

GIT SICHERHEIT

MAGAZIN FÜR SAFETY UND SECURITY



GIT
SICHERHEIT
AWARD
FINALISTS

JETZT ABSTIMMEN

WWW.SICHERHEIT-AWARD.DE

Titelthema Seite 62:

Genehmigt ≠ sicher

Markus Boberg und Tobias Dankert im Gespräch: Gefahrstoffmanagement zwischen Mindeststandard und Vision Zero



CORPORATE SECURITY

Im Gespräch mit
Alexandra Forster:
Global Security bei Bayer S. 14

TIME-SENSITIVE NETWORKING

Zukunftstechnologie für
industrielle Kommunikation S. 80



VIP

Oliver Giesen, Leiter Werk-
feuerwehr Bayer AG,
Standort Berlin S. 98

HEFT IM HEFT



**BRAND-
SCHUTZ**
ab S. 59

WILEY



Verband für Sicherheit
in der Wirtschaft

Hessen – Rheinland-Pfalz – Saarland

VSW-Sicherheitstag

Gemeinsam die Sicherheit in der Wirtschaft stärken

Der jährliche VSW-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.

Save the date!

Nähere Informationen
und Möglichkeit
zur Anmeldung:



[www.vsw.de/themen/
vsw-sicherheitstag](http://www.vsw.de/themen/vsw-sicherheitstag)

30. September 2026

Ort: Schloss Waldthausen bei Mainz

Verband für Sicherheit in der Wirtschaft
Hessen – Rheinland-Pfalz – Saarland e.V. (VSW-Mainz)
info@vsw-mainz.de | vsw.de



Genehmigung und Gewissheit

■ Normen, Regularien und Prüfverfahren sind unverzichtbar – doch sie ersetzen nicht den kritischen Blick auf reale Risiken, operative Abläufe und die Resilienz von Organisationen. Es besteht eben ein Unterschied zwischen formaler Genehmigung und tatsächlicher Wirksamkeit und der Gewissheit, alles für die Sicherheit getan zu haben. Eben hier setzt unsere Titelstory „Wenn genehmigt nicht gleich sicher heißt“ an (ab Seite 62). Am Beispiel des Umgangs mit Gefahrstoffen macht sie deutlich, warum genehmigte Prozesse allein keine Sicherheit garantieren. Ein Umdenken ist notwendig: weg vom reinen Erfüllen formaler Anforderungen, hin zu ganzheitlichen, präventiven Sicherheitskonzepten.

Ergänzt wird das Titelthema durch unser „Heft im Heft“ im Bereich Brandschutz (ab Seite 59). Denn Brandschutz bleibt auch in Zeiten von Cyberangriffen ein zentrales Fundament betrieblicher Sicherheit – nicht nur technisch, sondern auch organisatorisch.

Einen strategischen Blick auf die Unternehmenssicherheit wirft unser Interview mit Dr. Alexandra Forster, Head of Corporate Global Security bei der Bayer AG (ab Seite 14). Sie beschreibt, wie sich Corporate Security in einem global agierenden Konzern neu positioniert: vernetzt mit Cyber Security, Compliance und Risikomanagement, stärker datenbasiert und gleichzeitig näher an den Menschen und den operativen Realitäten.



Auch technologisch richten wir den Blick nach vorn: Mit dem ersten Fachbeitrag zur neuen Reihe „TimeSensitive Networking – TSN in der Anwendung“ (ab Seite 80) starten wir eine vertiefende Auseinandersetzung mit einer Schlüsseltechnologie für industrielle Kommunikation. TSN steht exemplarisch für den wachsenden Anspruch, Verfügbarkeit, Echtzeitfähigkeit und Sicherheit in industriellen Netzen zusammenzuführen – ein Thema, das weit über die Automatisierung hinausreicht.

Außerdem startet unser GIT SICHERHEIT AWARD in eine neue Runde. Ab Seite 8 stellen wir die Finalisten vor und laden Sie ein, aktiv mit abzustimmen. Der Award zeigt, wie vielfältig, innovativ und dynamisch sich Sicherheitslösungen aktuell entwickeln – von der Maschine bis zum Perimeter, vom Brandschutz bis zum Sicherheitsmanagement.

Blieben Sie aufmerksam, bleiben Sie kritisch – und bleiben Sie sicher.

Herzlichst,
Ihr

Dr. Timo Gimbel
für das Team GIT SICHERHEIT



Jetzt sind Sie dran:
Wählen Sie die
nächsten Gewinner!



www.sicherheit-award.de

Speedgate SG Expression

Moving by Design

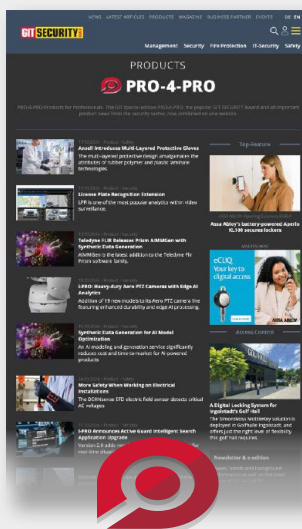




TITELTHEMA

Genehmigt ≠ sicher
Gefahrstoffmanagement
zwischen Mindeststandard
und Vision Zero

ab Seite 62



GIT-SICHERHEIT.DE/DE/PRODUKTE
PRODUCTS FOR PROFESSIONALS

Produkt- und Lead-Plattform
für Sicherheit



14 Alexandra Forster



18 Wolfgang Hofmann



28 Simone Schön



36 Jürgen Maronn

3 Editorial

Dr. Timo Gimbel

GIT SICHERHEIT AWARD

8 JETZT ABSTIMMEN!

www.sicherheit-award.de

MANAGEMENT

CORPORATE SECURITY

14 Security in Zeiten der Transformation

Im Gespräch mit Dr. Alexandra Forster, Head
of Corporate Global Security bei der Bayer AG

18 Tornados, Masern, Grenzkontrollen

Aktuelle Tipps für die Sicherheit auf
Geschäftsreisen in die USA

20 Sicherheitsindustrie als zentraler Wachstumstreiber

Neue europäische Verteidigungs-
Fachmesse „Euro Defence Expo“
startet am 22. September

22 SicherheitsExpo München 2026

Aktuelle Entwicklungen, Trends und
Lösungen

23 PMRExpo 2026

Leitmessen für hybride, kritische
Kommunikation

PERSONENSCHUTZ

24 Wie unsichtbare Schatten

Schutz für exponierte Personen und
wohlhabende Familien

MUSEUMSSICHERHEIT

28 Aktuelle Fragen der Museumssicherheit

Schutz von Kulturgütern durch
innovative Lösungen

PRE-EMPLOYMENT SCREENING

30 Pre-Employment Screening als Sicherheitskonzept

Wie Unternehmen Sicherheitsrisiken im
Bewerbungsprozess minimieren

SECURITY

SCHLIESSTECHNIK

34 Vertrauen und Leidenschaft

SimonsVoss: Zutrittssystem für
Wiener Steuerberatungskanzlei

SCHLIESSTECHNIK

36 Den Wandel aktiv mitgestalten

Vor 90 Jahren wurde in der Kölner
Domstraße das heutige Unternehmen
Dom Sicherheitstechnik gegründet

38 Wechsel an der ESSA-Spitze

Sicherheitsbranche auf künftige Risiken
vorbereiten

ZUTRITT

41 Vom Schloss zum System

BKS: Intelligente Sicherheitslösungen auf der
SicherheitsExpo München 2026

CASINOS

42 Eine Lösung die mitwächst

Skalierbare Videosicherheitstechnologie für
das Snoqualmie Casino & Hotel

MONITORE

44 Wenn Ausfälle keine Option sind

Monitore für Leitstellen, Leitwarten und
Kontrollräume

EVENT

46 Sicherheit im Realtest

Live-Demos, Fachvorträge und
Einordnung neuer Gesetze beim
TechDay in Rödermark

FÄLSCHUNGSSICHERHEIT

48 Standard für Authentizität

Vom Fraunhofer-Forschungsprojekt zur
globalen Sicherheitslösung für physische
Produkte

50 Zwischen Einfachheit und Skalierbarkeit

GIT SICHERHEIT untersucht die neue
Zutrittskontrollzentrale Axon2600 von Aritech



38 Myriam Bevillon



66 Johannes Falk



72 Christoph Bahlmann



88 Philipp Heinemann

CYBER-SECURITY

JAMMING & SPOOFING

52 Gegen GNSS-Jamming und Spoofing
Lösungen zum Schutz kritischer Infrastrukturen

SAAS

56 Höchste Priorität: Sicherung der Identität
SaaS-Bedrohungslandschaft 2025: Verletzungen um 300 Prozent angestiegen

SAFETY

MASCHINEN & ANLAGEN

80 Time-Sensitive Networking – TSN in der Anwendung
Zukunftstechnologie für die industrielle Kommunikation

EVENT

84 Verdichtet statt verteilt
Neues Hallenkonzept, klare Themencluster: Wie die Hannover Messe 2026 dem Wandel in der Messelandschaft in Deutschland begegnet

COMPUTER VISION

86 Am Wendepunkt
Von Kontext bis Edge-KI: Computer Vision in der Industrie

SCHUTZHANDSCHUHE

88 Handschutz mit Herkunft: Showas Weg nach Deutschland
Wie Japans Handschutzspezialist durch Materialkompetenz und Produktionskontrolle den deutschen Markt erobern will

SCHUTZKLEIDUNG

90 70 Jahre Workwear von Kübler
Wie das Familienunternehmen seine Position im Markt für Arbeits- und Schutzbekleidung kontinuierlich ausbaut

HEFT IM HEFT – BRANDSCHUTZ

INNENTITEL

60 Wenn Energie zum Risiko wird
Warum die kWh das zentrale Schutzziel bei Lager- und Ladeschränken für Lithium-Ionen-Batterien ist

TITELTHEMA

62 Wenn genehmigt nicht gleich sicher heißt
Gefahrstoffmanagement zwischen Mindestanforderung und Vision Zero

SPRINKLER

66 Der intelligente Sprinkler
Neues Systemkonzept ermöglicht gezielte, proaktive Brandbekämpfung statt rein thermischer Auslösung

MESSEN

68 Feuertrutz 2026
Treffpunkt der Brandschutzbranche

KANALRAUCHMELDER

70 Früherkennung statt Brandfall
Vorbeugender Brandschutz im Gebäudebetrieb: Oppermann zeigt Überwachungs-lösungen auf der Feuertrutz 2026

KRISENVORSORGE

71 Blackout
Was passiert, wenn der Strom wegbleibt?

ÖFFENTLICHE SICHERHEIT

72 Schutz und Rettung rund um die Uhr
Feuerwehr Hannover: Von Brand- bis Katastrophenschutz

MUSEUMSSICHERHEIT

76 Bewahrung des Unwiederbringlichen
Brandschutz für Museen

INDEX

QUICK-FINDER

ORGANISATIONEN, INSTITUTIONEN UND UNTERNEHMEN IM HEFT

@risc	71
ABB Stotz-Kontakt	83
AFAQ	22, 57
AG Neovo	19
ASW-BW e.V.	13
Apem	83
Asecos	87
Assa Abloy Entrance Systems	3
Assa Abloy Sicherheitstechnik	47, 51, 65
ASW West e.V.	21
Atlas Schuhfabrik	10
Aug. Winkhaus	49
Axis	7, 86
Barox	41
Bayer	14
Bihl & Wiedemann	85, U4
BKS	41
Blakläder Deutschland	10
Bosch Secure Authentication	48
BSI	55
Bundeskriminalamt	17, 7
BVFA e.V.	69
BVSW e.V.	18
Cemo	59, 60
CLPA Europe	80
Corporate Trust Business Risk & Crisis Management	24
d&d Brandschutzsysteme	69
Dallmeier	42
Denios	Titelseite, 62
Deutsche Messe	84
Dom Sicherheitstechnik	36
Dupont de Nemours	10, 87
E. Dold & Söhne	9, 83
Eizo	35, 44
eks Engel FOS	27
Erfolgslabor Schraner	67
Euchner	9
ESSA e.V.	38
Fire Protection Solutions	51
Fraunhofer SIT	55
Genetec Deutschland GmbH	55
Geze	6
Gloria	75
Gretsch-Unitas	41
HB Protective Wear	91
Helly Hansen	87
Hensec	52
Hertek	78
Hilscher	80
Hirsch Secure	10, 11, 12
Inotec	79
Interkey .e.V.	39
Johnson Controls	12
KGS Fire & Security	23, 50
Koelnmesse	23
Kötter	6, 17
Krause-Werk	11
Landeshauptstadt Hannover - Fachbereich Feuerwehr	72
Landesstelle für die nichtstaatlichen Museen in Bayern	28
Leuze	85
Lupus	69
Messe Essen	6, 20, 45
Minimax Fire Solutions	69
Minimax Mobile Services	65, 79
Mobotix	39
NürnbergMesse	39, 68, 79
Obsidian	56
Oppermann Regelgeräte	70
Paul H. Kübler Bekleidungswerk	90
PCS	43
PHG Peter Hengstler	31
Primion	6
Salto Systems	37, 57
Sälzer	57
Schraner	67
Securiton	65
Showa	88
Siemens	49
Signum Consulting/DISA	30
SimonsVoss	33, 34
Sinfiro	27, 79
Stöber	83
Talentus	Beilage
Telenot	7, Beilage
TÜV Nord	87
Uhlmann & Zacher	39
Uvex Safety	91
VDMA e.V.	80
VSW Hessen - Rheinland- Pfalz - Saarland e.V.	U2
Videor E. Hartig	46
Vinci Building Solutions	66
Wagner Group	76, 79
Wichmann	65, 69

Messe-Geschäftsführer Oliver P. Kuhrt zur Euro Defence Expo

Die veränderte sicherheitspolitische Lage wirkt zunehmend auf die industrielle Entwicklung in Deutschland. Der Krieg in der Ukraine, Konflikte im Nahen Osten und der wachsende Fokus auf Zivilschutz verändern Märkte, Geschäftsmodelle und Investitionsentscheidungen spürbar. Genau hier setzt die Euro Defence Expo an. Die neue internationale Fachmesse der Verteidigungsindustrie feiert vom 22. bis 25. September in der Messe Essen ihre Premiere. Rund 250 Aussteller werden erwartet. Für Messe-Geschäftsführer Oliver P. Kuhrt ist klar: Die wirtschaftlichen Auswirkungen dieser Entwicklung sind erheblich. „Deutschland diskutiert Verteidigung noch immer vor allem politisch – tatsächlich erleben wir aber gerade eine tiefgreifende industrielle Verschiebung“, so Oliver P. Kuhrt. „Wer heute über die Zukunft von Industrie spricht, kommt an diesem Thema nicht mehr vorbei. Dahinter steckt enorme Dynamik für Innovation, Investitionen und Beschäftigung.“



www.messe-essen.de

Aus G.I.P. wird Kötter Cyber Security

Die Kötter Security Gruppe entwickelt ihren ganzheitlichen Sicherheitsansatz konsequent weiter: Der Cybersicherheits-Spezialist G.I.P., an dem Deutschlands größter familiengeführter Sicherheitsdienstleister eine Mehrheitsbeteiligung hält, agiert nun als Kötter Cyber Security. Die Umbenennung macht die enge Verzahnung von physischer und digitaler Sicherheit sowie Risikomanagement innerhalb der Unternehmensgruppe künftig auch im Marktauftritt sichtbar. „Die Bedrohungslage verändert sich grundlegend: Angriffe erfolgen heute zunehmend hybrid – also durch die Kombination physischer und digitaler Angriffsvektoren“, erklärt Dirk H. Bürhaus, Geschäftsführender Direktor innerhalb der Kötter Security Gruppe und zugleich Geschäftsführer der Kötter Cyber Security SARL. „Deshalb reicht es längst nicht mehr aus, Cyber Security isoliert zu betrachten.“



Dirk H. Bürhaus,
Geschäftsführender
Direktor innerhalb der
Kötter Security Gruppe
und zugleich Geschäftsführer der Kötter Cyber Security SARL

www.koetter.de

Primion verstärkt Engagement im österreichischen Markt

Die Primion Technology GmbH baut ihre Aktivitäten in Österreich gezielt weiter aus. Mit Herbert Henninger hat das Unternehmen jetzt einen erfahrenen Manager und Vertriebsprofi für den österreichischen Markt gewonnen und setzt damit ein klares Signal für die strategische Bedeutung Österreichs innerhalb der DACH-Wachstumsstrategie.

Österreich ist für Primion ein Markt mit hohem Potenzial und klarer Priorität. Die starke Industriebasis des Landes, ein ausgeprägtes Bewusstsein für Compliance und Sicherheitsstandards sowie eine Vielzahl von Unternehmen aus den Zielbranchen von Primion schaffen ideale Voraussetzungen. Herbert Henninger kennt den österreichischen Markt, seine Strukturen und seine Entscheider aus langjähriger beruflicher Praxis. Mit diesem wertvollen Know-how schafft das Unternehmen die Grundlage, um österreichische Kunden und Interessenten noch näher und gezielter zu betreuen: von der ersten Beratung bis zum langfristigen Support.

„Österreich ist ein Markt hohem Anspruch an Sicherheit, Effizienz und Zukunftsfähigkeit: Unternehmen, die Sicherheit und operative Effizienz nicht mehr als getrennte Welten begreifen, sondern als zwei Seiten derselben Medaille. Genau hier setzt Primion an – mit Converged Security und Workforce Management auf einer gemeinsamen Plattform, unterstützt durch KI-basierte Lösungen, die nicht nur reagieren, sondern antizipieren. Ich freue mich darauf, diesen Dialog mit österreichischen Unternehmen zu führen und gemeinsam bedarfsgerechte Lösungen zu entwickeln“, so Herbert Henninger, Primion Austria.



Herbert Henninger

www.primion.io



Dimitri Milahin, Branch Officer Sales & Service East bei Geze, nahm den Preis für den TS 7000 entgegen

Geze Türschließer TS 7000 erhält den German Innovation Award 2026

Der TS 7000 von Geze setzt seine beeindruckende Erfolgsgeschichte fort: Mit dem German Innovation Award 2026 in der Kategorie „Excellence in Business to Business – Building & Elements“ sichert sich die innovative Türschließer-Generation bereits die dritte hochkarätige Auszeichnung. Die Expertenjury prämierte den Türschließer als „Winner“ und würdigt damit eine herausragende Innovationsleistung, die das Leben durch Fortschritt und gesellschaftlichen Mehrwert nachhaltig verbessert. Dass der TS 7000 den Nerv der Zeit trifft und hohe Ansprüche moderner Architektur erfüllt, beweist die anhaltende Anerkennung durch unabhängige Fachjurys. Nach dem Gewinn des Iconic Award 2025 und dem German Design Award 2026 macht der German Innovation Award das Auszeichnungs-Triple nun komplett – und das noch vor seiner offiziellen Markteinführung im Sommer.

www.geze.com

Bedeutung von Auslandstaten bei Cybercrime und Betrug nimmt zu

Die im Inland registrierten Fälle sind bei Betrug (-8,4 Prozent) und Cyberkriminalität (-4,1 Prozent) zwar rückläufig, im Gegenzug steigen jedoch die aus dem Ausland heraus begangenen Taten deutlich an (Betrug: +7,0 Prozent, Cyberkriminalität +3,0 Prozent). Bei Betrug nähert sich die Anzahl der Inlands- und Auslandstaten und die Schadenssumme zunehmend an (PKS-Ausland 2,3 Mrd. Euro, +65,1 Prozent; PKS-Inland 2,7 Mrd. Euro, -6,7 Prozent). Im Bereich der Cyberkriminalität übersteigt die Anzahl der Auslandsstaten bereits die der Inlandstaten.

Nach den Ergebnissen der Dunkelfeldstudie SKiD war bereits jede fünfte Person Opfer von Delikten aus dem Bereich der Cyberkriminalität. Datenmissbrauch sowie Waren- und Dienstleistungsbetrug im Internet sind dabei die häufigsten Delikte, die auch im Vergleich zur vorherigen Erhebung 2020 signifikant zugenommen haben. Mit der zunehmenden Betroffenheit fürchtet mittlerweile mehr als jeder Zweite, Opfer von Betrug im Internet zu werden.

BKA: Rückgang bei Gewaltkriminalität – Anstieg bei tatverdächtigen Kindern

Bundesinnenminister Alexander Dobrindt, der IMK-Vorsitzende Senator Andy Grote und BKA-Präsident Holger Münch haben die Polizeiliche Kriminalstatistik vorgestellt. Zeitgleich wurden die Ergebnisse der bundesweiten Dunkelfeldstudie „Sicherheit und Kriminalität in Deutschland 2024“ präsentiert.

Erstmals seit 2021 ist 2025 die Zahl der Fälle von Gewaltkriminalität in Deutschland wieder leicht gesunken (-2,3 Prozent). Auch die Anzahl der Tatverdächtigen ging hier zurück (-2,6 Prozent), insbesondere die der tatverdächtigen Jugendlichen (-7,4 Prozent) und der tatverdächtigen Zuwanderer (-7,2 Prozent). Dagegen stieg die Zahl der tatverdächtigen Kinder erneut an (+3,3 Prozent). Nichtdeutsche Tatverdächtige sind bei der Gewaltkriminalität mit 42,9 Prozent weiterhin deutlich überrepräsentiert.



Manuel Neuer steht für Werte wie Sicherheit, Vertrauen und Zuverlässigkeit – Werte, für die auch Telenot als Hersteller elektronischer Sicherheitstechnik steht. „Damit ist er die perfekte Besetzung als Markenbotschafter für Telenot“, betonen Anja Wunderle und Dr. Timo Stock von der Geschäftsführung des Unternehmens

Manuel Neuer ist mehr als nur ein Markenbotschafter

Die DNA von Telenot spiegelt sich auch im neuen Markenbotschafter des Unternehmens wider: Manuel Neuer – Torhüter des FC Bayern, Weltmeister, Champions-League-Sieger, mehrfacher Deutscher Meister sowie Pokal- und Triple-Sieger. Er gilt weltweit als einer der prägendsten und revolutionärsten Spieler auf seiner Position und hat mit seinem Stil neue Maßstäbe für modernes Torwartspiel gesetzt.

Mit diesen Eigenschaften ist Manuel Neuer für Telenot „die ideale Wahl“, wie Telenot-Geschäftsführer Dr. Timo Stock erläutert: „Telenot gehört nach der Archetypen-Theorie von C. G. Jung zu den klassischen Beschützermarken.“ Gezielt habe man nach einer Persönlichkeit gesucht, die das Profil eines vertrauenswürdigen, sympathischen und absolut zuverlässigen Beschützers verkörpert – als Personifikation der Telenot-Philosophie sozusagen. „Mit Manuel Neuer haben wir nicht nur eine herausragende sportliche Persönlichkeit gefunden, sondern auch einen authentischen Menschen, der für die Werte Sicherheit, Vertrauen und Zuverlässigkeit steht“, so Dr. Timo Stock. Zudem nutze er selbst seit Jahren eine Alarmanlage von Telenot.

Die neue Kampagne von Telenot steht unter dem Motto „Sicherheit Neuer Gedacht.“ Der Torhüter wird dabei auf allen relevanten Kanälen die Produkte und Systeme in Fach- und Publikumsmedien präsentieren. „Hier trifft sportliche auf sicherheitstechnische Weltklasse“, ergänzt Telenot-Geschäftsführerin Anja Wunderle.

www.telenot.com

Erfassen. Sehen. Verifizieren.

AXIS Q2802-E Bispectral Camera

Setzen Sie neue Maßstäbe im Perimeterschutz und der Grenzkontrolle: Diese leistungsstarke All-in-One-Bispektralkamera vereint hochauflösende Wärmebildtechnologie mit gestochen scharfem 4K-Video. So erkennen Sie Bedrohungen frühzeitig, erfassen jedes Detail präzise und verifizieren Ereignisse in Sekunden. Die nahtlose Fusion aus thermischem und sichtbarem Bildmaterial sorgt dabei für ein außergewöhnlich klares Situationsbewusstsein.

Mehr erfahren: www.axis.com/de-de/products/axis-q2802-e



JETZT ABSTIMMEN

www.sicherheit-award.de

dort auch ausführliche Infos zu den Produkten

Auf geht's in die nächste Runde. Es geht wieder um innovative Produkte und Lösungen, die das nächste Jahr sicherheitstechnisch prägen können. Gemeinsam mit einer neutralen Jury wurden Einreichungen und Anmeldungen von Anbietern bewertet: Wie innovativ ist eine Lösung, wie bedeutend kann sie für welchen Markt und welche Zielgruppe sein? Finden Sie auf den folgenden Seiten die neuen Kategorien und die Shortlist für den GIT SICHERHEIT AWARD.

Wer sind ihre Favoriten?

Treffen Sie jetzt online je eine Auswahl in jeder Kategorie:

- A – Maschinen- & Anlagensicherheit
- B – Arbeitsschutz & Ex-Schutz
- C – Video-Sicherheit & Video-Management
- D – Zutritt & Einbruchschutz
- E – Sicherheitsmanagement, Gebäudesicherheit & Perimeterschutz
- F – Brandschutz

Um für eine faire Abstimmung zu sorgen, ist es nicht gestattet, für das eigene Unternehmen zu stimmen. Daher sehen die Regeln vor, dass ausschließlich online und unter Angabe eines Firmennamens gevotet werden kann. Privatpersonen sind nicht stimmberechtigt. Weitere Informationen (siehe auch QR-Code rechts) auf www.sicherheit-award.de

Leserpreis gewinnen

Unter allen gültigen Stimmabgebenden verlosen wir drei hochwertige Ledlenser Taschenlampen P7R Work UV.



**Leser
Preis**

**GIT
SICHERHEIT
AWARD
FINALISTEN**

Jetzt abstimmen

vom 1. Juni bis

1. September 2026 auf

www.sicherheit-award.de

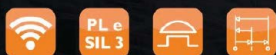


Kategorie A: Maschinen- & Anlagensicherheit

Bihl+Wiedemann	ASi-5 Safety Leiterplattenmodul
E. Dold & Söhne	Innovatives Funk-Sicherheitssystem RE 6900
Euchner	Transpondercodiertes Schlüsselsystem CKS2
K. A. Schmersal	SFB Port Extender für flexible Sicherheitsarchitekturen
Mersen	ProGrid Solutions – Sicherungslasttrennschalter für die Energiewende
Moxa Europe	NPort 6000-G2 Serie – Sichere Serial Device Server
Murr	MVK Fusion CIP Safety – 3-in-1 Hybrid-Feldbusmodul
Phoenix Contact	Multifunktionales Sicherheitsrelais PSR-UNI
Sick AG	Sicherheitssteuerung Flexi Net – für stationäre und mobile Maschinen

Shortlist Highlights**Kategorie A: Maschinen- & Anlagensicherheit****E. Dold & Söhne:
Innovatives Funk-Sicherheitssystem RE 6900**

Wartungsarbeiten, Service- und Einrichtbetrieb an Roboterzellen oder die Not-Halt-Abschaltung von weitläufigen Maschinen und Anlagen stellen hohe Anforderungen an die Sicherheit – vor allem dann, wenn Abschalten und Zustimmung kabellos erfolgen müssen. Genau hier setzt das neue Funk-Sicherheitssystem RE 6900 der Safemaster W Serie von Dold an: Das System ermöglicht das sichere Abschalten per Funk-Not-Halt oder die sicherheitsgerichtete Zustimmung im Einrichtbetrieb mit dem Funk-Zustimmtaster. Entwickelt für maximale Bewegungsfreiheit bei gleichzeitig höchstem Sicherheitsniveau bis Kat. 4 / PL e bzw. SIL 3, ist der Funk-Handsender die ideale Lösung für moderne Automatisierungs- und Instandhaltungskonzepte. Der Funk-Zustimmtaster ermöglicht ein sicheres Bedienen und verhindert das unbeabsichtigte Starten gefährlicher Bewegungen, da nur eine aktiv betätigte Mittelstellung des Dreistufentasters die Zustimmung für die Maschinenbewegung per Funk erteilt.

Wireless Safety System**Mehr
Infos**

© E. Dold & Söhne GmbH & Co. KG

Kategorie A: Maschinen- & Anlagensicherheit**Euchner: Transpondercodiertes Schlüsselsystem CKS2**

Das transpondercodierte Schlüsselsystem CKS2 von Euchner ist ein sicheres Zugangs- und Freigabesystem für Maschinen und Anlagen. Es richtet sich an Maschinen- und Anlagenbauer sowie Betreiber, die Manipulation zuverlässig verhindern möchten. Codierte Schlüssel mit Transpondertechnologie sorgen für klare Berechtigungen, erhöhen die Maschinensicherheit und unterstützen einen sicheren, kontrollierten Betrieb. Dank der integrierten Auswerteelektronik ist das CKS2 ein kompaktes System, das durch verschiedene Schlüsselausführungen für vielseitige Anwendungen eine Lösung bietet. Ob als Sperrsystem, Schlüsseltransfersystem oder Berechtigungssystem – überall dort, wo gefährliche Maschinenbewegungen unabhängig von den vorhandenen Schutzeinrichtungen sicher gestartet oder gestoppt werden müssen, ist das CKS2-System die richtige Wahl. Dank der bewährten Transpondertechnologie und der hohen Codierung ab Werk entfällt ein aufwändig projektiertes Schlüsselmanagement.

**Mehr
Infos**

Weitere
Shortlist Highlights
im nächsten Heft

Kategorie B: Arbeitsschutz & Ex-Schutz

Ansell Healthcare	Acetonbeständige Handschuhe TouchNTuff 93-800
Atlas Schuhfabrik	Max Series – Sicherheitsschuhe für extreme Einsatzbedingungen
Blaklaeder	Multinorm-Langarmshirts 3436/3437
Denios	Real-time Asset Monitoring für Sicherheitsschranke
Dupont	Chemikalienschutz mit Fokus auf Tragekomfort
Ejendals	Schutzhandschuh Tegera Uniform 9078
Fristads	Multinorm Green – Schutzkleidung mit transparenter Umweltbilanz
HB Protective Wear	Softshelljacke HB-ArcFlash Pro 4kA und 7kA
Krause-Werk	Stabilo Stufen-Stehleiter 135 XL
Munk Group	Modulare Montageplattform

Kategorie B: Arbeitsschutz & Ex-Schutz**Atlas: S3S-Sicherheitsschuhe der Max Series**

Mit der Max Series stellt Atlas eine S3S-Schuhserie für anspruchsvolle Arbeitsbedingungen vor, die auf Robustheit, geringes Gewicht und Formstabilität ausgelegt ist. Im Zentrum steht das leichte und widerstandsfähige Obermaterial ProTraX, das sich durch geringe Wasseraufnahme und schnelle Rücktrocknung auszeichnet und so konstanten Tragekomfort in feuchten Umgebungen ermöglicht. – Für Trittsicherheit und Dämpfung sorgt die XR-MPU-Sohlentechnologie mit Flexkerben, Dynamic Plates und Cloudzone zur Unterstützung der Beweglichkeit und Auftrittsdynamik. Eine metallfreie Durchtrittshemmung sowie eine abriebfeste Überkappe erhöhen den Schutz zusätzlich. Je nach Modell stehen klassische Schnürsysteme oder das Boa Fit System zur Verfügung. Insgesamt verbindet die Serie Schutz, Funktionalität und Komfort mit dem Ziel, Ermüdung bei intensiver Nutzung zu reduzieren.

**Kategorie B: Arbeitsschutz & Ex-Schutz****Bläkläder: Multinorm-Langarmshirts 3436/3437**

Mit den Multinorm-Langarmshirts 3436 (Herren) und 3437 (Damen) adressiert Bläkläder die zentrale Herausforderung mangelnder Trägerakzeptanz bei Schutzkleidung. Die Shirts bestehen aus leichtem Piqué-Strick und bieten einen an Freizeitbekleidung orientierten Tragekomfort bei gleichzeitig umfassendem Schutz für anspruchsvolle Einsatzbereiche. – Die Materialien sind inhärent flammhemmend und antistatisch, wodurch die Schutzwirkung dauerhaft erhalten bleibt. Zertifizierungen nach EN ISO 11612, EN 61482-2, EN 1149-5 sowie EN ISO 20471 gewährleisten den Einsatz bei thermischen Gefahren, Lichtbogenrisiken und Sichtbarkeitsanforderungen. Ein speziell entwickelter Damenschnitt stellt im Multinorm-Segment eine Besonderheit dar. Insgesamt verbindet die Lösung Schutz, Komfort und Passform mit dem Ziel, die konsequente Nutzung von PSA im Arbeitsalltag zu erhöhen.

**Mehr
Infos****Kategorie B: Arbeitsschutz & Ex-Schutz****DuPont: Chemikalienschutzanzug Tyvek APX**

Tyvek APX von DuPont ist ein Chemikalienschutzanzug mit hoher Luftdurchlässigkeit (Hohenstein-Klassifizierung) und kombiniert Schutz, Haltbarkeit sowie geringes Gewicht. Dadurch eignet er sich besonders für Einsätze in warmen, feuchten und körperlich anspruchsvollen Arbeitsumgebungen. – Unabhängige Labortests zeigen eine reduzierte Hitzebelastung im Vergleich zu herkömmlichen Anzügen, da der Anstieg von Körper- und Hauttemperatur langsamer erfolgt und die Regeneration unterstützt wird. Praxistests bestätigen zudem einen verbesserten Tragekomfort und eine höhere wahrgenommene Leistungsfähigkeit unter realen Einsatzbedingungen. Die Lösung verbindet somit zuverlässigen Schutz mit gesteigertem Komfort und fördert die konsequente Nutzung im Arbeitsalltag.



Kategorie B: Arbeitsschutz & Ex-Schutz

Krause-Werk: Stabilo Stufen-Stehleiter 135 XL

Die Stabilo Stufen-Stehleiter 135 XL ist für hohe Belastungen bis 225 kg ausgelegt und bietet durch ihre stabile Konstruktion sowie einen extra hohen Sicherheitsbügel ein sicheres Arbeiten. Eine integrierte Werkzeugablage mit Eimerhaken und eine große Aluminium-Sicherheitsplattform ergänzen die Ausstattung. – Die 135 mm tiefen Stufen sorgen für hohen Standkomfort, insbesondere bei längeren Einsatzzeiten. Hochwertige Gelenkverbindungen, robuste Gurtbänder sowie rutschhemmende Fußstopfen erhöhen Stabilität und Sicherheit zusätzlich. Die Leiter ist für intensive Beanspruchung konzipiert und unterstützt mit durchdachten Details eine zuverlässige und ergonomische Nutzung im Arbeitsalltag.



**Mehr
Infos**

Shortlist Highlights

Kategorie C: Video-Sicherheit & Video-Management

Ajax Systems	Serie Superior NVR H2D – KI-gesteuerte Netzwerkvideorekorder
Axis Communications	Q6411-LE Bispectral PTZ Camera
Dallmeier Electronic	Multifocal-Sensorkamera Panomera V8
Hanwha Vision	PTZ-Kameras für raue Umgebungen
LiveEye	Digitales Planungstool für temporäre Sicherheitskonzepte
Security Robotics	Sicherheitsplattform ACUDA
Spectro AI	Spectro AI: DockWatch Trailer

Kategorie D: Zutritt & Einbruchschutz

Ajax Systems	Superior MotionCam G3 (PhOD) Jeweller – Kabelloser PIR-Bewegungsmelder
ASL-Ademco	Klinkenwächter ABAX
Aug. Winkhaus	Elektronisches Schließsystem BlueEvo
Dom Sicherheitstechnik	Online Mesh zur Vernetzung digitaler Schlösser
Dormakaba	Automatische Schiebetür ST PRO Green RC3
Hirsch	Zutrittssystem Microsesame
Ksenia	Conexa ist die IP-Touchscreen-Tastatur
MP-Bos	Digitaler Ausweis BOS-ID
Portier Global	Schließenanlagen-Software Portier Vision 5
Satel	Be Wave Hybrid – Sicherheits- und Gebäudeautomationssystem
Schmeissner	Kapazitive Durchbruchsicherung
Telenot Electronic	hiline1 – Übertragungseinrichtung
Tell Software	Nachrüstmodul OPEN.ioting Smart Gate Opener

Kategorie D: Zutritt & Einbruchschutz

Hirsch Secure: Zutrittssystem Microsesame

Microsesame von Hirsch ist ein zentrales System für Zutrittskontrolle, Gebäudesicherheit und technische Gebäudeverwaltung. Die Management-Software ermöglicht die Zentralisierung aller elektronischen Informationen aus dem Gebäude. – Die Umsetzung der NIS2-Richtlinie rückt für viele Unternehmen immer näher. Sie verfolgt einen „All-Hazards“-Ansatz und macht deutlich, dass Cyber- und physische Sicherheit untrennbar verbunden sind. Veraltete Türen, unklare Berechtigungen oder fehlende Protokollierung können damit schnell zum Compliance-Risiko werden – und im Ernstfall teuer. Die zukunftssichere Zutrittskontrolllösung Microsesame setzt auf bewährte Standards, ist in Europa entwickelt und wurde jetzt an die gewachsenen Cybersicherheitsanforderungen angepasst. Die Lösung unterstützt moderne Technologien wie IP-Netzwerke, RS485-Bus sowie aktuelle Windows- und SQL-Systeme. Das vollständig von der ANSSI zertifizierte und vom BSI anerkannte System gewährleistet nachhaltige Cybersicherheit und lässt sich flexibel an die individuellen Anforderungen von Standorten und Gebäuden anpassen.



Kategorie E: Sicherheitsmanagement, Gebäudesicherheit & Perimeterschutz

Advancis	AIM – Advanced Identity Management
Ajax Systems	Superior Hub G3 Jeweller – Kabellose Hub-Zentrale mit Fotoverifizierung
Ambient System	ICO Emergency – Notrufsprechstelle für kritische Situationen
Axis	D2122-VE Radar und Axis D2123-VE Radar
Chubb	Connected Services – Vernetzte Sicherheitsdienstleistung
Hirsch	Lumor Faseroptik-Intrusionsdetektion
Hiscout	GSS – Geheim- und Sabotageschutzmodul der HiScout GRC Suite
ID-ware	Softwarebasierte Management-Plattform PIAM-Suite
IVMS	Lynx – Gefahrenmanagement-System
KGS Fire & Security	Fusion – Sicherheitsplattform
Octave	Coda Spatial – 3D-Sicherheits- und Perimeter-Überwachung
Quanergy Solutions	Q-Shield – LiDAR-Sensor für Intrusion Detection
Security Robotics	Autonome mobile Sicherheitsroboter (AMSR)

Shortlist Highlights**Kategorie F: Brandschutz**

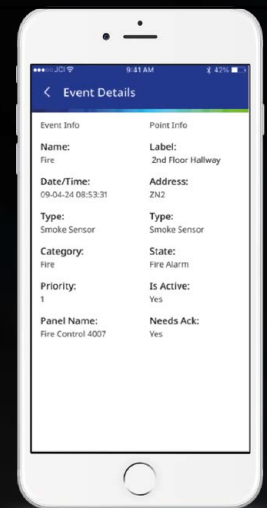
Ajax Systems	EN54 Fire Hub Jeweller – Funk-Brandwarnzentrale
Axis	D6310 Air Quality Sensor für sicherheitsrelevante Innenbereiche
Dehn	Geprüfte E30-Lösung für Überspannungsschutz im Brandfall
Gekartel	VdS 6024-zertifiziertes Brandschutztablet
Hanwha Vision Europe	Bi-Spektrum-Kameras für Brandfrüherkennung
Inotec	Sicherheitsleitsystem GMS zur Evakuierung
Johnson Controls	SafeLinc-Cloud-Weboberfläche und mobile App
Securiton	SecuriGas – Ansaugrauchmelder-System mit hochsensibler Gassensorik
Munk Group	Modulare Montageplattform

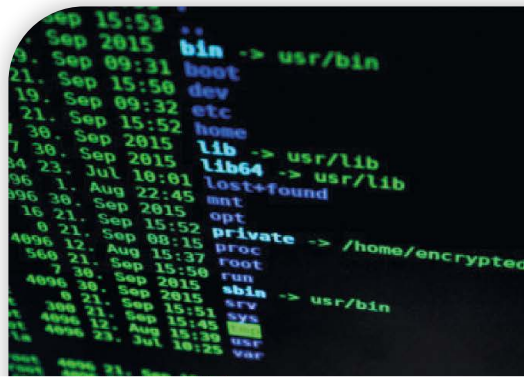
Kategorie E: Sicherheitsmanagement, Gebäudesicherheit & Perimeterschutz**Hirsch Secure:****Lumor Faseroptik-Intrusionsdetektion**

Lumor ist eine Innovation im Bereich der Perimetersicherung und Zaundetektion. Es ist ein hochmodernes Faseroptik-Detektionssystem auf Basis der quantitativen DAS-Technologie (Distributed Acoustic Sensing), das eine kontinuierliche und präzise Überwachung großer Flächen ermöglicht und damit neue Maßstäbe in der Perimetersicherheit setzt. Die DAS-Technologie verwandelt eine Standard-Glasfaser in ein virtuelles Netzwerk aus Tausenden von „Mikrofonen“, die in regelmäßigen Abständen entlang des Kabels angeordnet sind. Diese Sensoren erkennen Veränderungen des im Glasfaserkabel rückgestreuten Lichts und ermöglichen so eine präzise Ereigniserkennung in Echtzeit sowie die Geolokalisierung und Klassifizierung von Aktivitäten. Im Vergleich zu qualitativen Systemen bietet die quantitative DAS-Technologie einen größeren Dynamikbereich, was eine feinere Erkennung und eine optimierte Steuerung von Sicherheitsmaßnahmen gewährleistet. Das System unterscheidet Geräusche z. B. von Motorrädern von Autos, Vierbeinern/Pferden und Menschen und lässt sich vor Ort einlernen, um so ungewöhnliche Geräusche von standorttypischen Geräuschen zu unterscheiden.

**Kategorie E: Sicherheitsmanagement, Gebäudesicherheit & Perimeterschutz****Johnson Controls: Brandmeldezentrale SafeLinc**

SafeLinc von Johnson Controls ist eine cloudbasierte Schnittstelle für den Echtzeit-Fernzugriff auf Daten von Brandmeldezentralen und ermöglicht Facility-Managern sowie Technikern effizientere Notfallmaßnahmen, Verwaltungsfunktionen und Wartungsprozesse. Das Gateway lässt sich an bestehende Systeme anschließen und überträgt detaillierte Ereignisdaten wie Gerätetyp, Zone und Punktadresse in eine zentrale Plattform. – Angesichts steigender Anforderungen an Betriebssicherheit und Verfügbarkeit bietet SafeLinc mit Funktionen wie Ereignisüberwachung, Verlaufsanalysen und Push-Benachrichtigungen eine verbesserte Transparenz über alle angeschlossenen Anlagen. Die Lösung unterstützt Unternehmen dabei, Ausfallzeiten zu reduzieren, Kosten zu senken und Fachkräfte gezielter einzusetzen. Gleichzeitig erleichtert sie die Einhaltung von Compliance-Vorgaben sowie die Koordination von Einsatzkräften im Notfall durch präzise und jederzeit abrufbare Informationen.





© ASW-BW

Lakeside Security Summit 2026

17.–19.
Juni 2026

Vom **17. bis 19. Juni 2026** findet zum fünften Mal der **Lakeside Security Summit** der **ASW Baden-Württemberg** statt. Eine feste Größe für alle, die in der Corporate Security Verantwortung tragen.



Im exklusiven Ambiente des **Hotels Vier Jahreszeiten am Schluchsee** tauschen sich Security-Expertinnen und -Experten aus der baden-württembergischen Industrie, von Beratungs-, Bewacher- und Errichtungsunternehmen zu aktuellen Bedrohungen, innovativen Lösungsansätzen und täglichen Herausforderungen aus. Fachlich fundiert, offen und zugleich in entspannter Atmosphäre.

Hochkarätige Speaker, darunter Vertreter von **BND**, **LfV Baden-Württemberg**, **LKA Baden-Württemberg** sowie der **Bundeswehr**, konnten gewonnen werden und geben Einblicke in ihre jeweiligen Arbeitsbereiche. Als spannenden Exkurs dürfen wir zudem **Dr. Alessandro Bellardita** begrüßen, der über „Mafia in deutschen Unternehmen“ sprechen wird.

Wir freuen uns auf den Austausch mit vielen bekannten und neuen Gesichtern am Schluchsee!

Anmeldungen sind ab sofort unter diesem Link möglich. Die Plätze sind begrenzt! Wie immer gilt bei der Buchung: **First come, first serve!**

Weitere Informationen zu Programm und Inhalten: asw-bw.com



Baden-Württemberg

Allianz für Sicherheit in der Wirtschaft
Baden-Württemberg e.V.
mail@asw-bw.com | asw-bw.com

Security in Zeiten der Transformation

Im Gespräch mit Dr. Alexandra Forster, Head of Corporate Global Security bei der Bayer AG

Als zentrale Fachfunktion entwickelt die Corporate Global Security bei Bayer weltweite Sicherheitsstandards für die drei Divisionen Crop Science, Pharma und Consumer Health. Im Fokus stehen dabei die Verknüpfung von Governance und operativer Umsetzbarkeit sowie die enge Verzahnung mit Cyber Security, Compliance und Risikomanagement. Dr. Alexandra Forster, Head of Corporate Security für den Gesamtkonzern, beschreibt im Gespräch mit GIT SICHERHEIT die aktuelle Bedrohungslage als vielschichtig, geprägt durch geopolitische Spannungen, Wirtschaftsspionage und Cyberangriffe, die den Schutz von Mitarbeitern, Standorten und sensiblen Daten erfordern.

■ GIT SICHERHEIT: Frau Dr. Forster, Sie sind Head of Corporate Global Security bei Bayer. Könnten Sie zum Einstieg bitte einmal Ihre Unit vorstellen?

Alexandra Forster: Corporate Global Security ist bei Bayer die zentrale Fachfunktion für Unternehmenssicherheit. Unsere Aufgabe ist es, weltweit ein gemeinsames Sicherheitsverständnis zu schaffen: mit klaren Standards, belastbaren Prozessen und einem professionellen Lagebild für die relevanten Risiken des Konzerns. Wir unterstützen unsere drei Divisionen Crop Science, Pharma und Consumer Health unter anderem in den Bereichen Standort- und Reisesicherheit, Event Security, Personenschutz, Krisenmanagement, Threat Intelligence und Investigations.

Besonders wichtig ist dabei die Verbindung von Governance und operativer Umsetzbarkeit. Ein Standard ist nur dann wirksam, wenn er auch an einem Produktions-, Forschungs- oder Verwaltungsstandort praktisch funktioniert. Dafür arbeiten wir mit regionalen Sicherheitsverantwortlichen und lokalen Teams in den Ländern zusammen, in denen Bayer tätig ist. An vielen Standorten arbeiten wir mit externen Sicherheitsdienstleistern. Gerade deshalb ist es entscheidend, dass Rollen, Erwartungen und Qualitätsstandards klar beschrieben sind.

Wie definieren Sie für sich Ihre eigene Aufgabe?

Alexandra Forster: Meine eigene Aufgabe sehe ich darin, Orientierung zu geben, Prioritäten zu setzen und unser Team handlungsfähig zu halten. Sicherheit ist heute kein statisches Schutzkonzept mehr, sondern ein kontinuierlicher Anpassungsprozess. In der aktuellen Transformation des Unternehmens ist mir besonders wichtig, meinem Team den Rücken freizuhalten, damit wir uns auf das konzentrieren können, worum es im Kern geht: die Menschen, Standorte, Informationen und die Handlungsfähigkeit von Bayer zu schützen.

Wie arbeitet Corporate Global Security bei Bayer mit anderen Konzernbereichen zusammen?

Alexandra Forster: Corporate Security funktioniert heute nicht mehr in Silos. Viele Sicherheitsfragen liegen genau an den Schnittstellen, etwa zwischen physischer Sicherheit, Cyber Security, Compliance, Legal, HR, Safety oder Risk Management. Wir arbeiten deshalb sowohl strategisch als auch operativ eng mit diesen Funktionen zusammen. Strategisch geht es um gemeinsame Risikobewertungen, Governance und Prioritätensetzung. Operativ arbeiten wir in funktionsübergreifenden Teams, etwa bei Themen wie Produktfälschungen, Bedro-

hungslagen, Reisesicherheit, Schutz sensibler Informationen oder KI-gestützten Betrugsversuchen.

Für mich ist dabei entscheidend, dass Zusammenarbeit nicht erst im Krisenfall beginnt. Wir brauchen belastbare Beziehungen, klare Eskalationswege und ein gemeinsames Verständnis davon, wer in welcher Situation welchen Beitrag leistet. Nur dann können wir schnell und wirksam reagieren.

Es handelt sich bei Bayer um einen Life-Science-Konzern, der mit Produktions- und Forschungsstandorten in etwa 80 Ländern der Erde aktiv ist. Wirtschaftsspionage, politisch motivierte Sabotage, Cyberangriffe, etc. sind Dinge, mit denen sich insbesondere Pharmaunternehmen auseinandersetzen müssen. Könnten Sie uns einmal einen Einblick geben, welche Bedrohungsszenarien für Bayer vor allem relevant sind?

Alexandra Forster: Für ein globales Life-Science-Unternehmen wie Bayer ist die Bedrohungslage sehr vielschichtig. Aus Sicht der Corporate Security stehen für uns mehrere Risikofelder im Fokus. Erstens geht es um den Schutz unserer Mitarbeitenden, insbesondere bei Reisen, Entsendungen, Veranstaltungen oder in Ländern mit erhöhter politischer Instabilität. Geo-



Der Chempark in Leverkusen (ehemals Bayerwerk Leverkusen), ist einer der Standorte, an denen Bayer ansässig ist



Der Life-Science-Konzern Bayer unterhält Produktions- und Forschungsstandorte in etwa 80 Ländern

© Marcus Müller-Saran – stock.adobe.com / Bayer AG

politische Spannungen, soziale Unruhen, Naturereignisse oder regionale Konflikte können sehr schnell Auswirkungen auf unsere Handlungsfähigkeit haben.

Zweitens spielt der Schutz unserer Standorte und Lieferketten eine zentrale Rolle. Produktions- und Forschungsstandorte müssen nicht nur physisch geschützt, sondern auch in ihrer Resilienz betrachtet werden. Das betrifft Zugangskontrollen, Dienstleistersteuerung, Notfallplanung und die Fähigkeit, bei Störungen schnell wieder handlungsfähig zu sein.

Drittens beschäftigen uns der Schutz sensibler Informationen, geistigen Eigentums und Forschungsdaten sowie die Integrität unserer Produkte. Produktfälschungen sind im Pharmabereich nicht nur ein wirtschaft-

liches Risiko, sondern können unmittelbar die Sicherheit von Patientinnen und Patienten betreffen. Cyberangriffe sind dabei ein wesentlicher Teil der Gesamtrisikolage. Die technische Abwehr liegt bei den zuständigen Cyber-Security-Funktionen. Aus Sicht der Corporate Security ist für uns aber entscheidend, dass physische Sicherheit, Lagebild, Krisenmanagement und Cyber Security eng zusammenspielen.

Ihre Einrichtungen zählen vielfach zu den Kritischen Infrastrukturen. Hier gibt es ja derzeit starke normative Veränderungen. Stichwort NIS2 oder KRITIS-Dachgesetz. Wie stellt sich das aus Ihrer Sicht dar – und inwieweit müssen Sie hier sozusagen nachrüsten?

Alexandra Forster: Die regulatorischen Anforderungen rund um Kritische Infrastrukturen, NIS2 und das KRITIS-Dachgesetz sind für uns sehr relevant. Auch wenn mein Verantwortungsbereich primär auf der physischen Sicherheit liegt, lassen sich diese Themen heute nicht isoliert betrachten. Resilienz entsteht nur, wenn physische Sicherheit, Cyber Security, Business Continuity, Krisenmanagement und Governance ineinandergreifen.

Für Corporate Security bedeutet das vor allem: Wir überprüfen bestehende Schutzkonzepte, schärfen Verantwortlichkeiten und schauen sehr genau auf Schnittstellen. Dazu gehören Zugangskontrollen, Dienstleistermanagement, Lagebewertung, Notfallprozesse und regelmäßige Übungen.

Ich sehe die neuen Vorgaben weniger als reines Compliance-Thema, sondern als Anlass, unsere Sicherheitsarchitektur konsequent weiterzuentwickeln. Entscheidend ist, dass regulatorische Anforderungen nicht nur dokumentiert werden, sondern im Ernstfall tatsächlich Wirkung entfalten.

Die Sicherheit von Unternehmen stellt sich heute durch die oft so beschriebenen Veränderungen geopolitischer Art anders dar als noch vor einigen Jahren. Es geht dabei auch um die Risiken für Mitarbeiter, um Reiserisiken etc. Wie spiegelt sich das in Ihrer Strategie für die Corporate Global Security?



Crop Science ist neben Pharma und Consumer Health eine der drei Konzern-Divisions von Bayer

Alexandra Forster: Die sicherheitspolitische Lage hat sich in den vergangenen Jahren deutlich verändert. Risiken entstehen heute oft schneller, sind schwerer vorhersehbar und wirken sich unmittelbarer auf Unternehmen aus. Für Corporate Security bedeutet das: Wir müssen näher an der Lage sein, schneller bewerten und klarer kommunizieren.

Ein Schwerpunkt ist der Schutz unserer Mitarbeitenden. Dazu gehört ein kontinuierliches Monitoring der Sicherheitslage in relevanten Ländern, aber auch eine gute Vorbereitung von Reisen, Entsendungen und Veranstaltungen. Wir unterstützen Mitarbeitende und Führungskräfte mit Lageinformationen, Reisehinweisen und Schulungen, sowie digitalen Reise- und Notfall-Tools.

Wichtig ist mir dabei die Balance: Wir wollen ermöglichen, nicht verhindern.

Unsere Aufgabe ist nicht, pauschal Risiken auszuschließen, sondern verantwortungsvolle Entscheidungen zu unterstützen. Gute Sicherheit schafft Handlungsfähigkeit, gerade in einem komplexen globalen Umfeld.

Wie fließen Erfahrungen mit Sicherheitsvorfällen in Ihr Krisenmanagement ein, wie verändert es sich?

Alexandra Forster: Jeder Sicherheitsvorfall ist auch ein Lernmoment. Entscheidend ist, dass man nach einer Krise nicht einfach zur Tagesordnung übergeht, sondern strukturiert auswertet: Was hat funktioniert? Wo waren Entscheidungswege zu langsam? Welche Informationen haben gefehlt? Und welche Annahmen haben sich im Ernstfall nicht bestätigt?

Wir arbeiten deshalb mit Lessons-Learned-Reviews, passen Krisenpläne und Leitfäden an und nutzen Erkenntnisse für Trainings und Übungen. Besonders wichtig ist aus meiner Sicht, nicht nur Prozesse zu verbessern, sondern auch das Zusammenspiel der beteiligten Funktionen. Krisenmanagement ist Teamarbeit unter Zeitdruck.

Gleichzeitig verändert sich Krisenmanagement selbst. Es muss heute globaler, schneller und vernetzter funktionieren. Eine lokale Störung kann sehr rasch Auswirkungen auf Lieferketten, Reputation, Mitarbeitende oder regulatorische Verpflichtungen haben. Deshalb investieren wir in Lagebild, klare Rollen, belastbare Kommunikationswege und regelmäßige Krisenübungen.

Welche Themen beschäftigen Sie in nächster Zukunft?

Alexandra Forster: Ein zentrales Projekt ist derzeit die Harmonisierung unseres Zutrittsmanagements. Bayer ist über viele Jahre gewachsen, auch durch Akquisitionen. Entsprechend unterschiedlich sind heute auf Standort-Ebene die Systeme und Prozesse. Das ist aus Sicherheitssicht nicht ideal, weil Transparenz und Vergleichbarkeit erschwert werden. Zugleich entsteht hoher administrativer Aufwand. Auch Geschäftsreisende erleben diese Komplexität ganz praktisch, mit langwierigen und uneinheitlichen Voranmelde-Prozessen, um vor Ort ein lokales Badge zu erhalten.

Wir wollen deshalb zunächst unsere Standorte in Deutschland harmonisieren und einen einheitlicheren, skalierbaren Ansatz schaffen. Ziel ist mehr Transparenz, einfachere Administration, klarere Berechtigungen und ein besseres Nutzererlebnis für Mitarbeitende, Besucher und Geschäftsreisende. Wenn der Pilot erfolgreich abgeschlossen ist, soll der Ansatz international weitergeführt werden. Für mich ist das ein sehr gutes Beispiel dafür, wie moderne Corporate Security wirken kann: nicht nur Risiken reduzieren, sondern Prozesse vereinfachen und den Alltag im Unternehmen spürbar verbessern.

Frau Dr. Forster, vielen Dank für das Gespräch. **GIT**



Bayer AG
www.bayer.com

Rückgang bei Straftaten insgesamt

Insgesamt hat die Polizei im Jahr 2025 bundesweit rund 5,5 Mio. Straftaten registriert – das entspricht einem Rückgang von 5,6 Prozent im Vergleich zum Vorjahr. Auch die Zahl der Tatverdächtigen insgesamt ist um 5,9 Prozent auf ca. 2,05 Mio. gesunken. In den Zahlen schlägt sich die (Teil-) Legalisierung von Cannabis aus 2024 nieder, es ist aber selbst dann noch ein Rückgang vorhanden, wenn Straftaten im Zusammenhang mit Cannabis herausgerechnet werden (-4,7 Prozent).

Insgesamt wurden rund 3,2 Mio. Fälle aufgeklärt. Die Aufklärungsquote liegt somit bei 57,9 Prozent und damit auf nahezu gleichem Niveau wie in den Vorjahren (2024: 58,0 % Prozent).

„Der Rückgang der Gewaltkriminalität ist ein Anfang, aber kein Grund zur Entwarnung. Entscheidend ist, dass sich Menschen im Alltag sicher fühlen. Dafür braucht es weitere Maßnahmen: mit einem harten Aktionsplan gegen Organisierte Kriminalität, mit konsequenten Abschiebungen von Intensivtätern und mit klaren, unmissverständlichen Gesetzen zum Schutz unserer Polizistinnen und Polizisten“, so Bundesinnenminister Alexander Dobrindt.

„Das zweite Jahr rückläufiger Kriminalität ist eine ermutigende Entwicklung. Mein Dank gilt den Polizistinnen und Polizisten in unserem Land, die mit ihrer enormen Einsatzbereitschaft maßgeblich dazu beitragen, dass sich die Menschen in Deutschland sicher fühlen. Gleichzeitig müssen wir feststellen, dass unsere Gesellschaft gerade für Frauen nicht so sicher ist, wie sie es sein sollte. Steigende Zahlen im Bereich der Sexualstraftaten und das erschreckende Ausmaß sexualisierter digitaler Gewalt machen deutlich, dass wir Betroffene noch besser schützen müssen. Der hohe Anteil der Beziehungsgewalt zeigt, dass es weiterhin den Mut der Frauen zur Anzeige braucht, aber auch die Entschlossenheit des Rechtsstaats. Als Innenministerkonferenz wollen wir im Hamburger Vorsitzjahr spürbare Verbesserungen erreichen, damit Frauen ihr Recht und Täter ihre Strafe bekommen“, so Senator Andy Grote, Vorsitzender der Innenministerkonferenz.

„Die Datenlage zeigt ein differenziertes Bild: Die registrierte Kriminalität ist 2025 gesunken, wir sehen Rückgänge bei Gewaltkriminalität und bei der Zahl der Tatverdächtigen. Gleichzeitig verändert sich Kriminalität – sie wird digitaler, internationaler und in manchen Bereichen auch brutaler. Sicherheit ist kein Selbstläufer. Deshalb müssen wir Kriminalität früh erkennen und wirksam bekämpfen. Durch die nun zusätzlich zu den Helfelddaten der PKS veröffentlichten Ergebnisse der Dunkelfeldstudie ‚Sicherheit und Kriminalität in Deutschland 2024‘ haben wir insgesamt ein umfassenderes Bild und klare Hinweise zur Kriminalitätsentwicklung in Deutschland und können unsere Bekämpfungsstrategien weiter anpassen“, sagt BKA-Präsident Holger Münch.

Ergebnisse der zeitgleich durch das BKA veröffentlichten Opferbefragung „Sicherheit und Kriminalität in Deutschland 2024“ (SKiD) zeigen, dass besonders junge Menschen von Gewaltstraftaten betroffen sind – mit steigender Tendenz. So sind bei der aktuellen Erhebung 8,5 Prozent der Jugendlichen im Alter von 16 und 17 Jahren Opfer einer Körperverletzung geworden, ein Anstieg um 5,4 Prozentpunkte gegenüber der Befragung von 2020 und damit mehr als eine Verdopplung (2020: 3,1 Prozent). **GIT**



Leben retten,
Existenzen
sichern



Ob medizinische Notfälle, Brandgefahren oder feuergefährliche Arbeiten – ein umfassender Feuerwehr- und Rettungsdienst ist für Unternehmen unerlässlich. KÖTTER Security bietet maßgeschneiderte Lösungen, um Ihre Mitarbeitenden, Anlagen und Betriebsprozesse zuverlässig zu schützen. Mit über 90 Jahren Erfahrung und qualifizierten Fachkräften sorgen wir für höchste Sicherheit – präventiv, reaktionsschnell und professionell.

Vorbeugender und abwehrender Brandschutz

Erstellung von Brandschutzkonzepten

Erstellung von Risikoanalysen zur Brandlastenreduzierung

Kennzeichnung, Festlegung und Freihaltung von Rettungswegen

Betrieblicher Rettungsdienst

Service- und Wartungsarbeiten

Konzeption und Outsourcing von Werk- und Betriebsfeuerwehren

Konzeption und Finanzierung von Fahrzeugen und Technik

Stellung von Feuerwehrkräften als Dienstleistung und als Arbeitnehmerüberlassung

Zertifizierte Aus- und Weiterbildungen nach FwDV2 & AGBF

KÖTTER Security
Wilhelm-Beckmann-Straße 7
45307 Essen

Tel. +49 201 2788-388
info@koetter.de
koetter.de

KÖTTER Services im Social Web: [f](#) [X](#) [in](#) [v](#) [K](#) [ig](#) [koetter.de](#)

Tornados, Masern, Grenzkontrollen

Aktuelle Tipps für die Sicherheit auf Geschäftsreisen in die USA



© Andrey Popov - stock.adobe.com

Die USA gehören zu den wichtigsten Zielen für Geschäftsreisen deutscher Unternehmen. Doch die Rahmenbedingungen für Einreise und Aufenthalt verschärfen sich. International SOS, seit 2026 Mitglied beim BVSU, weiß, worauf sich Reisende einstellen müssen und wie die Vorbereitung gelingt. Ein Beitrag von Wolfgang Hofmann, Regional Security Manager Germany & Austria bei International SOS.



© Mario Andree / BVSU

■ Die gute Nachricht vorweg: Die Sicherheitslage in den USA hat sich im Vergleich zur Zeit vor Donald Trumps zweiter Präsidentschaft nicht wesentlich verändert und das Land gilt nach wie vor als sicheres Reiseziel. Zwar gab es zuletzt immer wieder Proteste, doch deren Ausmaß entspricht vergleichbaren Ereignissen in der Vergangenheit, etwa den Unruhen im Zusammenhang mit dem Tod von George Floyd im Jahr 2020.

ESTA-Verfahren: Digitale Vergangenheit im Fokus

Was sich allerdings zukünftig verändern wird, sind die Einreisebedingungen in die USA. Grundsätzlich haben Reisende dafür zwei Möglichkeiten: Entweder nutzen sie das ESTA-Verfahren (Electronic System for Travel Authorization) oder sie beantragen ein B1/B2-Visum.

Die verpflichtenden Angaben beim ESTA-Verfahren sollen künftig auch Social-Media-Profilen, Telefonnummern und E-Mail-Adressen umfassen, teilweise rückwirkend bis zu zehn Jahre. Das Ziel dabei ist, die digitale Vergangenheit der Einreisenden zu durchleuchten. In Kombination mit einer KI-gestützten Auswertung lässt sich aus diesen Angaben ein umfassendes Profil des Reisenden ableiten. Bereits heute enthält der ESTA-Antrag eine Abfrage der Social-Media Accounts, allerdings auf freiwilliger Basis.

Ob diese Verschärfungen vor oder nach der Fußballweltmeisterschaft 2026 eingeführt werden, ist derzeit noch nicht entschieden. Wer für das Turnier in die USA reisen möchte und bereits einen FIFA-Pass besitzt, soll jedoch einen bevorzugten Termin für das Visum-Interview erhalten.

Umfassende Überprüfungen bei der Einreise

Das Visum-Interview oder der ESTA-Antrag sind allerdings keine Garantie für die Einreise. Die endgültige Entscheidung trifft immer der US-Grenzbeamte. Schon jetzt gibt es sehr intensive Sicherheitsüberprüfungen an der Grenze. Diese begründen sich auf eine sogenannte „Presidential Action“, die bereits am 20. Januar 2025 veröffentlicht wurde. Darin werden die US-Grenzbeamten aufgefordert, alle Ausländer so umfassend wie möglich zu überprüfen und zu kontrollieren – insbesondere diejenigen, die aus Ländern oder Regionen stammen, in denen Sicherheitsrisiken festgestellt wurden.

Zwar zählen Länder, die am ESTA-Verfahren teilnehmen, nicht zu den Ländern mit besonderen Risiken. Aber die Verordnung hatte bereits Auswirkungen auf die

Art und Weise, wie die Überprüfungen durchgeführt werden.

Wichtig ist es vor allem, die Fragen im ESTA-Verfahren ehrlich zu beantworten, denn Unstimmigkeiten führen immer zu Rückfragen. Auch die Frage nach den zuvor bereisten Ländern spielt eine wichtige Rolle: Es gibt mehrere Länder, nach deren Besuch eine Einreise per ESTA-Verfahren ausgeschlossen ist. Zu diesen Ländern zählt seit dem 21. Januar 2021 auch Kuba, das allgemein ein beliebtes Reiseziel ist.

Gerätesicherheit und Datenschutz

US-Behörden sind berechtigt, elektronische Geräte bei der Einreise zu kontrollieren. Dies kann kooperativ erfolgen, indem der Reisende aufgefordert wird, das Gerät freizugeben, oder im Rahmen einer forensischen Untersuchung. Auch hier richtet sich das Augenmerk besonders auf die Social-Media-Aktivitäten. Die Kontrollen finden stichprobenartig statt.

Unternehmen sollten systematisch prüfen, ob schützenswerte Informationen auf den Reisegeräten gespeichert sind, und überlegen, wie sie damit umgehen wollen. Die Daten zu verschlüsseln, könnte weitere Nachfragen zur Folge haben. Auch wird davon abgeraten, Datenträger nach „James-Bond-Manier“ zu verstecken, etwa an vermeintlich sicheren Plätzen im Gepäck.

Die Auslagerung der Daten in eine Cloud-Umgebung ist eine praxistaugliche Alternative. Der Zugriff auf die Daten sollte ausschließlich über den Browser erfolgen und nicht über vorinstallierte Apps. Trotzdem ist zu berücksichtigen, dass das Risiko eines Datenabflusses damit allenfalls verlagert wird, denn schließlich erfolgt der Zugriff über einen amerikanischen Provider.

Empfehlungen zur Reisevorbereitung

Reisende briefen: ESTA-Angaben gewissenhaft ausfüllen, insbesondere besuchte Drittländer.

Digitale Geräte: Festlegen, welche Daten auf den Geräten gespeichert werden dürfen. Sensible Informationen auslagern oder auf sicheren Remote-Zugang umstellen.

Verhalten trainieren: Mitarbeitende schulen, wie sie sich an der Grenzkontrolle zu verhalten haben – ruhig, kooperativ, höflich.

Dokumente: Neben den Reisepass auch Rückflugticket und Hotelbuchung bei der Einreise parat halten, gegebenenfalls auch ein Einladungsschreiben des Unternehmens.

Gesundheitsvorsorge strukturieren: Impfstatus prüfen, Versicherungsschutz für USA sicherstellen, bei Bedarf spezialisierte Assistance-Dienstleister einbinden.

Lagebeobachtung institutionalisieren: Wetterextreme, Protestgeschehen und regulatorische Änderungen kontinuierlich beobachten und in Reisegenehmigungsprozesse integrieren.

Teure Gesundheitsversorgung

Ein Aspekt, der bei USA-Reisen häufig unterschätzt wird, ist die Gesundheitsversorgung. Die ist in den Vereinigten Staaten zwar grundsätzlich leistungsfähig, kann aber schnell zu erheblichen Kosten führen. Spezialisierte Dienstleister können dabei helfen, eine angemessene Versorgung zu vertretbaren Kosten sicherzustellen. Größere Unternehmen sind in diesem Bereich in der Regel gut aufgestellt, während sich bei kleinen und mittelständischen Unternehmen immer wieder Lücken zeigen.

Darüber hinaus sollten alle USA-Reisenden ihren Impfstatus überprüfen. Der Masernausbruch des vergangenen Jahres, einer der größten seit drei Jahrzehnten in den USA, verdeutlicht, dass sich vermeintlich besiegte Krankheiten auch in Industrieländern schnell wieder ausbreiten können.

Die USA – ein Land der (Wetter-)Extreme

Die geografischen und klimatischen Extreme des Landes – von Metropolen bis zur Wildnis, von Hitze bis zu Tornados und Hurrikanen – stellen zusätzliche Anforderungen an die Reisevorbereitung und das Krisenmanagement.

Tatsächlich fällt die Fußballweltmeisterschaft 2026 in die Hurrikan-Saison. Solche extremen Wetterlagen kommen aber nie überraschend, ein Hurrikan beispielsweise baut sich über längere Zeit auf. Es ist daher empfehlenswert, regelmäßig einen Blick auf die Wettervorhersage zu werfen. **GIT**



Bayerischer Verband für
Sicherheit in der Wirtschaft
www.bvsw.de

AG neovo

35 YEARS GIT
HAPPY BIRTHDAY!

RUND UM DIE UHR IM DIENST

AG Neovo Displays mit NeoV™ Glastechnologie -> gebaut für 24/7/365 durch:

- Hochqualitative Selektion aller Komponenten
- Kratz- und stoßfeste NeoV™ Glas-Oberfläche
- Minimierung von Helligkeitsverlusten durch NeoV™
- patentierte Anti-Burn-in™ Technologie
- Solide und Wärme-ableitende Metallgehäuse
- NDAA-Konformität aller Produkte

AG Neovo's Design und jahrzehntelange Erfahrung sichern so verlässlichen Dauerbetrieb für Ihre Displays - unabhängig von Ort und Aufgabe.



Kontakt | vertrieb@ag-neovo.com
+ 49-2256-6289820

www.agneovo.com/de

Sicherheitsindustrie als **zentraler** Wachstumstreiber

Neue europäische Verteidigungs-Fachmesse „Euro Defence Expo“ startet am 22. September

Die veränderte sicherheitspolitische Lage wirkt zunehmend auf die industrielle Entwicklung in Deutschland. Der Krieg in der Ukraine, Konflikte im Nahen Osten und der wachsende Fokus auf Zivilschutz verändern Märkte, Geschäftsmodelle und Investitionsentscheidungen spürbar. Vor diesem Hintergrund hat die neue internationale Fachmesse „Euro Defence Expo“ vom 22. bis 25. September in der Messe Essen Premiere. Rund 250 Aussteller werden erwartet. Eine Vorschau von Messe-Geschäftsführer Oliver P. Kuhr.



Oliver P. Kuhr, Geschäftsführer Messe Essen

„Deutschland diskutiert Verteidigung noch immer vor allem politisch“ – so bringt es Oliver P. Kuhr, Geschäftsführer der Messe Essen, auf den Punkt. „Tatsächlich erleben wir aber gerade eine tiefgreifende industrielle Verschiebung. Wer heute über die Zukunft von Industrie spricht, kommt an diesem Thema nicht mehr vorbei. Dahinter steckt enorme Dynamik für Innovation, Investitionen und Beschäftigung“, so Kuhr weiter.

Die Zahlen unterstreichen diese Entwicklung: Die deutsche Rüstungsbranche beschäftigt weit über 100.000 Menschen. Gleichzeitig stiegen die Militärausgaben in der Bundesrepublik im Jahr 2025 auf über 97 Milliarden Euro – ein Plus von 24 Prozent im Vergleich zum Vorjahr. Oliver P. Kuhr: „Die Nachfrage nach Sicherheits- und Verteidigungstechnologien wächst so schnell wie seit Jahren nicht mehr. Davon profitieren längst nicht nur klassische Rüstungsunternehmen – auch Mittelstand und Technologieanbieter erschließen neue Märkte.“

Dual-Use-Technologien

Parallel vollzieht sich ein struktureller Wandel: Immer mehr Unternehmen aus

traditionellen Industrien steigen in sicherheitsrelevante Geschäftsfelder ein. „Automobilzulieferer, Maschinenbauer oder Technologieunternehmen entwickeln Lösungen für Drohnenabwehr, Aufklärung oder den Schutz kritischer Infrastrukturen“, erläutert Kuhr. „Genau der Bereich der Dual-Use-Technologien wächst derzeit besonders dynamisch.“

Diese Entwicklung soll auf der Euro Defence Expo sichtbar gemacht werden. Unternehmen wie Airsense Analytics, Analyticon Instruments oder ARX Robotics stehen exemplarisch für Technologien, die sowohl im zivilen Katastrophenschutz als auch im militärischen Einsatz genutzt werden können. Etablierte Industrieunternehmen wie Binder, Bernd Siegmund oder Alexander Binzel Schweissttechnik bringen ihre Kompetenzen ebenfalls verstärkt in sicherheitsrelevante Anwendungen ein. Gleichzeitig nutzen führende Akteure die Messe als Plattform: KNDS Deutschland Tracks, ein zentraler europäischer Anbieter für militärische Landsysteme, ist ebenso vertreten wie Heckler & Koch als einer der bekanntesten Hersteller im Sektor Infanteriebewaffnung.

Militärische und zivile Sicherheit gemeinsam

Die entscheidende Frage für Unternehmen laute heute nicht mehr, ob sie sich mit Sicherheit befassen, so Kuhr, „sondern wie strategisch sie es tun“. Die Euro Defence Expo mache diesen Transformationsprozess sichtbar und bringe die entscheidenden Akteure zusammen.

Vertreter aus Industrie, Militär, Politik, Sicherheitsbehörden und Forschung werden vom 22. bis 25. September in der Messe Essen erwartet. Zeitgleich wird die Security Essen veranstaltet – eine der führenden Fachmessen für zivile Sicherheit. Damit, so Kuhr, vereint die Messe Essen erstmals militärische und zivile Sicherheitslösungen an einem Ort und wird zum zentralen Treffpunkt für die sicherheitsrelevante Industrie. **GT**



Messe Essen

www.eurodefenceexpo.de

NRW **24. Juni 2026** Sicherheitstag

Unter der Schirmherrschaft des Ministers des Innern des Landes Nordrhein Westfalen Herbert Reul

**Zwischen Geopolitik
und Unternehmensrealität –
Wirtschaftsschutz als Erfolgsfaktor**



24. Juni 2026
Deutsches Zentrum für
Luft- und Raumfahrt
(DLR) in Köln-Wahn

Anmeldungen sowie
weitere Informationen zu
Programm und Inhalten
sind ab sofort unter
obigem Link möglich.



West

Allianz für Sicherheit in der
Wirtschaft West e.V.
(ASW West e.V.)
info@aswwest.de
www.aswwest.de

SicherheitsExpo München 2026

Aktuelle Entwicklungen, Trends und Lösungen

Die SicherheitsExpo München am 1. und 2. Juli findet im MOC München statt. Sie widmet sich aktuellen Entwicklungen, Trends und Lösungen im Bereich Sicherheitstechnik. Rund 120 Aussteller präsentieren ihre Produkte und Anwendungen, ergänzt durch ein begleitendes Fachforum mit Vorträgen und Diskussionen.



Die Messe versteht sich als Plattform für Wirtschaft und öffentliche Einrichtungen, um sich über Technologien zum Schutz vor internen und externen Gefährdungen zu informieren. Ein besonderer Schwerpunkt liegt auf dem Schutz Kritischer Infrastrukturen. Zu den behandelten Themen zählen unter anderem Zutrittskontrolle, Videoüberwachung, Brandschutz, Perimeterschutz und IT-Sicherheit. Die SicherheitsExpo München ist Teil eines Messeportfolios des Veranstalters AFAG, der im Jahresverlauf weitere Veranstaltungen zu Sicherheit und Krisenvorsorge an verschiedenen Standorten organisiert.

Technik und Praxis

Fachbesucher erhalten auch in diesem Jahr die Möglichkeit, sich umfassend über aktuelle Sicherheitsanforderungen und Lösungsansätze zu informieren. Im Fokus stehen sowohl technologische Entwicklungen als auch praxisorientierte Strategien zur Risikominimierung und zur Umsetzung gesetzlicher Vorgaben.

Das begleitende Vortragsprogramm greift zentrale Themen der Branche auf. Dazu gehören unter anderem moderne

Zutritts- und Identitätsmanagementsysteme, integrierte Sicherheitsplattformen, Fragen der Resilienz und des Kritis-Schutzes sowie physische Sicherheitskonzepte. Darüber hinaus werden neue Technologien wie Drohnendetektion, Robotik und Sensorik vorgestellt.

Cloud bis KI

Ein Schwerpunkt liegt auf der Zukunft der Zutrittskontrolle und Identitätsmanagementsystemen. Im Fokus stehen Cloud- und Mobile-ID, Smart Access, KI-gestützte Sicherheitsprozesse sowie die Weiterentwicklung klassischer Systeme. Zudem werden die Migration von Legacy-Architekturen in Cloud- und Hybridumgebungen sowie softwarebasierte Lösungen thematisiert, die Hardware zunehmend ersetzen.

Ein weiterer Fokus gilt integrierten und vernetzten Sicherheitsplattformen. Behandelt wird die Zusammenführung von Zutrittskontrolle, Besuchermanagement, Videoüberwachung und Sensorik in zentralen Systemen. Ziel sind automatisierte Workflows, effizientes standortübergreifendes Management sowie skalierbare, cloud-basierte Sicherheitsarchitekturen.

Geopolitik und Resilienz

Im Bereich Kritis, Resilienz und geopolitische Sicherheitslage stehen aktuelle Bedrohungsszenarien und deren Auswirkungen auf Unternehmen und Behörden im Mittelpunkt. Diskutiert werden Resilienzstrategien, regulatorische Anforderungen sowie die wirtschaftlich und operativ ausgewogene Umsetzung von Sicherheitsmaßnahmen.

Ein weiterer Themenblock widmet sich der physischen Sicherheit und operativen Schutzkonzepten. Dazu zählen moderne Zutritts- und Schließsysteme, Perimeterschutz, zonenbasierte Sicherheitsarchitekturen sowie schnelle Reaktions- und Alarmierungskonzepte. Auch die Weiterentwicklung klassischer Leitstellen hin zu integrierten Steuerungszentren wird thematisiert.

Abgerundet wird das Programm durch innovative Technologien wie Drohnendetektion, Robotik und Sensorfusion. Diese sollen künftig als Teil intelligenter Gesamtsysteme Bedrohungen frühzeitig erkennen und automatisierte Reaktionen ermöglichen. **GIT**



AFAG Messen und Ausstellungen GmbH
www.sicherheitsexpo.de



EVENT

PMRExpO 2026

Leitmessen für hybride, kritische Kommunikation

■ Vor dem Hintergrund wachsender Investitionen in KRITISchutz, Zivilschutz und digitale Führungsfähigkeit rückt die Messe den Kern moderner PMR-Systeme die Themen Interoperabilität, Resilienz, Betriebsrealität, Integration und Zukunftsfähigkeit in den Mittelpunkt. Angesprochen werden Verantwortliche aus den Bereichen BOS und Kritis, Leitstellen, IndustrieSecurity, Energie und Netzbetreiber, Logistik, Aviation sowie Akteure der Zivil-Militärischen Zusammenarbeit (ZMZ).

Inhaltlich gliedert sich die PMRExpO 2026 in drei komplementäre Formate: Der Summit richtet sich an strategische Entscheider und beleuchtet technologische Trends, Sicherheitsaspekte und Geschäftschancen. Das Symposium vertieft Themen wie interoperable Netze, Krisenvorsorge, Netzresilienz und zivilmilitärische Zusammenarbeit. Die Connecting Area demonstriert praxisnahe Use Cases – etwa resiliente Netze in der Fläche, ZMZ-Schnittstellen oder geschäftskritische Kommunikation mit SecuritybyDesign.

Mit Beispielen privater 5G-Campusnetze – von Lufthansa Technik über BASF bis zur Koelnmesse – zeigt die PMRExpO, wie hybride Netze bereits heute produktiv eingesetzt werden. Die Messe 2026 schärft damit ihr Profil als zentrale Integrations- und Orientierungsmesse für alle, die kritische Kommunikation der Zukunft gestalten. **GIT**



Koelnmesse
www.pmrexpO.com



AXON 2600 Zutrittskontrolle

Einfach starten - flexibel erweitern



2-6 Türen
(max. 102 Türen)



Lokaler Betrieb
Autarkes Management



Systemskalierung
Einfache Erweiterung



API-Schnittstelle
Offene Systemintegration



65.000 Personen
Standard



Multi-Standorte
Zentrale Verwaltung



Cloud
Erweiterter Service



Cybersicher
NFA2P @ Cyber Level 3

Axon

JEDE BEWEGUNG UNTER KONTROLLE





PERSONENSCHUTZ

Wie unsichtbare Schatten

Schutz für exponierte Personen und wohlhabende Familien

Es mag eine ziemlich stabile Konstante der Geschichte sein, dass die Zeiten von den Zeitgenossen als besonders unruhig oder gar unsicher empfunden werden. Wie berechtigt dieses Gefühl ist, lässt sich nicht so einfach messen. Allerdings: Die Nachfrage nach Personenschutz steigt. Anlass genug, für GIT SICHERHEIT, sich mit einer Expertin darüber zu unterhalten: Christina Schwung ist gemeinsam mit Sascha Neukirch bei dem Sicherheitsberatungsunternehmen Corporate Trust für das Thema verantwortlich.

Frau Schwung, Sie befassen sich bei Corporate Trust mit Personenschutz. Bevor wir das Thema weiter ausdifferenzieren: Wie prall sind Ihre Auftragsbücher gefüllt – und wie entwickelt sich Ihre Branche derzeit?

Christina Schwung: Die Auftragslage im Bereich Personenschutz ist derzeit ausgesprochen positiv. Nahezu wöchentlich gewinnen wir neue Klienten hinzu, wobei wir sowohl kurzfristige als auch langfristige Mandate betreuen. Der überwiegende Teil unserer Aufträge sind langfristige Schutzkonzepte, die eine kontinuierliche Betreuung erfordern.

Was wir besonders beobachten: Das Sicherheitsempfinden vermögender Personen hat sich in den letzten Jahren merk-

lich verändert. Es ist nicht unbedingt eine konkrete Bedrohungslage, die unsere Klienten zu uns führt, sondern vielmehr ein gestiegenes Bewusstsein für potenzielle Risiken. Die geopolitischen Spannungen, zunehmende soziale Ungleichheit und die Verbreitung von Informationen über soziale Medien haben dazu beigetragen, dass High-Net-Worth-Individuals ihre Sicherheitsvorkehrungen überdenken und professionalisieren.

Sie unterstützen vor allem wohlhabende Familien, aber es gehören auch zum Beispiel Persönlichkeiten die für Unternehmen an exponierter Stelle tätig sind zu Ihren Kunden. Hier wird es eine große Schnittmenge geben. Wie kommt der Kontakt zu Ihnen zustande?

Christina Schwung: In der Regel erfolgt der erste Kontakt über die Vorzimmer oder bei Vorständen über die Sicherheitsverantwortlichen der Unternehmen. Die Kundenakquise im Personenschutzbereich stellt uns vor besondere Herausforderungen, da unsere Zielgruppe bewusst abgeschirmt und schwer direkt erreichbar ist. Klassische Werbemaßnahmen greifen in unserer Branche kaum. Stattdessen setzen wir auf gezielte Netzwerkarbeit und persönliche Präsenz bei exklusiven Veranstaltungen. Dort steht für uns die Vertrauensbildung im Vordergrund – nicht das aktive Verkaufen. Besonders wertvoll sind Empfehlungen bestehender Klienten sowie unsere Kontakte zu Family Offices, die als wichtige Vermittler zwischen uns und potenziellen Kunden fungieren.

Wovor brauchen Ihre Kunden vor allem Schutz – und woher kommen die Bedrohungen vor allem?

Christina Schwung: Unsere Klienten benötigen Schutz vor digitalen und physischen Bedrohungen. Im Cyberbereich dominieren Phishing, Ransomware und maßgeschneiderte Malware-Kampagnen. Physisch bleiben Entführungen, Einbrüche, Stalking und körperliche Angriffe relevant. Hinzu kommen finanzielle Betrugsmaschinen, Social Engineering und zunehmend Reputationsrisiken durch Desinformationskampagnen. Die Bedrohungen stammen von organisierten kriminellen Gruppierungen, Insidern mit Zugang zu persönlichen Informationen und immer raffinierteren Cyberkriminellen. Auch geopolitische Faktoren und soziale Ungleichheit spielen eine wachsende Rolle. Die erhöhte Sichtbarkeit und der digitale Fußabdruck unserer Klienten erfordern maßgeschneiderte Schutzkonzepte statt Standardlösungen.

Was gehört alles zu Ihrem Angebot?

Christina Schwung: Bei Corporate Trust bieten wir im Bereich Personenschutz und Familiensicherheit ein ganzheitliches Schutzkonzept mit unserem „Family Care“-Programm. Dieses schafft einen unsichtbaren Schutzschirm für maximale Sicherheit, ohne die persönliche Lebensführung einzuschränken. Elementar ist dabei die Voraufklärung – eine diskrete Überwachung des Umfelds, um Gefahren frühzeitig zu erkennen und präventiv zu handeln. Unser „Perfect Matching“-Verfahren mit psychologischer Eignungsdiagnostik stellt sicher, dass wir den optimal passenden Personenschützer für jede Familie finden. Auf Basis einer individuellen Gefährdungsanalyse entwickeln wir maßgeschneiderte Sicherheitslösungen, die von umfassender Objektsicherheit mit Perimeterschutz und Einbruchmeldetechnik über digitalen Schutz mit Darknet-Recherchen und IT-Sicherheit bis hin zu Background-Checks und Auskunftssperren reichen. Ein persönlicher Sicherheitsmanager koordiniert alle Maßnahmen und steht Ihnen mit unserem 24/7-Krisenteam jederzeit zur Verfügung – quasi wie eine eigene kleine Unternehmenssicherheit für Ihre Familie. Alle Komponenten werden diskret implementiert, damit Sie sich unbeschwert auf Ihre Ziele konzentrieren können.

Können Sie mal anhand eines praktischen Beispiels darstellen, wie der Schutz etwa für einen CEO eines mittelständischen Familienunternehmens aussieht und was es alles umfasst?

Christina Schwung: Herr Müller führt in dritter Generation ein mittelständisches Familienunternehmen mit 500 Mitarbeitern. Nach Drohungen eines entlassenen Mitarbeiters und zunehmender Geschäftstätigkeit in instabilen Regionen entscheidet er sich für ein Sicherheitskonzept. Wir beginnen mit einer umfassenden Gefährdungsanalyse seiner Routinen, Wege und Immobilien. Eine Sichtbarkeitsrecherche zeigt öffentlich zugängliche private Details und im Darknet finden wir seine E-Mail-Adresse auf einer Liste gehackter Konten. Sofort implementieren wir Schutzmaßnahmen: Adresssperren bei Behörden, Bereinigung der Online-Präsenz und Installation moderner Sicherheitssysteme. Sein Fahrzeug erhält ein Tracking-System und er bekommt einen geschulten Fahrer, der gleichzeitig als Personenschützer fungiert.

Die Voraufklärung ist essenziell: Bevor Herr Müller sein Haus verlässt, hat unser

Team die Umgebung gesichtet. Bei seiner wöchentlichen Golfrunde ist ein unauffälliger Begleiter in der Nähe. Für Geschäftsreisen erstellen wir detaillierte Sicherheitskonzepte mit lokalen Risikoanalysen. Unser Konzept ist modular erweiterbar: Bei abstrakter Gefährdung setzen wir auf indirekten Personenschutz mit intensiver Voraufklärung. Bei konkreteren Bedrohungen erweitern wir um direkten Personenschutz mit permanenter Begleitung und speziellen Sicherheitsfahrzeugen. Im Unternehmen schulen wir das Personal und implementieren ein Besuchermanagementsystem. Die Familie erhält Sicherheitsschulungen und Zugang zu einer Echtzeit-Überwachungsplattform. Diese ineinandergreifenden Maßnahmen bilden einen unsichtbaren Schutzschirm, der Herrn Müller ein weitgehend normales Leben ermöglicht.

Bitte umblättern ▶

Christina Schwung, Senior Security Consultant bei Corporate Trust



Sie beschäftigen sich ja sogar mit dem Thema Cyberangriffe?

Christina Schwung: Bei Corporate Trust vertreten wir die Überzeugung, dass moderner Personenschutz nur ganzheitlich funktionieren kann, wenn physische und digitale Sicherheitsmaßnahmen integriert werden. Viele Angriffe beginnen heute im digitalen Raum, bevor sie in der physischen Welt sichtbar werden. Unser Ansatz zur Cybersicherheit folgt dem Grundsatz „Angriffe abwehren, bevor sie passieren“. Wir bieten präventive Sicherheitsdienstleistungen, die auf realen Angriffsszenarien basieren und individuell angepasst werden.

Die digitalen Bedrohungen reichen von Ransomware über Industriespionage bis zu staatlich unterstützten Akteuren. Wir entwickeln technische Lösungen, die einen digitalen Grundschutz bilden, bevor physische Schutzmaßnahmen notwendig werden.

Besonders wichtig ist die Verbindung zwischen digitaler und physischer Sicherheit. Wenn wir etwa feststellen, dass persönliche Informationen im Darknet gehandelt werden, ergreifen wir präventive Maßnahmen, bevor diese für physische Angriffe genutzt werden können.

In der heutigen vernetzten Welt ist effektiver Personenschutz ohne robuste Cybersicherheitsmaßnahmen undenkbar. Durch die Integration beider Bereiche schaffen wir einen umfassenden Schutzschild für die ganzheitliche Sicherheit unserer Klienten.

Es steckt schon im Wort Personenschutz: Einen Menschen effektiv zu schützen, ist etwas wirklich sehr Persönliches. Das heißt, zwischen beiden

Seiten muss die Chemie stimmen. Wie schwierig ist das?

Christina Schwung: Die Beziehung zwischen Schutzperson und Personenschützer ist hochkomplex. Unsere Klienten wünschen sich oft einen widersprüchlichen Mix: höchste Professionalität kombiniert mit persönlicher Sympathie. Das Schlüsselkonzept ist „Nähe-Distanz“ – die Fähigkeit, situativ zwischen vertrautem Begleiter und distanzierterem Profi zu wechseln. Ich beschreibe es bildlich: Der Personenschützer steht vor dem Fenster, sieht hinein, geht aber nicht hinein. Er gehört zum „inner circle“, ist aber nie wirklich Teil davon.

Besonders herausfordernd ist die Anforderung, stets im Hintergrund zu bleiben – der unsichtbare Schatten, der präsent, aber nie dominant ist. Dies erfordert außergewöhnliche Selbstdisziplin und die Bereitschaft, ohne öffentliche Anerkennung zu arbeiten.

Deshalb verfechte ich unser „Perfect Matching“-Konzept mit psychologischer Eignungsdiagnostik. Wir analysieren Persönlichkeitsprofile, um die optimale Übereinstimmung zu finden, denn ein erfolgreicher Personenschützer braucht neben technischen Fähigkeiten vor allem emotionale Intelligenz und Anpassungsfähigkeit.

Es gibt ja keine fest definierte Aufgabe für so einen Job. Wie sieht sie denn idealerweise aus und wie kann man die Qualität sichern, die auch für den Kunden als solche erkennbar ist?

Christina Schwung: Es gibt tatsächlich klare Aufgabendefinitionen für Personenschützer im Familienkontext, auch wenn das Berufs-

bild in Deutschland nicht standardisiert ist. Bei Corporate Trust setzen wir ausschließlich auf Personenschützer mit behördlichem und militärischem Hintergrund. Diese spezielle Sozialisierung ist ein absoluter Qualitätsmarker für diese anspruchsvolle Tätigkeit. Ein entscheidender Vorteil ist ihre „Mission-first“-Mentalität: sie arbeiten nicht in starren Schichten, sondern bis der Auftrag erfüllt ist. Zu den Qualitätsmerkmalen gehören Situationsbewusstsein, Deeskalationstechniken, Selbstverteidigungsfähigkeiten und medizinische Kenntnisse. Wichtig sind vorausschauendes Denken, diskrete Integration ins Familienumfeld und die Fähigkeit, situativ unsichtbar oder präsent zu sein. Die Qualität zeigt sich darin, dass die Schutzperson ihr Leben ohne Einschränkungen führen kann, während im Hintergrund ein durchdachtes Sicherheitskonzept wirkt.

Frau Schwung, die Zeiten sind vergleichsweise unruhig, und wir haben eine neue Bundesregierung gewählt. Haben Sie von Ihrem Standpunkt aus Erwartungen auch an die Politik?

Christina Schwung: In meiner Funktion beobachte ich die aktuelle Lage mit professioneller Sorge. Ja, ich habe klare Erwartungen an die neue Bundesregierung. Vor allem wünsche ich mir eine Stärkung der Sicherheitsbehörden – nicht nur finanziell, sondern auch durch modernere rechtliche Rahmenbedingungen, die den aktuellen Bedrohungen gerecht werden.

Die Cybersicherheit muss deutlich mehr Priorität erhalten. In meiner täglichen Arbeit erlebe ich, wie verwundbar selbst wohlhabende Familien und Unternehmen im digitalen Raum sind. Hier brauchen wir dringend bessere Strukturen und eine engere Verzahnung zwischen staatlichen und privaten Sicherheitsdienstleistern.

Was mich persönlich umtreibt: Die zunehmende gesellschaftliche Polarisierung. Sie führt zu einer spürbaren Verrohung und steigenden Gewaltbereitschaft, die auch unsere Klienten direkt betrifft. Hier erwarte ich von der Politik klare Signale und Maßnahmen, die den gesellschaftlichen Zusammenhalt stärken. Letztlich geht es um eine Balance – zwischen notwendigen Sicherheitsmaßnahmen und dem Erhalt unserer freiheitlichen Lebensweise. Diese Balance zu finden, ist die große Herausforderung für die neue Regierung. Und daran werde ich sie messen. **GIT**



© Elena - stock.adobe.com



Corporate Trust
www.corporate-trust.de

Schulzentrum Stockbrünnele Böblingen Zukunftsweisender Holz-Hybridbau

Das zukunftsweisende Schulbauprojekt der Stadt Böblingen begleitet die Firma Sinfiro von Beginn an mit großem Engagement. Im neuen Schulzentrum Stockbrünnele sind die Theodor-Heuss-Werkrealschule und die Friedrich-Schiller-Realschule unter einem Dach vereint – in einem kompakten, modernen Gebäudekomplex.

Das fünfgeschossige Gebäude wurde als Hybridbau realisiert und schafft optimale Voraussetzungen für zeitgemäße pädagogische Konzepte. Zwei L-förmige Baukörper fassen einen zentralen Innenhof ein, der gemeinsam mit der angrenzenden Mensa einen offenen, kommunikativen Begegnungsraum bildet. In den Obergeschossen bieten großzügige Lernlandschaften ein

flexibel nutzbares und zukunftsorientiertes Lernumfeld.

Holzbau-Gremium eingerichtet

Die besondere Komplexität des Holz-Hybrid-Baus wurde frühzeitig in einer eigens eingerichteten „Holzbau-Runde“ behandelt. Dieses Gremium – bestehend aus Vertretern der Stadt Böblingen, des Landkreises sowie den beteiligten Fachplanern – klärte technische und genehmigungsrelevante Machbarkeiten und bereitete den Bauantrag umfassend vor.

Noch mehr Brandschutz
ab Seite 59



Als Sonderbau der Gebäudeklasse 5 umfasst das Schulzentrum pro Obergeschoss sechs Nutzungseinheiten mit jeweils rund 400 m². Sinfiro begleitet das Projekt in allen brandschutztechnischen Belangen. Während Sockel- und Erdgeschoss sowie die aussteifenden Treppenräume und die Brandwand in mineralischer Bauweise ausgeführt wurden, entstand der übrige Gebäudeteil in Massivholzbauweise.

Der Baukörper ist in zwei Brandabschnitte gegliedert. Das Tragwerk wurde als feuerbeständige Skelettkonstruktion mit tragenden Außenwänden ausgebildet. Die Treppenraumkerne sind in den Verlauf der Brandwand integriert. Die Fluchtwege werden über die Treppenräume sowie über direkte Ausgänge ins Freie sichergestellt. Die entwickelten pragmatischen und zielgerichteten Brandschutzlösungen erfüllen die Anforderungen der Landesbauordnung.

Das Projekt zeichnet sich insbesondere durch die frühzeitige, konstruktive Abstimmung aller Beteiligten aus. Die offene Haltung der Brandschutzdienststelle gegenüber dem Holzbau, die früh geklärte technische Machbarkeit sowie das gemeinsame Ziel aller Projektpartner – der konsequente Einsatz von Holz – trugen maßgeblich zum Projekterfolg bei.

www.sinfiro.de



Für sichere Datenverbindungen

Wir bieten Glasfaser-Systeme für Industrie-Anwendungen:

- Höchste Bandbreiten und Echtzeitkommunikation
- Mehr Sicherheit – nicht abhörbar, manipulationsarm
- Störungsfrei auch bei EMV-belasteten Umgebungen
- Sehr große Reichweiten, geringe Verluste
- Zukunftssicher und hochverfügbar

Für maximale Performance und Resilienz beraten wir Sie unverbindlich.

Tel. +49 2762 9313-600

vertrieb@eks-engel.de

eks»



MUSEUMSSICHERHEIT

Aktuelle Fragen der Museumssicherheit

Schutz von Kulturgütern durch innovative Lösungen

Museen stehen im Spannungsfeld zwischen öffentlichem Auftrag und Sicherheitsanforderungen. Mit über 6.800 Häusern in Deutschland, rund 800 in Österreich und mehr als 1.100 in der Schweiz stellt sich die Frage, wie gut Kulturgüter tatsächlich geschützt sind. Moderne Technologien wie KI-gestützte Videoüberwachung können unterstützen, ersetzen aber nicht die menschliche Wachsamkeit. Der Kulturgüterschutz muss heute umfassender gedacht werden – von Einbruch und Raub über Naturkatastrophen bis hin zu Konflikten, die Museen und ihre Sammlungen in Europa direkt betreffen. GIT SICHERHEIT sprach mit Simone Schön, Referentin für Museale Sicherheit und Notfallprävention an der Landesstelle für die nichtstaatlichen Museen in Bayern.



Frau Schön, in Deutschland gibt es heute mehr als 6800 Museen, in Österreich etwa 800 und in der Schweiz mehr als 1100 – das umfasst zumindest die Häuser, die den internationalen Standards des International Council of Museums entsprechen. Wie schätzen sie den sicherheitstechnischen Standard dieser Einrichtungen derzeit ein?

Simone Schön: Der Standard ist unterschiedlich und immer abhängig von den Möglichkeiten der Häuser und deren Sammlung. Hier spielen Faktoren wie monetäre Werte als auch emotionale Werte eine Rolle, die die Grundlage für ein Schutzkonzept darstellen. Was die bayerischen Häuser betrifft, ist der Sicherheitsstandard etwas, das immer hinterfragt werden sollte. Es passiert sehr leicht, die Gefahren durch

das Gefühl von Scheinsicherheit zu unterschätzen.

Sehen Sie häufig eine größere Distanz zwischen dem Stand der Technik und dem tatsächlichen Sicherheitsniveau in den Museen?

Simone Schön: Ein Museum hat einen öffentlichen Auftrag. Das bedeutet, dass

diese Gebäude immer in einem Spannungsverhältnis stehen. Dem Besucher soll das Exponat so nah wie möglich gebracht werden. Hier kommt es bei einem Einsatz von Vitrinen schon zu Diskussionen. Ebenso sollen diese Gebäude und Bauteile eine höchstmögliche Sicherheit des Exponats garantieren. Jetzt stellen Sie sich noch vor, dass das Gebäude des Museums denkmalgeschützt ist. Somit gibt es Ansprüche von vielen Seiten, unter denen ein Schutzkonzept ganzheitlich zu gestalten ist. Dabei tun Museen und Träger, was in deren Macht steht. Doch dieser Macht sind finanzielle und personelle Grenzen gesetzt.

Was sind typische Schwachstellen?

Simone Schön: Wenn es eine Schwachstelle gibt, dann die, dass die Museen finanzielle und personelle Unterstützung benötigen, um ein Sicherheitskonzept am Leben zu halten und regelmäßig hinterfragen und upgraden zu können. Es darf nicht nur eine einmalige Investition sein. Es muss immer als Teil von Museumsarbeit verstanden werden, sei es von den Trägern, den Museen und auch dem Staat.

Wie sieht es mit Gefahren von innen aus, also mit Blick auf das eigene Personal?

Simone Schön: Wie die Vergangenheit zeigt, gab es auch hier einige Vorfälle. Innentäter sind für Museen ein Thema. Das ist sehr unangenehm zu hören und im Team zu bearbeiten.

Interne Kontrollen können auch zum Schutz der Mitarbeiter beitragen, wenn es einen Vorfall gab, kann im Zweifel durch Dokumentation und Zutrittsberechtigungen ein bestimmter Kreis an Mitarbeitern schneller ausgeschlossen werden. Dies lässt sich bereits mit einfachen Routinen und Kontrollen erreichen. Es darf dabei aber nicht zu einem Überwachungskonzept für Mitarbeiter werden. Das stört erheblich die Atmosphäre.

Es fand vor einiger Zeit ausgerechnet in einem der sicher wichtigsten und prestigeträchtigsten Museen der Welt, dem Louvre in Paris, ein spektakulärer und gleichzeitig recht simpel aufgezogener Raub statt. Was ist Ihre Meinung zu diesem Vorfall?

Simone Schön: Simpel war die Tat nicht. Aus anderen Fällen wissen wir, dass die Vorbereitungen der Täter teilweise Jahre

dauern können. Das macht es für Museumsaufsichten und Mitarbeiter auch so komplex, weil man jeden Tag sein Umfeld und die Besucher aufmerksam wahrnehmen muss und prüfen sollte, ob es Auffälligkeiten gibt.

Wir sehen zudem ganz eindeutig, dass sich das Tatverhalten drastisch verändert hat. Gerade in dem Bereich von Edelmetallen und Edelsteinen, geht es nicht mehr um den kunsthistorischen oder ideellen Wert eines Exponates. Hier steht der monetäre Wert absolut im Vordergrund. Dafür wird in Teilen auch Sprengstoff eingesetzt bis hin zu Waffengewalt und Geiselnahmen. Es gibt einen Punkt, ab dem kann ein Museum nichts mehr unternehmen ohne die Unterstützung des Staates.



Wie reagierte die Fachwelt, also vor allem Fachleute für Museen speziell im Bereich Kulturschutz auf den Fall?

Simone Schön: Die Fachleute wissen genau, was zu unternehmen ist und sind an der Umsetzung von Lösungen bemüht. An einem Schutzkonzept sind mehrere Instanzen beteiligt, die alle zusammenarbeiten. Dies ist manchmal nicht ganz einfach. Zudem hat jedes Bauteil auch seine Grenzen des Möglichen. Ein Museum wird immer ein Teil der Öffentlichkeit bleiben, somit auch immer Begehrlichkeiten wecken. Die Sammlungen wegzusperren und der Öffentlichkeit gänzlich vorzuenthalten, ist bislang keine Option, aber eine stark diskutierte.

Wenn wir aus dem großen Bereich der Sicherheitstechnik vor allem auf die Security schauen, und dabei auf Alarmsysteme, Videoüberwachung, etc.: Welche technologischen Entwicklungen verdienen aus Sicht der Museumssicherheit derzeit besonderes Augenmerk?

Simone Schön: Ich denke, dass solche Technologien eine sehr gute Ergänzung sein können. Ein Schutzkonzept steht auf unterschiedlichen Säulen. Sicherlich sind ein gutes Kamerasystem mit KI, Gangbildanalyse und Bildauswertung super Techniken. Dennoch benötigt es weiterhin auch Menschen hinter den Systemen, die die Bilder be- und auswerten.

Was halten Sie derzeit insgesamt für das Dringlichste, wenn wir von der Stärkung des Kulturgüterschutzes in Europa sprechen?

Simone Schön: Ich denke, dass in den letzten Monaten sehr stark der Kulturgüterschutz im Falle eines bewaffneten Konflikts in den Fokus gerückt ist. Durch Beispiele aus der Ukraine, lernen wir gerade nochmal was Kulturgüterschutz unter diesen Bedingungen bedeutet. Die Szenarien sind nicht neu, dennoch waren sie in den letzten Jahrzehnten kein Thema für deutsche Museen. Auch Fälle wie die Ahrtaflut oder der Einsturz des Kölner Archives sind Ereignisse, welche die Notwendigkeit eines funktionierenden Kulturgüterschutzes auf dramatische Weise unterstrichen haben. All das sind Themen, die zum Alltagsgeschäft Sicherheit im Museum noch hinzukommen. Die Lage für Kulturgut hat sich also in vielen Bereichen sehr stark verändert, in dem das die Bedrohungen konkreter geworden sind. Sei es durch Einbrüche und Raubvorfälle, die Veränderungen durch das Klima, als auch die geopolitischen Spannungen.

Brandschutz im Museum
siehe Seite 76



Landesstelle für die nichtstaatlichen
Museen in Bayern
<https://museumsberatung-bayern.de>

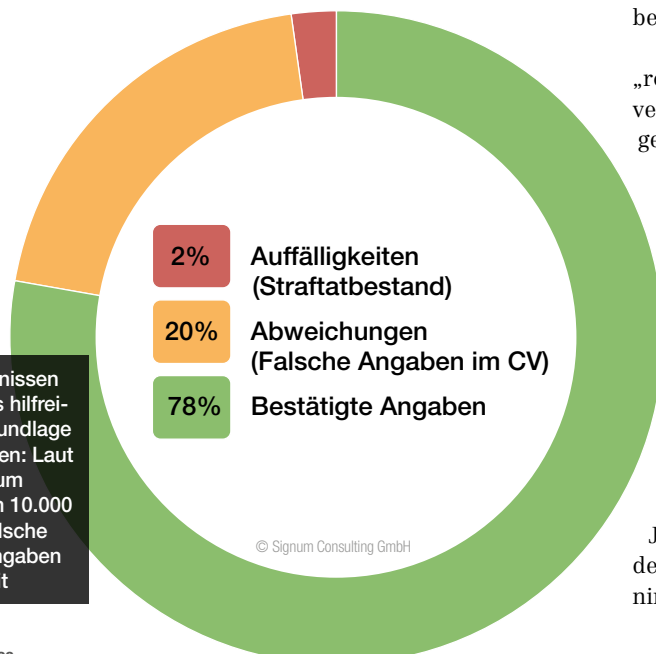


PRE-EMPLOYMENT SCREENING

Pre-Employment Screening als Sicherheitskonzept

Wie Unternehmen Sicherheitsrisiken im Bewerbungsprozess minimieren

Gefälschte Angaben im Lebenslauf sind kein Einzelfall – und ein echtes Sicherheitsrisiko. Pre-Employment Screening hilft Unternehmen, Bewerberdaten verlässlich zu prüfen und Fehlbesetzungen zu vermeiden.



Prüfbericht mit Ergebnissen von Einzel-Checks als hilfreiche Entscheidungsgrundlage für Personalabteilungen: Laut einer Studie der Signum Consulting GmbH von 10.000 Prüfergebnissen sind falsche oder abweichende Angaben im CV keine Seltenheit

■ Auf Nachfrage bei der vermeintlich ausstellenden Universität wurde die Ernüchterung schnell zur Gewissheit: kein Abschluss, kein Zeugnis. Dennoch hatte der Bewerber genau solche Dokumente eingereicht – für eine sicherheitskritische Position. Zwar bestätigte die Uni eine partielle Teilnahme des Kandidaten am Studiengang, aber keine bestandene Prüfung und kein Abschlusszeugnis. So vor einiger Zeit geschehen bei einem echten Unternehmen.

Ein Einzelfall? Keineswegs. Auswertungen zeigen: Solche „roten Flaggen“ treten häufiger auf, als viele Unternehmen vermuten. Der Bewerber hatte das Dokument schlichtweg gefälscht und sich damit auf eine risikosensible Stelle beworben. Ziemlich dreist, aber leider kein Einzelfall, wie die Statistik einer Auswertung von Prüfergebnissen zeigt.

Aus dieser Statistik ergeben sich folgende Sicherheitsrisiken:

- Fehlbesetzungen mit den damit verbundenen Kosten
- Abfluss von internen Daten, Wissen und Informationen
- Reputations- und/oder finanzielle Schäden
- Mögliche Spionage oder Sabotage

Was ist, was kann Pre-Employment Screening?

Jede Personalabteilung, die Lebensläufe durchgeht oder sich den Ausweis zeigen lässt, wendet Pre-Employment Screening an. Gemeint ist damit die Verifizierung der im Bewerber-

bungsprozess gemachten Angaben unter Hinzunahme von jobrelevanten, öffentlich zugänglichen Informationen. Bei diesem risikobasierten Ansatz geht es nicht um Misstrauen den Bewerbern gegenüber, sondern um den Schutz von internen Informationen, Daten, Know-How und Reputation.

Dazu schreibt das Bundesministerium des Innern im diesjährigen Papier zur Nationalen Wirtschaftsschutzstrategie: „Für besonders sensible Bereiche in den Unternehmen ist es wichtig, vertrauenswürdigen Personal einzusetzen, um die Gefahr von Wissensabfluss oder Sabotage zu verringern.“ Des Weiteren empfiehlt das Ministerium „eine datenschutzkonforme Integritätsprüfung von Bewerberinnen und Bewerbern und Beschäftigten (Pre-Employment-Screening, Backgroundchecks)“.

Die Einteilung der Check-Ergebnisse in grüne, gelbe oder rote Risikoklassen befähigt Personalabteilungen, die passenden Einstellungsentscheidungen zu treffen (vgl. Grafik S. 30). Die Beurteilung der Relevanz der Prüfergebnisse für die Position verbleibt freilich ausschließlich beim Unternehmen.

DSGVO als Rahmenbedingung

Pre-Employment Screening ist immer eine risikominimierende Maßnahme, wobei es egal ist, wer sich auf eine Stelle bewirbt.

Damit ist auch die Gleichbehandlung aller Bewerbenden sichergestellt.

Der rechtliche Rahmen für Pre-Employment Screening wird durch die DSGVO vorgegeben. Danach haben Unternehmen ein berechtigtes Interesse, stellenbezogene Bewerberangaben zu hinterfragen und zu verifizieren. Natürlich möchte man wissen, ob die Person fachlich und menschlich für die Position geeignet ist.

Diese Begründung greift auch beim In-Employment Screening (interne Besetzung von Risikostellen) und Re-Screening (periodische Prüfung von Mitarbeitern auf sensiblen Positionen). Wie weit das berechtigte Interesse geht, ergibt sich aus einer Risiko-evaluierung der Position oder Jobgruppe.

Im eingangs beschriebenen Fall der roten Flagge handelte es um eine Ingenieursposition, für die ein hohes technisches Niveau zwingend erforderlich ist. Da der Kandidat das Studium abgebrochen hatte, wäre eine Einstellung ein erhebliches fachliches Risiko, was das Unternehmen auf keinen Fall eingehen wollte. Daher ist eine Verifizierung der beruflichen Qualifikation essenziell und berechtigt.

Bei Mitarbeitern im Finanzbereich mit Budgetverantwortung ist ein finanzieller Integritätscheck erforderlich, während das für einen Programmierer ohne administra-

tive Rechte vielleicht nicht notwendig wäre. Für alle Prüfmaßnahmen gilt der Grundsatz der Verhältnismäßigkeit.

Die DSGVO setzt auch klare Grenzen. Alle Checks müssen sich im Fragerecht des zukünftigen Arbeitgebers bewegen. Außerdem sind die Kandidaten frühzeitig über anstehende Maßnahmen zu informieren, vor allem wenn Dienstleister eingebunden werden. Pre-Employment Screening ist auch in Deutschland eine etablierte Präventivmaßnahme. Datenrechtliche Unstimmigkeiten entstehen nur dann, wenn der Prozess nicht fachgerecht und nicht DSGVO-konform durchgeführt wird.

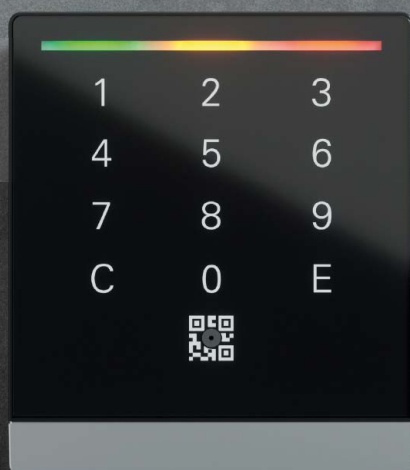
Wer sollte und wer muss prüfen?

Bis auf einige regulatorische Ausnahmen entscheiden Organisationen selbst, ob sie PES als Präventivmaßnahme einführen. Generell gibt es folgende Beweggründe dafür:

- Schutz von unternehmerischem Know-How
- Risikominimierung für die Besetzung risikosensibler Stellen
- Aufdeckung von digitalen Manipulationen der Unterlagen
- Reaktion auf negative, sicherheitsrelevante Vorfälle

Bitte umblättern ►

Nutzen Sie jetzt die absolute Flexibilität mit nur einem Leser



VOXIO Touch

jetzt auch mit Kamera für QR-Codes.

phg ist für Sie 2026 auf den wesentlichen Messen der Sicherheitsbranche:



1. + 2. Juli 2026
in München



22. - 25. September 2026
in Essen

Sie wollen alle Arten der Zutrittskontrolle nutzen? Dann haben Sie jetzt das perfekte Trio in einem Leser: klassisch über **physikalischen Ausweis** (RFID), komfortabel über **Credentials via Google-Wallet oder Apple-Wallet** oder kostengünstig über **QR-Code**. Dafür haben wir unseren formschönen Alleskönner VOXIO Touch ganz neu mit einer Kamera ausgestattet. Die neue Funktionalität ist ab sofort verfügbar. Rufen Sie uns an für mehr Infos.

phg Peter Hengstler GmbH + Co. KG • Tel. +49 (0) 7420 89-0 • datentechnik@phg.de

Risikokriterien und Prüfansätze im Pre-Employment Screening. Systematische Verknüpfung von Risikofeldern und Prüfmaßnahmen – gezielte Checks helfen Unternehmen, sicherheitsrelevante Bewerberrisiken frühzeitig zu erkennen und zu bewerten:

Risikokriterium	Checks
Echtheit von Bildungsabschlüssen	Verifizierung von Abschlüssen durch die herausgebende Institution
Fachliche Kompetenz	Verifizierung von Beschäftigungen, Referenzen
Identität	ID-Check, Adressverifizierung
Vertrauenswürdigkeit	Sanktionslisten Check, Führungszeugnis
Finanzielle Integrität	Credit Check
Reputation	Medienrecherche, Soziale Medien
Plausibilität	Plausibilitätscheck Lebenslauf + professionelle Netzwerke
Risiko Sabotage / Spionage	Check von Institutionen und Arbeitgebern auf Staats- und Militärnähe

- Regulatorische Anforderungen, wie kritische Infrastruktur, IT-Zertifizierungen (ISO 27001, C5, TISAX u. ä.) und Vorgaben im Finanzbereich (DORA, VAG)

Bei Positionen mit hohem Risiko und viel Schadenspotenzial sollte auch entsprechend umfangreich geprüft werden.

Hürden auf dem Weg zum erfolgreichen Prüfprozess

Am Anfang steht die Managemententscheidung für die Einführung von Pre-Employment Screening. Um das effektiv umzusetzen, bedarf es einer klaren Verantwortlichkeit dafür im Unternehmen. Meistens kommen die Impulse aus der Unternehmenssicherheit bzw. der Personalabteilung. Für Unternehmen ohne Screening-Erfahrung ergibt sich eine Reihe von Herausforderungen beim Aufbau eines DSGVO-konformen Prüfablaufs.

- Einbeziehung der Interessen aller relevanten Abteilungen (Sicherheit, HR, Datenschutz / Compliance, falls erforderlich Betriebsrat)
- Identifizierung von prüfrelevanten Positionen und Jobfamilien
- Risikobewertung dieser Stellen und Definition von Prüfpaketen
- Einbindung von Pre-Employment Screening in den Bewerbungsprozess
- Erstellen einer Richtlinie für alle Beteiligten mit klar strukturierten Prozessschritten

Vor allem die Punkte 2 und 3 stellen regelmäßig eine Herausforderung dar. Unternehmen müssen zuerst die prüfrelevanten Stellen identifizieren, bewerten das Risikopotenzial und legen im nächsten Schritt ein sinnvolles Prüfpaket dafür fest.

Die Tabelle „Risikokriterien und Prüfansätze im Pre-Employment Screening“ oben zeigt für jedes Sicherheitskriterium ein oder mehrere Checks, die das erkannte Risiko minimieren.

Dienstleister können hier wertvolle Arbeiten und Beratung leisten, sofern sie die notwendige Erfahrung und Kompetenz mitbringen.

Lösungen

Pre-Employment Screening ist kein Hexenwerk. Entweder erledigen Unternehmen es intern oder über einen externen Dienstleister, der wie eine verlängerte Personalabteilung agiert. Vorteil der externen Lösung ist neben Erfahrung und Expertise, dass alle Prüfergebnisse übersichtlich in einem Bericht zusammengefasst sind, zu dem nur die berechtigten Personen Zugriff haben.

Vom Auslösen eines Screenings bis zum fertigen Bericht stellen die meisten Dienstleister für alle Prüfaktivitäten eine moderne und sichere Online-Plattform bereit. Typische Bearbeitungszeit ist 7–12 Werktage. Standardmäßig muss ein automatisches Löschkonzept implementiert sein. Alle personenbezogenen Daten müssen nach einer gewissen Zeitspanne routinemäßig gelöscht

werden, z. B. 90 Tage. Ist eine DSGVO-konforme Abwicklung aller Prüfprozesse gegeben, bekommen Unternehmen ein wirksames Instrument zur Risikominimierung und Sicherheitsstrategie.

Fazit

Kein Unternehmen möchte Mitarbeiter auf Grund dreister Schönfärberei oder Betrugs einstellen. Eine Neubesetzung muss menschlich, fachlich und sicherheitstechnisch den betrieblichen Anforderungen entsprechen. Das erreichen Organisationen unter anderem durch Pre-Employment Screening. Das Beispiel mit der roten Flagge zeigt, dass diese Präventivmaßnahme Fehlbesetzungen verhindern kann. Der Kandidat wurde nicht eingestellt und die Universität hat Strafanzeige wegen Urkundenfälschung gestellt. **GIT**



Autor:
Martin Mehner
Vertriebs & Marketing Manager bei Disa




Bequem auf dem Sofa durch die e-Ausgabe der GIT SICHERHEIT blättern: Registrieren Sie sich auf

www.git-sicherheit.de/newsletter



GIT SICHERHEIT

INNENTITEL – SECURITY



SimonsVoss ►

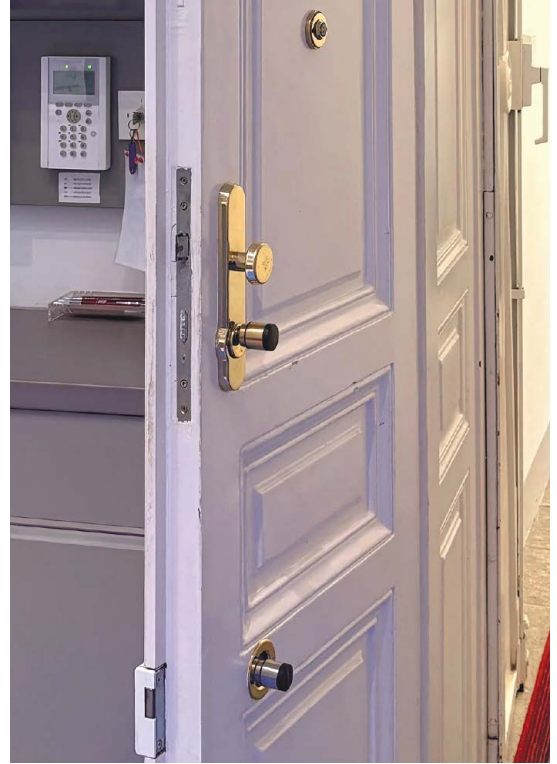
Zutrittssystem für Wiener
Steuerberatungskanzlei

SCHLIESSTECHNIK

Vertrauen und Leidenschaft

Zutrittssystem für Wiener Steuerberatungskanzlei

„Leidenschaft verbindet“ lautet das Motto der Steuerberatungsgesellschaft HFP in Wien. Für einen komfortablen, sicheren und kontrollierten Zutritt zur Kanzlei sorgt ein digitales Schließsystem von SimonsVoss.



Eingangstür zur Kanzlei – mit zwei digitalen Schließzylindern von SimonsVoss

Die Beatrixgasse ist einer der ältesten Straßenzüge des 3. Wiener Bezirks – die Historie reicht bis ins 17. Jahrhundert zurück. Eine lange Tradition hat auch die 1967 gegründete Steuerberatungskanzlei HFP aufzuweisen, die sich in der Beatrixgasse 32 in einem repräsentativen Altbau befindet. Hohe Räume, Doppelfenster, Stuck und Parkett tragen zum stilvollen Ambiente bei, in dem die Kunden mit ihren unterschiedlichen Anliegen individuell beraten werden. Geleitet wird das Unternehmen, das insgesamt rund 100 Mitarbeiter beschäftigt, von elf Partnerinnen und Partnern.

Vertraulichkeit ist ein wichtiger Faktor im Steuer- und Finanzbereich, in dem

mit sensiblen Informationen und Daten von Kunden gearbeitet wird. Um diese bestmöglich zu wahren und den Zutritt smart und lückenlos zu koordinieren, entschieden sich die Verantwortlichen für eine digitale Zutrittslösung von SimonsVoss. Die alte elektronische Schließanlage musste erneuert werden, da sie „in die Jahre gekommen war“ und den aktuellen Anforderungen nicht mehr entsprach.

25 AX-Zylinder, 120 SmartTags

Die Vorgaben der Auftraggebenden lauten: einfache Programmierung, Berechtigung auf Gruppenebene, voller Überblick über alle Türen und hohe Sicherheit. Nach eingehender Sondierung der Anforderungen und Beratung durch den SimonsVoss-Außendienstmitarbeiter Harald Thuri und die Partnerfirma Kratschmann & Partner Elektrotechnik fiel die Entscheidung daher auf die Locking System Management Software LSM Professional Edition. Die Türen im Bürobereich, die Zugänge zu den Büros und der Haupteingang wurden mit insgesamt 25 Digitalzylindern AX in der Lesevariante „passiv“ versehen, die passend zum Interieur teilweise in der Ausführung Messing





Ebenfalls integriert in die digitale Zutrittslösung von SimonsVoss: Die „Pinguin-Tür“ führt zum Aufzug zu den oberen Stockwerken

ausgewählt wurden. Hinzu kommen drei SREL3 und fünf SREL2.ZK.MH, die vor den Eingangstüren für das Update der SmartTags (Gateway) installiert wurden. Als Schließmedien dienen 120 SmartTags vom Typ Mifare Desfire.

Zylinder passend zum Ambiente

Der Kreis der Zutrittsberechtigten entspricht mit rund 100 der Anzahl der Mitarbeiter. Temporäre Zutrittsberechtigungen wurden bislang nicht vergeben, auch wenn die Möglichkeit im System besteht. Verwaltet wird es durch die zuvor geschulte IT-Abteilung von HFP. Sie ist auch für die Programmierung der SmartTags zuständig. Eine Anbindung an bereits bestehende Systeme war nicht notwendig, ist aber durch die gewählte Variante ebenfalls eine Option. Als besondere Herausforderungen für Planung und Installation der Zutrittslösung erwiesen sich die Leitungswege, da sich die Kanzlei in einem Altbau befindet. Hier war die Expertise der Elektrotechnik-Fachleute von Kratschmann & Partner gefragt. Zum historischen Ambiente passende Schließzylinder zu finden, erwies sich durch die Designvielfalt des AX hingegen als unproblematisch.

Einfaches und intuitives Handling

Das System ist seit Oktober 2024 im Einsatz und hat sich bereits bewährt. Mag. Christian Klausner, Steuerberater und Wirtschaftsprüfer, erklärt: „Die Anlage ist nun schon seit einiger Zeit bei uns im Einsatz, und wir sind sehr zufrieden. Die Funktionalität überzeugt in jeder Hinsicht, das Handling ist einfach und intuitiv – genau so, wie wir es uns erhofft hat-

ten. Besonders positiv ist, dass wirklich alle Altersgruppen, von jungen Kolleginnen und Kollegen bis hin zu Mitarbeiterinnen und Mitarbeitern im Alter von 80 Jahren, problemlos damit umgehen können.“ Auch die IT-Abteilung hatte nach Auskunft der Kanzlei keine Schwierigkeiten bei der Programmierung; alles lief reibungslos. „Die Optik der Zylinder macht zudem einen sehr hochwertigen Eindruck und fügt sich bestens in unsere Umgebung ein. Im Vergleich zur vorherigen Lösung spüren wir eine deutliche Verbesserung in der Benutzerfreundlichkeit und im täglichen Ablauf. Insgesamt können wir sagen: Alles funktioniert einwandfrei, und wir würden uns jederzeit wieder für dieses System entscheiden“, fügt Christian Klausner hinzu.

Aufgrund zusätzlicher Mietflächen fasst die Kanzlei bereits eine Erweiterung ins Auge. Und auch darüber hinaus gibt es Möglichkeiten der Optimierung, wie Harald Thuri seitens SimonsVoss aufzeigt: „Eine überarbeitete Graphical User Interface (GUI) mit zeitgemäßen Designprinzipien könnte die Attraktivität und Effizienz der Software weiter steigern.“ **GIT**



SimonsVoss Technologies GmbH
www.simons-voss.com
www.allegion.com

© Bilder: HFP/SimonsVoss

Entwickelt für Langlebigkeit, konzipiert für Zuverlässigkeit

Professionelle Lösungen von EIZO für die Videoüberwachung

DuraVision® | VisionCore™

Für jede Anwendung die passende Ausstattung: von IP-Decoder-Monitoren mit integrierter Hardware-Decodierung, flexiblen Installationen mit IP-Decoder oder Streaming Gateway-Boxen bis hin zu Bildoptimierungssystemen in Form von Hard- und Softwarelösungen.

Mehr Informationen unter
www.eizo.de/videoeueberwachung



Besuchen Sie EIZO auf der SicherheitsExpo
am 01. + 02. Juli 2026 am Stand G01





SCHLIESSTECHNIK

Den Wandel aktiv mitgestalten

Vor 90 Jahren wurde in der Kölner Domstraße das heutige Unternehmen Dom Sicherheitstechnik gegründet

Jürgen Maronn,
Geschäftsführer Dom
Sicherheitstechnik

Was 1936 als Kölner Handelsgesellschaft für Metallwaren begann, hat sich zu einem führenden Anbieter moderner, digital vernetzter Zutrittslösungen entwickelt. Als Teil der internationalen SFPI Gruppe setzt Dom Sicherheitstechnik heute auf europäische Produktion, technologische Weiterentwicklung und nachhaltige Unternehmensstrategien. GIT SICHERHEIT gratuliert – und sprach mit Geschäftsführer Jürgen Maronn.

— GIT SICHERHEIT: Herr Maronn, zunächst einmal herzlichen Glückwunsch zum Firmenjubiläum. Vor 90 Jahren sah die Welt noch etwas anders aus als heute. Können Sie uns kurz erzählen, wie alles angefangen hat?

Jürgen Maronn: Vielen Dank. Tatsächlich reichen unsere Wurzeln bis in eine Zeit, in der mechanische Sicherheitstechnik am Anfang stand. Alles begann 1936 in der Domstraße 12 in Köln. Dort gründete Josef Voss eine Handelsgesellschaft für industrielle Metallwaren unter seinem Namen, die auch Schlösser vertrieb. Bis heute verfolgt Dom den klaren Anspruch, hochwertige Schließsysteme „Made in Germany“ zu entwickeln und zu produzieren. Was als klassischer Hersteller mechanischer Zylinder begann, hat sich im Laufe der Jahrzehnte zu einem innovativen Anbieter ganzheitlicher, digitaler Zutrittslösungen entwickelt. Dabei sind Präzision, Ingenieurskunst und ein hoher Qualitätsanspruch von Anfang an prägend für unser Unternehmen.

Dom ist ein Familienunternehmen – und gehört zur SFPI-Gruppe. Könnten Sie uns die Struktur der Gruppe erläutern?

Jürgen Maronn: Die SFPI Group ist ein börsennotierter französischer Konzern mit Sitz in Paris, der sich auf Sicherheits, Gebäude und Industrietechnik spezialisiert hat. Das Unternehmen wurde 1985 gegründet und ist europaweit sowie international tätig. Die SFPI-Gruppe steht für „Safety for People and Industry“ und entwickelt hochwertige industrielle Lösungen für Bau und Industriekunden. Ein Schwerpunkt liegt auf Sicherheit, Energieeffizienz und industrieller Verantwortung unter Berücksichtigung sozialer und ökologischer Aspekte.

Die SFPI Group organisiert ihre Aktivitäten in vier Divisionen: SFPI Access mit mechanischen und elektronischen Schließ- und Zutrittssystemen, SFPI Home mit Lösungen für Gebäudekomfort und Energieeffizienz, also z.B. Rollläden und Sonnenschutz, sowie SFPI Air: Dort geht es um Luftaufbereitung sowie Filter- und Lufttechnik für anspruchsvolle industrielle Lösungen. Schließlich gibt es die Division SFPI Heat – dort geht es um Wärme, Prozess und Sterilisationstechnik für industrielle Anwendungen.

Können Sie einmal beispielhaft einige Highlights nennen, die für die Entwick-

lung des Unternehmens wie es sich heute darstellt, entscheidend waren? Was waren die jüngsten großen Entwicklungsschübe?

Jürgen Maronn: Zu den wichtigsten Meilensteinen zählen sicherlich die Markteinführung des ix-Wendeschlüsselsystems im Jahr 1970 und die kontinuierliche Weiterentwicklung unserer mechanischen Schließsysteme. Ein weiterer entscheidender Schritt war die Entwicklung des digitalen Knaufzylinders 999 im Jahr 2000.

In jüngerer Zeit haben insbesondere die Vernetzung von Zutrittslösungen, cloudbasierte Systeme und mobile Anwendungen unsere Entwicklung geprägt. Zudem haben wir unsere internationalen Aktivitäten ausgebaut und unsere Produktions- und Entwicklungsstandorte weiter gestärkt.

Was waren die wichtigsten Produkt- und Lösungsneuerungen der jüngeren Zeit?

Jürgen Maronn: Ein zentraler Fokus lag auf der Weiterentwicklung unserer digitalen Zutrittssysteme. Dazu gehören skalierbare Lösungen, die sich sowohl für kleine Objekte

Das ix-Schlüsselsystem startete bereits im Jahr 1970



als auch für komplexe Gebäudestrukturen eignen. Dabei sind Themen wie einfache Verwaltung, mobile Nutzung per Smartphone und die stetige Weiterentwicklung der Marktanforderungen in den Bereichen Normen, Zertifizierungen, Verschlüsselungen und Kommunikation besonders wichtig.

Im Herbst kommt ein neues Produkt auf den Markt. Können Sie dazu schon etwas sagen?

Jürgen Maronn: Im Herbst wird eine neue Ära der Sicherheit mit digitalen Dom-Schließsystemen beginnen. Diese überzeugen insbesondere durch eine noch einfachere Integration, erhöhte Flexibilität, verbesserte Benutzerfreundlichkeit und Sicherheitselemente.

Entwicklung und Produktion finden ja ausschließlich in Europa statt?

Jürgen Maronn: Ja, das ist ein zentraler Bestandteil unserer Unternehmensstrategie. Entwicklung und Produktion erfolgen ausschließlich in Europa. Dadurch können wir nicht nur höchste Qualitätsstandards gewährleisten, sondern auch kurze Lieferwege und eine hohe Flexibilität sicherstellen. Gerade in Zeiten globaler Unsicherheiten ist das von großem Vorteil.

Herr Maronn, die jüngere Zeit ist von politischen Verwerfungen geprägt, das hat für viele Unternehmen eine ganze Reihe von Folgen. Auch Ihr Unternehmen muss mit knirschenden Lieferketten umgehen, was sich etwa bei den Preisen für Metalle auswirkt. Wie sieht das bei Ihnen aus?

Jürgen Maronn: Die vergangenen Jahre waren tatsächlich herausfordernd, geprägt von hoher Volatilität, geopolitischen Spannungen und erheblichen Versorgungsrisiken.

Wir haben jedoch frühzeitig Maßnahmen ergriffen, um unsere Lieferketten zu stabilisieren. Dazu zählen unter anderem eine stärkere Diversifizierung unserer Lieferanten und eine engere Zusammenarbeit mit unseren Partnern. Dank unserer europäischen Fertigungsstandorte konnten wir viele Risiken abfedern. Dennoch beobachten wir die Entwicklungen sehr genau und passen unsere Strategien kontinuierlich an.

Es gibt ein neues Partnerprogramm?

Jürgen Maronn: Ja, wir bauen unsere Zusammenarbeit mit unseren Partnern gezielt aus. Mit dem erweiterten, mehrstufigen Keystone-Partnerprogramm möchten wir unsere Fachhandelspartner bei der Marktbearbeitung mit Dom-Produktlösungen stärker unterstützen. Es gibt unterschiedliche Partnerlevel für die Produktbereiche Mechanik und Elektronik, die speziell auf die Keystone-Partner ausgerichtet sind.

Mit welchen weiteren Plänen starten Sie in die nächsten 90 Jahre?

Jürgen Maronn: Unser Ziel ist es, unsere Position als führender Anbieter von Zutrittslösungen weiter auszubauen. Dabei setzen wir konsequent auf Innovation, Digitalisierung und Nachhaltigkeit. Gleichzeitig bleiben wir unseren Werten Qualität, Zuverlässigkeit und Kundennähe treu. Die kommenden Jahre werden stark von intelligenten, vernetzten, digitalen Lösungen geprägt sein – und wir wollen diesen Wandel aktiv mitgestalten. 



Vielseitige Zutrittslösungen

> HOHE SICHERHEIT

Salto Lösungen basieren auf modernsten Zutritts- und Sicherheitstechnologien, binden sämtliche Zutrittspunkte ein und bieten ein umfassendes Zutrittsmanagement.

> OPTIMIERTE PROZESSE

Salto digitalisiert und automatisiert Abläufe durch die Integration mit Management- und IT-Systemen sowie die Einbindung in Workflows.

> EFFIZIENTER BETRIEB

Anwender profitieren von flexibler Raumnutzung, hoher Sicherheit, optimierten Prozessen und niedrigen Lebenszykluskosten.

saltosystems.de

SICHERHEITSEXPO
MOC MÜNCHEN
1./2.7.2026
HALLE 1, STAND C04

SALTO WECSYSTEM





Wechsel an der ESSA-Spitze

Sicherheitsbranche auf künftige Risiken vorbereiten

Myriam Bevillon von Gunnebo Safe Storage ist neue Vorsitzende der European Security Systems Association (ESSA). Sie übernimmt den Staffelstab von Harald Lüling, der den internationalen Verband der physischen Sicherheitsbranche 20 Jahre maßgeblich mitgeprägt hat. Der CEO von Burg-Wächter bleibt Teil des Vorstands. Seine Nachfolgerin Myriam Bevillon erläutert ihre Prioritäten, Herausforderungen, Hürden, Ziele und Visionen.

■ GIT SICHERHEIT: Frau Bevillon, was sind aus Ihrer Sicht die aktuellen Prioritäten der ESSA?

Myriam Bevillon: Mein Hauptfokus ist die Ermittlung von Handelsbarrieren und diese zu überwinden. Eine weitere ist das „One-Stop-Testing“ mit gegenseitiger Anerkennung von Prüfergebnissen durch zugelassene Labore. Zusätzlich möchte ich sicherstellen, dass unsere Normen weiterhin marktkonform sind. Wir müssen z. B. die Anpassung der Tresor-Schlossnorm EN 1300 beschleunigen. Wichtig ist es auch, Smartphone-bediente Schlösser mit einzubeziehen und deren Einsatzgrenzen zu definieren.

Wo sehen Sie derzeit die größten Herausforderungen für die physische Sicherheit?

Myriam Bevillon: Da gibt es einige. Neben der Beschleunigung der Normenerstellung ist es z. B. der KI-Boom samt Folgen. Dazu kommt das Thema Nachhaltigkeit, bei dem das globale Geschäft für physische Sicherheit noch viel Arbeit vor sich hat.

Was sind die größten Hürden auf dem internationalen Markt?

Myriam Bevillon: Bisher war die größte Hürde vor allem unterschiedliche Standards. Neue staatliche Handelshemmnisse haben die Situation aber weiter verkompliziert.

Welche für die ESSA relevanten Sicherheitsthemen werden an Bedeutung gewinnen?

Myriam Bevillon: Cyberangriffe, nun verstärkt durch KI – kein neues Thema, aber eines, was zunimmt. Auch Brandrisiken im Zusammenhang mit der Lagerung von Lithium-Ionen-Batterien verstärken sich, da Batterien immer häufiger zum Einsatz kommen.

Was sind die langfristigen Ziele der Organisation?

Myriam Bevillon: Ich denke, wir werden viele Risiken durchdenken und überprüfen müssen. Es ist Aufgabe des ESSA-Vorstands, darüber auch mit den Mitgliedern zu diskutieren. Unsere Branche ist für ihren starken Fokus auf Sicherheit und Vertraulichkeit und die Einhaltung höchster Standards anerkannt. Dieser Ansatz wird unsere Kernkompetenz bleiben, wir müssen ihn aber um ein höheres Reaktionstempo ergän-

zen. Nur so können wir sich wandelnden Bedürfnissen und Anforderungen schnell gerecht werden. Unsere Märkte werden bei der Einführung neuer Technologien und Arbeitsweisen agiler.

Was ist Ihre eigene Vision für die zukünftige Arbeit der ESSA?

Myriam Bevillon: Ich möchte die Zusammenarbeit und den Austausch der Mitglieder zum Nutzen der Branche fördern. Wir müssen gemeinsam aktiver sein – zum Wohle aller. Für die Zukunft ist es zudem entscheidend, die Sicherheitsbranche so aufzustellen, dass sie künftige Risiken und Sicherheitsherausforderungen abdecken kann. Wir können als Industrie z. B. in der Normung gemeinsam an Sicherheitsanforderungen arbeiten – immer unter Einhaltung der europäischen Gesetze und des Kartellrechts. **GIT**



European Security Systems
Association (ESSA)
www.essa.world

Interkey Jahrestagung 2026 – Gemeinschaft mit fachlicher Tiefe

Mit über 190 Teilnehmern sowie 95 vertretenen Unternehmen aus dem Sektor der Sicherheitstechnik fand die diesjährige Interkey Jahrestagung in Heidelberg statt. Die traditionsreiche Stadt am Neckar bot den passenden Rahmen für eine Veranstaltung, die einmal mehr zeigte, wofür der Interkey Fachverband steht: fachlicher Austausch, persönliche Begegnungen, vertrauensvolle Gespräche und ein starkes Netzwerk, das weit über klassischen Small-talk hinausgeht. 29 Aussteller aus der Sicherheitstechnik präsentierten im Anschluss an die Mitgliederversammlung des Fachverbands ihre Produkte, Lösungen und Dienstleistungen und nutzten die Gelegenheit zum intensiven Austausch und der Kontaktpflege mit den Mitgliedsunternehmen. Dabei wurde deutlich, dass es bei Interkey nicht um oberflächliche Gespräche geht, sondern um konkrete Fragen, gemeinsame Herausforderungen und wertvolle Anregungen für die tägliche Praxis. www.interkey.de

Perimeter Protection Kongress feiert gelungene Premiere

Der Perimeter Protection Kongress fand erstmals im Messezentrum Nürnberg statt. Unter dem Titel „Die neue Dimension – der digitale Zwilling in der Perimetersicherung“, powered by Verband für Sicherheitstechnik e. V. (VfS) brachte das Connected Event der Fachmesse Perimeter Protection knapp 200 Teilnehmer zusammen. Experten aus Industrie, Planung und Betrieb diskutierten aktuelle sicherheitspolitische Entwicklungen, technologische Innovationen und neue strategische Ansätze rund um die Perimetersicherung in 3D. Ergänzt wurde das Kongressprogramm durch eine begleitende Table-Top-Ausstellung, in der 15 Unternehmen ihre Lösungen und Systeme präsentierten und den fachlichen Austausch vertieften. Mit Blick auf aktuelle regulatorische Entwicklungen und die veränderten sicherheitspolitischen Rahmenbedingungen eröffneten Carsten Feddern, Geschäftsführer des Verbands für Sicherheitstechnik, und Peter Ottmann, CEO der NürnbergMesse Group, den Perimeter Protection Kongress. www.nuernbergmesse.de

Mobotix schärft Portfolio



Die Mobotix AG richtet ihr Produktportfolio konsequent auf die Anforderungen moderner Sicherheits- und IoT-Anwendungen aus. Mit einer klaren Fokussierung auf leistungsstarke, modulare Plattformen vereinfacht das Unternehmen sein Angebot – ohne dabei funktionale Lücken entstehen zu lassen.

Im Zuge dieser strategischen Weiterentwicklung werden einzelne Produktlinien planmäßig auslaufen. Ziel ist es, die Komplexität für Partner und Kunden deutlich zu reduzieren und gleichzeitig die technologische Leistungsfähigkeit weiter zu steigern.

„Wir fokussieren uns bewusst auf weniger, dafür deutlich leistungstärkere Plattformen“, erklärt Dr. Christian Cabirol, CTO der Mobotix AG. „Unser Anspruch ist es, unseren Partnern und Kunden eine klare, zukunftssichere Systemlandschaft zu bieten – ohne Kompromisse bei Funktionalität oder Qualität.“

Im Zentrum dieser Neuausrichtung steht die neue Generation der Mobotix Plattformen rund um die Mobotix One Serie. Mit ihrer modularen Architektur, integrierten KI-Funktionalität und hohen Flexibilität decken die Systeme ein breites Spektrum an Anwendungen ab – von klassischer Videosicherheit über industrielle Anwendungen bis hin zu spezialisierten Branchenlösungen.

Insbesondere in Kombination mit dem noch in 2026 geplanten Launch der Mobotix c One entsteht eine leistungsstarke, skalierbare Plattform, die unterschiedlichste Anforderungen in einer einzigen Systemarchitektur vereint. Damit bietet das Unternehmen eine zukunftsfähige Lösung, die sowohl bestehende Einsatzszenarien abdeckt als auch neue Anwendungsfelder erschließt. Die Mobotix Move Serie bleibt weiterhin als qualitativ hochwertige und dennoch preissensible Videolösung für anspruchsvolle Kunden mit weniger systemkritischen Anwendungen im Produkt-Portfolio.

Für Partner bedeutet die Konsolidierung vor allem eines: mehr Übersicht, einfachere Projektierung und klare Upgrade-Pfade. Endkunden profitieren von einer höheren Investitionssicherheit, moderner Technologie und einer langfristig stabilen Produktstrategie.

„Unser Ziel ist es, Komplexität zu reduzieren und gleichzeitig Innovation zu beschleunigen“, so Dr. Christian Cabirol weiter. „Mit unserer neuen Plattformstrategie schaffen wir die Grundlage für nachhaltiges Wachstum – für uns, unsere Partner und unsere Kunden.“

www.mobotix.com

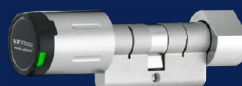
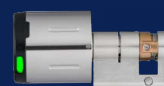
U&Z Uhlmann & Zacher

ASSA ABLOY

Die Zukunft des modernen Zutritts von Uhlmann & Zacher

Mit den elektronischen Türdrückern und Zylindern von U&Z haben Sie die volle Flexibilität – für jedes Objekt.

Entdecken Sie die ganze Bandbreite unseres Sortiments!
www.uhlmannzacher.com



SicherMacher

Der GIT-Talk mit den Marktführern



GIT SICHERHEIT

Kontakt:
Miryam.Reubold@Wiley.com

WILEY



ZUTRITT

Vom Schloss zum System

BKS: Intelligente Sicherheitslösungen auf der SicherheitsExpo München 2026



Am BKS-Messestand auf der SicherheitsExpo München wird vernetzte Gebäudesicherheit mit Echtzeitsteuerung und visueller Systemübersicht demonstriert



■ In einer Zeit, in der Gebäude zunehmend digitaler und die Sicherheitsanforderungen komplexer werden, rückt die intelligente Steuerung von Zutrittsberechtigungen ins Zentrum der Gebäudeplanung. BKS adressiert diesen Wandel auf der SicherheitsExpo mit einem klaren Fokus auf elektronische und vernetzte Systeme.

Ganzheitliches Zutrittsmanagement für alle Branchen und Anforderungen

Im Mittelpunkt des Messeauftritts stehen elektronische Zutrittslösungen, die weit über das klassische Öffnen und Schließen hinausgehen. BKS präsentiert Systeme, die maßgeschneidert für die teilweise sehr unterschiedlichen Anforderungen von Unternehmen, öffentlichen Einrichtungen, KRITIS-Umgebungen aber auch kleineren Büroeinheiten entwickelt wurden. Neue Lösungen wie Ixalo pro oder BKS | smart ermöglichen eine hochflexible Rechteverwaltung in Echtzeit und bieten maximale Sicherheit bei gleichzeitig intuitiver Bedienung. Ein weiterer Schwerpunkt liegt unter anderem auf dem Bereich „Hospitality“. Hier zeigt das Unternehmen zeitgemäße Hotelzutrittslösungen, die den „Guest Journey“ durch smarte Prozesse – vom Check-in bis zur schlüssellosen Türöffnung – digital unterstützen und gleichzeitig die betriebliche Effizienz optimieren. **GIT**

BKS auf der SicherheitsExpo München: Halle 2, Stand G08



BKS GmbH
www.bks.de

Unter dem Leitmotiv „Zutritt neu definiert. Intelligent. Schlüssellos. Vernetzt.“ präsentiert die BKS GmbH ihr zukunftsweisendes Portfolio auf der SicherheitsExpo München. Auf seinem Messestand zeigt der Hersteller, wie moderne Zutrittskontrolle und ganzheitliches Gebäudemanagement die Anforderungen an Sicherheit, Komfort und Effizienz verschmelzen lassen.

barox



Light Core Switch

RY-LGSO38-10

Für strukturierte Netze mit hoher Datenlast

- Speziell für Anwendungen mit hoher Datenlast (Video-over-IP und Video-Streaming)
- Realisation grosser Netzwerkprojekte mit den neuesten Kameramodellen möglich
- Umfangreiche Sicherheitsfunktionen für den Schutz des Switches und des Netzwerkes
- Durch vielseitige Verwaltungsoptionen werden selbst die komplexesten Netzwerkanforderungen erfüllt

barox Kommunikation GmbH

Weiler Strasse 7 | 79540 Lörrach | 07621 1593 100 | www.barox.de

Eine Lösung die mitwächst

Skalierbare Videosicherheitstechnologie für das Snoqualmie Casino & Hotel

Das Snoqualmie Casino & Hotel liegt rund 30 Minuten östlich von Seattle im US-Bundesstaat Washington. Der Name leitet sich vom gleichnamigen Indian Tribe ab – den „People of the Moon“. Das Spielangebot umfasst unter anderem fast 1.800 Spielautomaten und 58 Tischspiele im Vegas-Stil. Bereits seit 2015 vertraut das Snoqualmie Casino & Hotel bei der Videoüberwachung auf die Lösungen von Dallmeier und setzt auch bei der aktuellen Systemerweiterung auf die bewährten Technologien.

Die Videoüberwachung erstreckt sich über sämtliche relevante Zonen der Anlage: Gaming Floor, Front- und Back-of-House-Bereiche, Restaurants und Parkflächen. Das Dallmeier-System hat sich über ein Jahrzehnt hinweg als zuverlässig und skalierbar erwiesen – trotz wachsender Anforderungen und technischer Weiterentwicklungen. Umbauten, Ausbaupläne und neue Anforderungen an interne Abläufe machten jedoch eine Erweiterung der bestehenden Überwachungslösung erforderlich.

Kontinuierliche Überwachung vorgeschrieben

Die Washington State Gambling Commission schreibt eine kontinuierlich überwachte Casino-Umgebung vor. Ziel war es daher, das bestehende System funktional und technologisch an die veränderten Rah-

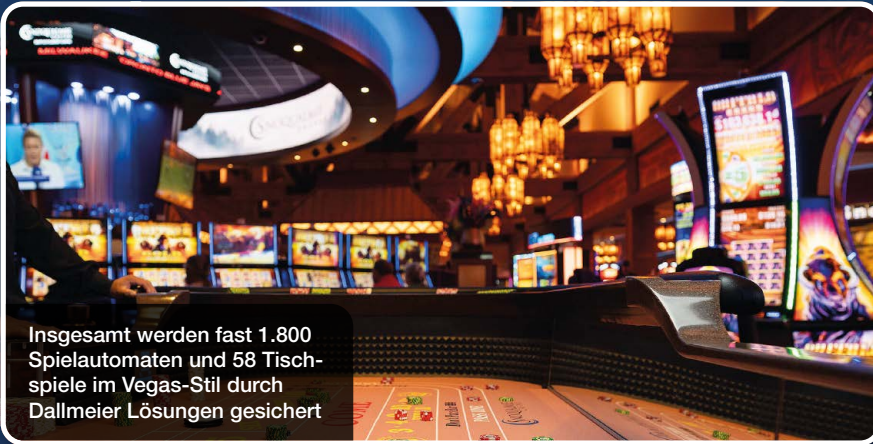
menbedingungen anzupassen, ohne dabei die bewährte Infrastruktur grundlegend zu ersetzen. Die regulatorischen Anforderungen sollten erfüllt und gleichzeitig ein sicheres und angenehmes Umfeld für Gäste und Mitarbeitende gewährleistet werden.

Die Videoüberwachung erstreckt sich über sämtliche relevante Zonen der Anlage



Das Snoqualmie Casino & Hotel bietet neben dem Spielbetrieb auch Hotel, Veranstaltungen und gastronomische Angebote

Zeit für Sicherheit.



Insgesamt werden fast 1.800 Spielautomaten und 58 Tischspiele im Vegas-Stil durch Dallmeier Lösungen gesichert

Neben einer Prozessoptimierung standen dabei insbesondere Zuverlässigkeit, Systemverfügbarkeit sowie die Möglichkeit zur einfachen Integration neuer Technologien im Fokus.

Im Rahmen der Erweiterung wurde das bestehende Überwachungssystem gezielt ausgebaut. Zum Einsatz kommen ausschließlich Komponenten von Dallmeier – darunter das modulare Video-Management-System Hemisphere Semsy und die Domera-Kameras von Dallmeier. Die Dome-Kameras überzeugen durch vorinstallierte neuronale Netzwerke und integrierte Edge Analytics-Apps für eine Vielzahl intelligenter Videoanalyse-Anwendungen. Außerdem ermöglicht die motorische Drei-Achsen-Verstellung einfache und flexible Remote-Einstellungen und Anpassungen. Die Gesamtlösung erlaubt eine zentrale Steuerung der 1.500 Kameras und eine effiziente Auswertung von Videodaten.

Planung und Umsetzung erfolgten in enger Zusammenarbeit mit dem Integrator North American Video (NAV), der das System bedarfsgerecht auf die räumlichen Gegebenheiten und operativen Abläufe anpasste. „Die langjährige und lösungsorientierte Zusammenarbeit mit allen Beteiligten war entscheidend dafür, dass

wir gemeinsam eine Lösung realisieren konnten, die den konkreten Anforderungen entspricht“, fügt Joe McDevitt, Präsident Dallmeier USA, hinzu.

Eine nachhaltige Lösung

„Wir konnten unsere Videosicherheits-technik über ein Jahrzehnt hinweg kontinuierlich mit den Anforderungen mitwachsen lassen“, so Jolene Stewart, Director of Surveillance des Snoqualmie Casino & Hotels. Die Lösung zeichnet sich durch hohe Zuverlässigkeit, null Ausfallzeiten und einfache Wartung aus. Eigenschaften, die für die Effizienz im täglichen Casino-Betrieb entscheidend sind.

Auch wirtschaftlich zahlt sich die Entscheidung langfristig aus: „In der Surveillance-Branche ist Verlässlichkeit ein zentraler Kostenfaktor. Die Tatsache, dass wir über Jahre hinweg keine teuren Ersatzanschaffungen oder unerwartete Serviceeinsätze hatten, spricht für sich“, so Jolene Stewart. **GIT**



Dallmeier electronic GmbH & Co. KG
www.dallmeier.com



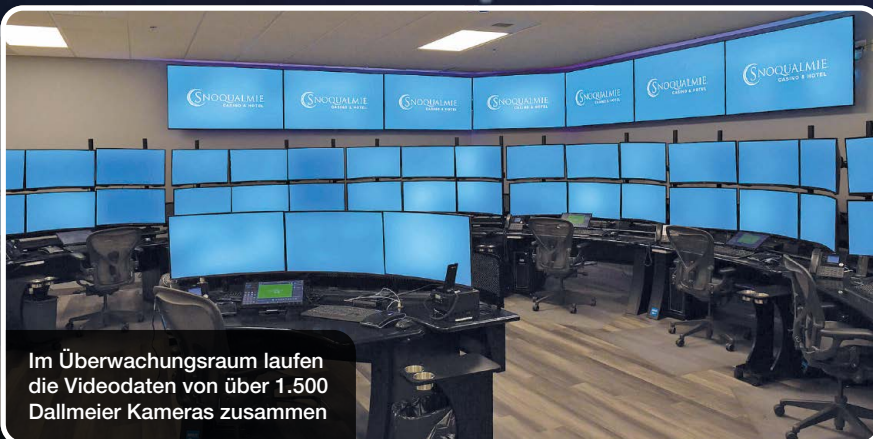
WIR GEBEN GRÜNES LICHT!

- Zeiterfassung
- Zutrittssteuerung
- Videoüberwachung
- Besuchermanagement

◆ Treffen Sie uns vor Ort:
SicherheitsExpo
01.-02.07.2026
München

pcs

www.pcs.com



Im Überwachungsraum laufen die Videodaten von über 1.500 Dallmeier Kameras zusammen



Wenn Ausfälle keine Option sind

Monitore für Leitstellen, Leitwarten und Kontrollräume

Stadler Systec ist Spezialist für schlüsselfertige Technologieintegration für hochverfügbare Kontrollräume aus einer Hand. In Eizo hat das Unternehmen einen langfristigen Partner gefunden.

In Leitzentralen kritischer Infrastrukturen sind Monitore ein wesentlicher Bestandteil der täglichen Arbeit. Sie müssen nicht nur eine hervorragende Bildqualität liefern, sondern auch über viele Jahre hinweg zuverlässig funktionieren – und das meist rund um die Uhr. Für das inhabergeführte Unternehmen Stadler Systec, spezialisiert auf schlüsselfertige Technologieintegration für Leitstellen, Leitwarten und Kontrollräume, ist die Wahl des richtigen Monitorherstellers daher eine strategische Entscheidung.

Dabei zählen sowohl die technische Leistungsfähigkeit der Produkte als auch eine verlässliche, langfristige Partnerschaft zu den entscheidenden Faktoren.

Technik, Qualität und Verlässlichkeit

„Im Projektgeschäft kommt es für uns auf schnelle Verfügbarkeit, Verlässlichkeit, Betreuung und Produktqualität an. Eizo liefert in all diesen Punkten. Man merkt, dass die Produkte für anspruchsvolle Umgebungen entwickelt sind. Die lange Garantie

vieler Modelle sind ein deutliches Signal dafür, dass der Hersteller von seiner Qualität überzeugt ist“, so Markus Stadler, CEO bei Stadler Systec. „Verlässliche Betreuung und Liefertreue sind für uns im Projektgeschäft extrem wichtig. Bei Eizo erleben wir eine Betreuung, die zuverlässig ist und bei der man auch wirklich jemanden erreicht. Gerade wenn man im laufenden Projekt schnell eine saubere Lösung braucht, ist diese direkte, freundliche und verbindliche Zusammenarbeit ein echter Pluspunkt“, so Stadler weiter.

Stadler Systec hat schon früher größere Office Projekte realisiert, unter anderem im Bankenumfeld, in dem Eizo bereits als feste Größe etabliert war. Mit der stärkeren Fokussierung auf Leitstellen und Kontrollräume, Umgebungen, in denen Technik dauerhaft funktionieren muss und Ausfälle keine Option sind, lag es nahe, auf eine Marke zu setzen, die sich in der Praxis bereits vielfach bewährt hat. Die Zusammenarbeit besteht inzwischen seit über zehn Jahren.

Mehrwert im Projektgeschäft

Aus Sicht des Vertriebs zeigt sich der Mehrwert der Partnerschaft vor allem im konkreten Projektgeschäft: „Wir haben Eizo-Monitore bereits in zahlreichen Projekten unterschiedlichster Branchen eingesetzt – etwa in der chemischen Industrie, in Netzleitstellen und Verkehrsleitzentralen sowie Freizeitparks“, berichtet David Mrnak, Vertriebsleiter bei Stadler Systec.



Systec montiert die Monitore meist an seinem eigens entwickelten Monitor-Tragarmsystem

38" Ultrawide-Monitor EV3895

Der Curved Ultrawide-Monitor mit 3840 x 1600 Pixeln bietet die fast dreifache Auflösung eines Full HD-Monitors:

- 24:10 Format
- 3840x1600 Pixel (111 ppi)
- USB-C mit DisplayPort-Signalkanal, LAN
- KVM-Switch und Picture-by-Picture
- 5 Jahre Garantie inkl. Vor-Ort-Austauschservice



„Je nach Einsatzszenario können aber auch Curved-Modelle interessant sein, vorausgesetzt, das Format passt sowohl zum Anwendungsfall als auch zu den eingesetzten technischen Komponenten zur Signalübertragung.“

Welche Monitorlösungen künftig bevorzugt werden,

hängt stark von Branche und Kundenanforderung ab. Denkbar ist auch ein zunehmender Einsatz größerer Displaydiagonalen, sofern die Technik zuverlässig arbeitet und die entsprechenden Mehrkosten vom Kunden mitgetragen werden. Zwar dominieren derzeit weiterhin 24 Zoll Modelle, doch wächst die Bereitschaft, für mehr Komfort und Übersicht in größere Formate wie 27 oder 32 Zoll zu investieren. Auch Ultrawide-Monitore werden dort interessant, wo Anwendungen flexibel genutzt werden können.“ **BIT**

„Überwiegend kommen dabei 24 Zoll Modelle wie EV2400R, EV2456 und EV2460 zum Einsatz, aber auch größere Displays wie EV2760 (27 Zoll) oder EV3895 (37,5 Zoll, Ultrawide). Für uns als Systemintegrator ist es entscheidend, dass wir uns langfristig auf Produktverfügbarkeit, Ersatzteile und einen durchgängig sehr guten Support verlassen können, von der schnellen Angebotserstellung über fundierte technische Beratung bis hin zum zuverlässigen After Sales Service. Genau das macht Eizo für uns und unsere Kunden so wertvoll.“

Sammelverpackungen

„In nahezu allen Projekten montieren wir die Monitore an unserem eigens entwickel-

ten Monitor-Tragarmsystem. So können wir optimierte und kundenspezifische Tisch- und Monitorkonfigurationen realisieren“, erklärt David Mrnak. „Klassische Standfüße benötigen wir dafür nicht. Sammelverpackungen ohne Standfüße sind daher ideal für uns, insbesondere, weil sich die Anforderungen im Office Bereich deutlich von denen im Mission Critical Control Room unterscheiden.“

Blick in die Zukunft

„Ergonomie und Bildqualität bleiben zentrale Faktoren, ebenso wie langfristige Verfügbarkeit und Ersatzteilhaltung. Standard-Monitore sind für viele Anwendungen nach wie vor eine sehr gute Wahl“, erläutert David Mrnak.



Eizo

www.eizo.de/videoeuberwachung

© Bilder: Eizo

22. – 25. September 2026

SECURE YOUR BUSINESS



JETZT TICKET SICHERN!

Zum 1. Mal parallel:
die EURO DEFENCE EXPO –
die neue internationale
Fachmesse der
Verteidigungsindustrie

Die Leitmesse für Sicherheit



security
essen 26

the number one

www.security-essen.de

MESSE
ESSEN

EVENT

Sicherheit im Realtest

Live-Demos, Fachvorträge und Einordnung neuer Gesetze beim TechDay in Rödermark

Mit dem Videor TechDay 2026 rückte am 7. Mai in Rödermark die physische Sicherheit kritischer Infrastrukturen (KRITIS) in den Mittelpunkt. Über 180 Fachbesucher aus Industrie, Behörden und Sicherheitsplanung erlebten live, wie moderne Perimeter- und Freigeländesicherung unter realistischen Bedingungen funktioniert. Im Fokus standen KI-gestützte Videoanalyse, Sensorik, Robotik und integrierte Reaktionsketten – praxisnah demonstriert im Stresstest.

Ob Scharfschützenanzug, wärmeisolierende Decken oder Dinosaurierkostüm, bei den Live-Demos wurden von Videor alle Register gezogen, um die Sicherheitssysteme zu irritieren

Der Videor TechDay 2026 war bewusst als Live-Veranstaltung konzipiert. Auf dem Außengelände der Videor E. Hartig GmbH wurden Freigelände und Perimeter mit Kameras und Sensorik ausgestattet. In realitätsnahen Angriffssimulationen am Zaun demonstrierten Hersteller bei Tageslicht und Dunkelheit, wie zuverlässig aktuelle Technologien Bedrohungen erkennen. Dabei kamen ein Scharfschützentrainingsanzug, wärmeisolierende Decken, ein Dinosaurierkostüm und eine Vielzahl farbiger Rauchbomben zum Einsatz. Ziel war es, Leistungsfähigkeit und Grenzen moderner Systeme transparent zu machen.

Technologien für den KRITIS-Schutz

Inhaltlich dominierte der Schutz kritischer Infrastrukturen vor Sabotage, Vandalismus und unbefugtem Zutritt. Gezeigt wurden unter anderem KI-gestützte Videoanalyse, faseroptische Sensorik zur Zaun- und Leitungsüberwachung, Radar und LiDAR-Lösungen sowie mobile Robotik. Mehrere Aussteller demonstrierten, wie sich diese Komponenten zu integrierten Sicherheitskonzepten verbinden lassen – ein Ansatz, der vor dem Hintergrund neuer gesetzlicher Anforderungen zunehmend an Bedeutung gewinnt.

Gesetzlicher Druck als Treiber

Ein wiederkehrendes Thema des Tages war das KRITIS-Dachgesetz sowie das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz. Beide verschärfen die Anforderungen an Betreiber kritischer Infrastrukturen und rücken – neben der IT-Sicherheit – die physische Absicherung stärker in den Fokus. Der TechDay verstand sich daher auch als Orientierungshilfe für Sicherheitsverantwortliche, die Investitionsentscheidungen auf eine realistische Bewertung aktueller Technik stützen müssen.

ASSA ABLOY

Kultur sichern



Der TechDay 2026 aus der Drohnenperspektive zum Start der Veranstaltung



Auch bei Nacht, mussten die Systeme zeigen, was in ihnen steckt

Austausch und Einordnung

Neben den Live-Demos bot die Veranstaltung bei Burger und Pizza Raum für Fachdialog und Networking. Hersteller, Planer, Integratoren und Betreiber nutzten den direkten Austausch, um Erfahrungen aus der Praxis zu teilen. Ergänzend kündigte Videor eine Webinarserie im Nachgang an, um ein breiteres Publikum vertieft über die Funktionsweise und Möglichkeiten einzelner Technologien und Anwendungsszenarien zu informieren.

Der Videor TechDay 2026 zeigte eindrücklich, wie sich physische Sicherheit unter Live-Bedingungen bewerten lässt. Statt geschliffener Produktinszenierungen standen realitätsnahe technologische Belastungstests im Vordergrund. Für die Sicherheitsbranche lieferte das Format eine wichtige Einordnung aktueller Technologien und machte deutlich, dass integrierte Lösungen angesichts wachsender KRITIS-Anforderungen unverzichtbar werden. **GIT**



Videor E. Hartig GmbH
www.videor.com/de

www.GIT-SICHERHEIT.de



Wir ziehen für jede
Situation eine flexible
Lösung aus der
Schublade – ganz sicher!

www.assaabloy.com/de

Standard für Authentizität

Vom Fraunhofer-Forschungsprojekt zur globalen Sicherheitslösung für physische Produkte

Was als wissenschaftliches Forschungsprojekt des Fraunhofer-Instituts für Physikalische Messtechnik (IPM) in Freiburg begann, hilft heute führenden Marken und Organisationen weltweit dabei, die Einzigartigkeit ihrer Produkte zu garantieren und Fälschungen lückenlos zu verhindern. Mit Origify lassen sich Produktfälschungen ganz einfach per Smartphone-App erkennen. Vor kurzem feierte Bosch Secure Authentication dessen einjähriges Bestehen. Damit haben eine Idee und ein Algorithmus, die 2008 ihren Anfang nahmen, den Weg aus dem Labor hin zu einem marktfähigen, industriell genutzten Produkt gemeistert.

Die ersten Ideen zur markierungsfreien Identifikation reichen am Fraunhofer IPM bis in die Jahre 2008 und 2009 zurück. Damals zeigten frühe Machbarkeitsstudien an Bosch-Zündkerzen, dass ein Fälschungsschutz durch individuelle Oberflächenstrukturen prinzipiell möglich ist. Dafür platzierte ein Roboter das Objekt in der exakt richtigen Position, fotografiert wurde mit einer hochauflösenden Industriekamera. Nur unter diesen optimalen Bedingungen war eine Identifikation möglich – an eine Aufnahme per Handykamera war vor 18 Jahren nicht zu denken.

Der entscheidende Durchbruch kam Jahre später: 2018 wurde Oliver Steinbis, heute Technischer Geschäftsführer der Bosch Secure Authentication, auf die bildbasierte Technologie aufmerksam. „Um zu beweisen, dass der Algorithmus funktioniert, haben wir das System 2018 in einem Bosch-Werk in Feuerbach für Partikelmesssensoren eingesetzt“, erinnert er sich. Das Ergebnis war ein voller Erfolg: Bei über 150.000 Teilen erreichten die Tester eine Wiedererkennungsrate, die selbst höchsten Sicherheitsanforderungen gerecht wird. Prof. Dr. Daniel Carl, stellvertretender Institutsleiter am Fraunhofer IPM

und von Beginn an Teil der Projektgruppe um Origify, stellt fest, dass die Zuverlässigkeit sogar so hoch ist, dass Zero-Tolerance-Anwendungen im Hochsicherheitsbereich möglich sind. Die Entwicklung von Origify zähle für ihn zu den Top-3-Erfolgsstorys seiner Berufskarriere.

Von der hochauflösenden Industriekamera zum Smartphone

Die Anforderungen von Bosch gingen jedoch weiter: „Wir wollten eine Lösung, die smartphonefähig, deutlich robuster und unabhängig von äußeren Einflüssen

wie Belichtung oder Aufnahmewinkel des Objekts ist“, erinnert sich Oliver Steinbis. Fraunhofer setzte diese Anforderungen konsequent um. Bosch investierte in diese exklusive Weiterentwicklung für das Smartphone und die Cloud und sicherte so den technologischen Vorsprung. Das Resultat ist ein Algorithmus, der weltweit als branchenführend im Bereich der markierungsfreien Identifikation gilt.

Das Fraunhofer-Modell

„Wir sehen uns in dieser Partnerschaft als verlängerte Werkbank und fühlen uns als Teil von Origify“, sagt Daniel Carl. „Neben allen Verträgen verbindet uns mittlerweile auch eine emotionale Zugehörigkeit – es liegt uns einfach am Herzen, dass Origify erfolgreich ist.“ Diese Begeisterung teilt das Team der Bosch Secure Authentication: „Die strategische Partnerschaft mit dem Fraunhofer Institut ist dem gegenseitigen Vertrauen zu verdanken, das beide Partner zueinander hatten. Es ist ein Paradebeispiel für das riesige Potenzial, das entfesselt wird, wenn Industrialisierungskompetenz wie bei Bosch auf den Forschungsdrang von Fraunhofer trifft, um ein funktionierendes Produkt mit realem Anwendungsfall zu konzipieren.“ 



Siemens stärkt Cyberresilienz für sichere Stromversorgung

Siemens Smart Infrastructure stärkt mit seinem Managed Detection and Response-Service die Cyberresilienz für Energieversorger und Betreiber energieintensiver Industrien sowie kritischer Infrastrukturen, wie Rechenzentren und Flughäfen.

Angesichts der zunehmenden Konvergenz von Informationstechnologie (IT) und Betriebstechnologie (OT) stehen Unternehmen vor der Herausforderung, eine wachsende Flut von Sicherheitsalarmen zu bewältigen. Oftmals stehen die dafür notwendigen, 365 Tage rund um die Uhr verfügbaren personellen Ressourcen, die das erforderliche Fachwissen haben, nicht zur Verfügung. Der Service von Siemens adressiert genau diese Lücke und unterstützt Unternehmen dabei ihre zunehmend digitalisierten Anlagen sicher, NIS-2-konform und aus einer Hand zu betreiben.

Der MDR-Service bietet einen 24/7-Schutz durch Überwachung, Analyse potenzieller Vorfälle und entsprechender Handlungsempfehlung. Dies ermöglicht eine bis zu 90 Prozent schnellere Erkennung von Cyberbedrohungen. Der Prozess beginnt mit der Sammlung sicherheitsrelevanter Daten aus den IT- und OT-Systemen des Kunden, die sicher an das SOC übermittelt werden.

www.siemens.com

Flexible Lösungen für Umkleiden und moderne Arbeitswelten

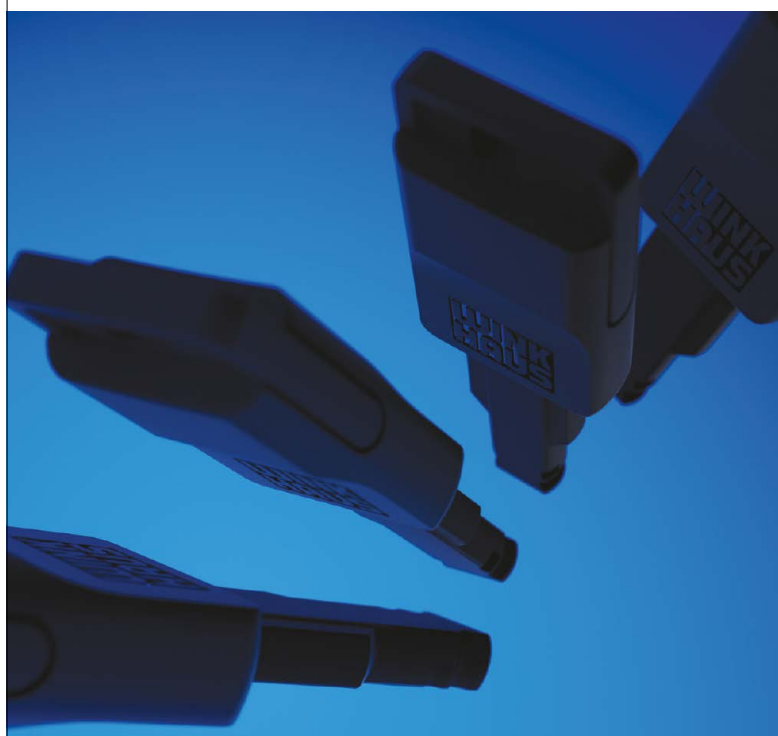
Mit dem BE 80 Möbelschloss ergänzt Winkhaus das Portfolio seines elektronischen Schließsystems blueEvo um eine vielseitige Lösung für Spinde und Wertfächer. Das System ist in zwei Varianten erhältlich und eignet sich für unterschiedliche Einsatzbereiche – von Umkleiden in Krankenhäusern und Pflegeeinrichtungen über Freizeit- und Sportstätten bis hin zu modernen Büro- und Open-Space-Konzepten. Die elektronischen Möbelschlösser ermöglichen sowohl eine feste Schrankzuordnung als auch eine freie Schrankwahl. Damit lassen sich individuelle Nutzungskonzepte realisieren, beispielsweise für Mitarbeiterspinde mit dauerhaftem Zugriff oder für wechselnde Nutzer, die sich bei Bedarf einen freien Spind auswählen. Die Bedienung ist komfortabel über ein Identmedium möglich – beispielsweise eine Karte oder einen elektronischen Schlüssel.

www.winkhaus.de



blueEvo

NIS-2-Richtlinie | Erfahren Sie mehr über die „Bedeutung der NIS-2-Richtlinie für Unternehmen und öffentliche Einrichtungen“ in unserem gleichnamigen kostenlosen Whitepaper.



Die Evolution einer Tradition.

Ihr Gebäude besteht aus unterschiedlichen Räumen, Türen, Toren und unzähligen Schlössern.

Sie entscheiden, wer welche öffnet. Und das mit nur einem Schlüssel.

blueEvo.com

**WINK
HAUS**

Zwischen Einfachheit und Skalierbarkeit

GIT SICHERHEIT untersucht die neue Zutrittskontrollzentrale Axon2600 von Aritech

Zutrittskontrollsysteme nehmen innerhalb ganzheitlicher Sicherheitskonzepte eine zentrale Rolle ein. Gleichzeitig zeigt die Praxis, dass der Einstieg in professionelle Zutrittskontrolle für kleinere und mittlere Anwendungen häufig mit erheblichem Planungs- und Installationsaufwand verbunden ist. Komplexe Systemarchitekturen, getrennte Werkzeuge für Errichter und Betreiber sowie begrenzte Erweiterbarkeit stehen dabei oftmals einer wirtschaftlichen Umsetzung im Weg. Vor diesem Hintergrund gewinnen Lösungen an Bedeutung, die bewusst auf einen einfachen Einstieg setzen und dennoch langfristige Skalierbarkeit ermöglichen.

Die Zutrittskontrollzentrale Axon2600 von Aritech im geöffneten Gehäuse: kompakte Standalone-Lösung für zwei bis sechs Türen mit modularer Erweiterungsoption

■ Mit der Axon2600 stellt Aritech – Teil der internationalen Kidde-Gruppe – eine neue Zutrittskontrollzentrale vor, die genau diesen Spagat adressieren soll. Die Fachzeitschrift GIT SICHERHEIT kündigt daher einen redaktionellen Produkttest an, in dem die Axon2600 unter Praxisbedingungen untersucht wird.

Standalone-Zutrittskontrolle mit Erweiterungsperspektive

Normativ ist die Axon2600 klar als Zutrittskontrollzentrale einzuordnen. Sie ist als eigenständiges System konzipiert und unterscheidet sich damit sowohl von reinen Einzeltürlösungen als auch von vollintegrierten Gefahrenmanagementplattformen. Im Grundausbau lassen sich zwei bis sechs Türen unmittelbar an der Zentrale betreiben – ohne zusätzliche Türcontroller oder komplexe Infrastruktur.

Gleichzeitig ist das System auf Erweiterung ausgelegt: Über zusätzliche Türcontroller kann die Installation schrittweise auf größere Anwendungen ausgebaut werden. In Verbindung mit der Management-Software Advisor Management ATS8600 oder dem neuen Fusion Management-System sind dabei deutlich größere Tür- und Benutzerzahlen realisierbar. Dieser modulare Ansatz erlaubt es, Zutrittskontrolle zunächst standortbezogen umzusetzen und später in übergeordnete Sicherheitsstrukturen zu integrieren.

Software-Kompatibilität

- UltraSync Web-Anwendung für Errichter
- Web-Anwendung für Endanwender
- Android Mobile-App
- IOS Mobile App
- ATS8600 Lokales Management
- ATS8600 UltraSync Fern-Steuerung
- API Integration

Installation, Inbetriebnahme und Bedienkonzept

Ein zentrales Merkmal der Axon2600 ist das einheitliche Bedienkonzept für Errichter und Betreiber. Konfiguration und Verwaltung erfolgen über eine gesicherte Weboberfläche (HTTPS) sowie über eine mobile Applikation, die abhängig von der Benutzerrolle unterschiedliche Funktionen freigibt. Separate Errichter-Tools oder lokale Management-Stationen sind für den

Basiseinsatz nicht erforderlich.

Die Inbetriebnahme erfolgt browserbasiert und soll insbesondere bei kleineren Installationen eine

schnelle Umsetzung ermöglichen. Für den laufenden Betrieb stehen Funktionen zur Benutzer-, Tür- und Zeitplanverwaltung zur Verfügung. Ereignisse und Systemzustände lassen sich protokollieren und auswerten, was eine kontinuierliche Systemüberwachung erlaubt.

Vernetzung, Integration und Cyber-Security

Die Axon2600 unterstützt sowohl IP-basierte Kommunikation als auch Mobilfunkanbindung über 4G. Über die Ultra-Sync-Sicherheitscloud können Fernzugriffe, Wartung und Firmware-Updates realisiert werden. Darüber hinaus lassen sich Systemmeldungen an externe Stellen, etwa Leitstellen oder Serviceeinrichtungen, übertragen.

Auf der Feld- und Systemebene setzt Aritech auf verschlüsselte Kommunikation und etablierte Sicherheitsprotokolle. Unterstützt werden unter anderem OSDP

v2 mit Secure Channel sowie Mifare Desfire EV2/EV3. Die Anbindung unterschiedlicher Leser- und Schließsysteme – einschließlich Funk-Schlössern verschiedener Anbieter – ist realisierbar. Über eine offene API kann die Zutrittskontrolle zudem in bestehende Gebäude-, Besucher- oder Sicherheitsmanagementsysteme eingebunden werden.

Abgrenzung und typische Einsatzbereiche

Die Axon2600 richtet sich primär an Anwendungen, bei denen wenige Türen, aber viele Nutzer verwaltet werden müssen. Typische Einsatzbereiche sind kleinere Unternehmensstandorte, Verwaltungsbauwerke, Bildungseinrichtungen oder dezentrale Liegenschaften. Der Fokus liegt dabei auf einfacher Nachrüstbarkeit, klarer Systemstruktur und der Möglichkeit, die Lösung bei steigenden Anforderungen ohne Systemwechsel zu erweitern.

Ausblick auf den Produkttest

Der von GIT SICHERHEIT geplante Test setzt genau an dieser Schnittstelle zwischen Konzept und Praxis an. Untersucht werden unter anderem:

- Installation und Inbetriebnahme,
- Bedienbarkeit für Errichter und Betreiber,
- Alltagstauglichkeit im laufenden Betrieb,
- Erweiterbarkeit und Integrationsfähigkeit,
- sowie die praktische Umsetzung von Cyber-Security-Funktionen.

Die Ergebnisse des Tests werden redaktionell ausgewertet und in einer der kommenden Ausgaben der Fachzeitschrift veröffentlicht. Der vorliegende Beitrag markiert damit den Auftakt zu einer praxisnahen Bewertung der neuen Axon2600-Zutrittskontrollzentrale. **GIT**



Aritech (Kidde Global Solutions)
www.aritech.de

Assa Abloy Fachseminar: Integrierte Sicherheitskonzepte für KRITIS

Assa Abloy führte gemeinsam mit namhaften Partnerunternehmen die kostenfreie Online-Fachseminarreihe zum Thema „Brandschutz im System unter Beachtung der KRITIS 27001“ weiter fort. Die Veranstaltung richtete sich an Planer, Architekten, Sicherheitsverantwortliche sowie Betreiber kritischer Infrastrukturen, die sich über die aktuellen Anforderungen und praxisorientierte Lösungen informieren möchten. Im Mittelpunkt stand die Frage, wie sich Brandschutz, physische Sicherheit, Zutrittsmanagement und Videosicherheit zu einem ganzheitlichen NIS2-konformen Schutzkonzept für KRITIS-relevante Gebäude und Anlagen verbinden lassen.

Den Auftakt bildete der Vortrag von Dirk Möbius von der Sälzer GmbH, in dem die neuesten Entwicklungen rund um das KRI-

TIS-Dachgesetz und die daraus resultierenden Resilienzplichten für Betreiber kritischer Anlagen im Fokus standen. In diesem Kontext stellte er außerdem Systemlösungen für hochsichere Eingangsbereiche vor, die kombinierten Schutz gegen Einbruch, Beschuss und Sprengwirkung bieten.

Ein weiterer Schwerpunkt lag auf modernen Zutrittslösungen nach ISO 27001. Ergänzend beleuchtete Jochen Sauer von der Axis Communications GmbH aktuelle Entwicklungen in der Videosicherheit 4.0 – von betrieblichen Anforderungen nach EN 62676-4 bis hin zu Aspekten der Netzwerksicherheit.

Im zweiten Teil der Veranstaltung galt anschließend baulichen Schutzsystemen und Brandschutzlösungen besonderes Augenmerk. Unter anderem sprach Thomas May

von der Schüco International KG über Feuerenschutzabschlüsse nach DIN 4102-5, Aspekte der Gebrauchstauglichkeit von Türen sowie Lösungen zur Einbruchhemmung nach EN 1627ff. Darüber hinaus hob Thomas Meissner von Vetrotech in seinem Vortrag die Rolle von Brandschutz- und Sicherheitsglas als zentraler Bestandteil eines erfolgversprechenden KRITIS-Schutzkonzepts hervor – insbesondere im Hinblick auf Verfügbarkeitssicherung und Schutz vor Sabotage oder Angriffen. www.assaabloy.com/de

Noch mehr Brandschutz
ab Seite 59



CLEVER SPRINKLER

Unser SmartFit® bringt digitale Präzision in Ihr Löschanlagenkonzept.

- **Gezielt oder großflächig:** Schützt genau die Bereiche, in denen Gefahr entsteht.
- **Reagiert in Sekunden:** Brände werden abgefangen, bevor sie sich ausbreiten.
- **Passt sich Ihrem System an:** Ideal für automatisierte Lager und sensible Zonen.
- **Einfacher Betrieb:** Digitale Kontrolle, weniger Aufwand, mehr Sicherheit.



JAMMING & SPOOFING

Gegen GNSS-Jamming und Spoofing

Lösungen zum Schutz kritischer Infrastrukturen

Absichtliche Störungen von GNSS-Signalen nehmen zu und werden zum Risiko für kritische Systeme. Die Lösungen von Hensec ermöglichen die Detektion und Ortung von Jamming und Spoofing, damit Betreiber rechtzeitig gegensteuern können.

„Position, Navigation und insbesondere hochpräzises Timing bilden das unsichtbare Fundament digitaler Kommunikation, autonomer Systeme und kritischer Infrastrukturen. Gerät dieser Taktgeber aus dem Schritt, funktionieren diese Systeme nicht mehr“,

sagt Kevin Heneka, Gründer von Hensec. „Mit unserer Lösung, die komplett in Europa entwickelt und gehostet wird, bieten wir eine Möglichkeit, das GNSS-Signal zu überwachen und schaffen so eine Grundlage für sichere und resiliente PNT-Systeme.“



GNSS-Satellitennetz bietet Orientierung

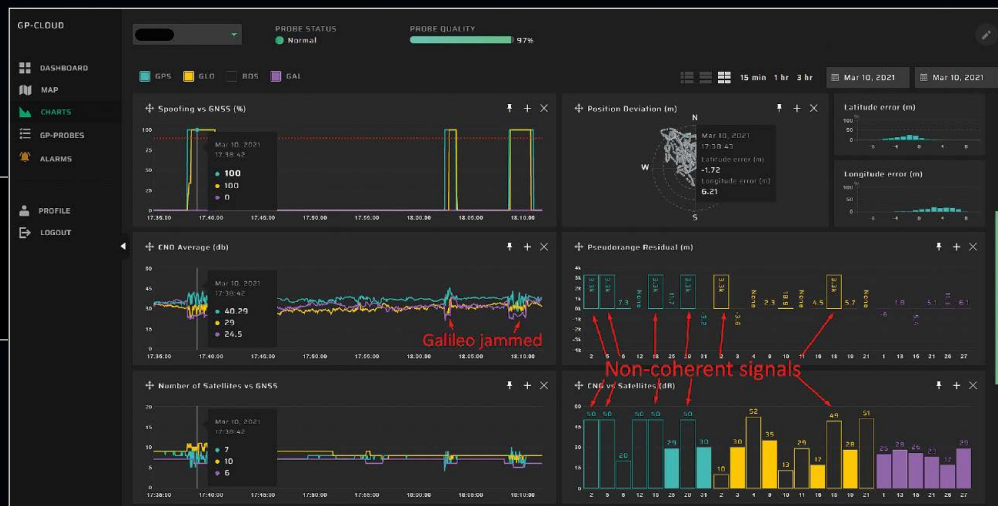
In unserer digitalen Welt sind immer mehr Systeme von GNSS-Daten abhängig. GNSS ist dabei die Abkürzung für Global Navigation Satellite System. Das vermutlich bekannteste davon ist das US-amerikanische Global Positioning System. Seine Abkürzung GPS hat sich als Synonym für alle Satellitennavigationssysteme etabliert. Neben GPS gibt es u. a. noch Galileo aus Europa, Beidou aus China sowie Glonass aus Russland.

Das GNSS besteht aus einem Netzwerk von Satelliten, die in einer Höhe von rund 20.000 Kilometern um die Erde kreisen. Jeder dieser Satelliten funkt permanent Signale zu seiner genauen Position sowie der Zeit, zu der das Signal versendet wurde. Dieser Zeitstempel wird durch eine hochgenaue Atomuhr ermittelt, die sich an Bord jedes Satelliten befindet.

Ein GNSS-Empfänger auf der Erde empfängt einfach gesagt die Signale von mehreren Satelliten gleichzeitig. Ausgestattet mit einer normalen Quarzuhr, erfasst er auch, wie lange das Signal vom Weltall bis zu ihm gebraucht hat. Da sich die Signale mit Lichtgeschwindigkeit ausbreiten, lässt sich die Entfernung zum jeweiligen Satelliten berechnen: Entfernung = Laufzeit x Geschwindigkeit.

Für die Berechnung seiner Position auf der Erde, benötigt der GNSS-Empfänger die Signale von mindestens vier Satelliten. Dabei sind drei Satelliten ausreichend, um die Position in einem dreidimensionalen Raum zu bestimmen. Für die Korrektur der Zeitabweichung im Empfänger ist ein vierter Satellit erforderlich.

Interferenz, Jamming oder Spoofing? Die GP Cloud liefert Antworten



GNSS-Timing: Taktgeber in der digitalen Welt

GNSS-Systeme bieten drei Hauptfunktionen, nämlich Position, Navigation und Timing (kurz: PNT). Vor allem die Funktionen für Position und Navigation sind allgemein bekannt, weil sie mittlerweile selbstverständlich für Routenplanungen auf dem Smartphone oder anderen Navigationsgeräten genutzt werden. Wie eingangs erklärt, beeinträchtigen GNSS-Störungen die Navigation im Flug- und Schiffsverkehr und bekommen viel mediale Aufmerksamkeit.

Die Timing-Funktion ist für unsere moderne Gesellschaft entscheidend. Die gesamte digitale Kommunikation ist auf exakte Zeitsynchronisation angewiesen, damit Daten von Systemen, die sich an verschiedenen Standorten befinden, korrekt übertragen werden. Wird für diese Übertragung das Internet genutzt, so ist eine Genauigkeit von rund zwei Millisekunden zu erreichen. Durch den Einsatz eines GNSS-Empfängers auf den Geräten lässt sich die Genauigkeit auf ungefähr zwei Nanosekunden steigern.

Kommt es zu Störungen des GNSS-Signals, so sind also davon nicht nur die Navigation im Flug- oder Schiffsverkehr betroffen, sondern alle zeitkritischen Systeme wie Mobilfunk, Energieübertragungsnetze, Rechenzentren, Fahrzeugtechnologie und Drohnen. So sind beispielsweise Mobilfunknetze der vierten und fünften Generation (4G/5G) im besonderen Maße auf präzise Zeit- und Frequenzsynchronisation angewiesen. Basisstationen müssen ihre Funkzellen exakt aufeinander abstimmen, damit mobile Endgeräte nahtlos von einer Zelle in die nächste wechseln können. GNSS liefert dafür eine hochgenaue Zeitbasis und eine Frequenzreferenz. Besonders in 5G-Netzen, in denen Techniken wie Time Duplexing und Beamforming zum Einsatz kommen, sind

die Anforderungen an die Synchronisation nochmals enorm gestiegen. Die GNSS-Zeitinformation wird in Mobilfunknetzen häufig direkt an den Basisstationen empfangen und dient dort als Referenz für alle Synchronisationsprozesse. Kommt es zu Störungen des GNSS-Systems, so verlieren einzelne Zellen ihre zeitliche Ausrichtung. Dies führt gegebenenfalls zu Interferenzen zwischen den Zellen, Verbindungsabbrüchen oder einer drastisch reduzierten Netzkapazität.

GNSS-Störungen als systemisches Risiko

Satelliten bewegen sich in großer Höhe und mit einer enormen Geschwindigkeit über der Erdoberfläche. Ihr ausgesendetes Signal ist damit vergleichsweise schwach und kann bereits durch nur geringfügig stärkere Sender, die sich direkt auf der Erde befinden, überlagert werden. Auch die rasante technische Entwicklung ist für die Zunahme der Störfälle verantwortlich: Die Preise für Störsender fallen zusehends, während die Geräte immer mobiler werden. Außerdem sind sie relativ einfach über das Internet zu erwerben, obwohl ihr Betrieb in Deutschland verboten ist. Grundsätzlich unterscheidet man zwei Arten von absichtlichen Störungen:

Jamming

Ein Jammer überlagert die GNSS-Signale, indem er Störsignale auf den selben Frequenzen sendet, die auch vom GNSS-System genutzt werden. Das sogenannte GPS-L1 Band hat die Frequenz 1575,42 MHz. Da die Frequenzen der GNSS-Satelliten bekannt sind, so ist auch ihre Störung technisch nicht besonders aufwändig.

Spoofing

Etwas komplexer und gleichzeitig gefährlicher ist das sogenannte Spoofing. Dabei wird ein manipuliertes GNSS-Signal ausge-

sendet, um das authentische Signal zu überlagern. So lassen sich falsche Positions- und Zeitangaben vortäuschen, die lange nicht als gefälscht wahrgenommen werden.

Signalüberwachung

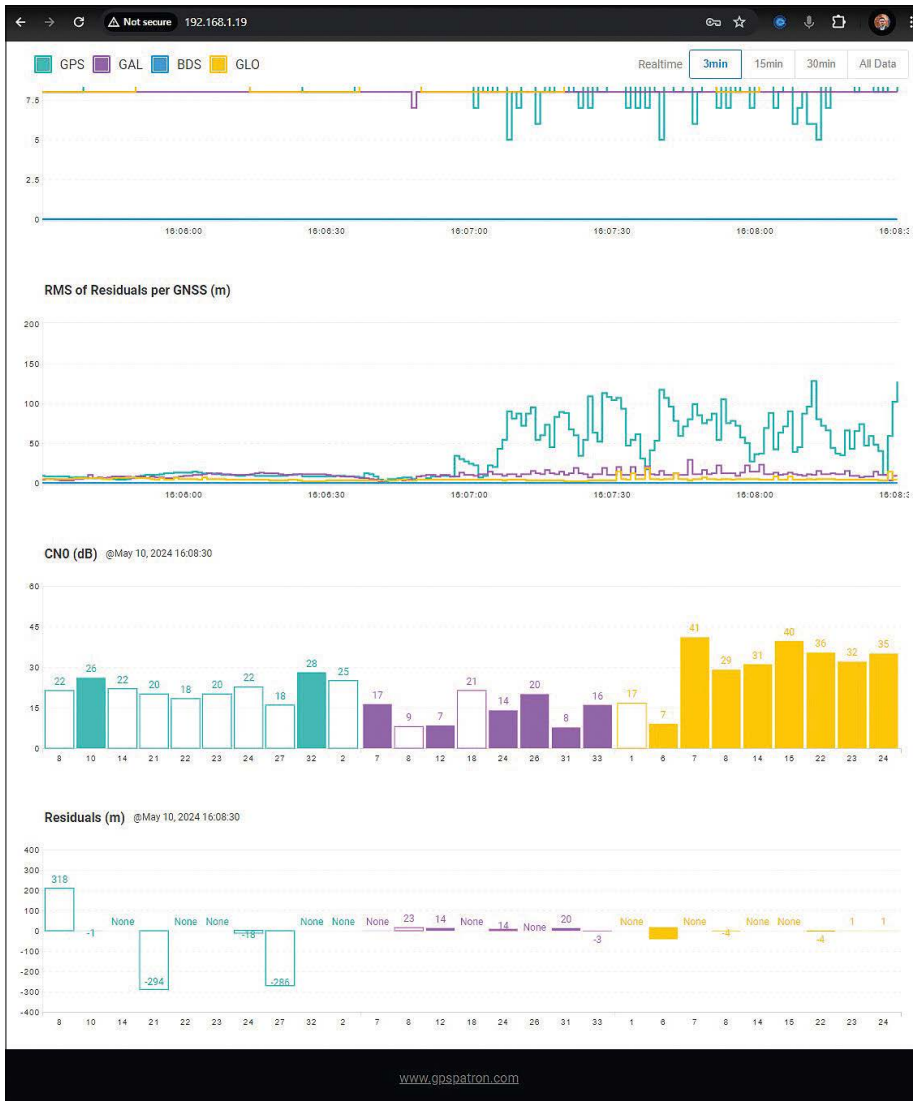
Die technische Entwicklung der GNSS-Empfänger kann mit den massiven Ausweitungen der Störfälle nicht mithalten. Der alljährlich in Norwegen stattfindende Jammertest hat auch 2025 wieder belegt, dass die überwiegende Mehrheit der Empfänger für gezielte Störungen anfällig ist – trotz technischer Verbesserungen. Folglich ist eine kontinuierliche Überwachung des GNSS-Signals für alle Systeme entscheidend, die von den satellitenbasierten Signalen abhängig sind.

Drohnen sollten beispielsweise nur dann starten, wenn die Signalqualität nachweislich stabil ist. Das betrifft sowohl Drohnenbetreiber im Werks- und Objektschutz als auch Veranstalter von den zunehmend beliebten Drohnenshows. Auch autonome Systeme sind ohne verlässliche GNSS-Daten nicht einsatzbereit. Bei Robotern im Werkschutz beispielsweise kann gezielt eingesetztes Spoofing eine Alarmierung hervorrufen und Sicherheitskräfte zu einem falschen Ort lotsen. Betreiber müssen deshalb wissen, ob der GNSS-Empfang ausreichend ist, oder ob Störungen auftreten können.

Kritische Infrastrukturen, wie beispielsweise mobile Kommunikationssysteme, sind auf einen exakten Empfang des Zeitsignals angewiesen. Ausfälle und Manipulationen müssen sofort erkennbar sein, um rechtzeitig gegenzusteuern und Kettenreaktionen zu stoppen.

Jamming und Spoofing sicher erkennen

Hensec entwickelt Lösungen, die GNSS-Störungen nicht nur detektieren, sondern auch



Welches GNSS wird gestört? Das Dashboard zeigt es

wertet und bei Bedarf ebenfalls über das Netzwerk an die GP-Cloud übertragen. Die Alarmierung erfolgt in Echtzeit sowohl lokal als auch über die WebApp.

Web-Applikation GP-Cloud

Hensec bietet diese Lösung auch als Software an. Die GP-Cloud ist eine Webanwendung, die Detektion, Klassifizierung und Ortung von GNSS-Störungen in Echtzeit ermöglicht. Erfasst sie Störungen, so kann die GP-Cloud Alarme oder Benachrichtigungen ausgeben. Außerdem besteht die Möglichkeit, die Ereignisse für nachträgliche Auswertungen zu speichern.

Grundlage für die Messungen liefern die GNSS-Spoofing Sensoren des Anbieters, die über einen API-Key direkt in die Systeme der Kunden eingebunden werden. Alternativ oder ergänzend ist auch die Verbindung vorhandener RTK-BS (via RTCM@NTRIP) oder anderer GNSS-Empfänger (via NMEA@NTRIP) z. B. von Septentrio möglich.

Die Webanwendung aggregiert alle Daten und bereitet sie in übersichtliche Dashboards auf. Es besteht die Möglichkeit, Benutzer mit individuellen Berechtigungen anzulegen, Alarme und Grenzwerte zu konfigurieren und die Sensoren zu verwalten. **GIT**

analysieren und orten können – ganz gleich, ob es sich um einfache Interferenzen, Jamming oder aufwendiges Spoofing handelt. Damit erhalten Betreiber ein umfassendes Gesamtbild der GNSS-Verfügbarkeit am Einsatzort.

Die Lösungen verfügen über einen integrierten RF-Signal Analyser, um die Funkfrequenzen (Radio Frequency, kurz RF) zu überprüfen. Darüber lassen sich Störquellen ermitteln, die das GNSS-Signal beeinträchtigen. Parallel wird analysiert, wie viele Satelliten verfügbar sind und ob die Signalstärke für einen sicheren Empfang ausreicht.

Die Lösungen können klassifizieren, ob eine registrierte Störung auf Interferenzen, Jamming oder Spoofing zurückzuführen ist. Auch eine Lokalisierung der Störquellen ist möglich. Die Hensec-Lösungen sind als Hardware- und als Softwarevariante erhältlich und lassen sich somit nahtlos an die Anforderungen der Kunden anpassen.

Hardware

Der Sensor GP-Probe DIN-L1 ist ein kompaktes Modul für die Hutschiene. Er analysiert

das L1-Band und enthält selbst einen eingebauten RF-Blocker und Jammer, um das GNSS-Signal der Antenne im Falle von erkanntem Spoofing zu unterbrechen. Dadurch werden nachgeschaltete Geräte wie Zeitserver zuverlässig vor Manipulation geschützt. Gleichzeitig wird ein digitaler oder analoger Alarm ausgegeben.

Ein breiteres Erkennungsspektrum weist der GP-Probe TGE2 Sensor auf: Er verfügt über drei Hochfrequenz-Kanäle zur erweiterten Echtzeitanalyse, um auch fortschrittliche Spoofing-Angriffe zuverlässig zu erkennen. Werden drei dieser Sensoren auf einem Gelände positioniert, können sie sofort die Störungsquelle lokalisieren.

Weitere Hardwarelösungen gibt es als ultraportablen Stick, als Outdoor-Koffer für wechselnde Einsatzorte oder als wetterfester Outdoor-Schrank, der für die Installation im Freien oder als Mastmontage geeignet ist. Auch individuelle Lösungen, die speziell an die Bedürfnisse der Kunden angepasst sind, sind möglich.

Die empfangenen HF-Parameter werden direkt auf dem Gerät verarbeitet, ausge-



Hensec Secure Solutions
www.Hensec.com

BSI empfiehlt Ende klassischer asymmetrischer Verschlüsselungsverfahren

In der jährlichen Aktualisierung seiner kryptographischen Empfehlungen (TR-02102) spricht sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) erstmals für ein Ablaufdatum klassischer asymmetrischer Verschlüsselungsverfahren aus. Ende 2031, für höchst sensitive Anwendungen bereits Ende 2030, sollten diese Verfahren aus Sicht des BSI nicht mehr alleine eingesetzt werden. Stattdessen sollten diese Verfahren in hybrider Form mit Post-Quanten-Kryptographie kombiniert werden. Für klassische Signaturverfahren ist eine Abkündigung der alleinigen Nutzung bis Ende 2035 geplant.

„Mit der Abkündigung der klassischen Verschlüsselungsverfahren setzen wir neue Maßstäbe. Der Umstieg auf Verfahren der Post-Quanten-Kryptographie ist alternativlos, die Technische Richtlinie gibt nun konkreten Handlungsbedarf vor“, so BSI-Präsidentin Claudia Plattner. www.bsi.bund.de

KI verstärkt Cyber Risiken

Genetec fordert Organisationen dazu auf, die Kontrolle über Authentifizierungs- und Zutrittsinformationen in vernetzten physischen Sicherheitssystemen zu verstärken. Hintergrund ist, dass KI das Ausmaß und die Komplexität von Cyberbedrohungen weiter erhöht. Passwortänderungen allein reichen nicht mehr aus, um physische Sicherheitsumgebungen zu schützen, warnt Genetec.

KI-gestützte Tools verstärken Angriffe auf Authentifizierungsdaten und Passwörter: Attacken erfolgen schneller, in größerem Ausmaß und mit mehr Präzision. In Unternehmen, die vernetzte Kameras, Zutrittskontrollsysteme, Server und Cloud-Dienste einsetzen, können schwache oder unzureichend verwaltete Zutrittsdaten und Passwörter sensible Betriebsabläufe gefährden und neue Angriffswege in die Unternehmensinfrastruktur eröffnen.

Dazu gehören auch die Passwörter, die für die direkte Verbindung mit den Geräten verwendet werden. Diese werden oft übersehen, können aber bei unsachgemäßer Verwaltung einen direkten Angriffspunkt bieten. In diesem Umfeld reicht es nicht mehr aus, sich auf regelmäßige Änderungen von Passwörtern oder einfache Cybersicherheitsmaßnahmen zu verlassen.

www.genetec.de

Gehacktes E-Mail-Konto: BSI und ProPK veröffentlichen Checkliste

Um Verbraucher im Ernstfall gezielt zu unterstützen, veröffentlichen das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Programm Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) eine gemeinsame Checkliste. Diese beschreibt Schritt für Schritt das Vorgehen im Ernstfall und gibt zugleich Tipps zur Prävention. Fast jede zehnte Person, die im Vorjahr von Cyberkriminalität betroffen war, erlebte laut Cybersicherheitsmonitor 2025 einen Fremdzugriff auf einen Online-Account (8 %). Insbesondere ein kompromittiertes E-Mail-Konto kann dabei gravierende Folgen haben. Die Checkliste ist kostenfrei auf den Webseiten von BSI und ProPK verfügbar. Sie ist ein Teil des umfangreichen Informationsangebots der beiden Kooperationspartner rund um die Themen IT-Sicherheit und Cyberkriminalität. www.bsi.bund.de

Prof. Dr. Adi Akavia übernimmt Athene-Professur

Die international anerkannte Expertin für angewandte Cybersicherheit, Prof. Dr. Adi Akavia, hat zum Jahresbeginn eine Athene-Professur am Fachbereich Informatik der TU Darmstadt und die Leitung einer Abteilung am Fraunhofer-Institut für Sichere Informationstechnologie SIT übernommen. Die Doppelfunktion verbindet akademische Spitzenforschung mit praktischer Anwendung in einem Schlüsselbereich der Cybersicherheit. Prof. Dr. Adi Akavia gehört zu den führenden Expertinnen in der angewandten Cybersicherheitsforschung. Sie verbindet zwei aktuell besonders wichtige Themenbereiche der Informatik, Cybersicherheit und Künstliche Intelligenz. Mit ihrer Forschung baut Adi Akavia Brücken zwischen den theoretischen Grundlagen der Kryptografie und dem praktischen Einsatz von KI. Anwendungen ihrer Forschung finden sich z. B. in der Medizin und der Bioinformatik. www.sit.fraunhofer.de



Prof. Dr. Adi Akavia, Athene, TU Darmstadt, Fraunhofer SIT

AWS European Sovereign Cloud startet: BSI unterstützt bei Ausgestaltung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterstützt den US-Cloud-Anbieter Amazon Web Services (AWS) bei der Ausgestaltung von Sicherheits- und Souveränitätsmerkmalen seiner gestarteten European Sovereign Cloud (ESC): einer eigenständigen Cloud-Infrastruktur, die sich vollständig innerhalb der EU befindet und deren Betrieb physisch wie auch logisch von der globalen AWS-Instanz unabhängig sein wird. Um mit digitalen Innovationen Schritt zu halten und gleichzeitig digitale Souveränität zu ermöglichen, verfolge das BSI eine Doppelstrategie. Der europäische Markt und die hiesige Digitalindustrie müssten gestärkt werden. Außer-europäische globale Produkte müssten so angepasst und eingebettet werden, dass eine sichere und selbstbestimmte Nutzung möglich wird. Voraussetzung dafür seien im Bereich Cloud-Computing innovative Angebote, die als europäische Instanzen sowohl technisch als auch organisatorisch unabhängig betrieben werden, so BSI-Präsidentin Claudia Plattner.

www.bsi.bund.de



Bequem auf dem Sofa durch die e-Ausgabe der GIT SICHHERHEIT blättern: Registrieren Sie sich auf www.git-sicherheit.de/newsletter

SAAS

Höchste Priorität: Sicherung der Identität

SaaS-Bedrohungslandschaft 2025: Verletzungen um 300 Prozent angestiegen

Obsidian, ein kalifornisches Unternehmen im Bereich Software as a Service (SaaS)-Sicherheit, hat einen Bedrohungsbericht zu SaaS-Sicherheit 2025 veröffentlicht. Die Ergebnisse zeigen einen beispiellosen Anstieg der SaaS-Verletzungen um 300 Prozent im Vergleich zum Vorjahr (von September 2023 bis 2024).

Die Zunahme der Cyberattacken hat nach dem „Threat Report“ Organisationen in allen Branchen betroffen, darunter große Technologie- und Telekommunikationsunternehmen. Obsidian Security hat ein großes Datenarchiv für SaaS-Sicherheitsverletzungen der Branche aufgebaut und war direkt am Incident Management von über 150 Sicherheitsvorfällen beteiligt.

Die Daten des Unternehmens zeigen, dass 99 Prozent der SaaS-Kompromittierungen ihren Ursprung im „Identity Provider (IdP)“ haben. IdP-Dienste speichern und verifizieren die Identität eines Benutzers und unterstützen so bei der Verwaltung von SaaS-Zugriffen. Doch wenn IdPs kompromittiert werden, können Angreifer quer durch das gesamte System eindringen und so sensible Daten gefährden.

Obwohl die Multi-Faktor-Authentifizierung (MFA) generell als unverzichtbar angesehen wird, zeigen die Daten des Anbieters, dass MFA in 84 Prozent der Fälle Angriffe nicht verhindern konnte. MFA allein sei nicht ausreichend, was den Bedarf an robusteren, mehrschichtigen Sicherheitslösungen zur Abwehr moderner Bedrohungen deutlich mache.

SaaS-Verletzungen geschehen in einem alarmierenden Tempo. Die Daten von Obsidian zeigen, dass die schnellste Zeit vom ersten Zugriff bis zur Datenexfiltration nur neun Minuten beträgt. Herkömmliche Sicherheitskontrollen können nicht schnell genug reagieren, was das Risiko eines Datenverlusts erhöht und Echtzeit-Überwachungs- und Reaktionsstrategien erforderlich macht.

Sicherung der Identität

„Die Daten sprechen eine eindeutige Sprache und sind unmissverständlich; die Sicherung der Identität und ihrer fortlaufenden Wechselwirkungen mit Diensten und Anwendungen sollte für jedes Sicherheitsteam oberste Priorität haben“, sagte Glenn Chisholm, CPO von Obsidian Security. Der Datensatz des Unternehmens „aus realen, Echtzeit-Telemetriedaten zu SaaS-Kompromittierungen, kombiniert mit unserem ‚Knowledge Graph‘ von Identitäten aus Hunderten von großen Unternehmen“ habe es ihm ermöglicht, Künstliche Intelligenz-Modelle zu entwickeln, die enorm effizient agieren. „Diese KI- und Language Learning Modelle lernen kontinuierlich und passen sich an, um Angreifer zu erkennen, bevor

sie die Umgebung eines Unternehmens über SaaS kompromittieren.“

Aufkommende Bedrohungen und Prognosen

Der Bericht hebt außerdem wichtige aufkommende Risiken in SaaS-Umgebungen hervor. SaaS-Integrationen böten eine anfällige Angriffsfläche: Die Verbreitung von Drittanbieteranwendungen habe neue Angriffsvektoren geschaffen, wobei sich der Missbrauch von Microsoft-Integrationen zunehmend verbreitet. Des Weiteren gebe es Risiken bei der Anwendung Künstlicher Intelligenz. Organisationen setzten typischerweise etwa 100 KI-Anwendungen ein, von denen 60 Prozent keine angemessenen Sicherheitskontrollen oder Föderation hinter dem IdP aufwiesen. Außerdem konstatiert das Unternehmen eine Ausweitung von Shadow-SaaS: Unbefugte Anwendungen verbinden sich weiterhin mit den zentralen Systemen, was die Sicherheitsrisiken erheblich erhöht. **GIT**



Obsidian Security
www.obsidiansecurity.com

SicherheitsExpo 2026: Salto zeigt vernetzte Zutrittslösungen

Salto Systems zeigt auf der SicherheitsExpo intelligente Zutritts- und Identity-Managementlösungen eingebettet in ein ganzheitliches Portfolio, das Sicherheit, Effizienz und Benutzerkomfort optimal vereint. Am Messestand können Besucher die Salto Plattformen Space, KS und Homelok live erleben. Die On-Premise-, Cloud- und Hybridlösungen für die Zutrittskontrolle decken unterschiedlichste Anforderungen ab – vom einzelnen Gebäude bis hin zu komplexen, verteilten Liegenschaften. Allen Plattformen gemeinsam ist der hohe Sicherheitsstandard bei gleichzeitig großer Flexibilität im Betrieb.

Die Cloud-Hybrid-Lösung Salto Homelok adressiert speziell die steigenden Anforderungen der Wohnungswirtschaft. Sie ermöglicht eine vollständig schlüssellose Verwaltung von Wohn- und Gemeinschaftsbereichen und erschließt damit neue Effizienzpotenziale für Betreiber, Verwalter und Dienstleister.

Ergänzt werden die Zutrittslösungen durch das intelligente Identity Management von Salto IDM. Die Plattform automatisiert system- und anlagenübergreifend den gesamten Lebenszyklus von Identitäten – von der rollenbasierten Vergabe von Zutrittsrechten über die Registrierung von Besuchern, die Zuweisung von Zutrittsmedien und die Raumreservierung bis hin zu identitätsbasierten Zutrittsanfragen oder deren gezielter Löschung.

Das verschlankt Prozesse, vermeidet Fehlerquellen und reduziert den Betriebsaufwand. Die Lösung ist insbesondere für Kritische Infrastrukturen interessant, um gesetzlichen Vorgaben wie dem KRITIS-Dachgesetz oder den NIS-2- und DORA-Richtlinien zu entsprechen.

Mit XS4 Com zeigt der Hersteller zudem seine moderne, cloudbasierte Video-Intercom-Lösung. Besucher

nehmen per Smartphone und NFC oder QR-Code Kontakt mit dem Gastgeber auf, während dieser die Tür bequem aus der Ferne öffnen kann. Ein weiteres Highlight in München ist XS4 Face, die biometrische Zutrittslösung des Unternehmens. Sie nutzt das Gesicht als eindeutiges Identifikationsmerkmal und ermöglicht damit einen besonders schnellen und komfortablen Zutritt – ganz ohne Karten, Schlüssel oder mobile Geräte.

Abgerundet wird der Messeauftritt durch Lösungen von Gantner. Präsentiert werden unter anderem smarte Lockersysteme, bargeldlose Zahlungs- und Kassensysteme sowie intelligente Paketfachlösungen. Ganz neu ist die Gantner LX Suite, eine workflowbasierte Smart-Locker-Plattform, die Paket-, Dokument- und Warenübergaben in modernen Gebäuden grundlegend vereinfacht.

Sicherheitsexpo München: Halle 1, Stand C04

www.saltosystems.de

Höchster Schutz bei Vandalismus

Das ift Rosenheim hat 2025 eine neue Richtlinie zum Schutz vor Vandalismus veröffentlicht. Als Spezialist für Hochsicherheitslösungen brachte Sälzer sein umfassendes Know-how in die Entwicklung des Regelwerks ein. Gleichzeitig wurden die eigenen Fenster-, Tür- und Fassadensysteme gezielt an die neuen Anforderungen angepasst. Mit der Überarbeitung seines Produktportfolios reagiert Sälzer auf die wachsende Bedeutung eines wirksamen Schutzes vor Vandalismus an Gebäuden. Das Unternehmen setzt dabei auf einen praxisorientierten Ansatz, der hohe Sicherheitsniveaus mit wirtschaftlichen Lösungen und architektonischer Gestaltungsfreiheit verbindet. Dadurch lassen sich Fenster-, Tür- und Fassadensysteme für unterschiedliche Nutzungen gezielt in der jeweils erforderlichen Widerstandsklasse planen und ausführen.



www.saelzer-security.com

KRIFA

Fachkongress + Ausstellung
Sicherheit und Krisenvorsorge

15.+16. Juli 2026
MCC Halle Münsterland

Die KRIFA ist das neue Event

für Prävention, Krisen, Bevölkerungsschutz, Feuerwehr, Polizei, Rettungsdienst, Hilfsorganisationen, Gesundheitswesen sowie die zuständigen zivilen Gefahrenabwehr- und Sicherheitsbehörden im Münsterland.

Fachlicher Träger

BSKI 
 Bundesverband für den Schutz
 Kritischer Infrastrukturen e.V.

Veranstalter

AFAG
 WIR MACHEN MESSEN

www.krifa.de

SICHERHEITS EXPO Alpe Adria

**Die neue Sicherheitstechnik-
Fachmesse in Österreich**

*The new security technology
trade fair in Austria*

Messe Klagenfurt

14. + 15. Okt 2026

14 + 15 Oct 2026

Save the Date!



www.sicherheitsexpo.at

Diesen Monat auf GIT-SICHERHEIT.de

IMPRESSUM

NEWS AKTUELLE INHALTE PRODUKTE MAGAZIN BUSINESS PARTNER EVENTS DE EN

GIT SICHERHEIT

MANAGEMENT SECURITY BRANDSCHUTZ IT-SECURITY SAFETY

35 Jahre GIT SICHERHEIT
Jetzt die Landing-Page zum Jubiläum lesen

VIP-Interview
Die VIPs in Sachen Sicherheit

Neue Ausgabe jetzt online!
GIT SICHERHEIT zum Download

Brandschutz im Feuerwehrhaus: Warum kritische Infrastruktur besseren Eigenschutz braucht
Warum Feuerwehrgerätehäuser als kritische Infrastruktur besondere Brand- und Sicherheitskonzepte benötigen

SECURITY
Manuel Neuer ist Markenbotschafter von Telenor

ANZEIGE • IT-SECURITY
NIS2 & OT Security – was jetzt zu tun ist: Live Webinar am 19. Mai, 11 Uhr

ANZEIGE
Lakeside Security Summit 2026
Hier anmelden! Baden-Württemberg

NEWS

PSA-Innovationen auf der Interschutz

André F. Kunt vom ASW BW über GIT SICHERHEIT: Sicherheit wirksam verbessern

BDSW: Sicherheitswirtschaft fordert entschlossene Reformen

DRZ auf der Interschutz 2026

Hekatron Unternehmen im Aufwärtstrend

THEMEN

TOPSTORY • MANAGEMENT
TechDay 2026: Live Demos zeigen KI Videoanalyse und Sensorik für KRITIS Sicherheit im Praxistest
TechDay 2026: Live-Demos zur KRITIS-Sicherheit – KI-Videoanalyse, Sensorik & neue Gesetze im Praxistest

TOPSTORY • MANAGEMENT
Zukunft des Brandschutzes: Trendbericht von Honeywell-Manager Klaus Hirzel
Brandschutz im Wandel: Ein Trendbericht von Klaus Hirzel, Business Leader Europe Central Region (DACH) bei Honeywell Fire Products

TOPSTORY • SAFETY
Generationenwechsel bei Elten: Hendrik van Elten über Wachstum, Marke und neue Anforderungen an Sicherheitschuhe
Elten im Wandel: Hendrik van Elten über internationales Wachstum und moderne Sicherheitschuhe

TOPSTORY • MANAGEMENT
Peter H. Bachus, Vizepräsident & Vorstand der VSW: Warum Wirtschaftsschutz zur Schlüsselfrage wird
Warum Wirtschaftsschutz zur Schlüsselfrage geworden ist, ein Trendbericht von Peter H. Bachus, Vizepräsident & Vorstand der Vereinigung für die Sicherheit in der Wirtschaft e.V.

ANZEIGE
DOSSIER WHITEPAPER

LANDING-PAGE

35 Jahre GIT SICHERHEIT
Trendberichte, Interviews & Specials
JUBILÄUM
35 Jahre GIT SICHERHEIT
Trendberichte, Interviews und Specials

Sicherheit für JVA und Forensiken
GIT SICHERHEIT beleuchtet organisatorische, bauliche und speziell sicherheitstechnische Konzepte - und gibt praktische Handlungsempfehlungen. In Zusammenarbeit mit dem Verband für Sicherheitstechnik VFS.

GIT SICHERHEIT AWARD 2026
Die aktuellen Sieger aller Kategorien.

PRODUKTE

GU BKS Service GmbH
erhält ISO 27001: zertifizierungsempfehlung

Ballastierte Geländersysteme von Hymer-Steigtechnik

Secunet und Innosystec bündeln ihre Kompetenzen

Converged Credentials von HDI Global GmbH

Hanwha: Appliances für das Blaze Hybrid KI Videomanagementsystem

BELIEBTE INHALTE

SicherMacher
Der GIT-Talk mit den Marktführern

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.-Betw. Steffen Ebert
+49 6201 606 709

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

Dr. Timo Gimbel
+49 6201 606 049

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@vservice.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 33
IBAN: DE5501108006161517443

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 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



WILEY

GIT SICHERHEIT

HEFT IM HEFT – BRANDSCHUTZ



Cemo ▶

Kilowattstunden statt Minuten

Paradigmenwechsel beim Schutz für Ladeschränke

INNENTITEL

Wenn Energie zum Risiko wird

Warum die kWh das zentrale Schutzziel bei Lager- und Ladeschränken für Lithium-Ionen-Batterien ist



Niedrigeres Brandrisiko dank Kennzeichnung der maximalen Energiekapazität



Die Sicherheitsbetrachtung von Gefahrstoffschränken ist historisch stark durch die klassische Gefahrstofflagerung geprägt. Entsprechend steht insbesondere die Feuerwiderstandsfähigkeit gegenüber einem externen Brand im Fokus. Beispielsweise definiert durch die DIN EN 14470-1. Bewertet wird dabei in der Regel, wie lange ein Schrank einem Brand von außen standhält, um den Inhalt zu schützen und eine Brandausbreitung zu verhindern. Bei Lager- und Ladeschränken für Lithium-Ionen-Batterien greift diese Betrachtungsweise jedoch nur eingeschränkt. Die Besonderheit besteht darin, dass hier nicht nur Gefahrstoffe gelagert werden, sondern gleichzeitig Energie gespeichert wird. Dadurch entsteht ein eigenständiges, qualitativ anderes Gefahrenpotenzial, das primär aus dem Schrankinneren heraus wirkt.

Das zentrale Risikoszenario bei Lithium-Ionen-Batterien ist der bekannte Thermal Runaway. Mechanische Beschädigungen, elektrische Fehler, Überladung oder interne Zellfehler können zu einer unkontrollierten exothermen Reaktion führen. Diese ist gekennzeichnet durch sehr hohe Temperaturanstiege, die Freisetzung brennbarer und toxischer Gase sowie explosionsartige Druckentlastungen.

Dass es sich hierbei nicht um ein theoretisches Szenario handelt, zeigen unter anderem Statistiken und Untersuchungen, wie etwa die Studie des IFS (Ausgabe 03/2024). Mit der weiter zunehmenden Verbreitung von Lithium-Ionen-Batterien in Industrie, Handwerk und Logistik steigt zwangsläufig auch die absolute Anzahl potenzieller Schadensereignisse. Vor diesem Hintergrund stellt sich die grundlegende Frage: Welche Schutzziele sind für einen Lager- und Ladeschrank für Lithium-Ionen-Batterien tatsächlich relevant?

Fokus auf den Batteriebrand

Der aktuelle Stand der Technik wird maßgeblich durch das VDMA-Einheitsblatt 24994 definiert. Dieses setzt einen klaren Schwerpunkt: Das primäre Schutzziel ist

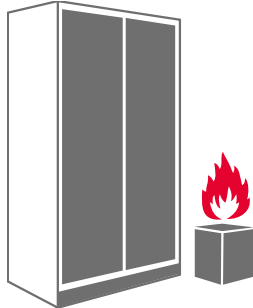
Brandschutz für Lithium-Ionen-Akkuschränke

Warum die Feuerwiderstandsfähigkeit von außen nicht die relevante Anforderung ist



DIN 14470-1 – Sicherheitsschrank Brandschutz für brennbare Flüssigkeiten

Feuer kommt von außen
(Raumfeuer)



PRÜFKRITERIUM 90 Minuten

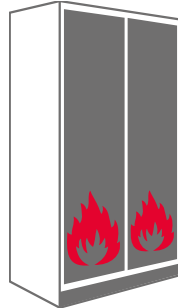
zeitbasierte Widerstandsprüfung

Schützt Inhalt vor externem Brand – ein interner Batteriebrand wird dabei nicht berücksichtigt



Lager- und Ladeschrank Brandschutz für Li-Io-Batterien

Feuer entsteht von innen
(Thermal Runaway)



PRÜFKRITERIUM max. kWh

gelagerte Energiemenge vollständig ausgebrannt

Prüft den kompletten Abbrand der gelagerten Energie – keine Zeitbegrenzung, der Schrank muss den Batteriebrand vollständig überstehen

Fazit

Batteriebrandversuche gehen nicht über eine definierte Zeit, sondern prüfen den vollständigen Abbrand der eingelagerten Energie. Deshalb ist nicht eine Widerstandszeit in Minuten, sondern die maximal zulässige Energiemenge in kWh die entscheidende Kenngröße für Lithium-Ionen Lager- und Ladeschränke.

der Schutz gegenüber einem Batteriebrand aus dem Inneren des Schrankes.

Im Gegensatz zu klassischen Feuerwiderstandskonzepten erfolgt die Bewertung dabei nicht zeitbasiert (z. B. 90 Minuten), sondern energetisch. Maßgeblich ist die maximal zulässige Lagermenge an elektrischer Energie, angegeben in Wattstunden (Wh).

Der Schrank muss einem Batteriebrand dieser definierten Energiemenge vollständig standhalten. Konkret bedeutet dies, dass:

- keine Flammen oder Funken aus dem Schrank austreten dürfen,
- keine unkontrollierte Brandausbreitung in die Umgebung erfolgt und
- die Schutzfunktion über die gesamte Dauer des Ereignisses erhalten bleibt.

Besonderheit realer Batteriebrandprüfungen

Ein entscheidender Unterschied zu klassischen Feuerwiderstandsprüfungen besteht darin, dass beim Batteriebrand reale physikalische und thermodynamische Effekte berücksichtigt werden. Dazu zählen insbesondere:

- sehr schnelle und hohe Temperaturanstiege
- punktuelle Extrembelastungen durch Zellreaktionen

- explosionsartige Druck- und Gasfreisetzen

Diese Effekte sind nicht vergleichbar mit normierten Temperatur-Zeit-Kurven, wie sie beispielsweise bei der Prüfung nach DIN EN 14470 zugrunde gelegt werden. Entsprechend greift hier ein eigenständiges Sicherheitskonzept, das gezielt auf das spezifische Risiko von Lithium-Ionen-Batterien ausgelegt ist.

Feuerwiderstandsfähigkeit von außen – optionales Schutzziel

Die Feuerwiderstandsfähigkeit gegenüber einem Brand von außen kann bei Lager- und Ladeschränken für Lithium-Ionen-Batterien weiterhin ein zusätzliches Schutzziel darstellen. Nach dem aktuellen Stand der Technik wird sie jedoch nicht als zwingend erforderlich angesehen und daher im VDMA-Einheitsblatt 24994 als optionales Prüfkriterium geführt.

Das dominierende Gefahrenpotenzial entsteht beim Lithium-Ionen-Batterieschrank primär im Schrankinneren, ausgelöst durch einen möglichen Thermal Runaway. Eine externe Feuerwiderstandsfähigkeit trägt zwar dazu bei, den Schrank gegenüber externen Brandlasten abzusichern und weitere Brandschutzanforderungen zu erfüllen, sie

hat jedoch keinen entscheidenden Einfluss auf die Erreichung der zentralen Schutzziele im Hinblick auf den Batteriebrand.

Konsequenzen für Anwender und Planung

Für den Anwender ergibt sich daraus eine klare Priorisierung der Schutzziele:

- Batteriebrandwiderstandsfähigkeit
- Zentrales Kriterium ist die definierte maximale Lagermenge an elektrischer Energie (kWh), für die der Schrank geprüft und ausgelegt ist.
- Erweiterte Brandschutzziele (optional)
- Sofern zusätzliche Anforderungen an den baulichen oder organisatorischen Brandschutz bestehen, kann der Schrank um eine geprüfte Feuerwiderstandsfähigkeit von außen ergänzt werden.

Diese Struktur ermöglicht eine sachgerechte, risikobasierte Auswahl von Lager- und Ladeschränken für Lithium-Ionen-Batterien und trägt dazu bei, Sicherheitsmaßnahmen gezielt dort einzusetzen, wo das tatsächliche Gefahrenpotenzial entsteht.

Modulares System von Cemo zum Lagern und Laden von Lithium-Ionen-Batterien

Mit den Lager- und Ladeschränken lockEX 2.0 stellt Cemo ein modulares System bereit, das konsequent auf ein energiemengenbasiertes Sicherheitskonzept ausgelegt ist. Je 500 mm Lagerhöhe ist eine Lagerkapazität von 3 kWh definiert. Die modulare Bauweise ermöglicht eine Skalierung der zulässigen Gesamtenergiemenge und macht das zentrale Schutzziel klar quantifizierbar. **GIT**



Autor: Simon Manz,
Produktmanager
Gefahrstofflagerung
Cemo GmbH

In unserem Ratgeber zum
Thema Akkusicherheit
klären wir weiter auf.
www.akkusicherheit.de



Cemo GmbH
www.cemo.de



TITELSTORY

Wenn genehmigt **nicht** gleich **sicher** heißt

Gefahrstoffmanagement zwischen Mindestanforderung und Vision Zero

Wie viel Sicherheit im Gefahrstoffmanagement ist notwendig – und wie viel ist sinnvoll? Anlässlich des 40-jährigen Bestehens von Denios diskutieren Markus Boberg (Denios), Maik Reimann (RNX) und Tobias Dankert (ARU) im Interview das Leitbild der Vision Zero.

Sie beleuchten den Unterschied zwischen gesetzlichen Mindestanforderungen und ganzheitlicher Risikobetrachtung, ordnen die Rolle von Versicherern und Wasserrecht ein und zeigen, warum präventives Sicherheitsmanagement auch wirtschaftliche Vorteile bietet.

■ GIT SICHERHEIT: Herr Boberg, Denios feiert dieses Jahr sein 40-jähriges Bestehen. Was verbindet Denios mit dieser langen Erfahrung und wie spiegelt sich das im Umgang mit heutigen Sicherheitsanforderungen wider?

M. Boberg: In 40 Jahren haben wir uns vom Hersteller und Produktanbieter zur Sicherheitsinstanz für Gefahrstofflagerung und -handling gewandelt. Auf dem Weg haben wir Erfahrungen gesammelt, Wissen aufbereitet und neue Technikstandards für die Branche geschaffen. Doch darauf ruhen wir uns nicht aus. Wir verfolgen stets die Haltung, es geht noch sicherer. Das spiegelt sich in unserem Leitbild der Vision Zero

wider: eine Welt ohne Schäden durch Gefahrstoffe.

Dabei wissen wir, dass Unternehmen wirtschaftliche und sicherheitsrelevante Entscheidungen stets abwägen müssen. Während sich Präventionskosten klar beziffern lassen, hängt das Sicherheitskonzept jedoch von der individuellen Gefährdungssituation ab. Deshalb entwickeln wir gemeinsam mit unseren Kunden ganzheitliche Konzepte, die wirtschaftliche Rahmenbedingungen, individuelle Schutzziele und gesetzliche Anforderungen optimal in Einklang bringen.

Herr Reimann, findet die Idee der Vision Zero auch bei den Versicherern Anklang?

M. Reimann: Absolut. Entscheidend ist aus meiner Sicht die unterschiedliche Perspektive von Gesetzgeber und Versicherer. Gesetzliche Anforderungen setzen wichtige Mindeststandards zum Schutz von Mensch und Umwelt. In der Praxis führt das jedoch häufig zu der Annahme, dass eine genehmigte Anlage automatisch auch umfassend sicher sei. Genau hier liegt der Unterschied: Auch wenn gesetzliche Anforderungen erfüllt sind, können weiterhin erhebliche Risiken bestehen – etwa durch Sachschäden, Betriebsunterbrechungen und wirtschaftliche Folgekosten. Deshalb bedeutet „genehmigt“ aus Sicht des Versicherers nicht automatisch auch „versicherbar“.



Markus Boberg, Denios



Tobias Dankert, ARU



Maik Reimann, RNX

Das Leitbild der Vision Zero ist in diesem Zusammenhang hilfreich, weil es den Blick über die reine Erfüllung von Mindestanforderungen hinaus erweitert. Wenn neben den Schutzziele auch mögliche Schadensfolgen berücksichtigt werden, lassen sich Risiken ganzheitlicher bewerten. Das verbessert die Risikotransparenz und kann sich positiv auf Versicherbarkeit und Rahmenbedingungen auswirken.

Herr Dankert, wie bewerten Sie das Konzept Vision Zero aus Sicht des Wasserrechts und des regulatorischen Rahmens?

T. Dankert: Aus meiner Sicht passt das Leitbild der Vision Zero gut zum präventiven Ansatz des Wasserrechts, das auf die Vermeidung nachteiliger Gewässeränderungen ausgerichtet ist. Ein zentrales Instrument ist die Eignungsfeststellungspflicht nach der Verordnung über Anlagen zum Umgang mit wassergefährdenden Stoffen (AwSV). Sie verlangt den Nachweis, dass Anlagen so geplant, errichtet und betrieben werden, dass keine schädlichen Gewässeränderungen zu erwarten sind.

Damit setzt das Wasserrecht nicht auf Schadensbegrenzung im Nachhinein, sondern auf eine präventive Risikobewertung und -beherrschung. Vision Zero verfolgt einen ähnlichen Gedanken, geht jedoch als Leitbild über den Rechtsrahmen hinaus, da es grundsätzlich auf die Vermeidung jeglicher Schadensereignisse abzielt.

Unternehmen, die dieses präventive Sicherheitsverständnis verinnerlichen, erfüllen die Anforderungen der Eignungsfeststellung in der Regel strukturierter und erleichtern dadurch behördliche Verfahren sowie die Nachweisführung im Genehmigungsprozess.

Welche Rolle spielen organisatorische und personelle Maßnahmen ergänzend zu den technischen Auflagen?

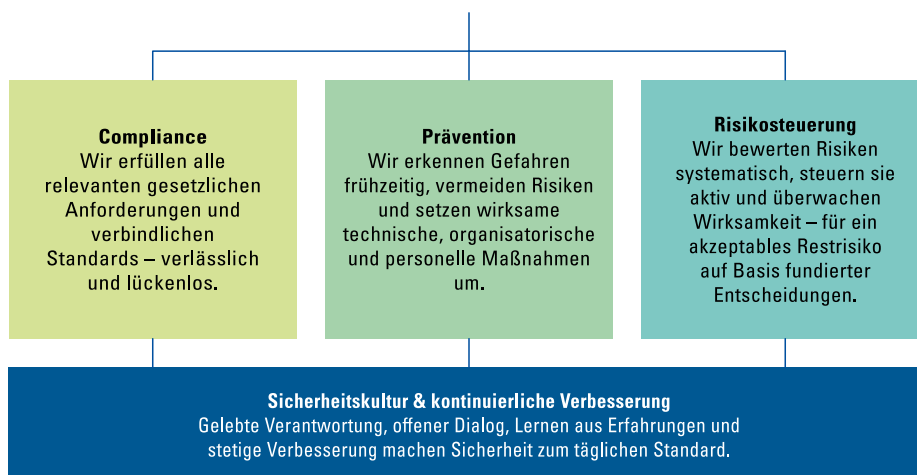
Bitte umblättern ►



Mit dem Spillguard von Denios wird die gesetzlich vorgeschriebene Auffangwanne auf ein höheres Sicherheitslevel gebracht

VISION ZERO

Unser Ziel: eine Welt ohne Schäden an Mensch und Umwelt.



M. Boberg: Schadensvermeidung funktioniert nur dann zuverlässig, wenn technische Schutzmaßnahmen konsequent durch organisatorische und personelle Maßnahmen ergänzt werden. Entscheidend sind klare Abläufe, eindeutig definierte Verantwortlichkeiten sowie regelmäßig Unterweisungen der Beschäftigten als auch widerkehrende Wartungen der Anlagen. Daher ist unser Produktportfolio in ein ganzheitliches Leistungsangebot aus Beratung, Produkten, Services und Schulungen eingebettet, das über den gesamten Produktlebenszyklus reicht. Dabei greifen wir nicht nur auf interne Kompetenz zurück, sondern nutzen ein belastbares Netzwerk aus Branchen- und Sicherheitsexperten zur stetigen Weiterentwicklung von Wissen und Leistungen. Wir arbeiten zum Beispiel eng mit Sachverständigen wie ARU zusammen, um Kunden auch im Genehmigungsmanagement, bei AwSV-Gutachten sowie beim Bauantrag für Gefahrstoffcontainer Unterstützung bieten zu können.

Herr Reimann, wie kann der wirtschaftliche Nutzen eines höheren Sicherheitsniveaus belegt werden?

M. Reimann: Sicherheit ist am Ende keine Frage von Kosten, sondern von Stabilität. Natürlich zeigen Studien, dass sich Prävention wirtschaftlich lohnen kann – entscheidend ist aber etwas anderes: Wie gut ist ein Unternehmen auf den Ernstfall vorbereitet? Gerade bei größeren Schäden sehen wir immer wieder, dass nicht der Schaden selbst das größte Problem ist, sondern die Folgen – insbesondere Betriebsunterbrechungen. Unternehmen, die hier gut aufgestellt sind, haben einen klaren Vorteil: Sie

bleiben handlungsfähig – und genau das entscheidet im Ernstfall über die Zukunft des Unternehmens.

Herr Boberg, wie lebt Denios die Vision Zero heute? Können Sie ein ganz konkretes Beispiel nennen?

M. Boberg: Ein gutes Beispiel ist der Umgang und die Detektion von Leckagen. Auffangwannen, die auslaufende Stoffe am Lagerort zurückhalten, bilden seit 40 Jahren den Kern unseres Sortiments und sind eine gesetzlich geforderte Schutzmaßnahme.

Darüber hinaus hat Denios mit dem Spillguard einen batteriebetriebenen Leckagesensor entwickelt, der ortsunabhängig einsetzbar ist und bei einer Leckage sofort ein Alarmsignal auslöst. Für ein höheres Sicherheitsniveau kann der Sensor in die Denios Connect Cloud eingebunden werden. In diesem Fall kann das Signal per SMS oder E-Mail direkt an zuständige Mitarbeiter geschickt werden, sodass unmittelbar Gegenmaßnahmen eingeleitet werden können. Die Einbindung in das kundenseitige Prozessleitsystem ist unter bestimmten Voraussetzungen ebenfalls möglich.

Ihr wichtigster Ratschlag zum Thema Sicherheit im Gefahrstoffmanagement in jeweils einem kurzen Statement?

M. Boberg: Wer Sicherheit im Gefahrstoffmanagement konsequent weiterentwickeln will, sollte nicht bei einzelnen Produkten ansetzen, sondern bei einem durchdachten Gesamtkonzept. Entscheidend ist eine fundierte Expertenberatung, die wirtschaftliche Rahmenbedingungen, individuelle Schutz-

ziele und gesetzliche Anforderungen in Einklang bringt. Denios gestaltet diesen Prozess mit praxisnaher Beratung, einem starken Netzwerk, passenden Produktlösungen und dem Ziel, Sicherheit systematisch und nachhaltig zu verbessern.

T. Dankert: Als AwSV-Sachverständiger beurteile ich Anlagen, deren Versagen weitreichende Folgen für Mensch und Umwelt haben kann – und das bevor etwas passiert. In diesem Sinne teile ich die Vision von Denios im Umgang mit Gefahrstoffen: Jeder vermiedene Schaden ist kein Zufall, sondern das Ergebnis konsequenter Vorsorge.

M. Reimann: Am Ende ist es ganz einfach: Der beste Schaden ist der, der gar nicht erst entsteht. Und genau darin liegt der größte wirtschaftliche Vorteil für Unternehmen. Unternehmen, die Sicherheit nur als Pflicht sehen, unterschätzen ihr eigenes Risiko. Die wirklich erfolgreichen Unternehmen nutzen Sicherheit als Wettbewerbsvorteil.

Vielen Dank für die eindrücklichen Impulse! GIT



Denios SE
www.denios.de

N2 ORS erhält VdS Systemanerkennung

Die aktive Brandvermeidung durch Sauerstoffreduktion erreicht einen neuen Meilenstein: Das System N2 ORS von Isolcell, das in Deutschland und der Schweiz exklusiv von der Wichmann ATB GmbH & Co. KG vertrieben wird, ist nun offiziell als Systemlösung vom VdS anerkannt. Damit wird eine Technologie ein weiteres Mal bestätigt, die einen grundlegenden Paradigmenwechsel im Brandschutz verkörpert: Brände gar nicht erst entstehen lassen, statt sie zu bekämpfen. N2 ORS setzt nicht auf reaktive Brandbekämpfung, sondern auf Prävention. Durch die gezielte Reduktion des Sauerstoffgehalts in der Umgebungsluft wird die Entstehung eines Brandes bereits im Ansatz verhindert. Das reduziert nicht nur das Risiko eines Brandes selbst, sondern verhindert auch Folgeschäden durch Löschmittel und Betriebsunterbrechungen. Technologisch basiert das System auf einer modularen Architektur mit flexibel kombinierbaren Stickstoffgeneratoren.

www.wichmann.biz



Mobiler Brandschutz mit Rollcontainer-Löschanlagen

250 kg Löschpulver für die Brandklassen ABC, BC oder D sowie 120 kg CO₂ für Löscheinsätze in sensiblen Bereichen: Mit einem neuen Serienmodell macht Minimax Mobile Services ihre Löschanlagen auf Rollcontainern einer breiten Nutzerschicht einfach zugänglich. Brennt es in Produktions- oder Lagerbereichen, muss viel Löschpower schnell an der richtigen Stelle sein. Die mobilen Rollcontainer-Löschanlagen von Minimax Mobile Services sind eine ideale Lösung. Die Löschanlagen sind nicht länger nur als individuelle Sonderanfertigung erhältlich, sondern können als standardisiertes Produkt direkt bestellt werden. Die Spezifikationen beruhen auf bewährten Konstruktionen und sind abgestimmt auf die Bedürfnisse typischer Anwender. Das einheitliche Palettenmaß von 1200 mm x 800 mm macht die Anlagen nicht nur kompakt, sondern auch flexibel einsetzbar und transportabel auf Fahrzeugen mit Ladebordwand oder in Abrollbehältern.

www.minimax-mobile.com



FeuerTrutz: Assa Abloy zeigt intelligente Türlösungen für Brandschutz

Wie sich Anforderungen des vorbeugenden Brandschutzes sowie komfortablen Zutritt intelligent miteinander verbinden lassen, zeigt die Assa Abloy Sicherheitstechnik GmbH auf der FeuerTrutz 2026 in Nürnberg. Auf seinem Messestand präsentiert das Unternehmen ein breites Spektrum moderner Türlösungen – von mechanischen und elektromechanischen Verriegelungen über Türschließer bis hin zu vernetzten Zutrittskontrollsystemen. Im Mittelpunkt des Messeauftritts stehen Lösungen, die Sicherheit, Brandschutz, Barrierefreiheit und Bedienkomfort zusammendenken. Dazu gehören die Schlosslinie „Solution Locks“ mit Kippfallentechnologie, Freilauf-Türschließer für Feuer- und Rauchschutztüren, leistungsstarke Komponenten für Flucht- und Rettungswege sowie elektronische Schließ- und Zutrittskontrollsysteme wie Cliq und Aperio.

FeuerTrutz: Halle 4 A, Stand 419

www.assaabloy.com/de

SECURITON

Die Zukunft
beginnt jetzt.

Wenn Sicherheitstechnik
vom Brandschutzpionier
weiter gedacht wird.

**EXKLUSIVE
PRODUKTPREMIERE**

auf der **FeuerTrutz 2026**

24./25.06.26 Stand 4-216

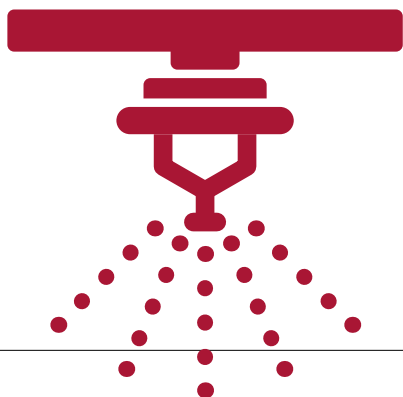
SPRINKLER

Der intelligente Sprinkler

Neues Systemkonzept ermöglicht gezielte, proaktive Brandbekämpfung statt rein thermischer Auslösung



© Fire Protection Solutions Group/Vinci



Sprinkleranlagen folgen seit über einem Jahrhundert demselben Prinzip: Sie reagieren erst, wenn Hitze entsteht. Johannes Falk von Fire Protection Solutions erklärt im Interview, wie das SmartFit-System diesen Ansatz verändert. Durch die Vernetzung von Brandmeldern, Steuerung und speziell ansteuerbaren Sprinklern wird Brandbekämpfung planbar und gezielt steuerbar. Das eröffnet neue Möglichkeiten für Nachrüstung, Anlagenplanung und ein aktives Brandmanagement – mit dem Ziel, Brände früher zu kontrollieren und Schäden zu begrenzen.

— GIT SICHERHEIT: Herr Johannes Falk, was genau macht den SmartFit Sprinkler so besonders im Vergleich zu einem klassischen Sprinklersystem?

Johannes Falk: Bei Sprinklern hat sich in den letzten 150 Jahren praktisch nichts verändert – das Auslöseprinzip blieb immer gleich. Mit dem SmartFit Sprinkler revolutionieren wir das System. Klassische Sprinkler werden thermisch ausgelöst, das heißt, sie reagieren erst, wenn sie sich stark erhitzen. Unser System dagegen kann proaktiv auslösen – der Sprinkler muss sich also nicht mehr erst durch das Feuer erhitzen, bevor er aktiv wird.

Wie erklären Sie einem Laien, warum der Sprinkler selbst gar nicht „smart“ ist – sondern erst das Zusammenspiel mehrerer Komponenten?

Johannes Falk: Der Sprinkler ist nur ein Teil des Systems – ähnlich wie eine Smart-Home-Lampe. Die Lampe kann nur an- und ausgehen oder dimmen; „smart“ wird sie erst durch die Steuerung, die ihr Befehle gibt. Bei unserem System machen Brandmelder, Löschsteuerzentrale, das Ansteuermodul und die optionalen Brandmelder

den Unterschied. Erst das Zusammenspiel dieser Komponenten sorgt dafür, dass das Ganze wirklich intelligent arbeitet.

Könnten Sie uns ein einfach nachvollziehbares Beispiel nennen, bei dem ein SmartFit Sprinkler dem Nutzer einen klaren Vorteil gegenüber herkömmlichen Systemen bietet?

Johannes Falk: Mit unserem Sprinkler lassen sich Sprühflutgruppen direkt in bestehende Nass-Sprinkleranlagen integrieren. Bei einem Neubau können die vorhandenen Stränge weiter genutzt werden, wodurch eine separate Sprühflutanlage – und damit ein zusätzliches Rohrnetz – meist entfällt. Selbst eine elektrische Brandmeldung ist nicht zwingend erforderlich: Über die thermische Auslösung des SmartFit Sprinklers lässt sich auch die übrige Anlage steuern. Natürlich gibt es noch viele weitere Einsatzmöglichkeiten, aber dieser Fall ist offensichtlich: Er spart in der Regel Kosten und Montageaufwand.

Viele Betreiber verfügen bereits über bestehende Sprinkleranlagen: Wie leicht lässt sich SmartFit nachrüsten, und welche Schritte sind dafür nötig?

Johannes Falk: Die bestehende Anlage bleibt erhalten. Es müssen lediglich die Sprinklerköpfe ausgetauscht und die Aktivierungsmodule an die meist schon vorhandene Brandmeldeanlage angeschlossen werden – danach ist das SmartFit-System sofort einsatzbereit.

Ein häufiges Problem klassischer Anlagen ist der sogenannte „Skipping-Effekt“. Wie verhindert SmartFit dieses Risiko und warum ist das sicherheitsrelevant?

Johannes Falk: Unser System steuert gezielt mehrere Sprinkler an. Bei klassischen Anlagen ist man auf die thermische Auslösung jedes einzelnen Sprinklers angewiesen, was zu Lücken führen kann – der sogenannte „Skipping-Effekt“. SmartFit wählt die notwendigen Sprinkler im Voraus aus, aktiviert sie gezielt und verhindert so das Ausbreiten des Brandes, sodass das Feuer effektiv und vollständig bekämpft wird.

Sie erwähnten, dass SmartFit es ermöglicht, Löschmuster aktiv zu beeinflussen. Wie hilft das dabei, Brände zielgerichteter zu bekämpfen?

Johannes Falk: FM Research hat Sprinkler-Auslösealgorithmen für unterschiedliche Brandszenarien entwickelt. In enger Zusammenarbeit zwischen FM und unserem Team haben wir diese Algorithmen anschließend in das SmartFit-System integriert. Dadurch können Brände gezielt bekämpft werden. Außerdem lässt sich das System an die örtlichen Gegebenheiten anpassen – sei es unterschiedliche Raumgrößen, Rollbänder oder spezielle Baukonstruktionen.

Ihr Team arbeitet mit FM an einem Research Agreement. Welche Fragestellungen werden dabei untersucht und welchen Nutzen erwarten Sie für die Branche?

Johannes Falk: Die bereits erwähnten Löschalgorithmen wurden von FM-Research entwickelt. In unserem gemeinsamen Projekt untersuchen wir, wo herkömmliche Sprinklersysteme an ihre Grenzen stoßen und wie SmartFit in solchen Fällen optimal unterstützen kann. Die Ergebnisse sollen in

den FM Data-Sheets veröffentlicht werden. Für die Branche bedeutet das, dass speziell auf die Risiken zugeschnittene Schutzkonzepte verfügbar werden.

Wie verändert SmartFit das Brand-schutzverständnis insgesamt – insbesondere die Möglichkeit, ein Feuer tatsächlich „aktiv zu managen“, statt nur passiv zu reagieren?

Johannes Falk: Wenn aufgrund örtlicher Gegebenheiten von Standardlösungen abgewichen werden muss, liegt die Verantwortung stärker beim Planer der Anlage – er muss aktiv überlegen, wie sich ein Brand entwickeln könnte. Genau an dieser Stelle eröffnet SmartFit neue Möglichkeiten: Der Sprinkler dient nicht mehr nur der Brandkontrolle. Das SmartFit-System soll den Brand möglichst früh erkennen, kontrollieren und löschen, bevor es zu erheblichen Schäden oder einer Brandausbreitung kommt. Im besten Fall ist ein Eingreifen der Feuerwehr dann gar nicht mehr erforderlich.

Und zuletzt: Erhöht sich der Wartungsaufwand durch die elektronischen Komponenten, oder bleibt SmartFit im Alltag ebenso unkompliziert wie herkömmliche Sprinkler?

Johannes Falk: Der Sprinkler selbst bleibt klassisch wartungsfrei. Es entsteht kein höherer Wartungsaufwand als bei ohnehin vorhandenen Löschsteuerzentralen oder Brandmeldezentralen, die das System überwachen. SmartFit meldet automatisch, wenn ein Austausch einzelner Komponenten erforderlich ist – noch bevor ein Versagen auftreten könnte. Das ist ein großer Vorteil: Während herkömmliche Sprinkler erst nach rund 25 Jahren geprüft werden, erhalten Betreiber beim SmartFit-System frühzeitig Rückmeldungen und können proaktiv handeln. **GIT**



Fire Protection Solutions Group
www.fire-protection-solutions.com

ADVERTORIAL

SCHRANER-Group: „Begegnung schafft Mehrwert“

Unter diesem Leitgedanken wird der Stand der SCHRANER-Group erneut während der FeuerTrutz zum Treffpunkt für fachlichen Austausch und Netzwerk. Basketball verbindet.

Austausch zu technischen Fachthemen und herausragende Events: Dafür ist die SCHRANER-Group bekannt. Auch während der FeuerTrutz können Besucher/-innen am Stand 4A-300 in der Halle 4A ihr Branchen-Netzwerk pflegen und gleichzeitig einige Highlights erleben. Ob

zukunftsweisende digitale Anwendungen, technisch ausgereifte Produkte oder maßgeschneiderte Dienstleistungen im Bereich der Brandmelde- und Sicherheitstechnik: Die SCHRANER-Group trägt mit ihren qualitativ hochwertigen, wirtschaftlichen und innovativen Lösungen dazu bei, Leben und Sachwerte zu schützen und die Arbeit von Systemintegratoren, von Feuerwehrleuten und Fachplanern zu erleichtern.

Brandschutz und Basketball

Basketball meets Brandschutz: Neben Neuerungen aus der Brandmelde- und Sicherheitstechnik dreht sich an den Messetagen vieles um Basketball. So besteht die Möglichkeit am bereits bekannten Basketballkorb einen SCHRANER-Basketball zu gewinnen und bei hochwertigen Kaffeespezialitäten vom Barista einen Blick auf den BBL-Pokal der erfolgreichen BMA365 Bamberg Baskets zu werfen. Das Maskottchen Gluto sorgt für gute Stimmung auf dem Messegelände und freut sich auf einen Schnappschuss mit den Gästen. Ein Besuch des Messestandes auf der FeuerTrutz lohnt sich auf jeden Fall!



Weitere Infos und die Möglichkeit für einen kostenlosen Eintritt:



Kontakt

Schraner Holding GmbH
www.schraner-group.de



FeuerTrutz 2026

MESSEN

Feuertrutz 2026

Treffpunkt der Brandschutzbranche

Baulicher, anlagentechnischer und betrieblicher Brandschutz: Wer den umfassenden Überblick sucht, findet sie alljährlich auf der Feuertrutz im Messezentrum Nürnberg – dieses Jahr vom 24. und 25. Juni.

Die neuesten Produkte und Lösungen aus allen Segmenten der Brandverhütung und -eindämmung werden auch dieses Jahr auf der von Nürnberg Messe organisierten Feuertrutz präsentiert. Parallel dazu gibt es wieder den Brandschutzkongress mit Expertenvorträgen aus allen Bereichen. Angesprochen sind Fachplaner, Sachverständige, Architekten und Bauingenieure sowie Brandschutzbeauftragte, ebenso wie Mitarbeiter von Behörden und Brandschutzdienststellen.

Fachwissen und Live-Erlebnisse

Ein umfassendes Rahmenprogramm bietet fundiertes Fachwissen – u. a. präsentiert in Form von interaktiven Live-Erlebnissen. Geplant sind Diskussionen, Experimental-Vorträge und Industry Insights mit Experten. Auf einer Aktionsfläche gibt es Live-Demonstrationen von Brandschutzlösungen.

Dazu kommen Foren mit dem Fokus auf Weiterbildung und Startup-Förderung. Für letztere gibt es auch den Gemeinschaftsstand „Startups@Feuertrutz“ als Plattform

für Innovationen und Networking mit jungen Unternehmen. Zum Thema Aus- und Weiterbildung steht außerdem der „Treffpunkt Bildung & Karriere“ als zentraler Ort bereit, an dem entsprechende Anbieter zu finden sind. In der Feuertrutz-Arena finden Fachvorträge und Diskussionen statt. Ergänzend dazu kommen Afterwork-Treffen zum Netzwerken – einschließlich einer After-Work-Party am ersten Messetag.

Zukunftsraum und Brandschutzkongress

Ein neues Format der Feuertrutz ist der „Zukunftsraum“ in Halle 4, eine zentrale Plattform für visionäre Ideen und Technologien rund um den Brandschutz von morgen. Hier geht es u. a. um die Digitalisierung in der Brandschutzbranche. Thema sind etwa KI-gestützte Tools, papierlose Prozesse, aber auch um Strategien zur Fachkräftegewinnung.

Um Weiterbildung und Austausch im Rahmen von rund 40 Vorträgen und Diskussionen geht es auf dem Brandschutz-

kongress für Planer, Behördenmitarbeiter, Sachverständige, Errichterfirmen, etc. Der Schwerpunkt liegt hier bei der Praxis und dem direkten Bezug zum Arbeitsalltag im Brandschutz. Der Brandschutzkongress wird von vielen Architektur- und Ingenieurkammern als Fortbildung anerkannt.

Gefahrstoffe und Aktionsflächen

Um aktuelle Trends rund um die Lagerung und Handhabung gefährlicher Stoffe geht es im „Asecos Forum“ mit Vorträgen, und Diskussionen. Es gibt einen Experimentalvortrag über Risiken im Umgang mit Gefahrstoffen etwa bei Reaktionen und Explosionen, um Gefährdungsbeurteilung, Risiken von Lithium-Ionen-Batterien, um Brandschutzmaßnahmen bei Gefahrstofflagerung, richtige Einstufung, Trennung, Schutzkonzepte und anderes.

Wen es ins Freie zieht, kann sich die Vorführungen auf der Aktionsfläche Brandschutz im Außenbereich ansehen. Hier zeigen Aussteller ihre Innovationen in wirklichkeitsnahen Szenarien. Verschiedene Löschsysteme und mobile Brandschutzlösungen wird es hier zu sehen geben. **GIT**



Nürnberg Messe GmbH
www.feuertrutz-messe.de

Vernetzte Sicherheitslösungen auf der Interschutz

Lupus-Electronics zeigte auf der Interschutz 2026 in Hannover smarte Lösungen für vernetzte Sicherheits- und Gebäudeinfrastrukturen. Wie beispielsweise der Lupus Mobilfunkrauchmelder, der eine zentrale Komponente für die direkte, cloud-basierte Alarmierung bildet. Durch die Anbindung über Mobilfunknetze werden Ereignisse unabhängig von lokaler IT-Infrastruktur oder WLAN in Echtzeit übertragen. Er benötigt keine Vor-Ort-Inspektionen und erfüllt die Anforderungen der DIN 14676-1-C vollautomatisch. Alle 24 Stunden wird ein Selbsttest durchgeführt, die Dokumentation wird über die Lupus-Cloud realisiert. Im Brandfall werden definierte Kontakte via E-Mail oder Pushnachricht informiert, inklusive detaillierter Standortangabe auf einer digitalen Karte. Die Batterielebensdauer beträgt 10 Jahre, die Wartung geschieht rechtssicher und wird lückenlos dokumentiert. www.lupus-electronics.de

Ideal für Schulen, Kindertagesstätten, Wohnheime, Büro- und Verwaltungsgebäude sowie Herbergen bis zu 60 Betten: Die Lupus Brandwarnanlage



Zumischsystem eProp von Minimax mit VdS-Anerkennung

Das Verbot PFAS-haltiger Schaumlöschmittel erfordert die Umrüstung bestehender Schaumlöschanlagen. Hier stellen die PFAS-freien Schaumlöschmittel (F3) hohe Anforderungen an die Zumischtechnik: Sie sind häufig zähflüssiger und weisen stark wechselnde Fließeigenschaften auf. eProp ist das eigene Zumischsystem der Minimax Viking Gruppe für genau diese Anforderungen. Das System hat die VdS-Anerkennung für den Einsatz aller Schaumlöschmittel-Viskositäten. So sorgt es für eine präzise Funktion im Betrieb der Anlage. Dank kompaktem und flexiblem Design ist es einfach in Neu- und Bestandsanlagen zu integrieren.

www.minimax.de

Bvfa Kompakt-Seminar „Brandschutzdirekt Löschtechnik“

Am 24. Juni 2026 lädt der Bvfa – Bundesverband Technischer Brandschutz bereits zum zehnten Mal zur „Brandschutzdirekt Löschtechnik“ nach Nürnberg ein. Die Veranstaltung findet parallel zum Brandschutzkongress sowie zur FeuerTrutz statt und richtet sich an Fachkräfte aus Planung, Betrieb, Industrie, Versicherungswesen und Errichter von anlagentechnischen Brandschutzsystemen. Auch zum Jubiläum bietet das Seminar ein hochaktuelles Programm mit praxisnahen Vorträgen, neuen Forschungserkenntnissen und Einblicken in technische Entwicklungen der Branche. So zeigt Univ.-Prof. Dr.-Ing. Jochen Zehfuß von der TU Braunschweig, welche Erkenntnisse über anlagentechnische Brandschutzmaßnahmen in aktuellen Forschungsvorhaben gewonnen werden – etwa der direkte Einfluss der Sprinklerung auf die Branddynamik durch veränderte Thermik, Wasserdampf- und Rauchsichtbildung. www.bvfa.de

Spezialisierte Brandschutz für Flugzeughangars und Munitionsbunker

Militärstandorte zählen zu den sicherheitspolitisch sensibelsten Bereichen eines Staates. Die d&d Brandschutzsysteme GmbH, exklusiver Distributionspartner von Det-Tronics in Deutschland, bietet militärischen Einrichtungen spezialisierte Flammendetektoren für Flugzeughangars und Munitionsbunker.

Flugzeughangars weisen aufgrund zahlreicher brennbarer Stoffe eine hohe Brandlast auf. Abhilfe schaffen speziell entwickelte Flammenmelder mit flexibel einstellbarem Sichtfeld, individuellen Programmieroptionen und schneller Reaktionszeit. Für den militärischen Einsatz besonders relevant ist ihre Unempfindlichkeit gegenüber elektromagnetischen Störungen – ein entscheidender Faktor, da die Piloten ihre elektronischen Abwehrsysteme regelmäßig bereits beim Rollen oder Starten testen. Ein weiteres hohes Gefahrenpotenzial geht von Munitionsbunkern aus. Unterschiedlichste Explosivstoffe erfordern hochpräzise Detektionstechnik und kürzeste Reaktionszeiten.

Je nach Anforderungsprofil kommen ein UV-IR-Flammenmelder, wahlweise mit Hochgeschwindigkeits-Sprühflutmodul, ein UV-Flammenmelder oder ein IR-Flammenmelder zum Einsatz. In militärischen Hochrisikobereichen bilden diese spezialisierten Flammendetektoren in Kombination mit ultraschnellen Löschen- und Alarmierungsmechanismen die Grundlage für den effektiven Schutz von Menschen, Anlagen und sensiblen Materialien.

www.dd-brandschutzsysteme.de



Kabelabschottungen
Brandschutzkanäle
MCT Brattberg
Sauerstoffreduktion
Kleinlöschsysteme



Jetzt auch als Systemlösung **VdS-angemerkt!**

KANALRAUCHMELDER

Früherkennung statt Brandfall

**Vorbeugender Brandschutz im Gebäudebetrieb:
Oppermann zeigt Überwachungslösungen auf der Feuertrutz 2026**

Brände entstehen selten auffällig – meist beginnen sie unbemerkt im Verborgenen eines Gebäudes. Umso wichtiger ist der vorbeugende Brandschutz, der zunehmend zu einem festen Bestandteil moderner Gebäudeplanung wird. Hier setzt die Oppermann Regelgeräte GmbH an: Das Unternehmen entwickelt seit vielen Jahren Lösungen zur Überwachung technischer Anlagen, die den vorbeugenden Brandschutz im laufenden Gebäudebetrieb unterstützen. Diese Lösungen zeigt Oppermann am 24. und 25. Juni auf der Feuertrutz 2026 in Nürnberg.



Kanalrauchmelder KRM-X zur Überwachung von Lüftungsanlagen



Das Team von Oppermann auf der FeuerTrutz 2025

„Die FeuerTrutz ist für uns eine wichtige Plattform für den Austausch mit Fachleuten aus Architektur, Gebäudetechnik und Brandschutz.“ erklärt Matthias Fricke, Vertriebsleiter Außendienst bei Oppermann Regelgeräte. „Gerade im täglichen Gebäudebetrieb wird deutlich, wie entscheidend zuverlässige Technik ist, um brandschutzrelevante Anlagen dauerhaft sicher und effektiv zu betreiben.“

Technik für den sicheren Gebäudebetrieb

Oppermann Regelgeräte nutzt die Messe, um seine Brandschutzlösungen vorzustellen

– darunter den Kanalrauchmelder KRM-X. Solche Geräte spielen insbesondere in Gebäuden mit komplexer Lüftungstechnik eine wichtige Rolle.

Rauchgase stellen dabei eine erhebliche Gefahr dar: Sie können Flucht- und Rettungswege unbemerkt vernebeln, die Orientierung erschweren und innerhalb kurzer Zeit zu gesundheitlichen Beeinträchtigungen führen.

Der Kanalrauchmelder KRM-X überwacht kontinuierlich den Luftstrom in Lüftungssystemen und erkennt frühzeitig auch geringe Mengen sogenannter Kaltrauchteilchen – also Rauchpartikel, die bereits in

einer frühen Brandphase entstehen. So können Lüftungsanlagen rechtzeitig abgeschaltet und weitere Brandschutzmaßnahmen eingeleitet werden, bevor sich Rauch im Gebäude ausbreitet. Die frühzeitige Detektion durch solche Systeme kann dazu beitragen, zusätzliche Reaktionszeit zu gewinnen und die Ausbreitung von Rauchgasen zu begrenzen.

„Vorbeugender Brandschutz beginnt nicht erst im Ernstfall“ betont Matthias Fricke. „Er ist ein integraler Bestandteil des täglichen Gebäudebetriebs. Mit Lösungen wie dem KRM-X unterstützen wir Betreiber dabei, ihre Anlagen zuverlässig zu überwachen und sichere Räume zu gewährleisten.“

Persönlicher Austausch mit Oppermann

Fachbesucher haben die Möglichkeit, Oppermann Regelgeräte GmbH persönlich am Stand 4A-210 im Messezentrum Nürnberg zu treffen. Am 24. und 25. Juni 2026 von 9:00 bis 17:00 Uhr präsentiert das Unternehmen Systeme zur Überwachung und Regelung brandschutztechnischer Anlagen und steht für Fachgespräche und persönlichen Austausch zur Verfügung. **GIT**

Oppermann Regelgeräte auf der Feuertrutz 2026: Stand 4 A-210

Oppermann Regelgeräte GmbH
www.oppermann-regelgeraete.de



KRISENVORSORGE

Blackout

Was passiert, wenn der Strom wegbleibt?

Beim „Dortmunder Forum für Krisen-, Risiko- und Business Continuity Management“ – kurz „@risc-Forum“ – im Februar stand ein Thema im Mittelpunkt, das lange als theoretisches Szenario galt, inzwischen aber zunehmend als reale Herausforderung wahrgenommen wird: der großflächige Stromausfall. Unter dem Titel „Blackout – wie widerstandsfähig sind wir wirklich?“ sprach der Leitende Branddirektor und Diplom-Physiker Karsten Göwecke über Risiken, Erfahrungen aus realen Einsatzlagen und die Frage, wie Staat, Wirtschaft und Gesellschaft ihre Krisenfestigkeit stärken können.

■ Zu den Highlights des „@risc-Forum“ im Februar dieses Jahres zählte ein Beitrag zu einem brisanten Thema, nämlich dem Blackout und den Auswirkungen entsprechender Szenarien. „@risc – research. innovation. strategy. consulting“ ist ein auf Sicherheits-, Risiko- und Krisenmanagement spezialisiertes Beratungsunternehmen. Mit Fachveranstaltungen wie dem Dortmunder Forum schafft das Unternehmen zugleich eine Plattform für den Austausch zwischen Wissenschaft, Wirtschaft, Verwaltung und Einsatzorganisationen.

Extremwetter und gezielte Anschläge

Karsten Göwecke, der unter anderem langjähriger Vertreter des Landesbranddirektors der Berliner Feuerwehr war und heute als Experte für Bevölkerungsschutz und Krisenmanagement tätig ist, machte in seinem Vortrag im Februar deutlich, dass die Diskussion über Blackout-Szenarien längst nicht mehr allein von Naturereignissen geprägt wird. Neben Extremwetterlagen spielten inzwischen auch gezielte Anschläge, geopolitische Spannungen sowie die zunehmende Komplexität der Energieversorgung eine Rolle. Zwar sei die Wahrscheinlichkeit

eines langanhaltenden, mehrere Bundesländer betreffenden Stromausfalls vergleichsweise gering – die möglichen Folgen wären jedoch erheblich.

Anhand konkreter Beispiele zeigte Göwecke, wie schnell Stromausfälle weitreichende Auswirkungen entfalten können. Er erinnerte unter anderem an das „Münsterländer Schneechaos“ von 2005, bei dem rund 250.000 Menschen teils über mehrere Tage ohne Strom waren, sowie an den europaweiten Stromausfall von 2006. Einen besonderen Schwerpunkt bildeten mehrere Ereignisse aus Berlin, darunter der mehrtägige Ausfall in Köpenick 2019 sowie weitere großflächige Störungen in den Jahren 2025 und 2026. Die Beispiele verdeutlichten, wie eng moderne Infrastrukturen miteinander verknüpft sind: Neben der Stromversorgung geraten schnell auch Mobilfunknetze, Verkehrssysteme, Heizungen, Krankenhäuser oder Pflegeeinrichtungen unter Druck.

Kommunikation, Koordination, Resilienz

Der Referent machte deutlich, dass Krisen dieser Art nicht allein von Energieversorgern oder Katastrophenschutzbehörden

bewältigt werden können. Entscheidend seien funktionierende Kommunikationsstrukturen, schnelle Koordination und eine resiliente Verwaltung. Ebenso wichtig sei die Vorbereitung auf lokaler Ebene – von der Wartung von Netzersatzanlagen bis hin zu klaren Informationswegen für die Bevölkerung.

Auch Unternehmen seien gefordert, ihre eigene Widerstandsfähigkeit kritisch zu überprüfen. Notstromversorgung, unterbrechungsfreie Stromsysteme, Krisenpläne und funktionierende Kommunikationskonzepte würden zunehmend zu strategischen Faktoren. Gerade Betreiber kritischer Infrastrukturen müssten sich auf Szenarien vorbereiten, die bislang vielfach als Ausnahmefälle betrachtet wurden. **GIT**



@risc – research. innovation.
strategy. consulting
www.at-risc.de

ÖFFENTLICHE SICHERHEIT

Schutz und Rettung rund um die Uhr

**Feuerwehr Hannover:
Von Brand- bis Katastrophenschutz**



Christoph Bahlmann,
Direktor der Feuer-
wehr Hannover

GIT SICHERHEIT sprach mit Christoph Bahlmann, Direktor der Feuerwehr Hannover, über die Herausforderungen und strategischen Weichenstellungen seiner Organisation. Im Interview beleuchtet er Weiterentwicklungen in der Notfallrettung sowie zentrale Aspekte modernen Bevölkerungsschutzes: Von High Performance CPR über Notfallinformationspunkte bis hin zur Vorbereitung auf hybride Bedrohungslagen. Vor dem Hintergrund geopolitischer Spannungen und klimabedingter Extremereignisse gewinnt die kommunale Krisenvorsorge an Bedeutung. Bahlmann skizziert die Strukturen des Krisenmanagements, die Integration des Oplans Deutschland in zivile Planungen sowie konkrete Szenarien wie großflächige Stromausfälle. Das Gespräch fand im Vorfeld der kürzlich zu Ende gegangenen Messe Interschutz statt.

GIT SICHERHEIT: Herr Bahlmann, zunächst einmal herzlichen Dank, dass Sie sich Zeit nehmen für dieses Gespräch – Sie bereiten sich gerade auf die Interschutz vor, die ja bei Ihnen in Hannover stattfindet. Mit welchem Konzept werden Sie sich dort präsentieren?

Christoph Bahlmann: Die Interschutz ist uns Hannoveranern eine Herzensangelegenheit. Wir thematisieren auf unserem Stand unser Konzept der High Performance CPR (HP-CPR). Die HP-CPR umfasst standardisierte Abläufe in der Wiederbelebung unter Einbe-

ziehung der Besatzung eines Hilfeleistungslöschfahrzeuges. Weiterhin greifen wir aus dem Bereich Bevölkerungsschutz das Thema Notfallinformationspunkte, also Kontaktpunkte für die Bevölkerung in besonderen Krisenlagen auf. Da unsere Fachgruppe für die spezielle Rettung aus Höhen und Tiefen in diesem Jahr ihr 25-jähriges Jubiläum feiert, ist Höhenrettung ein wesentliches Thema. Der Pavillon 34 steht unter diesem Themenschwerpunkt und es gipfelt am Messesamstag im Nationalen Leistungsvergleich der Höhenrettungsgruppen, der auf dem Messegelände stattfinden wird. Dies sind

nur einige unserer Themen. Wir freuen uns, Sie am Stand B48 in Halle 12 zu begrüßen.

Sie sind ja seit etwa 25 Jahren bei der Feuerwehr Hannover – das ist eine schöne runde Zahl. Sie haben bei Ihrer Berufung als Direktor der Feuerwehr gesagt, Sie könnten sich keinen interessanteren Beruf vorstellen und haben sich vorgenommen, die Feuerwehr auf hohem Niveau weiterzuentwickeln. Könnten Sie vielleicht zum Einstieg eine (Zwischen-)Bilanz ziehen?

Christoph Bahlmann: Mein Einstieg als neuer Chef der Feuerwehr Hannover im Oktober 2022 fand unter dem Eindruck des russischen Angriffskrieges auf die Ukraine statt. Seitdem haben wir – wie viele andere Kommunen auch – den Bereich des Bevölkerungsschutzes und Krisenmanagements personell wie auch inhaltlich systematisch ausgebaut. Dieser Prozess ist seitdem ein Dauerthema. Daneben beschäftigen wir uns mit der Fortentwicklung unserer Regionsleitstelle, die eine Fläche so groß wie das Saarland versorgt. Gerade vor dem Hintergrund des Umbaus unseres Gesundheitssystems und der Notfallvorsorge in Deutschland sowie dem damit verbundenen Kostendruck ist das eine weitere Mammutaufgabe, die wir sukzessive erfolgreich umsetzen.

Ein anderer wichtiger Punkt ist, auf allen Ebenen des Unternehmens Feuerwehr Hannover fachlich versierte und hoch motivierte Fachkräfte zu gewinnen und zu binden – das ist die Basis für viele Projekte und damit unsere Zukunft. Des Weiteren sind wir dabei, den Neubau eines unserer fünf Standorte konkret zu planen – ein 130 Millionen Euro-Projekt. Sie sehen, es gibt allen Grund für eine sehr positive Zwischenbilanz.

Könnten Sie uns einmal Struktur und Aufgabenspektrum der Feuerwehr Hannover kurz vorstellen?

Christoph Bahlmann: Wir sind eine kommunale Großstadtfirewehr mit 925 Mitarbeitenden auf fünf Feuer- und Rettungswachen. Wir decken ein breites Aufgabenspektrum der nichtpolizeilichen Gefahrenabwehr in den Gebieten Brandschutz und Hilfeleistung, dem Rettungsdienst, der Regionsleitstelle sowie dem Bevölkerungsschutz und dem Krisenmanagement ab. Die Feuerwehr ist einer von 26 Fachbereichen der Landeshauptstadt Hannover. Zur Wahrnehmung der umfangreichen Anforderungen sind wir in sieben Bereichen und einer Stabsstelle organisiert.

Die Themen Bevölkerungsschutz und Katastrophenschutz haben in jüngerer Zeit vor dem Hintergrund neuer geopolitischer Bedrohungen einen veränderten Zungenschlag bekommen. Zunächst



Die Fachgruppe Hochwasserschutz im Einsatz – dazu gehört beispielsweise die Sandsacklogistik

einmal aus Ihrer Perspektive als kommunale Katastrophenschutzbehörde: Welche Aufgaben lassen sich auf lokaler Ebene eigenständig bewältigen und wo stoßen Kommunen an ihre Grenzen?

Christoph Bahlmann: Als Landeshauptstadt sind wir es in Hannover gewohnt, auf die vielfältigen Gefahrenlagen einer Großstadt wirkungsvoll zu reagieren. Auch verfügen

wir über ein schlagkräftiges Netzwerk aus kommunalen Stellen, Hilfsorganisationen und der Polizei, die im Einsatzfall Hand in Hand arbeiten. Unsere Grenzen erreichen wir, wenn multiple Bedrohungslagen aufeinandertreffen. Hier kann die Bedrohung durch hybride Angriffe genannt werden, die das Ziel haben, die Grundlagen der öffentlichen Sicherheit und Ordnung, wie z. B. die Versorgung der Bevölkerung mit Energie und lebensnotwendigen Waren zu stören. Die Landeshauptstadt Hannover baut auch hier ihre Fähigkeiten weiter aus. So haben wir 2025 ein neues flächendeckendes Sirenenwarnnetz in Betrieb genommen.

Die Grenzen sind aber umso deutlicher zu spüren, wenn es an verbindlichen rechtlichen Anforderungen und Zuständigkeitsregelungen auf kommunaler, Landes- und Bundes-Ebene fehlt. Zudem merken wir, dass Konzepte des Bevölkerungsschutzes aufgrund fehlender finanzieller Mittel nicht immer in ausreichendem Maße umgesetzt werden können. Hier brauchen wir eine noch intensivere Vernetzung zwischen zivilen und hoheitlichen Stellen von der kommunalen Ebene bis rauf zur Landes- und Bundesebene. Und vor allem braucht es eine stärkere finanzielle Unterstützung der kommunalen Haushalte durch den Bund und die Länder.

Wie fließt der Oplan Deutschland in Ihre Konzeptionen ein? Er hat ja gleichzeitig eine militärische und zivile Seite, d. h. wir sprechen hier über die Vorbereitung auf einen wie auch immer aussehenden Ernstfall im Rahmen einer Gesamtverteidigung?



Die HP-CPR umfasst standardisierte Abläufe in der Wiederbelebung unter Einbeziehung der Besatzung eines Hilfeleistungslöschfahrzeuges

Bitte umblättern ►

Christoph Bahlmann: Der Operationsplan Deutschland ist zunächst mal eine militärische Planung der Bundeswehr und unterliegt demnach den Anforderungen des Geheimschutzes. An den Stellen, an denen im Sinne der zivilmilitärischen Zusammenarbeit Unterstützungsleistungen durch die zivil-hoheitliche oder zivil-gewerbliche Stellen erforderlich ist, findet nach und nach eine gezielte Ansprache durch die Bundeswehr statt. In diesen Fällen werden die zivilen Planungen mit den Anforderungen der Bundeswehr abgestimmt.

Mit welchen Szenarien setzten Sie sich diesbezüglich auseinander?

Christoph Bahlmann: Es geht z. B. um die Sicherstellung der Versorgung der Bevölkerung und die Aufrechterhaltung der Funktionen der Stadtverwaltung Hannover. Daneben bereiten wir uns auf Lagen vor, in denen die Versorgung der Bevölkerung mit Gas, elektrischer Energie oder Trinkwasser gestört ist.

Ein weiteres Feld ist die Sicherstellung der stationären medizinischen Versorgung im Verteidigungsfall. In einem Runden Tisch mit Krankenhausbetreibern, dem öffentlichen Gesundheitsdienst und der ministeriellen Ebene haben wir zwölf Handlungsfelder zur Krisenvorsorge von Krankenhäusern im Verteidigungsfall identifiziert. Die Anforderungen an Krankenhäuser gehen dann weit über die üblichen Themen der Krankenhausalarmplanung hinaus.

Könnten Sie uns einmal die Struktur des Krisenmanagements skizzieren? Welche Stabsstrukturen werden im Ernstfall aktiviert, wie erfolgt die Koordination zwischen den verschiedenen Akteuren?

Christoph Bahlmann: Das Krisenmanagement der Landeshauptstadt Hannover befasst sich aktuell mit der Identifizierung von Prozessen und Leistungen der Stadtverwaltung Hannover, die im Krisenfall zu jeder Zeit aufrechterhalten werden müssen. In weiteren Schritten ist die Resilienz dieser Prozesse zu verbessern. Für kritische Prozesse müssen in vielen Teilen der Verwaltung Notfallpläne erstellt werden. Daneben werden auch die Tätigkeiten erfasst, die in einem Krisenfall nicht notwendig sind. An dieser Stelle können personelle und technische Ressourcen für die Krisenbewältigung freigesetzt werden.

Auf den Eintritt eines Krisenfalls reagiert die Landeshauptstadt Hannover durch Einrichtung eines Verwaltungsstabes in dem die Lage aus organisatorisch-administrativer Sicht gesteuert wird. Der Verwaltungsstab trifft übergeordnete Entscheidungen und

steuert die Arbeit der Stadtverwaltung in der Krise. Die operativ-taktische Lenkung der Gefahrenabwehr erfolgt im Führungsstab. Beide Stäbe können abhängig von Art und Umfang des Ereignisses gemeinsam oder getrennt eingesetzt werden. In beiden Stäben werden Fachberater und Verbindungspersonen relevanter externer Stellen einbezogen.

Lassen Sie uns das Grundszenario „Stromausfall“ einmal durchspielen – dazu kann es ja aus verschiedenen Gründen kommen. Welche Maßnahmen haben Sie für so einen Fall in der Schublade?

Christoph Bahlmann: Im Falle eines großflächigen und länger andauernden Stromausfalls werden mehrere Einsatzkonzepte parallel aktiviert. Neben dem Aufruf der beschriebenen Stabsstrukturen ist es wichtig, die Versorgung mit Kraftstoff für Netzersatzanlagen wichtiger Objekte und Fahrzeuge von Feuerwehr, Hilfsorganisationen und Polizei sicher zu stellen. Besondere Bedeutung hat für uns die Information der Bevölkerung. Wir müssen davon ausgehen, dass die etablierten Informationskanäle nicht mehr zur Verfügung stehen. Wir werden daher mit sogenannten Notfallinformationspunkten in die Fläche gehen und als Stadtverwaltung und damit auch wir als Feuerwehr zusammen mit der Polizei Präsenz in allen Teilen der Stadt zeigen und so ansprechbar sein und den Menschen Sicherheit vermitteln.

Ein eigenes Szenario, das aber auch Folge eines längeren Stromausfalls sein kann, wäre das Ausfallen des Mobilfunknetzes. Welche Konzepte gibt es hier?

Christoph Bahlmann: Die Landeshauptstadt Hannover wird Notfallinformationspunkte (NIP) über das gesamte Stadtgebiet verteilt einrichten. Sie dienen der Bevölkerung als Anlaufstelle um Hilfeersuchen wie Notrufe in Präsenz abzusetzen und um sich über die Lage zu informieren. Die Notfallinformationspunkte bestehen im Wesentlichen aus einem Pavillonzelt, Stromerzeuger, Beleuchtungsmaterial und Kommunikationsmitteln. Sie werden an 43 vorgeplanten Orten im Stadtgebiet eingerichtet. Es wurden die Orte ausgewählt, die von den Bürgern intuitiv aufgesucht werden, weil sie an diesen Stellen Hilfe erwarten. Dazu gehören zum Beispiel die Feuerwehrrhäuser unserer 17 Ortsfeuerwehren, Rettungswachen oder das Neue Rathaus sowie einige Bürgerämter. Wir sind dadurch präsent in der Fläche und zeigen den Betroffenen, dass wir auch in der Krise vor Ort und handlungsfähig sind.

Notfallinformationspunkte (NIP) können über das gesamte Stadtgebiet verteilt eingerichtet werden. Sie dienen der Bevölkerung als Anlaufstelle um Hilfeersuchen wie Notrufe in Präsenz abzusetzen und um sich über die Lage zu informieren. Die Notfallinformationspunkte bestehen im Wesentlichen aus einem Pavillonzelt, Stromerzeuger, Beleuchtungsmaterial und Kommunikationsmitteln



Ein weiteres Metathema des Katastrophenschutzes hängt mit dem Klimawandel zusammen. Hier geht es beispielsweise um starke Hitze in der Stadt oder um Hochwasser und Starkregen. Wie werden im von der Leine durchflossenen Hannover die Konzepte diesbezüglich angepasst – und welche Rolle spielt hier die Feuerwehr?

Christoph Bahlmann: Die Landeshauptstadt Hannover hat in den maßgeblichen Fachbereichen der Verwaltung zentrale Stellen für die Koordination der Vorbereitungen auf Starkregenereignisse, Hitzewellen und Hochwasser eingerichtet. Beispielsweise wird aktuell das für das hannoversche Stadtgebiet bestehende Hochwasserschutzkonzept an die neuen Anforderungen angepasst. Das Konzept beschreibt, wo die bereits vorhandenen baulichen Hochwasserschutzmaßnahmen ausgebaut werden müssen. An Stellen, an denen dies nicht möglich ist, werden halbstationäre oder mobile Hochwasserschutzmaßnahmen vorbereitet, die im Ereignisfall kurzfristig durch ausgewählte Fachbereiche der Stadtverwaltung errichtet werden müssen.

Veränderungen am Hochwasserschutz haben aber nicht nur Auswirkungen auf unser Stadtgebiet, sondern auch auf die uns umgebenden Leineanrainer. Als Teil der überregionalen Hochwasserpartnerschaft mittleres und unteres Leinetal ist es unser Ziel, die Maßnahmen des Hochwasserschutzes mit unseren benachbarten Kommunen an der Leine abzustimmen. Wir verfügen schon heute über ein umfangreiches Maßnahmenkompendium, das für verschiedene Pegelstände der Leine dezidierte Maßnahmen beschreibt, die im Ereignisfall abgearbeitet werden können und dem Führungsstab als Planungs- und Handlungshilfe dienen.

Zum Abschluss: Was wird Ihre Arbeit bei der Feuerwehr Hannover in nächster Zeit vor allem prägen?

Christoph Bahlmann: Zunächst freuen wir uns auf die Weltleitmesse Interschutz auf unserem Messegelände in Hannover in der ersten Juniwoche. Hier fühlen wir uns als Feuerwehr Hannover traditionsgemäß als (Mit-)Gastgeber – insofern fließt in unseren Messestand in der Halle 12 ganz viel Herzblut. Danach werden wir uns mit der technischen Fortentwicklung unserer Leitstelle intensiv befassen, gleiches gilt für organisatorische Aspekte unserer Notfallrettung.

Ein wichtiges Thema in Niedersachsen und auch für uns ist z. B. die Einführung der Telenotfallmedizin. Schwerpunktmäßig im nächsten Jahr wollen wir für die Landeshauptstadt Hannover eine Feuerwehr- und Katastrophenschutzbedarfsplanung durchführen. Dieses Thema ist mir besonders wichtig, um für die mittel- und langfristige Fortentwicklung der Feuerwehr eine solide Basis in eher schwierigen Zeiten zu bekommen. Zudem denke ich immer an unser „Team F“ – Team Feuerwehr Hannover: Nur wenn es gelingt, möglichst viele Mitarbeitende für ihre Feuerwehr wirklich zu begeistern, werden wir uns als Feuerwehr Hannover auch langfristig erfolgreich weiter entwickeln können. Dazu gehört für mich auch immer eine enge und vertrauensvolle Zusammenarbeit mit unserer Personal- und Jugend- und Auszubildenden-Vertretung. **GIT**



Landeshauptstadt Hannover,
Fachbereich Feuerwehr
www.Feuerwehr-Hannover.de



Die Fachgruppe der Feuerwehr Hannover für die spezielle Rettung aus Höhen und Tiefen feiert in diesem Jahr ihr 25-jähriges Jubiläum

WIR SIND TEIL DER FEUERTRUTZ 2026!

Besuchen Sie uns am
24. + 25. Juni 2026 in Nürnberg
in Halle 4A Stand 211



JETZT TICKETS SICHERN!

 **VR FIRE TRAINER™**

GLORIA®



Um die wertvollen Artefakte in den Depots des Kunstmuseums Basel zuverlässig vor Bränden zu schützen, setzt das Museum bei seinem Neubau auf eine ganzheitliche Brandschutzlösung mit Titanus Ansaugrauchmeldern und dem Sauerstoffreduzierungssystem Oxyreduct von Wagner

MUSEUMSSICHERHEIT

Bewahrung des Unwiederbringlichen

Brandschutz für Museen

Museen, Archive und Bibliotheken sind nicht nur Orte der Kunst und Kultur, sondern auch besonders sensible Sicherheitsbereiche, denn sie schützen einzigartige Zeugnisse unserer Geschichte: Gemälde und andere Kunstgegenstände, Handschriften, Fotografien, Bücher und archäologische Funde. Ein Brand kann diese Werte in kürzester Zeit unwiederbringlich vernichten. Deshalb ist Brandschutz in diesen Institutionen weit mehr als eine technische Pflicht: Er ist ein integraler Bestandteil des Sicherheitskonzepts, das neben Einbruch- und Cyber-Schutz auch den physischen Erhalt des Kulturguts gewährleistet.



Ganzheitlicher Brandschutz bewahrt in Archiven wertvolle Werke: Ansaugrauchmelder (2) erkennen Brände frühzeitig, Sauerstoffreduzierungssysteme (4) verhindern offene Brände in geschlossenen Räumen (1), und im Ernstfall flutet eine Gaslöschanlage (3) den Schutzbereich



Ein Sauerstoffreduzierungssystem kann unter definierten Bedingungen Brandentstehung und -entwicklung verhindern. Das System wird platzsparend untergebracht und benötigt keine besonderen Zusatzeinrichtungen wie etwa Löschwasserbehälter

■ Die Sicherheitsarchitektur von Museen umfasst heute komplexe Systeme mit Zutrittskontrolle, Videoüberwachung, IT-Schutz und baulichen Sicherungen. Dennoch zeigen gerade jüngste Ereignisse, dass es bei der Sicherheit oft noch Optimierungspotenzial gibt. Das gilt für die öffentlich zugänglichen Bereiche ebenso wie für Archive und Depots. Und gerade hier lauert eine unterschätzte Gefahr: Feuer. Moderne Lagertechnik, automatisierte Systeme und präzise Klimatisierung sind unverzichtbar für die konservatorische Qualität und die wirtschaftliche Lagerung, gehen aber mit einer erhöhten Anzahl elektrischer Anlagen einher. Hierin steckt ein entscheidender Risikofaktor, denn defekte Kabel oder Überlastungen elektrischer Komponenten, auch mit Hitzeentwicklung, können schnell zur Zündquelle werden.

Leicht entflammables Material in den Depots stellt zusätzlich eine hohe Brandlast dar, die durch eine hohe Dichte der gelager-

ten Objekte noch erheblich gesteigert wird. In kompakten oder selten frequentierten Depots bleibt ein Schmelbrand oftmals für längere Zeit unentdeckt. Das kann fatale Folgen haben. Denn selbst eine beginnende Rauchentwicklung kann Kulturgüter bereits irreversibel schädigen, auch ohne offene Flammen. Ruß und toxische Gase kontaminieren Bestände flächendeckend – ein Szenario, das selbst modernste Löschanlagen nicht verhindern können.

Früherkennung und aktive Prävention

Die Basis effektiven Brandschutzes ist daher zunächst nicht die Löschung, sondern die Früherkennung. Werden Brände bereits in ihrer Frühphase detektiert, ist es möglich, rasch einzugreifen und Schäden durch Brand oder Löschmittel minimal zu halten.

Klassische Rauchmelder stoßen sowohl in großen, offenen Räumen mit variabler Luftströmung – etwa im Publikumsbereich eines Museums – als auch in kompakten Lagersituationen oft an ihre Grenzen. Hierfür bieten hochsensible Ansaugrauchmelder eine Lösung: Sie detektieren bereits geringste Rauchpartikel in der Entstehungsphase eines Brandes. Diese Früherkennung schafft einen entscheidenden Zeitvorteil, um geeignete Maßnahmen zu ergreifen, die eine weitere Brandausbreitung nach Möglichkeit verhindern und damit Personen und Kunstwerke schützen.

Auch bei einem Brandfall im Archiv oder Depot gilt es, nach einer Detektion schnell zu handeln – und dabei zum größtmög-

lichen Schutz der wertvollen Bestände rückstands- und zerstörungsfreie Löschmittel zu verwenden. Noch besser ist es natürlich, Brände bereits präventiv zu verhindern.

Der Einsatz innovativer Systeme zur Branderkennung, Brandvermeidung und Brandbekämpfung bietet entscheidende Vorteile:

■ Ansaugrauchmeldesysteme (z. B. Titanus)

Diese Systeme detektieren Brände bereits im Frühstadium, indem sie kontinuierlich Luftproben analysieren. Mit bis zu 2.000-fach höherer Empfindlichkeit im Vergleich zu herkömmlichen Punktmeldern gewinnen Sicherheitsverantwortliche wertvolle Minuten für Intervention und zum Schutz der Bestände. Intelligente Algorithmen verhindern Täuschungsalarme, die durch Staub oder Feuchtigkeit ausgelöst werden könnten. Dadurch wird diese Funktion zu einem Muss für sensible Bereiche wie Depots, aber auch für Ausstellungsräume, in denen beispielsweise auch menschliches Fehlverhalten zu einer Brandentstehung führen kann.

■ Sauerstoffreduzierungssysteme (z. B. Oxyreduct)

Mit diesen Systemen wird aus der Umgebungsluft Stickstoff generiert, der direkt in den Schutzbereich eingebracht wird. Dadurch wird dort der Sauerstoffgehalt kontrolliert abgesenkt. Für das Entstehen offener Flammen reicht der Sauerstoff nicht mehr aus. Dies verhindert bzw. minimiert auch eine Rauchentwicklung und schützt vor einer Kontamination durch Rauch. Die aktive Brandvermeidung ist besonders für geschlossene Archive geeignet. Der zeitlich begrenzte Zutritt bleibt möglich, während die Schutzatmosphäre Brände zuverlässig verhindert.

■ Gaslöschanlagen (z. B. Firexting)

Wo Brandvermeidung in Depotbereichen nicht praktikabel ist, kommen vorzugsweise Gaslöschanlagen zum Einsatz. Sie bekämpfen Brände rückstands- und zerstörungsfrei und unmittelbar nach der Detektion, ohne empfindliche Objekte durch Wasser oder Schaum zu gefährden. Silent-Düsen und Druckentlastungskappen minimieren zusätzliche Risiken für empfindliche Exponate.



Ansaugrauchmelder zur Brandfrüherkennung detektieren Brände bereits in ihrer Entstehungsphase

Bitte umblättern ►



Ein Gaslöschsystem sorgt im Brandfall für schnelle und rückstandsfreie Löschung

Gut geschützt: das Kunstmuseum Basel

Die IFS-Brandursachenstatistik zeigt: Defekte elektrischer Anlagen sind mit 30 % die häufigste Brandursache, gefolgt von menschlichem Fehlverhalten. Eine detaillierte Risikoanalyse ist für jedes Archiv und für jedes Depot daher unverzichtbar. Das Kunstmuseum Basel setzt auf eine Kombination aus Brandfrüherkennung mit Ansaugrauchmeldern der Titanus-Serie und Sauerstoffreduzierung mit Oxreduct. Fünf Depotbereiche mit bis zu 1.750 m³ werden permanent überwacht und durch kontrollierte Absenkung des Sauerstoffgehalts auf ca. 13,2 % bis 13,4 % brandhemmend gesichert. So sind die Gefahren größerer Brandfolgeschäden oder der Beeinträchtigung von Artefakten, der Einrichtung oder von Personen durch zerstörerische Löschmittel gebannt.

Ganzheitliche Sicherheitsstrategie: ein wichtiger Aspekt auch für Versicherungen

Was im Kunstmuseum Basel bereits Realität ist, entspricht auch den wachsenden Anforderungen der Versicherer. Sie erwarten von Museen ein professionelles Risikomanagement mit hohem Sicherheitsniveau, das weit über den Abschluss einer Police hinausgeht. Im Zentrum stehen der Schutz der Werte, die Sicherung der Betriebsfähigkeit und wirkungsvolle Präventionsmaßnahmen zur Schadensvermeidung.

Brandschutz ist dabei kein isolierter Baustein, sondern Teil eines umfassenden Sicherheitskonzepts. Dazu gehört auch die Einbindung leistungsfähiger Gefahrenmanagementsysteme, die alle sicherheitsrelevanten Komponenten zentral überwachen – von Zutrittskontrolle und Videoüberwachung bis hin zur Branddetektion. So ent-

steht ein ganzheitlicher Schutz, der physische wie digitale Risiken gleichermaßen berücksichtigt.

Beim Brandschutz selbst bewerten Versicherer den Einsatz präventiver Technologien zunehmend positiv. Insbesondere Systeme zur Sauerstoffreduzierung verhindern bereits das Entstehen oder die Ausbreitung eines Brandes. Die zertifizierten Systeme und geprüften Lösungen von Wagner sind heute bei vielen internationalen Versicherern anerkannt und gelten als Best Practice für besonders sensible Bereiche wie Depots, Archive oder Magazine.

In Depots und Archiven schafft die Kombination aus individuellem Versicherungsschutz und aktiver Brandvermeidung ein Sicherheitsniveau, das deutlich über dem Standard liegt. Neben der finanziellen Absicherung durch spezifisch abgestimmte Policen bietet sie operative Sicherheit durch präventive Technologien, die Kulturgüter und Abläufe wirklich schützen. Damit ist die Reputation sichergestellt – und das unwiederbringliche kulturelle Erbe bleibt erhalten.

Fazit

Wer Museen und Archive betreibt, muss Brandschutz als strategische Sicherheitsaufgabe begreifen und diesen Ansatz konsequent verfolgen. Das abgestimmte Zusammenspiel aus baulichen, organisatorischen und anlagentechnischen Maßnahmen gewährleistet den zuverlässigen Schutz von Kulturgütern vor Feuer, Rauch und Folgeschäden – und bewahrt damit ein Stück unserer gemeinsamen Identität für kommende Generationen. **GIT**



Wagner Group GmbH
www.wagnergroup.com



Die neue Generation der Sockelsignalgeber Soteria Slicer ist auch in Schwarz für wahlweise weißes oder rotes Licht verfügbar

Sockelsignalgeber Soteria Slicer in Schwarz

Hertek ergänzt mit dem Soteria Slicer das Programm der schwarzen Komponenten. Damit bleibt die Raumästhetik auch in dunklen Umgebungen erhalten. Die neuen Signalgeber erfüllen alle relevanten EN-Normen. Die zweite Generation der Soteria Slicer ist ein Sirenen- und Kombisignalgeber und wahlweise mit weißem oder rotem Licht verfügbar. Dabei sorgt ein halbtransparenter Rand für bestmögliche Sichtbarkeit. Der Slicer in Schwarz vervollständigt das Programm, das bereits Multisensor-Melder und Sockel für den Einsatz in dunklen Umgebungen enthält. Wenn der Soteria Slicer zusammen mit einem Melder betrieben wird, benötigt die Kombination im CoreProtocol, zum Beispiel in Verbindung mit der Brandmelderzentrale Penta 6000, nur eine einzige Adresse. Dabei sind Sirene und Signalleuchte einzeln ansteuerbar. **www.hertek.de**



Löschanlage P250
auf KFZ-Anhänger

Mobile Löschanlagen

Die Minimax Mobile Services GmbH erweitert ihr Angebot an mobilen Brandschutzlösungen um neue Löschanlagen auf Kfz-Anhänger-Basis. Die leistungsstarken Einheiten sind als Serienmodelle bestellbar und ergänzen die bereits erfolgreich eingeführten mobilen Rollcontainer-Löschanlagen. Mit dem Ausbau des Portfolios bietet das Unternehmen nun ein abgestimmtes Sortiment für flexiblen, mobilen Brandschutz in Industrie, Gewerbe und bei Feuerwehren. Die Löschanlagen auf Kfz-Anhänger wurden speziell für Unternehmen und Einsatzkräfte entwickelt, die große Löschmittelmengen schnell und sicher an den Einsatzort bringen müssen. Als Serienmodelle stehen sie kurzfristig ohne individuelle Sonderkonstruktion zur Verfügung und bringen eine etablierte Standardausstattung mit – ideal für Werkfeuerwehren, kommunale Feuerwehren sowie Betriebe mit erhöhtem Brandrisiko. www.minimax-mobile.com



Feuertrutz 2026: Attraktives Rahmenprogramm

Am 24. und 25. Juni 2026 bringt die Fachmesse Feuertrutz im Messezentrum Nürnberg Hersteller, Fachplaner, Sachverständige und Behörden zusammen. Neben der Fachmesse erwartet die Besucher ein praxisnahes Rahmenprogramm mit Live-Demonstrationen und Fachforen. Dazu gehören beispielsweise das Forum by assecos academy, die Feuertrutz Arena oder die Aktionsfläche Erlebnis Brandschutz. Neu im Rahmenprogramm ist der Zukunftsraum, der als zentrale Plattform für Präsentationen, Austausch und Wissenstransfer dient. Er bietet praxisnahe Vorträge zu Digitalisierung, KI, Social Media und Fachkräftegewinnung – für alle Besucher, die ihren Betrieb zukunftssicher aufstellen wollen. Der parallel zur Feuertrutz stattfindende Brandschutzkongress, organisiert von RM Rudolf Müller Medien GmbH & Co. KG, findet als größte und vielfältigste Fortbildungsveranstaltung der Branche wie gewohnt auch 2026 parallel zur Feuertrutz im Messezentrum Nürnberg statt. www.nuernbergmesse.de

Wagner veröffentlicht Nachhaltigkeitsbericht

Die Wagner Group GmbH setzt ein deutliches Zeichen für verantwortungsvolles unternehmerisches Handeln: Mit der Veröffentlichung des ersten Nachhaltigkeitsberichts für das Geschäftsjahr 2024/25 nach dem VSME ESRS (Voluntary Small and Medium Enterprise European Sustainability Reporting Standard) dokumentiert das international tätige Familienunternehmen umfassend die ökologischen, sozialen und ökonomischen Leistungen des vergangenen Geschäftsjahres. Mit dem Nachhaltigkeitsbericht, der die Aktivitäten der Wagner-Gesellschaften in Deutschland darstellt, schafft das Unternehmen Transparenz über erreichte Fortschritte, Handlungsfelder und Maßnahmen innerhalb seiner Nachhaltigkeitsstrategie. Der Bericht verdeutlicht zugleich, wie eng Nachhaltigkeit und die Kernaufgabe des Unternehmens miteinander verbunden sind: Wirksamer Brandschutz schützt nicht nur Menschen, Werte und Prozesse, sondern bewahrt Ressourcen, vermeidet Umweltbelastungen und leistet damit aktiv einen Beitrag für die Umwelt – ganz im Sinne des Leitgedankens Brandschutz ist Umweltschutz.

www.wagnergroup.com



Wirtschaftliche Brandschutzlösungen

Inotec Sicherheitstechnik zeigte auf den VdS-Brandschutztagen in Köln praxistaugliche Antworten auf die Frage, wie sich Brandschutz und Wirtschaftlichkeit miteinander verbinden lassen. Richtungsvariable Sicherheitsbeleuchtung steigert nicht nur den Personenschutz, sondern kann gleichzeitig die Gesamtbaukosten deutlich reduzieren. Denn dynamische Fluchtweglenkungssysteme bieten eine wirtschaftliche Möglichkeit, bauliche Anforderungen zu kompensieren, die im Neubau oder im Bestand nur mit hohem Aufwand umsetzbar wären. In vielen Gebäuden lassen sich aktuelle bauordnungsrechtliche Vorgaben – etwa zusätzliche Treppenträume oder erweiterte Rettungswegführungen – nur mit erheblichem technischen und finanziellen Aufwand erfüllen. Dynamische Fluchtweglenkungssysteme können diese Maßnahmen teilweise ersetzen, indem sie im Brandfall automatisch sichere Fluchtrouten anzeigen und gefährdete Bereiche sperren. www.inotec-licht.de



Brandschutz
vorausgedacht.



Sinfiro

BRANDSCHUTZINGENIEURE

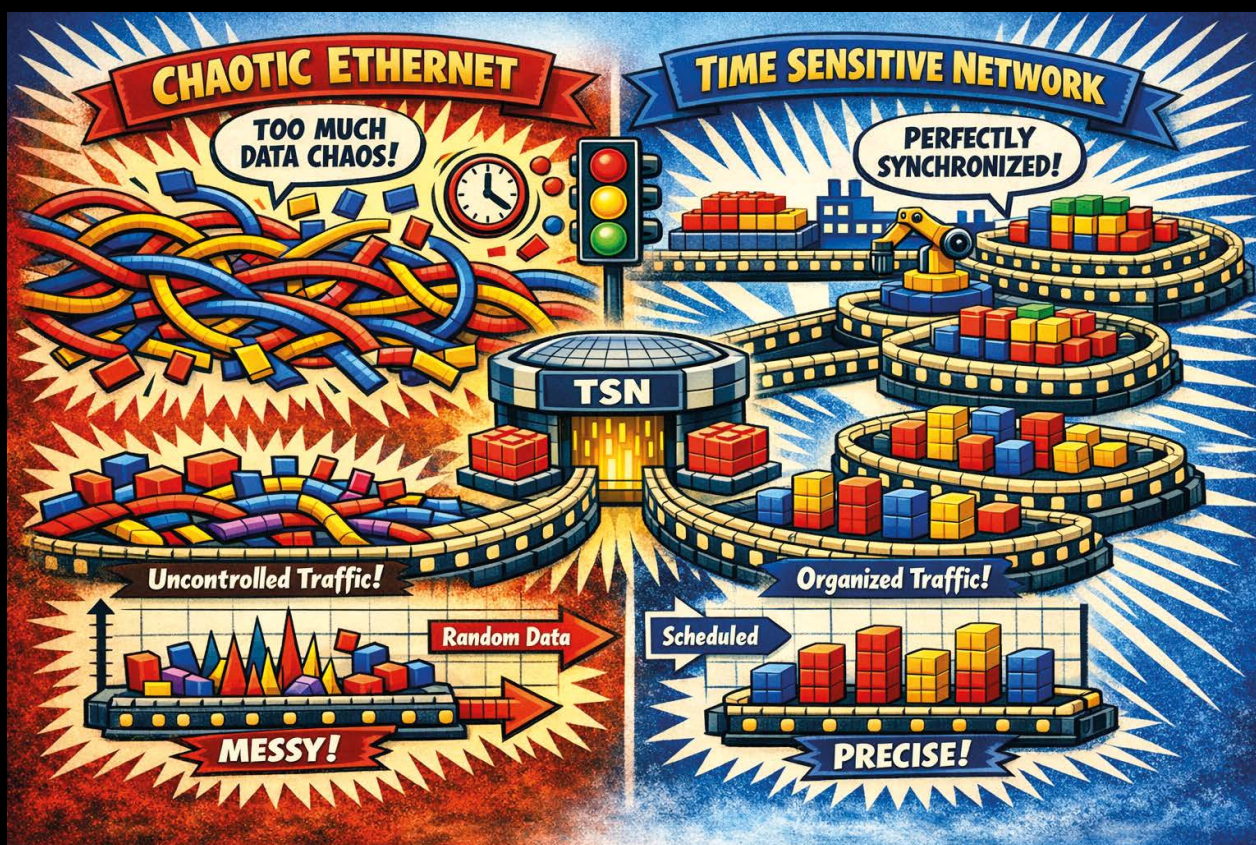
Sinfiro entwickelt individuelle Sicherheitslösungen im Bereich **Brandschutzplanung** für private, gewerbliche und kommunale Auftraggeber.

KONTAKT:

Sinfiro GmbH & Co. KG
Ebertstraße 2 | 72336 Balingen
info@sinfiro.de | sinfiro.de



sinfiro.de



© Generated with AI using Microsoft Copilot

Die Digitalisierung und IT/OT-Integration stellen neue Anforderungen an die industrielle Kommunikation in Maschinen und Anlagen: Neben Funktionaler Sicherheit und Cybersecurity rücken große – parallel zu übertragende – Datenmengen sowie steigende Erwartungen an Betriebssicherheit und Verfügbarkeit in den Fokus. Hier setzt Time-Sensitive Networking (TSN) an: Deterministische Kommunikation in Ethernet-basierten Netzwerken liefert die Grundlage für sichere und zuverlässige Automatisierungslösungen.

Die Artikel-Serie in Kooperation von VDMA Elektrische Automation und GIT SICHERHEIT gibt eine Einführung in die Technologie, beleuchtet verschiedene Anwendungsszenarien und zeigt anhand von drei Industrial-Ethernet-Ökosystemen, worauf es bei Auswahl und Einsatz von TSN zu achten gilt.

VDMA-Ansprechpartner Birgit Sellmaier betreut im Fachverband Elektrische Automation Technologiethemata wie Steuerungstechnik und Funktionale Sicherheit in der Anwendung im Maschinenbau.

Time-Sensitive Networking – TSN in der Anwendung

Zukunftstechnologie für die industrielle Kommunikation

Die fortschreitende Digitalisierung der Produktion führt zu wachsenden und unterschiedlichen Datenströmen. Neben klassischen zeitkritischen Steuerungs- und I/O-Daten müssen zunehmend auch datenintensive Anwendungen wie Bildverarbeitung sowie Zustands- und Diagnosedaten parallel übertragen werden. Gleichzeitig wächst der Bedarf, Produktionsdaten über die Maschine hinaus zu nutzen. Damit steigen die Anforderungen an industrielle Kommunikationsnetze: Sie müssen deterministische Echtzeit, hohe Datenlasten und die Konvergenz von IT und OT zuverlässig unterstützen. Time Sensitive Networking (TSN) adressiert diese Herausforderungen.



Christoph Behler,
Business Development
Manager bei CLPA



Florian Frick,
Oberingenieur, Gruppenleiter
„Echtzeitkommunikation und
Steuerungshardware“ beim ISW



Heiko Henkel,
Head of Product
Management Chip
bei Hilscher



Konrad Heidrich,
System Architect
bei Hilscher

■ Produktionsdaten werden zur treibenden Kraft der Fabrik der Zukunft und machen Prozesse messbar, schneller und flexibler. Für Maschinenhersteller in Branchen wie Automotive, Nahrungsmittel- und Getränkeindustrie, Halbleiterfertigung und vielen weiteren bringt das neue Herausforderungen mit sich. Digitalisierung ist dabei der gemeinsame Nenner.

Mit der Digitalisierung ändern sich auch die Anforderungen an Kommunikationsnetze: Neben zyklischen Steuerungs- und I/O-Daten kommen zusätzliche Datenströme hinzu – etwa Kamerabilder sowie Zustands- und Diagnosedaten aus Sensoren und Geräten. Das erhöht die Last im OT-Netz (Operational Technology auf der Feldebene). Gleichzeitig wächst der Bedarf, Daten außerhalb der Maschine zu nutzen – etwa für Analysen, Visualisierung oder Wartung in IT-nahen Diensten. Heute übermitteln Feldbusse und Industrial-Ethernet-Varianten sowohl zeitkritische als auch nicht zeitkritische Maschinen- und Produktionsdaten im Shopfloor. Doch die Landschaft ist heterogen und oft proprietär; viele Systeme sind untereinander und zur IT bedingt kompatibel. Deshalb existieren häufig getrennte IT- und OT-Netze. Die Kopplung ist aufwendig – Kosten entstehen,

bevor der eigentliche Nutzen der Daten erschlossen wird.

Die Konvergenz zwischen IT und OT – also die Zusammenführung von Produktionstechnik, -diensten und -daten mit IT-Systemen – gilt branchenübergreifend als Schlüssel: Ein gemeinsames Netz soll zeitkritische und nicht zeitkritische Daten parallel transportieren. So lassen sich IT-Dienste und -Methoden im Shopfloor effizienter nutzen, wie zum Beispiel virtualisierte Steuerungsfunktionen, Condition Monitoring, Diagnose oder Bildverarbeitung (Videostream). Zudem profitieren Cybersecurity und Safety-Funktionen von einer konsistenten Netzarchitektur. Und auch Edge-KI benötigt parallel stabile Kommunikation. Voraussetzung ist, dass die eingesetzten Technologien sowohl deterministische Anforderungen (vorhersagbare Latenzen und Jitter) als auch IT-Anforderungen erfüllen.

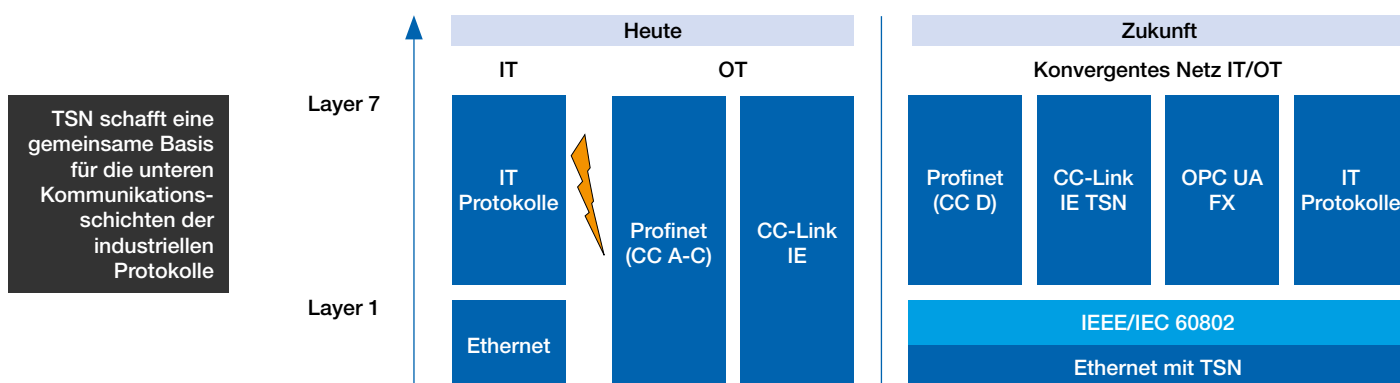
Time-Sensitive Networking

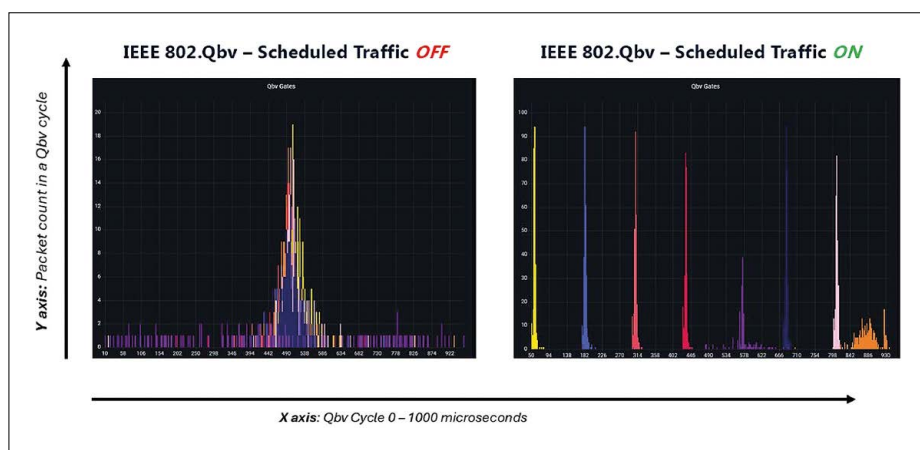
Time-Sensitive Networking (TSN) erweitert das Standard-Ethernet (IEEE 802.1) um deterministische Kommunikation. Dabei geht es vor allem um Synchronisation, Robustheit sowie garantierte Latenzen und kontrollierte Jitter. TSN entstand aus Lösungen im professionellen

Bitte umblättern ►

TSN-Mechanismen einfach erklärt

- Zeitsynchronisation (IEEE 802.1AS) ist ein zentraler Baustein und sorgt dafür, dass alle Geräte im Netzwerk exakt die gleiche Zeitbasis verwenden. So werden alle Beteiligten synchronisiert, und Daten können planbar übertragen werden.
- Der Time-Aware Shaper (IEEE 802.1Qbv) teilt die verfügbare Zeit im Netzwerk in feste Zeitfenster pro Zyklus ein. In jedem Zeitfenster dürfen nur bestimmte Datenklassen übertragen werden. Dadurch erreichen priorisierte Daten stets rechtzeitig ihr Ziel.
- Frame Preemption (IEEE 802.1Qbu) ermöglicht es, weniger wichtige Daten kurz zu unterbrechen, wenn zeitkritische Daten übertragen werden müssen. So werden Verzögerungen vermieden.
- Für Ausfallsicherheit sorgt Frame Replication and Elimination (IEEE 802.1CB). Dabei werden wichtige Daten über verschiedene Wege mehrfach versendet. Kommen Daten über einen Weg nicht an, ist trotzdem noch eine Kopie vorhanden.





TSN erlaubt eine zeitliche Isolation verschiedener Datenströme und verhindert Kollisionen und Datenverluste

Audio-Video-Bereich (AVB) und überträgt deren Prinzipien auf deterministische Kommunikation im Allgemeinen. Es verändert nicht die grundlegende Funktionsweise von Ethernet, sondern ergänzt die unteren Kommunikationsschichten in Switches und Endgeräten, um deterministische und somit planbare Kommunikation zu ermöglichen.

Für industrielle Automatisierung, Automotive-Anwendungen (In-Car-Ethernet) und die Luftfahrt wurden geeignete TSN-Profilen definiert. Das Industrial Profile IEC/IEEE

60802 für die Produktionstechnik soll im Jahr 2026 final veröffentlicht werden. Um Nutzbarkeit und Interoperabilität sicherzustellen, arbeitet die TSN Industrial Automation Conformance Collaboration (TIACC) an Konformitätstests und Zertifizierungen. In der TIACC kooperieren u. a. Avnu Alliance, CLPA (CC-Link Partner Association), ODVA, OPC Foundation und PI (PROFIBUS & PROFINET International).

TSN kann zudem die Betriebssicherheit erhöhen: Neben Determinismus tragen Redundanz und Überwachungsmechanismen zur Verfügbarkeit bei. Wichtig: TSN ermöglicht es, etablierte IT-Sicherheitskonzepte mit deterministischer Kommunikation zu kombinieren. Dazu zählen Segmentierung, Authentifizierung und Zugriffskontrolle.

TSN in der Industrie

In der Automatisierung treffen verschiedene Anforderungen und Datenarten aufeinander: Motion Control mit kurzen, stabilen Zykluszeiten, I/O-Daten mit festen Takten, sporadische Diagnose-/Engineering-Daten sowie Vision-Daten, die eine hohe Last erzeugen. All das muss parallel in einem konvergenten Netz funktionieren – ohne die Echtzeit zu gefährden. TSN liefert dafür die Transportmechanismen, um verschiedene Datenklassen planbar und störungsarm, d. h. deterministisch zu übertragen.

Wichtig: TSN ist kein Feldbusersatz. Feldbus-Ökosysteme umfassen neben dem Transport auch obere Schichten, Profile, Dienste, Geräteverhalten sowie Tools und Communities. Etablierte industrielle Protokolle wie PROFINET, CC-Link IE TSN, Ethernet/IP oder OPC UA verfolgen unterschiedliche Ansätze, um TSN-Vorteile zu nutzen:

- PROFINET und CC Link IE TSN integrieren TSN-Funktionalität in ihr Ökosystem; dieser Ansatz ist bereits heute praktisch einsetzbar.
- OPC UA betrachtet das Netzwerk als unabhängige Ressource, in der mittels

Management deterministische Verbindungen eingerichtet werden können. Ziel ist eine hohe Interoperabilität verschiedener Echtzeitanwendungen im selben Netz.

Mit allen Ansätzen lässt sich Konvergenz für nicht zeitkritische (Best-Effort-)Daten erreichen – eine Voraussetzung für durchgängige Anwendungen von der Feldebene bis zur Cloud.

Hardware und Software-Lösungen

Um TSN zu nutzen, braucht es Switches, die TSN-Funktionalitäten im Netz unterstützen, passend zum für die Anwendung gewählten Ökosystem.

Endpunktseitig werden die Hardwareanforderungen häufig überschätzt. In vielen Anwendungsfällen genügt Hardware mit einer Zeitstempereinheit und passenden Software-Stacks; bei höheren Anforderungen sind zusätzliche Funktionen – etwa zeitbasiertes Senden – sinnvoll. Bereits heute gibt es Switches, Endgeräte-Chips (z. B. für Remote-I/O-Module, Antriebe, Roboter, HMI), Betriebssysteme mit TSN-Support sowie Software-Stacks für höhere Protokollschichten. Konfigurations- und Diagnose-Werkzeuge helfen, Streams zu planen, Zeitpläne zu erzeugen und den Betrieb zu überwachen.

Per geeigneter Netz- oder Gateway-Konfiguration lassen sich bestehende Systeme mit TSN kombinieren – so lässt sich ein früher und risikoarmer Übergang realisieren, ohne bestehende Investitionen zu gefährden.

Von der Vision zur industriellen Realität

TSN unterstützt die IT/OT-Konvergenz und damit die Digitalisierung der Produktion. Die Standards haben inzwischen einen fortgeschrittenen Reifegrad erreicht, Hard- und Software sind verfügbar, und industrielle Kommunikationslösungen – von PROFINET über CC-Link IE TSN bis OPC UA – zeigen, wie sich TSN-Vorteile nutzen lassen, während bestehende Investitionen geschützt bleiben. Gleichzeitig eröffnen sich neue Möglichkeiten: von interoperablen, deterministischen Netzen über Edge-KI bis zur Cloud-Integration. Jetzt ist ein guter Zeitpunkt, sich strategisch mit TSN zu befassen und industrielle Netzwerke zukunftssicher auszurichten. **GIT**

TSN Vorteile für Anwender

- Deterministische Kommunikation: Vorhersagbare Latenzen und geringer Jitter für zeitkritische Anwendungen.
- Konvergente Netzwerke: Ein gemeinsames Netz für zeitkritische und nicht zeitkritische Daten.
- Hohe Verfügbarkeit: Redundanz und Überwachungsmechanismen erhöhen die Ausfallsicherheit.
- Präzise Synchronisation: Gemeinsame Zeitbasis für planbare und abgestimmte Übertragungen.
- Kompatibel mit bestehenden Protokollen: Nutzung mit PROFINET, CC-Link IE TSN, EtherNet/IP und OPC UA.
- Geeignet für moderne Anwendungen: Robuste Basis für Bildverarbeitung, Edge-KI und Condition Monitoring.
- Große Auswahl an Komponenten: Breites Ökosystem aus Switches, Chips, Software-Stacks und Tools erleichtert die Umsetzung.
- Kostenvorteile für Anwender: TSN nutzt Standard-Chips, Standard-Ethernet Treiber und handelsübliche Netzkomponenten.



ISW, Universität Stuttgart
www.isw.uni-stuttgart.de

CC Link Partner Association
Europe (CLPA)
www.cc-link.org

Hilscher Gesellschaft für
Systemautomation mbH
www.hilscher.com

Safety First in der Automation: LED-Signalleuchten



Die Signalsäulen der Serie LD6A von Apem/IDEC kombinieren ein modernes, funktionales Design mit hoher Signalwirkung und einfacher Handhabung. Sie dienen der klaren optischen Signalisierung von Maschinen- und Anlagenzuständen und sorgen für eine zuverlässige visuelle Kommunikation in industriellen Umgebungen – von der Produktionslinie bis zur Fertigungszelle. Das elliptische Linsensystem sorgt für eine deutliche optische Abgrenzung

zwischen beleuchteten und unbeleuchteten Zuständen. Eine spezielle Kombination aus streuender Diffusorlinse und bündelnder Kondensorlinse erzeugt eine besonders helle, gleichmäßige Lichtverteilung, die aus allen Richtungen gut erkennbar ist. Ein integrierter Lichtleiter verstärkt zusätzlich die Sichtbarkeit, wenn die Signalsäule von unten betrachtet wird – ideal bei der Montage über Augenhöhe.

www.apem.de

Sace Emax 3: Schaltzentrale für adaptive Energieverteilung



Der offene Leistungsschalter ABB Sace Emax 3 von ABB bündelt präzise Messtechnologie, zuverlässige Schutzfunktionen und hohe Verfügbarkeit in einer Plattform, die sich nahtlos in bestehende Systeme einfügt und für künftige Anwendungen erweitert werden kann. Aus einem Leistungsschalter wird die intuitiv bedienbare Schaltzentrale der Anlage: adaptiv, sicher und zuverlässig – bereit für die Herausforderungen von

morgen. Der ABB Sace Emax 3 vereinfacht die Bedienung und macht Funktionen im Feld erweiterbar ohne lange Stillstände. Er macht Schluss mit dem umständlichen Parametrieren von Schutzfunktionen per DIP-Schalter: Statt auf winzige Hebel, Kombinationscodes und verschachtelte Menüs setzt der Sace Emax 3 auf ein modernes HMI und ersetzt Schalterlogik durch ein intuitiv bedienbares Touch-Display. Konfiguration, Diagnose und Analyse werden direkt am Gerät realisiert, über die EPiC Mobile App am Smartphone oder die Ekip Connect Software am Laptop.

www.abb.com

Smarte Sicherheit und starke Systeme

Stöber zeigt auf der all about automation in Friedrichshafen einen Auszug seines breiten Portfolios – von einzelnen Komponenten bis zum kompletten Antriebssystem. Um die eigenen Präzisions- und Qualitätsansprüche zuverlässig zu erfüllen, fertigt der Antriebsspezialist viele Komponenten selbst. Zu den Exponaten am Messestand des Unternehmens gehört das Sicherheitsmodul SX6.

Damit lassen sich nun alle Antriebsregler der 6. Generation und somit auch seit Kurzem das Stand-alone-Gerät SB6 in sicherheitsrelevanten Anwendungen bis SIL 3, PL e (Kat. 4) nach DIN 61800-5-2 und DIN EN ISO 13849-1 einsetzen. Das Modul überwacht Bewegungen, führt Achsen zuverlässig in sichere Zustände und lässt sich über die integrierte Fail Safe over Ethercat (FSOE)-Schnittstelle nahtlos in Ethercat-basierte Automationssysteme einbinden.

www.stoeber.de



SAFEMASTER W Funk-Sicherheitssystem RE 6900

- Für Sicherheitsanwendungen bis Kat. 4 / PL e bzw. SIL 3
- Sichere Not-Halt-Funkübertragung
- 3-stufiger Funk-Zustimmtaster
- Maximale Bewegungsfreiheit bei höchster Sicherheit
- Ergonomisches Design für ermüdungsfreies Arbeiten



www.dold-safety.de

EVENT

Verdichtet statt verteilt

Neues Hallenkonzept, klare Themencluster: Wie die Hannover Messe 2026 dem Wandel in der Messelandschaft in Deutschland begegnet

Die Messelandschaft in Deutschland verändert sich seit dem Ende der Corona-Pandemie zunehmend. Diesen Wandel spürt auch die Hannover Messe: Mit einem grundlegend überarbeiteten Hallenlayout, einer neuen Themenstruktur und einem klaren Fokus auf industrielle KI ist die Hannover Messe 2026 angetreten, um rückläufigen Besucher- und Ausstellerzahlen entgegenzuwirken. Dennoch gingen die Zahlen auch in diesem Jahr deutlich zurück. Zugleich zogen die meisten Aussteller, mit denen wir gesprochen haben, ein durchaus positives Resümee.

■ Statt einer breiten Streuung über das gesamte Gelände konzentrierte sich die Ausstellung in diesem Jahr auf einen kompakten West, Nord und Südteil des Areals. Die Hallen 2 bis 9 blieben geschlossen; genutzt wurden unter anderem die Hallen 11 bis 17 sowie 23 bis 27. Ziel war eine kürzere Wegeführung, mehr thematische Nähe und eine bessere Orientierung für Fachbesucher.

Inhaltlich gliederte die Deutsche Messe die Veranstaltung in diesem Jahr in drei zentrale Ausstellungsbereiche: Automation

& Digitalization, Energy & Industrial Infrastructure sowie Research & Technology Transfer. Automatisierung, Software, industrielle Kommunikation und IT/OTSecurity rückten dabei räumlich enger zusammen – ein Abbild dessen, was in der industriellen Praxis längst Realität ist.

Neu war zudem eine Defense Production Area, in der erstmals Produktionstechnologien für sicherheits- und verteidigungsrelevante Anwendungen thematisiert wurden – ein Zeichen dafür, wie stark geopolitische

Rahmenbedingungen inzwischen auch industrielle Fachmessen prägen.

Kernthemen 2026: Industrielle KI, Safety, Cybersecurity

Inhaltlich zog sich Künstliche Intelligenz wie ein roter Faden durch nahezu alle Hallen. Neben klassischer Datenanalyse standen vor allem Physical AI, autonome Robotik, KIgestützte Assistenzsysteme sowie die sichere Integration von Software in bestehende Maschinenparks im Fokus.



Safety und SecurityAspekte wurden dabei zunehmend mitgedacht – etwa bei vernetzten Robotersystemen oder cloudbasierten Steuerungen.

Bei Gesprächen mit Unternehmen wie Pepperl+Fuchs, Pilz, Phoenix Contact, Lapp, SEW Eurodrive, Igus, Wibu, Bihl+Wiedemann, SySS und Innok Robotics wurde deutlich, dass funktionale Sicherheit, industrielle Cybersecurity und Resilienz nicht mehr als Zusatzthemen verstanden werden, sondern als Voraussetzung für Automatisierung und KI-Einsatz. Sicherheitskonzepte wurden dabei weniger als Produktversprechen, sondern als integraler Bestandteil von Systemarchitekturen diskutiert.

Zahlen, Daten, Internationalität

Nach Angaben des Veranstalters besuchten rund 110.000 Menschen die Hannover Messe 2026. Damit lag die Veranstaltung deutlich unter dem Vorjahreswert von 123.000 Besuchern. Als Gründe nannten die

Veranstalter unter anderem Warnstreiks im Flug und Nahverkehr sowie eine insgesamt zurückhaltendere Reisetätigkeit.

Bemerkenswert blieb der internationale Anteil von rund 40 Prozent, insbesondere aus China, Brasilien, den USA, Japan und Südkorea. Das Partnerland Brasilien setzte zusätzliche Akzente in den Bereichen Energie, Automatisierung und industrielle Transformation.

Auch die Zahl der Aussteller ging zurück: Rund 3.000 bis 3.500 Unternehmen präsentierten sich 2026. Als Konsequenz kündigte die Deutsche Messe an, die Hannover Messe ab 2027 auf vier Tage zu verkürzen und noch fokussierter auszurichten.

Fazit und Hannover Messe 2027

Die Hannover Messe 2026 war keine Messe der Superlative, sondern der Neujustierung. Weniger Fläche, weniger Besucher – dafür klarere Themen, dichtere Gespräche und ein stärkerer Fokus auf industrielle Umsetzbarkeit. Für die Sicherheitsbranche zeigte sich

deutlich: Ohne Safety, Security und Resilienz ist weder KI noch Automatisierung zukunftsfähig.

Diese Neuausrichtung wird 2027 konsequent fortgeführt. Die nächste Hannover Messe findet vom 5. bis 8. April 2027 statt und wird erstmals auf vier Messetage verkürzt – von Montag bis Donnerstag. Mit diesem Schritt reagiert die Deutsche Messe AG auf veränderte Besucherstrukturen und will die Veranstaltung fokussierter, effizienter und näher an den industriellen Entscheidungen ausrichten.

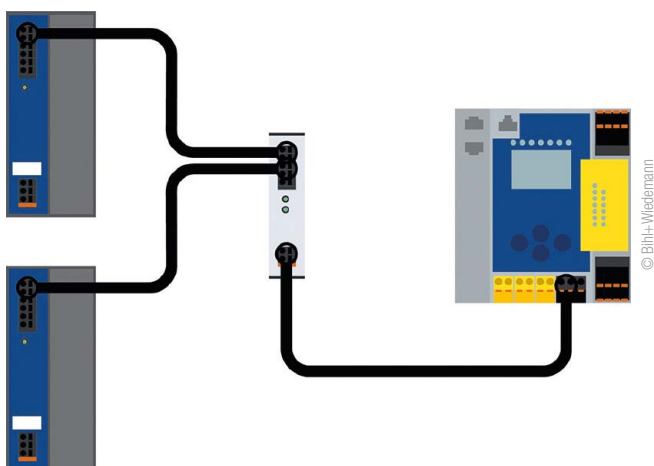
Als Partnerland 2027 ist Spanien vorgesehen. Inhaltlich sollen die Schwerpunkte Künstliche Intelligenz, Automatisierung, Robotik, Energieinfrastruktur sowie Safety und Security weiter vertieft werden. **GIT**



Deutsche Messe
www.hannovermesse.de

Anlagenverfügbarkeit mit dem 30-V-Redundanzmodul BW5182

Ein unerwarteter Maschinenstillstand kann teuer werden. Nicht selten ist der Auslöser dafür ein defektes Netzteil. Mit dem 30-V-Redundanzmodul BW5182 von Bihl+Wiedemann wird das ASi Gateway – und damit die gesamte Anlage – wirkungsvoll vor Ausfällen geschützt und so für dauerhaft hohe Verfügbarkeit und mehr Betriebssicherheit bei minimalem Aufwand gesorgt. Das kompakte Redundanzmodul in IP20, das ohne aufwendige Umbauten im Schaltschrank untergebracht und damit problemlos in bestehende Installationen eingebunden werden kann, erlaubt den Anschluss von zwei 30-V-Netzteilen mit jeweils bis zu 8 A. Fällt ein Netzteil aus, übernimmt automatisch das zweite – ohne Unterbrechung und ohne manuelles Eingreifen. Durch die integrierte aktive Entkopplung der Netzteile im Modul ist so eine stabile, redundante Stromversorgung des Gateways gewährleistet. www.bihl-wiedemann.de



Radarsystem LBK: sicher auch bei Staub und Rauch

Das Radarsystem LBK von Leuze ist auch mit CIP-Safety-Schnittstelle erhältlich. Personen im Gefahrenbereich werden durch das 3D-Radarsystem selbst bei rauen Bedingungen zuverlässig detektiert – statische Objekte führen nicht zur Abschaltung. Es erkennt die Körper von Personen selbst unter rauen Umgebungsbedingungen und überwacht den Schutzbereich auf Zugang und Anwesenheit. Praktisch: Die Radar-Technologie detektiert sowohl sich bewegende als auch stillstehende Personen – statische Objekte wie Paletten oder Behälter führen dagegen nicht zu einer Abschaltung des Sicherheitssignals. Außerdem lassen sich dank des 3D-Radar-Prinzips auch Bereiche an Stufen, Sockeln und hinter nicht-metallischen Abschattungen überwachen. Teil des Sicherheits-Radarsystems LBK ist ein separater Controller. Der Controller ist auch mit integrierter CIP-Safety-Schnittstelle erhältlich. www.leuze.com



COMPUTER VISION

Am Wendepunkt

Von Kontext bis Edge-KI: Computer Vision in der Industrie

Computer Vision steht an einem Wendepunkt: In den kommenden Jahren wird sich die Technologie von einer rein visuellen Beobachtungslösung zu einem integralen Bestandteil industrieller Datenarchitekturen entwickeln. Für industrielle Anwender eröffnet diese Entwicklung neue Möglichkeiten, Prozesse effizienter zu steuern, Sicherheit zu erhöhen und bestehende Anlagen schrittweise zu modernisieren. Wie moderne visuelle Sensorik diesen Wandel unterstützt und welchen strategischen Mehrwert sie in komplexen Produktionsumgebungen schaffen kann, zeigt Gabriele Mangiafico, Business Development Manager EMEA bei Axis Communications im Folgenden auf.



Gabriele Mangiafico,
Business Development Manager
EMEA bei Axis Communications

■ Drei Entwicklungen werden den Einsatz von Computer Vision in industriellen Umgebungen in den kommenden Jahren maßgeblich prägen. Eine davon ist das stärkere Zusammenspiel visueller Intelligenz mit anderen betrieblichen Signalen. Denn erst wenn visuelle Daten mit Maschinenzuständen, Alarmen, Umgebungsdaten und Workflow-Ereignissen verknüpft werden, liefern sie für Hersteller belastbare betriebliche Erkenntnisse statt isolierter Einzelinformationen. Computer Vision wird damit von einem reinen Beobachtungswerkzeug zu einem relevanten Baustein für Prozessoptimierung, Arbeitssicherheit sowie Fernwartung und -unterstützung.

KI in Edge-Computing-Umgebungen
Gleichzeitig wird KI in Edge-Computing-Umgebungen stark an Bedeutung gewinnen. Leistungsfähigere Chipsätze und eine bessere Verarbeitung auf dem Gerät selbst ermöglichen es, immer fortschrittlichere Analysen direkt dort auszuführen, wo die Daten erfasst werden. Dadurch steigen nicht nur Reaktionsgeschwindigkeit, Skalierbarkeit und häufig auch die Kosteneffizienz. In industriellen Umgebungen sinkt zugleich die Abhängigkeit von zentraler Infrastruktur, während Datenminimierung und die Analyse in unmittelbarer Nähe zu Maschinen und Prozessen erleichtert werden – ein Vorteil, der sich insbesondere in

Brownfield-Umgebungen und dezentralen Produktionsumgebungen bemerkbar macht.

Unternehmen können so Ereignisse früher erkennen und gezielter entscheiden, welche Daten überhaupt übertragen oder gespeichert werden müssen. Gerade in industriellen Anwendungen, in denen Erkenntnisgewinn, Infrastrukturkosten, Reaktionsfähigkeit und Datenschutz sorgfältig austariert werden müssen, ist das ein wichtiger Hebel für effizientere Prozesse.

Kontextbezogenes Verständnis

Den größten Wandel stellt jedoch der Übergang von reiner Erkennung hin zu kontextbezogenem Verständnis dar. Denn heute ist nicht mehr entscheidend, dass ein System einfach nur Bewegungen oder Objekte erkennt. Entscheidend ist, ob es Ereignisse im betrieblichen Kontext interpretieren kann – zum Beispiel indem es zwischen einem routinemäßigen Linienstillstand, einem sicherheitskritischen Vorfall und einem Engpass im Materialfluss unterscheidet oder eine routinemäßige Schwankung von einer Prozessabweichung erkennt, die das Eingreifen eines Mitarbeiters erfordert und entsprechend automatisiert einen Workflow anstößt oder eine Benachrichtigung auslöst.

Genau darin liegt das strategische Potenzial moderner Netzwerk-Kameras, die sich in industriellen Umgebungen zunehmend

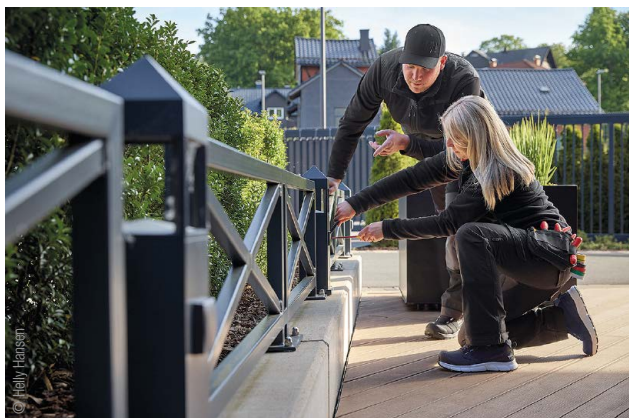
von reinen Aufzeichnungsgeräten zu intelligenten visuellen Sensoren innerhalb der industriellen Datenarchitektur entwickeln. Sie tragen dazu bei, den Hergang von Ereignissen zu rekonstruieren und Ursachen präziser zu analysieren. Insbesondere in Produktionsumgebungen, in denen klassische Maschinen- und Steuerungsdaten zwar ein Ereignis melden, aber häufig nicht den erforderlichen Kontext liefern, schafft das erheblichen Mehrwert.

Die eigentliche Chance liegt jedoch nicht darin, ein weiteres isoliertes Analysetool hinzuzufügen, sondern visuelle Daten für Sicherheit, Betrieb und Prozessoptimierung nutzbar zu machen – gerade in Umgebungen, in denen Hersteller ihre bestehende Infrastruktur schrittweise modernisieren müssen, anstatt sie vollständig zu ersetzen.

Entscheidend wird sein, dass sich diese Fortschritte in der industriellen Praxis als zuverlässig, transparent und sicher erweisen. In industriellen Umgebungen ist Innovation nur dann relevant, wenn sie sich in messbarem betrieblichem Nutzen niederschlägt.“ **GIT**



Axis Communications
www.axis.com



Oxford 2.0 Kollektion von Helly Hansen

Helly Hansen präsentiert zur Saison Frühjahr/Sommer 2026 eine überarbeitete Linie, die genau das bietet, worauf es beim Arbeitsalltag ankommt – Komfort, Langlebigkeit und Funktionalität. Die Oxford 2.0 Kollektion wurde in enger Zusammenarbeit mit Handwerkern und Fachkräften aus der Industrie entwickelt. Die neuen Oxford 2.0 Styles sind auf anspruchsvolle Einsätze in unterschiedlichsten Arbeitsumgebungen zugeschnitten. Alle Produkte bestehen aus einem baumwollreichen Hauptmaterial, das durch seine hohe Atmungsaktivität auch bei körperlich fordernden Tätigkeiten angenehm zu tragen ist – ideal für warme oder wechselhafte Bedingungen. Cordura-Verstärkungen an Hose, Shorts und Latzhose sorgen für zusätzliche Strapazierfähigkeit. Die Oxford 2.0 Arbeitsjacke kommt ohne Schulternähte, mit verlängertem Rücken, elastischen Einsätzen und weichem Fleecefutter im Kragen – für hohe Bewegungsfreiheit und Tragekomfort.

www.hhworkwear.com



FeuerTrutz 2026: Asecos setzt auf praxisnahen Wissenstransfer

Die Asecos GmbH ist auch 2026 auf der FeuerTrutz in Nürnberg vertreten. Das Unternehmen stellt den Wissenstransfer zur sicheren Gefahrstofflagerung in den Mittelpunkt seines Messeauftritts. Neben Produktlösungen für die sichere Lagerung von brennbaren Flüssigkeiten und Lithium-Ionen-Akkus erwartet die Besucher ein umfangreiches Vortragsprogramm des „Forum by asecos academy“. Der sichere Umgang mit Gefahrstoffen erfordert fundiertes Fachwissen. Das „Forum by asecos academy“ greift wichtige Fragestellungen aus dem Arbeitsalltag auf und vermittelt konkrete Lösungsansätze für ein sicheres Gefahrstoffmanagement. Die Vorträge sind an beiden Messetagen kostenlos zugänglich. Zum Auftakt steht ein Live-Experimentvortrag auf dem Programm, der anhand von Explosionen, Verpuffungen und Co. veranschaulicht, welche Risiken bereits geringe Gefahrstoffmengen bergen können. Ziel ist es, ein vertieftes Verständnis für die Risiken im Umgang mit Gefahrstoffen und Prozessen zu schaffen.

FeuerTrutz: Halle 4, Stand 4-436

www.asecos.com

Leichter Schutzanzug Tychem 6000 SFR

Dupont hat den Tychem 6000 SFR auf den europäischen Markt gebracht, einen leichten Schutzanzug mit Kapuze, der Arbeiter in schwierigen Umgebungen vor verschiedenen chemischen Gefahren und Stichflammen schützen soll. Tychem 6000 SFR Schutzanzüge sind besonders vorteilhaft in Umgebungen, in denen kombinierte Gefahren durch Chemikalien und Stichflammen ein ernstes Problem darstellen. Sie eignen sich für Anwendungen und Branchen, die einen Schutz gegen mehrere Gefahren erfordern, wie z. B. Raffinerien, Petrochemie-Anlagen, Labors, Wartungsarbeiten und Feuerwehren. Tychem 6000 SFR bietet einen Permeationsschutz von bis zu 30 Minuten gegen mehr als 250 chemische Gefahren, wie z. B. toxische Industriechemikalien, chemische Kampfstoffe und brennbare organische Lösungsmittel. Außerdem trägt der Schutzanzug auch zur sekundären Flammhemmung bei, wenn er über flammbeständiger Primärschutzkleidung (FR) getragen wird, wie z. B. aus Dupont Nomex.

www.dupont.com



TÜV-Verband veröffentlicht Leitfaden zu verunfallten Hochvoltbatterien

Mit der steigenden Zahl von Elektrofahrzeugen wächst die Bedeutung eines sicheren Umgangs mit Hochvoltbatterien, die bei einem Unfall beschädigt worden sind. Der TÜV-Verband hat hierzu einen Leitfaden veröffentlicht, der Sachverständigen und Gutachtern eine praxisnahe Orientierung für die Bewertung solcher Batterien bietet. „Nach einem Unfall können beschädigte Antriebsbatterien Brände, Stromschläge oder Leckagen mit giftigen Chemikalien auslösen“, sagt Robin Zalwert, Referent für nachhaltige Mobilität beim TÜV-Verband. „Die Batterie muss systematisch untersucht werden, um auch äußerlich unsichtbare Schäden zu erkennen.“ Auf dieser Basis können Werkstätten, Sachverständige und Halter entscheiden, ob eine Reparatur sinnvoll oder ein Austausch notwendig ist. „Verunfallte Hochvoltbatterien gehören zu den komplexesten Fällen in der Fahrzeugbewertung“, so Robin Zalwert. „Ohne klare Vorgaben besteht die Gefahr, technische Risiken zu unterschätzen oder wirtschaftlich falsche Entscheidungen zu treffen.“

www.tuev-verband.de



© TÜV-Verband | Robin Zalwert – Kfz-gefahren

SCHUTZHANDSCHUHE

Handschutz mit Herkunft: Showas Weg nach Deutschland

Wie Japans Handschutzspezialist durch Materialkompetenz und Produktionskontrolle den deutschen Markt erobern will



Philipp Heinemann, Country Manager DACH bei Showa

Showa ist ein traditionsreiches japanisches Unternehmen, das seit 1954 für qualitativ hochwertigen, innovativen und zunehmend nachhaltigen Handschutz steht. Im Interview erklärt Philipp Heinemann, Country Manager DACH bei Showa, wie der Hersteller mit seiner vollständig integrierten Fertigung, technologischen Alleinstellungsmerkmalen und einer starken Qualitätskultur den deutschen Markt erschließen will – und welche Strategien dabei den Unterschied zum starken Wettbewerb machen.



Das Mikrofaser-Innenfutter der MFT PRO-Reihe verbessert Komfort, Feuchtigkeitsmanagement und Tastgefühl

— GIT SICHERHEIT: Könnten Sie unseren Lesern zunächst einen kurzen Überblick über Showa geben – woher das Unternehmen stammt und was seine frühe Entwicklung geprägt hat?

Philipp Heinemann: Showa wurde 1954 in Japan gegründet und hat sich zu einem globalen Hersteller von Handschutz entwickelt, mit mehr als 70 Jahren Erfahrung und einer Präsenz auf zahlreichen internationalen Märkten. Von Anfang an verfolgte das Unternehmen eine klare Philosophie: „Immer innovativ. Niemals nachahmend.“

Ein prägendes Merkmal der Entwicklung von Showa ist sein vollständig integriertes Fertigungsmodell. Im Gegensatz zu vielen

Anbietern auf dem Markt entwickelt und produziert Showa seine Maschinen, Garne, Beschichtungen, Polymere und Handformer selbst im eigenen Haus. Dieser Ansatz hat sowohl die Qualität der Produkte als auch die Fähigkeit des Unternehmens geprägt, kontinuierlich innovativ zu sein.

Die Unternehmensgeschichte ist zudem von einer Reihe von Branchenneuheiten geprägt, darunter die Einführung des ersten PVC-Handschuhs, des ersten Einweg-Nitrilhandschuhs und des ersten biologisch abbaubaren Einweghandschuhs. In jüngerer Zeit spiegeln Innovationen wie das firmeneigene Mikrofaser-Innenfutter der MFT PRO-Reihe diesen anhaltenden Fokus auf Komfort, Leistung und Nachhaltigkeit wider.

Showa ist seit vielen Jahrzehnten tätig. Welche Momente oder Wendepunkte sehen Sie als besonders wichtig in der Unternehmensgeschichte an?

Philipp Heinemann: Aus einer marktorientierten Perspektive sind die wichtigsten Wendepunkte diejenigen, mit denen sich Showa deutlich von der Konkurrenz abgehoben hat. Ein Beispiel ist die Entwicklung der MFT PRO-Reihe. Die firmeneigene Mikrofasertechnologie stellt einen neuen Ansatz bei der Handschuhkonstruktion dar, insbesondere hinsichtlich der Kombination von Komfort, Atmungsaktivität und Haltbarkeit. Sie unterscheidet sich deutlich von Standardmaterialien und zeigt, wie Fasertechnik

die Leistung im täglichen Einsatz beeinflussen kann.

Eine weitere wichtige Entwicklung ist die kontinuierliche Investition in datengestützte Dienstleistungen wie ChemRest. Zwar sind Datenbanken zur chemischen Permeation kein Alleinstellungsmerkmal, doch die Bereitstellung detaillierter, anwendungsspezifischer Durchbruchdaten bietet Sicherheitsexperten eine fundiertere Entscheidungsgrundlage – insbesondere in Märkten wie Deutschland, wo eine datenbasierte Auswahl von PSA unerlässlich ist.

Showa betont oft, wie wichtig es ist, alles in eigenen Werken selbst herzustellen. Wie wirkt sich dieser Ansatz auf die Qualität und Zuverlässigkeit Ihrer Schutzhandschuhe aus?

Philipp Heinemann: Das Inhouse-Modell ist eines der wichtigsten Unterscheidungsmerkmale von Showa. Durch die Kontrolle jeder Produktionsstufe, von den Rohstoffen bis zur Endkontrolle, kann das Unternehmen einheitliche Qualitätsstandards anwenden.

In der Praxis führt dies zu geringerer Variabilität und höherer Zuverlässigkeit. Qualitätskontrollen lassen sich direkt umsetzen und bei Bedarf schnell anpassen – ein entscheidender Faktor bei sicherheitskritischen Anwendungen. Da Materialien und Prozesse intern entwickelt werden, können zudem Fasern, Beschichtungen und Ergonomie gezielt auf die Bedürfnisse der Anwender abgestimmt werden.

Wenn man andere Anbieter im Bereich Handschutz betrachtet, worin unterscheidet sich die Arbeitsweise oder Denkweise von Showa von den typischen Praktiken der Branche?

Philipp Heinemann: Einer der auffälligsten Unterschiede ist kultureller Natur. Showa ist ein Familienunternehmen mit starken japanischen Wurzeln, was sich in seinem Qualitätsansatz, langfristigem Denken und kontinuierlicher Verbesserung widerspiegelt. Es wird großer Wert auf Präzision gelegt, die über Mindestanforderungen hinausgeht. Anstatt branchenüblichen Standards zu folgen, ist das Unternehmen bereit, andere Wege zu gehen, wenn dies zu besseren Ergebnissen für den Anwender führt.

Diese Denkweise zeigt sich auch in Investitionen in Produktentwicklung, Nachhaltigkeit und Tools für den Kundensupport. Es geht nicht nur darum, Handschuhe zu liefern, sondern die Auswahl und Nutzung von Handschutz in realen Arbeitsumgebungen zu verbessern.

Showa expandiert stetig in Deutschland. Wie würden Sie den Prozess des Aufbaus Ihrer Präsenz hier beschreiben, und welchen Herausforderungen sind Sie begegnet?

Philipp Heinemann: Die aktuelle Entwicklungsphase in Deutschland konzentriert sich auf den Aufbau eines starken, aber ausgewählten Vertriebsnetzes sowie auf eine



Der CC700 kombiniert hohe Schnittfestigkeit mit zuverlässigem Chemikalienschutz in einem Handschuh

engere Zusammenarbeit mit Endnutzern.

Eine zentrale Priorität ist der Aufbau langfristiger Partnerschaften mit ausgewählten Händlern, die auf Vertrauen und Kooperation basieren, statt auf kurzfristigen Transaktionen.

Die größte Herausforderung ist die Markenbekanntheit. Im Vergleich zu etablierten Namen befindet sich Showa noch im Aufbau. Gleichzeitig wird die Unternehmenskultur, Produktqualität und technische Kompetenz oft als positiv anders wahrgenommen – insbesondere in einem Umfeld, in dem Zuverlässigkeit und Qualität stärker in den Fokus rücken.

Ihr Portfolio in Deutschland umfasst bereits Handschuhe wie die CC700- und die MFT PRO-Serie. Wie werden

diese Produkte angenommen, und welche Anwendungsbereiche treiben die Nachfrage an?

Philipp Heinemann: Die ersten Rückmeldungen sind sehr positiv, insbesondere nach praktischen Tests. Der CC700 hat großes Interesse geweckt, da er eine bekannte Herausforderung löst: Er kombiniert hohe Schnittfestigkeit mit zuverlässigem Chemikalienschutz in einem Handschuh – relevant für Anwendungen mit gleichzeitigen chemischen und mechanischen Risiken.

Die MFT PRO-Serie ist als Mehrzwecklösung für mechanische Anwendungen positioniert. Ihr Mikrofaser-Innenfutter verbessert Komfort, Feuchtigkeitsmanagement und Tastgefühl – wichtige Faktoren für Akzeptanz und lange Tragedauer.

Ein gemeinsamer Nenner ist, dass Anwender Unterschiede in Passform, Komfort und Qualität unmittelbar wahrnehmen. Die Aufgabe besteht nun darin, diese Eigenschaften breiter bekannt zu machen.

Welche Entwicklungen oder Veränderungen erwarten Sie für die Zukunft, die die Aktivitäten von Showa auf dem deutschen Markt prägen werden?

Philipp Heinemann: Ein wichtiger Teil der Strategie ist es, bestehende Lösungen sichtbarer und besser verständlich zu machen. So erfüllt die MFT PRO-Reihe bereits viele aktuelle Marktanforderungen an Komfort, Langlebigkeit und Nachhaltigkeit. Während der Branchentrend zu immer dünneren Handschuhen geht, setzt Showa darauf, Dünne und Langlebigkeit in Einklang zu bringen, um häufigen Austausch zu vermeiden. Auch Vorteile wie die durch selbst hergestellte Handschuhformern verbesserte Passform im Chemikalienschutz müssen bekannter werden.

Darüber hinaus werden Wachstum in Segmenten wie ESD-Schutz, Innovationen beim sicheren Ausziehen von Handschuhen sowie eine engere Zusammenarbeit mit Endnutzern durch Programme wie „Sentinel by Showa“ die künftigen Aktivitäten prägen. Nachhaltigkeit bleibt dabei ein zentrales Thema: Mit „Showa In Balance“ verfolgt das Unternehmen das Ziel, Umweltbelastungen zu reduzieren und gleichzeitig Leistungsstandards aufrechtzuerhalten – mit Fokus auf Langlebigkeit und Qualität als Mittel zur Abfallvermeidung. **GIT**



Showa

www.showagroup.com/eu-de



SCHUTZKLEIDUNG

70 Jahre Workwear von Kübler

Wie das Familienunternehmen seine Position im Markt für Arbeits- und Schutzbekleidung kontinuierlich ausbaut

In diesem Jahr feiert das Familienunternehmen Kübler sein 70-jähriges Bestehen. Anwender in Industrie, Handwerk und Dienstleistungsunternehmen verbinden Arbeitskleidung und Persönliche Schutzausrüstung des schwäbischen Herstellers mit Qualität, durchdachte Funktionen und hohem Tragekomfort.

■ Dass Kübler seit vielen Jahren eine wichtige Position im deutschen Markt einnimmt, beruht nicht nur auf der technischen Kompetenz bei Arbeits- und Schutzbekleidung, sondern auch auf dem steten

Austausch mit Fachhandelspartnern und Endkunden. Geänderte Anforderungen an Funktion, Strapazierfähigkeit und Design werden so schnell in praxisgerechte Bekleidungslösungen umgesetzt.

Die jüngst eingeführte Kollektion Kübler Reforce spiegelt die neuesten Trends im Markt wider. Mit ihrem nachhaltigen Gewebe und dem Einsatz industriewäscheoptimierter Materialien erfüllt sie die gestiegenen Erwartungen an Langlebigkeit und Reparierbarkeit bei hohem Tragekomfort. Das Design ist auf durchdachte Funktionalität statt modische Schnellebigkeit ausgerichtet. Die hochfunktionalen Stretch-Kollektionen, ermöglichen den Trägern Bewegungsfreiheit. Tragekomfort bieten auch die Multinorm- und Wetterschutz-Linien von Kübler und erzielen zugleich eine hohe Schutzwirkung unter Einsatz leichterer Gewebe.

Ganzheitliches Leistungsportfolio

Alle Produktlinien werden am Stammsitz in Plüderhausen von interdisziplinären Teams entwickelt. Neben den Abteilungen für Produktentwicklung beschäftigt Kübler dort hochqualifizierte Näherinnen.



Die in Plüderhausen regelmäßig im Rahmen des Kübler Campus stattfindenden Seminare rund um den Einsatz von Persönlicher Schutzausrüstung finden großen Anklang bei Fachhandelspartnern und Sicherheitsfachkräften

Davon profitieren Handelspartner und Endkunden in mehrfacher Hinsicht, etwa bei Programmergänzungen, anspruchsvollen Muster- und Sonderanfertigungen sowie bei der Fertigung von Bekleidungsteilen in Randgrößen. Die größeren Stückzahlen lässt Kübler überwiegend in Laos, Vietnam und Armenien fertigen. Damit setzt das Unternehmen auf langjährige, leistungsfähige Konfektionspartner mit klar definierten Qualitäts- und Sozialstandards.

Mit dem Beitritt zur Fair Wear Foundation bekennt sich das Unternehmen zur Verantwortung für die Menschen hinter den Produkten. „Die Mitgliedschaft in der Fair Wear Foundation ist ein klares Statement für faire Arbeitsbedingungen, Transparenz und kontinuierliche Verbesserung entlang unserer gesamten Lieferkette“, erklärt Kerstin Janßen, die Einkauf, Produktion und Nachhaltigkeit verantwortet. Verantwortungsvolle Produktion entstehe nicht durch bloße Zusagen, sondern durch konsequentes Handeln, ehrliche Bewertung des eigenen Status quo und die enge Zusammenarbeit mit den Lieferanten. Fair Wear verstehe man dabei als partnerschaftlichen Rahmen, der kontinuierliche Weiterentwicklung einfordere und fördere, so Janßen.

Weiterbildung im PSA-Bereich

Seit einigen Jahren ist eigens für den Wissenstransfer im PSA-Bereich der Kübler Campus ins Leben gerufen worden, der viel Zuspruch bei Fachhandelspartnern und Sicherheitsfachkräften findet. Im Rahmen von Seminaren vermittelt das Unterneh-



In der eigenen Fertigung in Plüderhausen werden spezifische Anforderungen der Kunden, wie zum Beispiel Bekleidungsteile in Randgrößen oder Programmergänzungen, umgesetzt

men umfassendes Know-how rund um den Einsatz von PSA, angefangen bei den gesetzlichen Pflichten gemäß neuesten Verordnungen, Haftungsrisiken, Normvorgaben für die verschiedenen Gefährdungsbereiche sowie Veredelung und Instandhaltung von Schutzbekleidung. Die PSA-Seminare sind vom deutschlandweit größten Verband für Sicherheit, Gesundheit und Umweltschutz bei der Arbeit, VDSI, mit Weiterbildungspunkten bewertet.

Auch künftig will man sich auf die Entwicklung und den Vertrieb hochwertiger Arbeits- und Schutzbekleidung konzentrieren. Damit verbunden ist die Fokussierung auf die Vertriebsbereiche Fachhandel und

Mietberufsbekleidung. „Die enge Partnerschaft mit dem technischen Fachhandel ist seit jeher eine zentrale Säule unseres Erfolgs im Markt“, erklärt CEO Richard Scheiner. Daneben hat sich die Sparte der Mietberufsbekleidung in den letzten Jahren zu einem wichtigen Absatzkanal entwickelt. In dieser Konstellation sieht Scheiner das Familienunternehmen gut aufgestellt „für gesundes, nachhaltiges Wachstum getragen von Qualität, Innovation und Verlässlichkeit“. **GIT**



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

© Bilder: Kübler

Sicherheitsschuh für schwere Anwendungen



© Uvex

Der PSA-Hersteller Uvex Safety hat mit dem Sicherheitsschuh Uvex 3 Mascole Boa einen Stiefel im Portfolio, der bei schweren Anwendungen glänzt. Für Langlebigkeit und Komfort sorgen zahlreiche Technologien des Heavy-Duty-Allrounders. Unebenes Gelände, extreme Witterungsbedingungen, chemische und mechanische Einflüsse: Je anspruchsvoller die Arbeitsumgebung ist, desto höher sind auch die Anforderungen an die persönliche Schutzausrüstung. Sicherheitsschuhe müssen in solchem Umfeld nicht nur Schutz bieten, sondern auch strapazierfähig, stabil und bequem sein. „Tough work. Easy going.“ – so beschreibt der global agierende fränkische PSA-Hersteller Uvex Safety sein neues Footwear-Highlight: den Uvex 3 Mascole Boa Schnürstiefel. Die Mascole Gummilaufsohle ist besonders hitze-, chemikalien-, und schnittbeständig. Die Sohlentechnologie bietet Rutschhemmung und sorgt für rutschfesten Stand auf extrem heißen wie kalten Untergründen.

www.uvex.de

HB-ArcSelect Pro: Verlässliche persönliche Schutzausrüstung

Die Kollektion HB-ArcSelect Pro von HB Protective Wear ist auf die besonderen Bedürfnisse von Störlichtbogenschutz ausgerichtet und in einem breiten Tätigkeitsfeld einsetzbar. Durch den hohen Baumwollanteil und den soften Griff des Materials entsteht ein sehr angenehmes Tragegefühl, vergleichbar mit Freizeitbekleidung. Die umfangreiche Schutzleistung, die Pflege mit Industriewäsche und die im Normenprofil ergänzte Nachtsichtbarkeit entsprechen den höchsten Ansprüchen an PSA und stehen für moderne multifunktionale Schutzbekleidung. Der zeitgemäße Look und die hochwertige Verarbeitung runden das Profil dieser Multi-Risk-Kollektion ab. www.hb-online.de



In **GIT Business Partner**, dem „Who is who in Sachen Sicherheit“, präsentieren sich Ihnen die kompetentesten Anbieter aus allen Bereichen der Sicherheit. Die hier vertretenen Firmen freuen sich über Ihre Kontaktaufnahme.

Alle Präsentationen, Einträge, Infos zum Unternehmen und Berichte über das jeweilige Unternehmen finden Sie auch im dazugehörigen Company Channel auf <https://git-sicherheit.de/de/business-partner> – mit Links zu den Unternehmen.

Sie gehören selbst zu den wichtigen Anbietern und wollen mit jeder Ausgabe mehr als 25.000 Entscheider direkt erreichen? Dann kontaktieren Sie uns für eine Präsentation.



© Vitaya_25 - stock.adobe.com

Sicherheitsmanagement



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 Sicherheitsfachrichter.

Sicherheitsmanagement



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



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

Service mit System



Sicherheitsmanagement



hensec – secure solutions
Luisenstr. 56, 76689 Karlsdorf-Neuthard
Tel.: +49(0)72519238750 · kontakt@hensec.com
360-Grad-Sicherheitslösungen für Industrie, Wirtschaft und Behörden um physische Sicherheit und Cybersecurity. **Drohnenabwehr**, Abhörschutz, OT-Security, Informationssicherheit, KRITIS, OsInt, Perimeterschutz. Prüfung, Entwicklung, Implementierung und Schulung.

Sicherheitsmanagement



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



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

SICHERHEITS MANAGEMENT

Sicherheitsmanagement



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 Privat- anwendern spezialisiert.

Sicherheitsmanagement



ADI Global Germany GmbH
Neuer Zollhof 3 · 40221 Düsseldorf
Tel.: +49 (0)211 869 42089
www.adiglobal.de · sales.de@adiglobal.com
Ihre zentrale Anlaufstelle für Sicherheit, Brandschutz und audiovisuelle Produkte. Unser Sortiment besteht aus über 200 führender Marken und einem globalen Lieferantennetzwerk sowie einem leistungsstarken 24/7 Onlineservice.

Sicherheitsmanagement

ASSA ABLOY

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



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



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

Signum Consulting GmbH
Marke **DISA**
Rungestraße 19 · 10179 Berlin
info@de.disa.com · martin.mehner@de.disa.com
<https://disa.com/de>



Signum Consulting GmbH / Marke DISA – Ihr Ansprechpartner für Pre-Employment-Screening und Geschäftspartnerprüfungen, prozessbegleitend von der Planung bis zur Umsetzung.

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

SimonsVoss Technologies GmbH
Münchner Str. 16 · 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

Südmittel

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

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

Gebäudesicherheit



Uhlmann & Zacher GmbH **ASSA ABLOY**
Gutenbergstraße 2-4 · 97297 Waldbüttelbrunn
Tel.: +49(0)931/40672-0 · Fax: +49(0)931/40672-99
contact.uz@assaabloy.com · www.uhlmannzacher.com
Elektronische Schließsysteme, modular aufgebaut und individuell erweiterbar.
Seit 2025 gehört das Unternehmen zur Assa Abloy-Firmengruppe.



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.

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

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.

Videoüberwachung



i-PRO EMEA B.V.
Herikerbergweg 292 · 1101CT 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-Angriffen im Einklang mit DSGVO, VMS: Video Insight

Videoüberwachung



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 Zufahrtsskontrollsysteme; biometrische Verifikation; Wächterkontrollsysteme; Verwahrung und Management von Schlüsseln und Wertgegenständen

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



DOM Sicherheitstechnik GmbH & Co. KG
Wesseling 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

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.

ZEIT ZUTRITT

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

ASSA ABLOY

ASSA ABLOY Entrance Systems GmbH
Lagerstr. 45 · 64807 Dieburg
Tel.: +49 6071 208 0 · Fax: +49 6071 208 111
sec.de@assaabloy.com · www.assaabloentrance.de
Speedgates, Durchgangs- und Sicherheitsschleusen,
Drehkreuze, Schwenktüren, Sicherheits-Karussell-
türen und -Portale für die Sicherheits-Zutritts-
kontrolle und Personenvereinzelung.

Zeit + Zutritt

A Z S
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 Schranken-
anlagen, OPC-Server

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

Connect people.
Create access.



CES
C.Ed. Schulte GmbH Zylinderschlossfabrik
Friedrichstraße 243 · D-42551 Velbert
Objektabteilung@ces.eu · www.ces.eu
Mechanische, mechatronische und elektronische
Schließsysteme, Zutrittskontrolle

Zeit + Zutritt

cichon
cryptin **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

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

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 ver-
netzte elektronische Zutrittslösungen, physische Zugangs- und
automatische Türsysteme, Türbänder, Beschläge, Türschließer,
Zeiterfassung inkl. ERP-Anbindungen, Hotelschließsysteme
und Hochsicherheitsschlösser.

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 Zufahrts-
kontrolle, Geländeabsicherung, Bezahlssysteme u.v.m.

Zeit + Zutritt

gantner **N**
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, Schließ-
systeme, Zugriffsschutz, Schrankschließsysteme

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, Zei-
terfassung, BDE, Türkommunikation, Besuchermanagement,
Parksysteme, Zufahrtskontrolle, Vending, ... Terminals,
Einbaumodule, Kartenspende, Tischlesegeräte, Leser für
Markenschalterprogramme, Identifikationsmedien,
... einfach und komfortabel zu integrieren.

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, Perso-
naleinsatzplanung, grafisches Alarmmanagement, SAP-
Kommunikationslösungen, Ausweiserstellung, Biometrie

Zeit + Zutritt

salto **A**
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.

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

NOTRUF SERVICE LEITSTELLE

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

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
Störungsbeseitigung in der Energieversorgung.

BRAND SCHUTZ

Brandschutz



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 Betriebsausrüstung, Gefahrstoff-Leckage-Warnsystem

Brandschutz

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 Brandschutzlösungen. Branchenspezifisches Fachwissen mit hochwertigen Brandschutzkomponenten vereint zu einem sicheren und verlässlichen Brandschutz. Flankiert wird dies mit Fachschulungen und einem umfangreichen, lösungsorientierten Kundenservice.



Brandschutz



Securitas Technology GmbH
SeTec Sicherheitstechnik

Hauptstr. 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

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

Arbeitssicherheit



KRAUSE-Werk GmbH & Co. KG

Am Kreuzweg 3 · D-36304 Alsfeld

Tel.: +49 (0) 6631 / 795 - 0

info@krause-systems.de

www.krause-systems.com

Tritte, Leitern, Steigtechnik, Podestleitern, Fahrgerüste

ARBEITS SICHERHEIT

GEFAHRSTOFF MANAGEMENT

Brandschutz

Arbeitssicherheit



ELTEN GmbH

Ostwall 7–13 · 47589 Uedem

Tel.: 02825/8068

www.elten.com · service@elten.com

Sicherheitsschuhe, Berufsschuhe, PSA,
ELTEN, Berufsbekleidung, Sicherheit

Gefahrstoffmanagement



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- und Arbeitsschutz,
Sicherheitsschränke, Chemikalien- und Umluft-
schränke, Druckgasflaschenschränke, Gefahrstoffar-
beitsplätze, Absauganlagen, Raumluftreiniger uvm.

Brandschutz

Arbeitssicherheit



Hailo-Werk

Rudolf Loh GmbH & Co. KG

Daimlerstraße 8 · 35708 Haiger

www.hailo-professional.de

professional@hailo.de

Steig-/Schachtleitern, Steigschutzsysteme,

Schachtabdeckungen, Servicelifte, Schulungsangebote

Gefahrstoffmanagement



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



Bequem auf dem Sofa durch die e-Ausgabe der GIT SICHERHEIT blättern: Registrieren Sie sich auf www.git-sicherheit.de/newsletter



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 Betriebs-
 ausstattung, Gefahrstoff-Leckage-Warnsystem

MASCHINEN ANLAGEN SICHERHEIT

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 Sicherheits-
 lichtschranken sowie Sicherheitsrelaisbausteine, program-
 mierbare Sicherheitssteuerungen und die Safety Services
 des Geschäftsbereichs tec.nicum

Gefahrstoffmanagement



SÄBU Morsbach GmbH
 Zum Systembau 1 · 51597 Morsbach
 Tel.: 02294 694-24 · Fax: 02294 694-38
 safe@saebu.de · www.saebu.de
 Gefahrstofflagerung, Gefahrstoffcontainer, Auffang-
 wannen, Bodenschutzsysteme, Gasflaschenlagerung,
 Gasflaschencontainer, Gasflaschenbox, Kleingebinderegale
 Unser 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.com · info@euchner.de
 Automation, Mensch/Maschine, 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

Ihr Eintrag in der Rubrik



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

Wir beraten Sie gerne!

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 Mikro-
 schalter, 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



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.

WILEY

35 Jahre

GIT SICHERHEIT**Die Jubiläumsausgabe**

Seit 35 Jahren begleitet GIT SICHERHEIT den Sicherheitsmarkt – kritisch, unabhängig und immer nah an den relevanten Fragen der Zeit. Dieses Jubiläum ist für uns mehr als ein Rückblick: Es ist Anlass, Entwicklungen einzuordnen, Stimmen zu Wort kommen zu lassen und den Blick nach vorn zu richten.

Auf unserer Jubiläums-Landing-Page finden Sie exklusive Interviews mit Entscheiderinnen und Entscheidern, fundierte Trendberichte, pointierte Analysen und besondere Specials, die zeigen, wie sich Sicherheitstechnologien, Strategien und Märkte verändert haben – und was heute wirklich zählt.

**Entdecken Sie 35 Jahre
SICHERHEIT im Kontext.**

Jetzt online auf:
[git-sicherheit.de/de/
35-jahre-GIT-SICHERHEIT](http://git-sicherheit.de/de/35-jahre-GIT-SICHERHEIT)



DIE VIP LOUNGE



© Daniel Koke / Bayer

Oliver Giesen

Leiter Werkfeuerwehr Bayer AG, Standort Berlin

- 1994 – 1998 Dipl. Chemieingenieur (FH)
- 2008 – 2010 Feuerwehrausbildung (gehobener Dienst)
- 2013-2015 Sachverständiger für vorbeugenden und gebäudetechnischen Brandschutz (EIPOS)
- Seit 2010 Leiter der Werkfeuerwehr der Bayer AG
- Seit 2016 Vorstandsvorsitzender der Arbeitsgemeinschaft betrieblicher Brandschutz e.V. (AGBB Berlin e.V.); www.agbb.berlin
- Fachbereichsleitung vorbeugender Brandschutz des Werkfeuerwehrverbandes Deutschland (WFVD e.V.)

Ihr Berufswunsch mit 20 war: Mit 20 war ich mitten in meiner Ausbildung zum Chemielaboranten und für mich war zu diesem Zeitpunkt klar, dass ich ein naturwissenschaftliches Studium absolvieren möchte. Ein Chemieingenieurstudium sollte es werden – eine hervorragende Vorbereitung auf meine heutigen Aufgaben.

Was hat Sie dazu bewogen, eine Aufgabe im Bereich Sicherheit zu übernehmen? Ich muss ehrlich gestehen, dass ich nicht schon als Kind von einer Karriere als „Grisu“ geträumt habe. Als mir die Leitung der Werkfeuerwehr angeboten wurde, war ich als Projektingenieur bei Bayer tätig und Mitglied der nebenberuflichen Werkfeuerwehr. Ich war zuerst skeptisch, ob dieser Karriereweg für mich Sinn macht, habe mich jedoch trotzdem dafür entschieden. Schnell habe ich gemerkt, dass mir das Arbeiten in den interdisziplinären Gefahrenabwehr-Teams und die Herausforderungen im vorbeugenden Brandschutz am Herzen liegen. Heute bin ich glücklich darüber, dass ich mich für diesen Weg entschieden habe.

Welche sicherheitspolitische Entscheidung oder welches Projekt sollte Ihrer Meinung nach schon längst umgesetzt sein? Ich bin großer Befürworter der Idee, dass Brandschutz effizient und wirtschaftlich sinnvoll sein kann und muss. Hierzu müssen Themen wie die Vereinfachung des Baurechts, die konsequente Minimierung des allgemeinen Vorschriftenwaldes und die bessere fachliche Ausbildung von Beteiligten im Brandschutz umgesetzt werden.

Die beste Erfindung im Bereich Sicherheit ist Ihrer Meinung nach? Als Verfechter des Betriebsmodells „Werkfeuerwehr“ ist es natürlich die Einführung der betrieblichen Gefahrenabwehrorganisationen in Deutschland, die im Rahmen der Industrialisierung etabliert wurden. Für Unternehmen bieten diese einen wesentlichen Mehrwert und schützen die Mitarbeiter, die Arbeitsplätze und die Sachwerte des Unternehmens. Richtig organisiert kann man mit einer Werkfeuerwehr nicht nur die Gefahrenabwehr sicherstellen, sondern einen wirtschaftlichen Mehrwert für das Unternehmen generieren.

Ein Erfolg, den Sie kürzlich errungen haben, war: Wir haben in den letzten zwei Jahren sehr viele Mitarbeiter aus der Baby-Boomer Generation in den wohlverdienten Ruhestand verabschiedet. Das reißt in der Regel eine große Lücke in unsere Organisation, da es bei einer Werkfeuerwehr auf optimale Ortskunde und Erfahrungswerte ankommt. Wir konnten durch ein

positives Recruiting alle Stellen mit engagierten und super ausgebildeten Feuerwehrleuten nachbesetzen, die alle unterschiedliche neue Stärken mitbrachten und sich prima in unser Team eingefügt haben. Das macht mich glücklich und schon ein bisschen stolz.

Wer hat Ihrer Meinung nach eine Auszeichnung verdient? Meine Familie! Weil Sie mich in all den Jahren immer unterstützt hat, und ich nur mit Ihnen so viel Erfolg haben konnte.

Wobei entspannen Sie? Mein persönlicher „mindfulness“ Moment ist jeden Mittwoch von 19-21 Uhr. Da findet die Probe von meinem Chor statt, in dem ich seit 3 Jahren singe.

Welchen Urlaubsort können Sie empfehlen? Ich bin mir nicht sicher, ob ich das mit den Lesern teilen möchte, sonst wird es dort noch voller. Mein absoluter Herzensort liegt in Andalusien, wo ich mindestens einmal pro Jahr mit meiner Familie Urlaub mache.

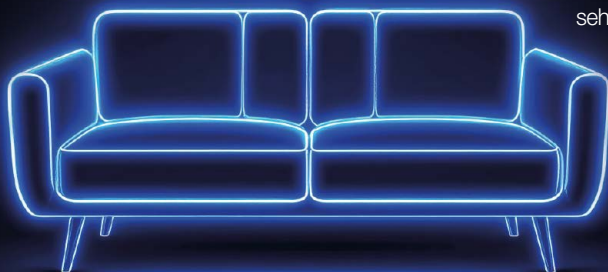
Welche Zeitschriften lesen Sie regelmäßig? Der Werkfeuerwehrverband bringt regelmäßig die WFVD-Info raus und diese Zeitschrift lese ich tatsächlich immer komplett.

Die GIT SICHERHEIT ist für mich wichtig, weil... durch sie Netzwerke wachsen, und ich ein großer Freund des 3K-Prinzips (Albrecht Broemme) bin: In der Krise Köpfe kennen!

Welches Buch haben Sie zuletzt gelesen? Bücher lese ich tatsächlich vorrangig im Urlaub und dann gerne Krimis. Im letzten Urlaub habe ich jedoch mal eine Ausnahme gemacht und mir das Buch von Albrecht Broemme „Deutschland in der Krise“ vorgenommen.

Was motiviert Sie? Mit meinem Team positiven Mehrwert für unseren Arbeitgeber zu generieren, durch Einsätze der Gefahrenabwehr Kollegen helfen, Sachwerte schützen und Betriebsunterbrechungen minimieren.

Worüber machen Sie sich Sorgen – und was stimmt Sie zuversichtlich? Die aktuelle politische Lage in der Welt und in Deutschland machen mir als Familienvater und Verantwortlicher in der Gefahrenabwehr große Sorgen. Was mich als Feuerwehrmann trotzdem positiv denken lässt, ist, dass in der betrieblichen Gefahrenabwehr und bei den öffentlichen Feuerwehren viele Menschen sind, die beruflich oder ehrenamtlich intrinsisch helfen wollen und im Ernstfall für unsere Sicherheit da sein werden.



WILEY

**JETZT
ABSTIMMEN**

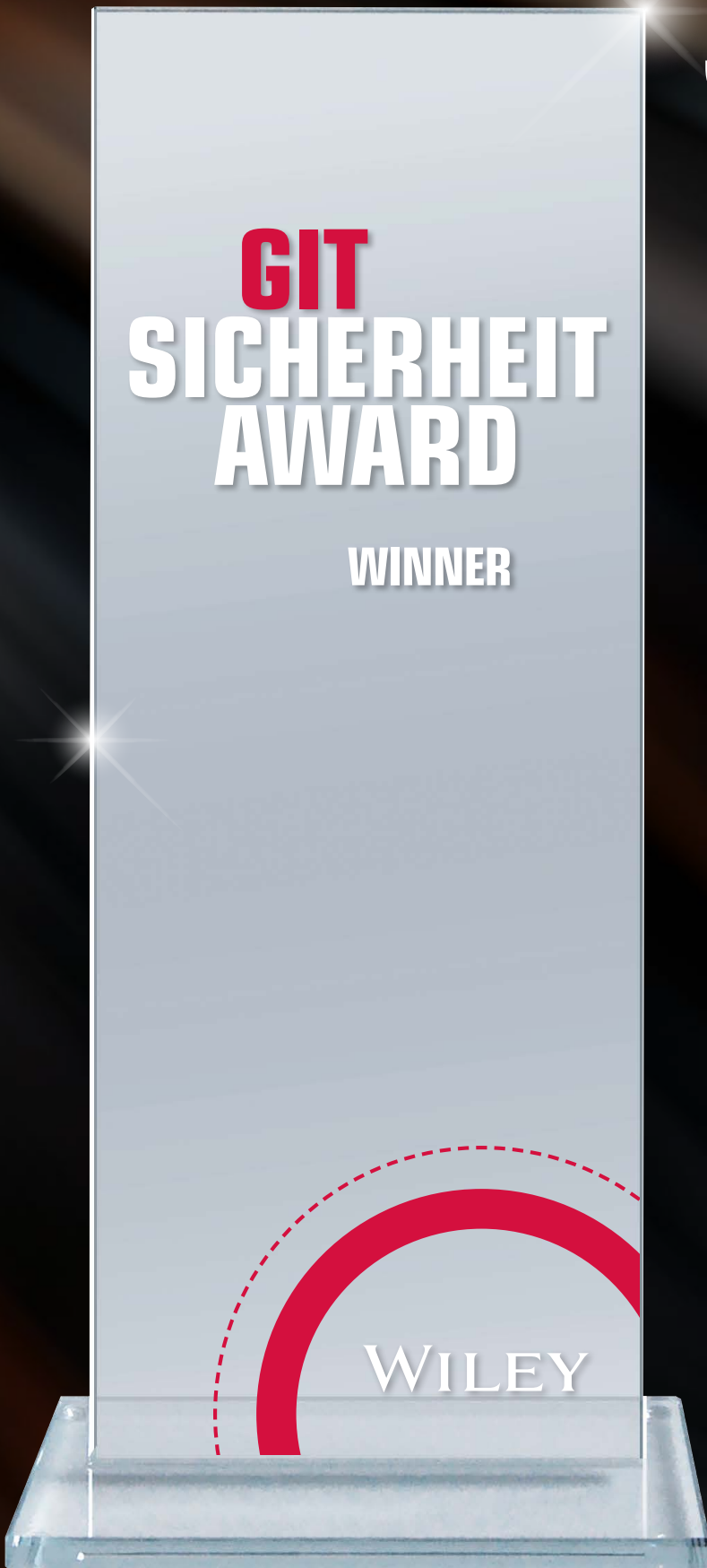
**GIT
SICHERHEIT
AWARD**

WINNER

bis spätestens
1. SEPTEMBER

Infos zu Finalisten,
Abstimmung und
Leserpreis:

www.sicherheit-award.de



WILEY

WENIGER STECKER **MEHR VERBINDUNG** DURCH AS-INTERFACE



MEHR-VERBINDUNG.DE



Automatisierungstreff
IT & AUTOMATION 2026

Cyber Resilience Act Tour 2026
17.06.2026
WTZ-Tagungszentrum, Heilbronn



Gebäudeautomation Tour 2026
24.06.2026
Motorworld, Köln



Cyber Resilience Act Tour 2026
24.06.2026
Motorworld, Köln



Cyber Resilience Act Tour 2026
30.06.2026
Heristo Arena, Halle (Westfalen)