Technologie

Die innovative Konstruktion mit mehreren Lagen Para-Aramid und robustem Ziegenleder an den exponierten Fingern und Handflächen schützt die Anwender nicht nur vor Nadelstichen, sondern sorgt darüber hinaus für Beweglichkeit und gefordertes Tastgefühl. Selbst filigrane Arbeiten, wie das Kontrollieren von Ausweisen oder das Durchsuchen von Gepäckstücken am Flughafen, können mit diesen Handschuhen sicher ausgeführt werden, ohne dass er als Fremdkörper empfunden wird. Die Zertifizierung nach ASTM F2878 und die nachgewiesene Beständigkeit gegen Injektionsnadeln mit bis zu 10 Newton an den Fingerspitzen – getestet und zertifiziert mit 25 Gauge Nadel –sind Resultat konsequenter Entwicklungsarbeit im Dialog zwischen Hersteller, Branchenexperten und den späteren Anwendern selbst. Somit schützt die spezielle Nadelstichschutz-Technologie die Fingerspitzen rundum, nicht nur auf der Vorder- und Rückseite.

Veronika Seliger, Distribution Relationship Manager bei Ejendals, betonte, dass ihre Rückmeldungen aus der Branche erkennen ließen, dass bis heute viele Sicherheitsdienste den Spagat zwischen kompromisslosem Schutz und funktionaler Alltagstauglichkeit als Herausforderung sehen.

Dank einer speziellen Gerbung des Tegera 9078 bleibt die Touchscreen-Fähigkeit erhalten, auch wenn die Fingerspitzen durch das Para-Aramid mehrfach verstärkt sind

Die Konstruktion mit mehreren Lagen Para-Aramid und robustem Ziegenleder an den exponierten Fingern und Handflächen schützt die Anwender nicht nur vor Nadelstichen, sondern sorgt auch für Beweglichkeit und Tastgefühl

Alltagstauglich, sicher und komfortabel

Insbesondere beim Einsatz an Flughäfen, beim mobilen Ordnungsdienst und in urbanen Brennpunktbereichen ist die Fähigkeit, das eigene Smartphone zur Koordination oder Dokumentation direkt mit den Handschuhen zu bedienen, inzwischen unverzichtbar. Durch die spezielle Gerbung bleibt die Touchscreen-Fähigkeit erhalten, auch wenn die Fingerspitzen durch das Para-Aramid mehrfach verstärkt sind. Anwender profitieren davon, flexibel auf wechselnde Einsatzlagen reagieren zu können, ohne ständig die Handschuhe ausziehen zu müssen.

Auch das Thema Hygiene gewinnt im Kontext von Rettungsdiensten, Krankenhäusern und Sicherheitskontrollen an Gewicht. Der Handschuh lässt sich mit alkoholhaltigen Desinfektionsmitteln reinigen, ohne dass Material oder Passform leiden. Die ist ein klarer Vorteil gegenüber herkömmlichen Lederhandschuhen, die unter häufiger Desinfektion schnell an Funktion und Optik verlieren.

Auch das An- und Ausziehen bietet dank des stabilen Klettverschlusses mit Grifflasche auch bei Hektik Halt und schnelle Verfügbarkeit. Passform und Ergonomie erleichtern das Tragen über längere Zeiträume oder in Kombination mit weiterer PSA – ein nicht zu unterschätzender Beitrag für Gesundheit und Motivation der Mitarbeiter.

Die Features im Überblick

- Touchscreen-Funktion für Mobilgeräte, ohne die Handschuhe ausziehen zu müssen
- Ergonomische Passform und Klettverschluss für sicheren Sitz – auch bei schnellen Einsätzen
- Reinigung mit Desinfektionsmitteln möglich, ein entscheidender Pluspunkt im medizinischen und öffentlichen Bereich
- Unisex-Passform bei einem Größenspiegel von 6-12

Zielgruppen

Die Branchen, in denen der Tegera zum Einsatz kommt, sind also vielfältig. Ob bei Personenkontrollen, Body-Scans, Taschenkontrollen, polizeilichen Ermittlungen oder in mobilen Notfalleinheiten: Überall dort, wo Schutz und Fingerspitzengefühl gefordert sind, ist der Handschuh optimal geeignet. Erhältlich ist er in den Größen von 6-12, wodurch ein gesamtes Team individuell ausgestattet werden kann. GIT

Ejendals AB
www.ejendals.com

© Bilder: Ejendals / Daniel Elfving

© Georg Schlegel | Benjamin Stollenberg

Schlegel erhält Focus Gold für innovative Displaytaste

Das Land Baden-Württemberg hat zum 35. Mal den Internationalen Designpreis Baden-Württemberg, Focus Open 2025 verliehen. Georg Schlegel hat für seinen variablen Displaytaster Flexitast erstmals den Focus Open in Gold erhalten. Die Preisträger wurden von einer unabhängigen Jury ausgewählt. Der Flexitast ist eine haptische Drucktaste mit integriertem ZBD-Display, auf dem Farbe, Symbolik oder Textinformationen dynamisch und in Echtzeit angepasst werden können. „Die freie Belegung der Tasteninformation ist ein großer technologischer Sprung und erlaubt eine erweiterte Kommunikation mit den Anwendenden. Das verbessert die User Experience, die Bediensicherheit und das Branding – nicht nur im industriellen Kontext“, so die Jury in ihrer Bewertung. Erstmals wurde nun mit dem Flexitast ein Produkt mit dem Focus Open in Gold ausgezeichnet, der nur für „zukunftsweisende und herausragende Lösungen“ verliehen wird. **www.schlegel.biz**

EVENTS

Essener Gefahrstofftage 2025

Ein Nachbericht

Im Essener Haus der Technik fanden 2025 zum 14. Mal die Essener Gefahrstofftage statt. Traditionell richtet sich die Hybrid-Tagung an Fachkräfte aus diesem breiten Themengebiet. Unser Nachbericht - anlässlich der kommenden Tagung im April 2026.

Tagungsleiter Prof. Dr. Herbert Bender (Gefahrstoff Consulting Compliance, Böhl-Iggelheim) stellte in seinem Eröffnungsvortrag die neuen nationalen und europäischen Vorschriften der beiden letzten Jahre aus allen Bereichen des Gefahrstoffrechts vor, ergänzt um Ausführungen zu den gesetzlichen Regelungen aus dem Bereich der Betriebssicherheit und dem Immissionsschutz. Bender informierte über die Änderungen der grundlegenden europäischen CLP- und REACH-Verordnung mit ihren unmittelbaren Auswirkungen auf das nationale Gefahrstoffrecht. Die neuen Anforderungen von TRGS 520 der – meist unter kommunaler Aufsicht geführten – Gefahrstoffsammelstellen, wurden ebenso wie die Änderungen der Arbeitsplatzgrenzwerte und der europäischen arbeitsplatzbezogenen Grenzwerte diskutiert.

Neuerungen der Gefahrstoffverordnung

Dr. Mirjam Merz vom Bundesverband der Deutschen Industrie (BDI) erklärte aus erster Hand die Neuerungen der Gefahrstoffverordnung, einschließlich der Konsequenzen für Immobiliengesellschaften und private Hausbesitzer bei anstehenden Gebäudesanierungen. Sie sprach über die Implementierung des Risikokonzeptes sowie über die neuen Vorschriften für krebserzeugende Gefahrstoffe sowie bei Tätigkeiten mit Biozidprodukten. Annika Wörsdörfer vom Deutschen Gewerkschaftsverband (DGB) beleuchtete die nationalen und europäischen Vorschriften aus Sicht der Arbeitnehmer. Sie hob die besondere Verantwortung der Sozialpartner bei der Erstellung der staatlichen Vorschriften und bei der Umsetzung hervor. Nur in kooperativem Konsens erarbeitete staatliche Vorschriften dienten der Stärkung der Position der Beschäftigten und dem Wirtschaftsstandort Deutschland.

Die neue Installation des Ausschusses für Sicherheit und Gesundheit (ASGA) durch das Bundesministerium für Arbeit und Soziales (BMAS) hat in der Fachwelt zu intensiven Diskussionen geführt.

Die Vorsitzende des ASGA, Prof. Dr. Anke Kahl von der Bergischen Universität Wuppertal, hat die neuen Strukturen im ASGA sowie des eingesetzten Steuerkreises überzeugend erläutert und konnte viele der bisherigen Bedenken zerstreuen.

© HDT

Pro und contra Bürokratieabbau

In einer Diskussionsrunde wurde debattiert, ob die zahlreichen technischen Regeln unter der Initiative Bürokratieabbau im Interesse der Wirtschaft und der Beschäftigten abgeschafft werden sollten. Einvernehmlich sprachen sich die Diskutanten für die Beibehaltung der technischen Regeln aus, da diese keine bürokratische Bürde, sondern notwendige Hilfestellungen für die Praxis darstellten und zur Rechtssicherheit beitrügen.

Dass auch europäische Regelungen zum Immissionsschutz unmittelbare Auswirkungen auf die deutschen Arbeitsplätze bei der Verwendung von Chemikalien haben, stellte Annette Giersch vom Bundesverband der Deutschen Industrie (BDI) eindrücklich dar. Die geplante Mantelverordnung der EU werde weitreichende Auswirkungen auf die konkreten Arbeitsplätze zur Folge haben. Die Mehrzahl der vorgesehenen Vorschriften werde allerdings als wenig hilfreich und als Überregulierung angesehen.

Stichwort PFAS

Kein zweites Gefahrstoffthema wurde in den letzten Jahren ähnlich intensiv diskutiert wie PFAS (Per- und polyfluorierte Alkylverbindungen). Die oft als „Ewigkeitschemikalien" bezeichneten Stoffe nehmen nicht nur in der öffentlichen Diskussion einen breiten Raum ein. Mirjam Merz vom BDI zeigte den derzeitigen Stand der fachpolitischen Diskussion auf, identifizierte Anwendungsbereiche, wo die besonderen Eigenschaften der PFAS unabdingbar sind und nicht durch andere Stoffe ersetzt werden können, sowie Anwendungsbereiche, wo auch Alternativstoffe ohne gravierende Eigenschaftsverluste eingesetzt werden können.

Arbeitssicherheit

Bei Gefährdungen durch krebserzeugende, keimzellmutagene und reproduktionstoxische Stoffe der Kategorie 1A oder 1B muss der Arbeitgeber ein Expositionsverzeichnis der Beschäftigten führen. Dr. Alexander Schneider vom Institut für Arbeitssicherheit der DGUV zeigte, wie diese gesetzliche Aufgabe mithilfe der ZED (Zentrale Expositionsdatenbank) effektiv und zeitsparend umgesetzt werden kann.

In das seit mehreren Jahren zunehmende Grenzwertwirrwarr am Arbeitsplatz brachte Dr. Martin Wieske vom Verband Nichteisenmetalle Licht. Der Zusammenhang zwischen nationalem Arbeitsplatzgrenzwert, Toleranz- und Akzeptanzkonzentration, MAK-Wert, europäischen IOELV- und BOELV-Werten und den von den Registranten abzuleitenden DNEL-Werten wurde anschaulich erläutert.

Die sichere Lagerung von Gefahrstoffen ist in allen Betrieben eine herausfordernde Aufgabe. Die Vorschriften zur sicheren Lagerung sowie mögliche praktische Umsetzungsbeispiele hat Tobias Authmann von Denios aufgezeigt. GIT

Die nächste Ausgabe der Tagung ist angekündigt für den 13. bis 14. April 2026

Haus der Technik e.V., HDT
www.hdt.de/gefahrstofftage

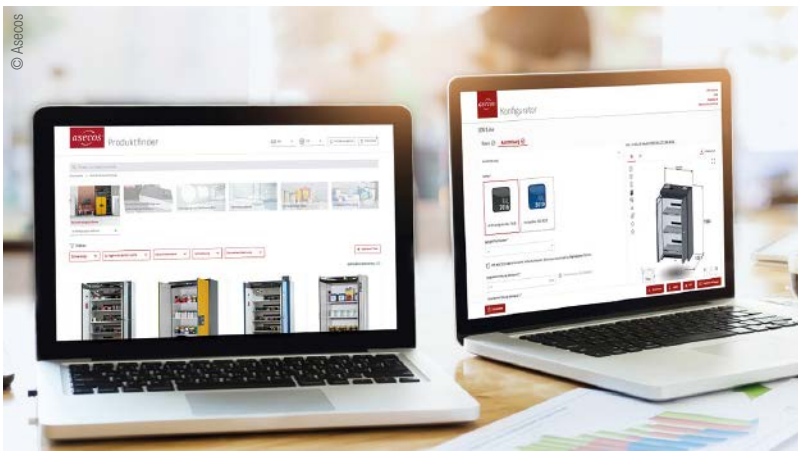
© Ejendals

Ejendals Tegera 7787 erhält Dupont Innovation Award

Ejendals wurde auf der Weltleitmesse A+A 2025 in Düsseldorf für ihr neues Premium-Schweißerhandschuh-Modell Tegera 7787 mit dem renommierten Dupont Innovation Award ausgezeichnet. Mit dieser internationalen Anerkennung würdigt Dupont den innovativen Einsatz von Kevlar und die fortschrittlichen Sicherheitsmerkmale in der Persönlichen Schutzausrüstung von Ejendals, speziell für industrielle Anwendungen. Der Tegera 7787 Schweißerhandschuh wurde entwickelt, um höchsten Ansprüchen an Komfort, Haltbarkeit und Fingerspitzengefühl gerecht zu werden. Dank hochwertigem, schwarzem Ziegennarbenleder und einer verstärkten Stulpe aus Rindsspaltleder bietet das Produkt optimalen Schutz bei intensiven Einsatzbedingungen. Der Handschuh hat die Schnittschutzklasse F nach EN 388 sowie eine spezielle Kevlar-Verstärkung, die vor Abrieb und Hitze schützt. **www.ejendals.de**

Vom Klick zur Lösung: Asecos setzt auf digitale Planungstools

Mit zwei neuen Online-Tools erleichtert die Asecos GmbH Produktauswahl und Planung: Der Produktfinder führt durch das gesamte Sortiment des Unternehmens, der 3D-Ion-Line-Konfigurator unterstützt die individuelle Konfiguration der Ion-Line-Sicherheitsschränke zur Batterielagerung. Beide Anwendungen sind unter www.asecos-configurator.com erreichbar und bieten Kunden einen schnellen, komfortablen und praxisnahen Weg zur optimalen Lösung – ob für den Überblick über das Produktportfolio oder für die passgenaue Ausgestaltung spezieller Modelle. Dank intelligenter Filterfunktionen, geführter Suchprozesse und umfassender Zusatzinformationen gelangen Nutzer zur Produktlösung, die exakt ihren Anforderungen entspricht. Der Produktfinder bietet einen vollständigen Überblick über das gesamte Sortiment — inklusive aller Varianten, Ausstattungsoptionen und zugehöriger Serviceleistungen. **www.asecos.com**



© Asecos

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

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
marketing.uz@assaabloy.com · www.uundz.com
Elektronische Schließsysteme, modular aufgebaut und individuell erweiterbar
Seit 2025 gehört das Unternehmen zur Assa Abloy-Firmengruppe.

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

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

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 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 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 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 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 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 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 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

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

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 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

Lana Djurkin-König

Director of Trust and Security Advocacy EMEA bei Lenovo

- Über 20 Jahre Erfahrung in Ministry of Defence, globaler Logistik, professionellen Dienstleistungen und Versicherungs- und Technologiesektor
- Aufbau und Koordination der globalen Sicherheitsinformationsfunktion bei DHL Group (GSSC)
- Aufbau und Führung globaler Sicherheitsfunktionen in intern. Konzernen:
- Sie entwickelte und leitete zentrale Sicherheits- und Informationsstrukturen in mehreren weltweit tätigen Unternehmen – von der Etablierung einer globalen Sicherheitsinformationsfunktion bis zur Transformation von Sicherheits- und Krisenmanagementsystemen mit umfassender internationaler Verantwortung für Unternehmenssicherheit und Resilienz
- Director of Trust & Security Advocacy, EMEA bei Lenovo
- ständiges Mitglied des OSAC Germany Steering Committee; Gründerin und CEO der Young Security Professionals Academy (YSPA)

Ihr Berufswunsch mit 20 war: Ich wollte für Interpol arbeiten. Kriminologie, Kriminalistik, Nachrichtendienst und Terrorismus sind seit meiner Schulzeit meine Leidenschaften.

Was hat Sie dazu bewogen, eine Aufgabe im Bereich Sicherheit zu übernehmen? Ich bin ein Kind des Krieges und die Tochter eines Militäroffiziers. Ich bin während des Heimatkrieges in Kroatien aufgewachsen und habe aus erster Hand miterlebt, wie fragil Stabilität sein kann und, dass Sicherheit nicht als selbstverständlich angesehen werden darf. Diese Erfahrungen haben mein Verständnis für die Bedeutung persönlicher und gesellschaftlicher Resilienz geprägt, und ich wollte meine Karriere darauf ausrichten, sicherzustellen, dass es im Krisenfall Systeme und Menschen gibt, die Schutz bieten.

Welche sicherheitspolitische Entscheidung oder welches Projekt sollte Ihrer Meinung nach schon längst umgesetzt sein? Eine echte cyber-physische Konvergenz in der Unternehmensführung. Wir verhalten uns immer noch so, als würden digitale Bedrohungen am Bildschirm und physische Bedrohungen am Tor Halt machen. Das tun sie aber nicht. In Wirklichkeit überschneiden sie sich ständig, ein Cyberangriff kann physische Infrastrukturen lahmlegen und eine physische Sicherheitsverletzung kann digitale Systeme gefährden. Eine effektive Unternehmensführung und -verwaltung erfordert die Integration beider Dimensionen in eine einheitliche Resilienzstrategie.

Was ist Ihrer Meinung nach die größte Erfindung im Bereich der Sicherheit? Open-Source-Intelligence und die Technologie, die Geheimdienstteams bei der Auswertung unterstützt. Die Demokratisierung der Lageerkennung hat die Bedrohungslandschaft völlig verändert.

Ein Erfolg, den Sie kürzlich errungen haben, war: Eine äußerst erfolgreiche Young Security Professionals Academy (YSPA) in Kopenhagen, die vom CSO von Novo Nordisk veranstaltet wurde. Wir schaffen ein echtes Vermächtnis und eine Gemeinschaft für junge, aufstrebende und sich im Wandel befindliche Sicherheitstalente. Und während wir uns der Aufgabe verschrieben haben, ein globales Sicherheitskollektiv zu bilden und auszubilden, begeistert es mich zu sehen, wie wir die nächste Generation von Führungskräften formen, die in einer immer komplexer werdenden Welt für Widerstandsfähigkeit und Vertrauen sorgen werden.

Wer hat Ihrer Meinung nach eine Auszeichnung verdient? Der Kollege mit dem ausländischen Akzent. Das ist ein Zeichen von Mut, das viele Menschen (Muttersprachler) nicht wirklich sehen (oder verstehen). Es spiegelt die Tapferkeit wider, in einem fremden Land neu anzufangen, und zeugt von Widerstandsfähigkeit und Anpassungsfähigkeit.

Wobei entspannen Sie? Ich entspanne mich beim Spazierengehen mit meinen Hunden in der Natur oder beim SUP-en auf dem See. Es ist schön hier zu leben (wenn es nicht regnet).

Welchen Urlaubsort können Sie empfehlen? Neuseeland ist magisch, surreal und es ist toll, ab und zu mal ganz ohne Handyempfang zu sein.

Welche Zeitschriften lesen Sie regelmäßig? Economist und Harvard Business Review. Zunehmend nutze ich auch Podcasts, um mich auf dem Laufenden zu halten.

Die GIT SICHERHEIT ist für mich wichtig, weil…die Zukunft der Sicherheit von informierten, kollaborativen Ökosystemen abhängt. Silos sind ein Luxus, den wir uns nicht leisten können.

Welches Buch haben Sie zuletzt gelesen? „How to Survive a Crisis“ von David Omand.

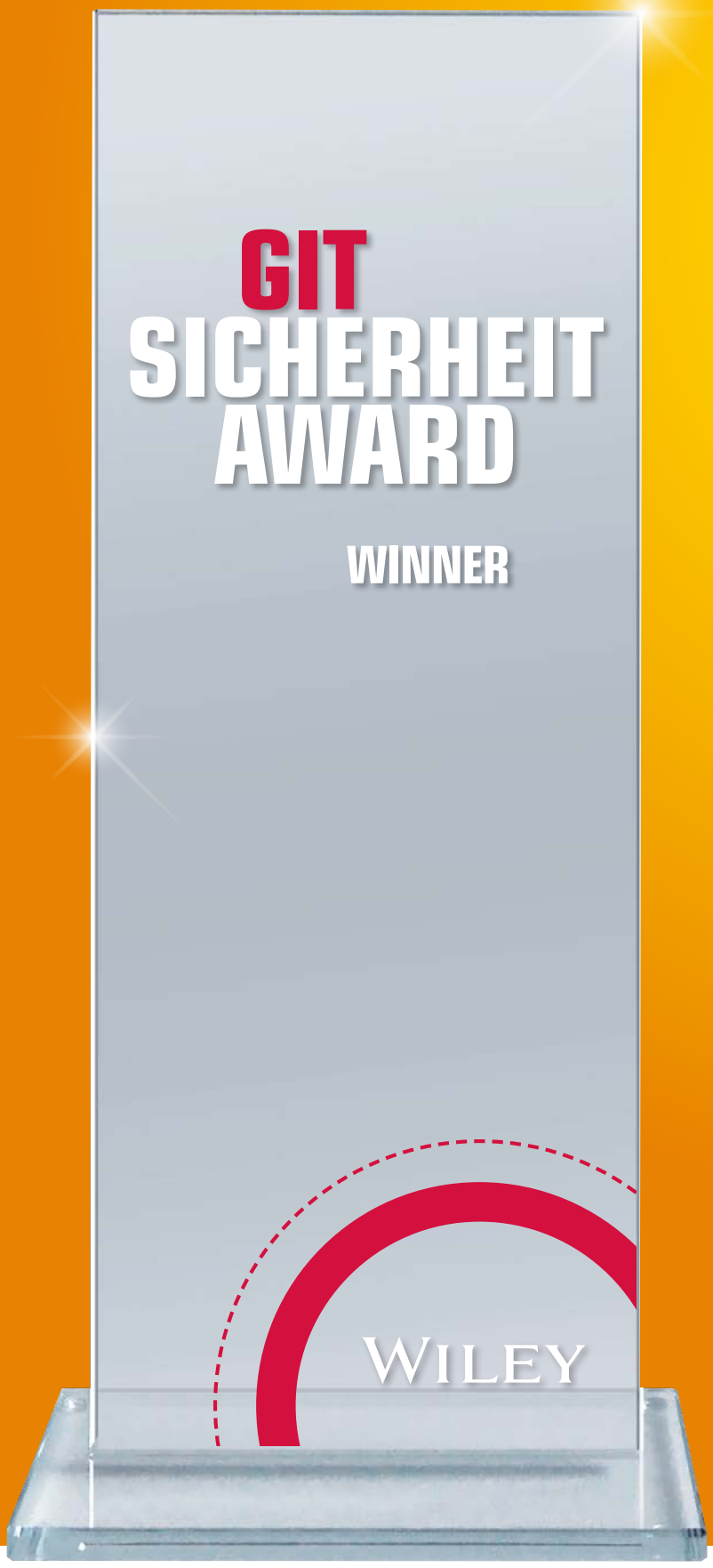
Welche Musik hören Sie am liebsten? Deep House, Bossa Nova und Acid Jazz. Mario Biondi, Incognito, Thievery Corporation und Compilations von Defected oder Glitterhouse.

Was motiviert Sie? Etwas aufzubauen, das mich überdauern wird, darunter die Förderung und Stärkung junger Menschen.

Worüber machen Sie sich Sorgen? Sorgen: Ein hybrider Krieg in Europa, den niemand als Krieg zu bezeichnen wagt, und das Übersehen subtiler Anzeichen einer Eskalation, bis es zu spät ist. Selbstgefälligkeit angesichts geopolitischer Veränderungen. Hoffnung: Eine Generation, die sich weigert, so zu tun, als sei alles in Ordnung. Ich arbeite im Rahmen der YSPA eng mit der Generation Z und Millennials zusammen, und es gibt mir Hoffnung, zu sehen, wie sie den Status quo in Frage stellen.

WILEY

JETZT EINREICHEN



ANMELDESCHLUSS
31. MÄRZ

Teilnahmebedingungen und
Produkt einreichen:

www.sicherheit-award.de

BHE | TÜV HESSEN | VDMA | ZVEI: Automation | ZVEI: Sicherheitssysteme | WILEY

Digitale oder physische Sicherheit?
Unsere Empfehlung: Beides!

Um Ihre Gebäudeinfrastruktur wirksam zu schützen, gibt es beim Thema Sicherheit kein Entweder-oder.

Denn erst das Zusammenspiel aus beidem sorgt für eine ganzheitliche Sicherheitsstrategie. Was nützt der beste IT-Schutz, wenn Serverräume kein Zutrittskontrollsystem haben oder IT-Komponenten für die Gebäudesicherheit sich ungeschützt im Netz befinden?

Es geht also nicht nur um die IT, sondern auch um die OT – etwa Gebäude-, Zutritts- und Versorgungstechnik oder Perimeter- und Videosicherheitslösungen, die es mit zunehmender Digitalisierung zu schützen gilt.

Wir können beides: Mit integrierten Lösungen für physische Sicherheit und unseren Cybersecurity-Services unterstützen wir Sie dabei, Ihre Resilienz zu stärken und regulatorische Anforderungen wie das **NIS-2-Umsetzungsgesetz** zu erfüllen.

Hier erfahren Sie mehr:

SIEMENS