

GIT SICHERHEIT

MAGAZIN FÜR SAFETY UND SECURITY



Titelthema Seite 60:

Effizienz und Sicherheit auf kleinstem Raum

Kompakte Sicherheitslösungen in der industriellen Automatisierung

VERBÄNDE

Branka Bernges über Gefährdungslage und Ausbildung s. 8

VERTEIDIGUNG

Euro Defence Messe parallel zur Security Essen ab S. 14

BRANDSCHUTZ

Digitalisierungs-Richtlinien s. 54

SAFETY

VDMA-Einheitsblatt 24994 s. 68

STEIGTECHNIK

Produktvergleich S. 74



VIP:
Andreas
Maack

S. 82

HEFT IM HEFT

GIT SICHERHEIT



KRITIS
ab S. 18

Ausgabe
ONLINE
lesen:

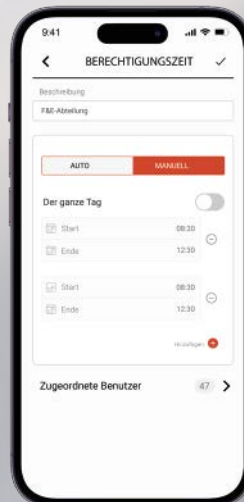
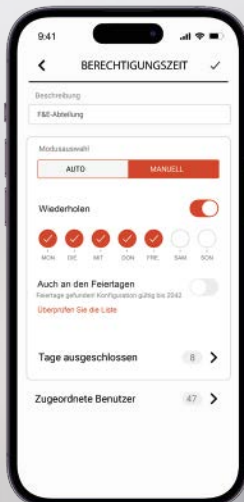


WILEY

Zutrittskontroll-Modul



intro



www.kseniasecurity.com/de

info@kseniasecurity.com



Finde mehr heraus

Die Zeit drängt!

Deutschland und Europa müssen erheblich mehr für die eigene Sicherheit tun. Spätestens die jüngsten politischen Entwicklungen zwingen uns dazu – und es rechtfertigt die Änderung des Grundgesetzes, deren Zeuge wir gerade waren. Sie hat den Weg für Investitionen von über 400 Milliarden Euro für die Infrastruktur frei gemacht. Vor allem auch die kritischen Infrastrukturen stehen hier im Zentrum der Aufmerksamkeit.

Dass sich große Teile unserer Branche und der Politik geradezu fieberhaft mit diesen Themen befassen, spiegelt unser „Heft im Heft KRITIS“ in dieser April-Ausgabe der GIT SICHERHEIT (ab Seite 18) deutlich wider: Einleitend erläutert Peter Lauwe, Leiter der Referatsgruppe Infrastrukturschutz beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), wie es um die Resilienz der kritischen Infrastruktur in Deutschland bestellt ist und welche Aufgaben das BBK nach Umsetzung der CER-Richtlinie der EU übernehmen könnte. Direkt im Anschluss daran beschreibt Dr. Daniela Lesmeister, Staatssekretärin Ministerium des Innern NRW, wie wichtig die Resilienz kritischer Infrastrukturen gerade mit Rücksicht auf die geopolitischen Verhältnisse ist und warum das KRITIS-Dachgesetz hierzu einen wichtigen Beitrag leisten kann (ab Seite 20).

Im Zeitalter hybrider Kriegsführung nimmt Cybersicherheit eine mindestens ebenso zentrale Stellung ein wie die physische Sicherheit. Auch hierauf hat die europäische Politik mit dem Erlass der NIS2-Richtlinie reagiert. Wie es um die gesetzlichen Grundlagen und Anforderungen dazu bestellt ist, erläutern Dr. Kai Nürnberger, Leiter Strategie & Markterschließung beim Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE, Jochen Sauer, Architect & Engineering Manager bei Axis Communications, und Jörg Brasas, Strategic Product Marketing Manager bei Phoenix Contact, in einem gemeinschaftlichen Beitrag ab Seite 32. Und wer mehr darüber erfahren möchte, warum das Thema Cybersicherheit verstärkt Einzug im Topmanagement von Unternehmen hält, dem sei unser Beitrag mit Dr. Harald Schönfeld, Geschäftsführer der Personalberatung Butterflymanager, ab Seite 24 ans Herz gelegt.

Deutschland hat sich als Industriestandort auch immer durch seine Innovationskraft ausgezeichnet. Wie gerade mittelständische Unternehmen bis heute dazu beitragen, zeigt unsere Titelstory (ab Seite 60). So bietet Leuze mit einem ultra-kompakten Sicherheits-Laserscanner ein zentrales Stück Technik für die sichere Nutzung autonomer mobiler Roboter und fahrerloser Transportsysteme.

Dass auch im Bereich der Maschinen- und Anlagensicherheit das Thema Security eine immer wichtigere Rolle spielt, erklärt Werner Varro, Consultant Safety & Certification bei Neura Robotics, im Interview mit GIT SICHERHEIT (ab Seite 64). Das Interview bildet den Auftakt zu unserer vierteiligen Interview-Serie mit dem Titel „Maschinensicherheit im Kontext von KI und Security“. Abschließend sei noch auf unser Interview mit Helmut Schmidt, Vorstand des Deutschen Robotik Verbands und Geschäftsführer HS Auxilium, verwiesen (ab Seite 66). Hier erfahren Sie, warum es nun mehr denn je gilt, an der Infrastruktur zu arbeiten und die Bürokratiebremse zu lösen, wenn Deutschland im Zukunftsmarkt Robotik mitmischen möchte.

Stärken auch Sie ihre Resilienz und bleiben Sie auf dem Laufenden!



Herzlichst,
Ihr

T. Gimbel

Dr. Timo Gimbel
für das Team von Wiley
und GIT SICHERHEIT

ASSA ABLOY Expression Speedgate



Moving by design

ASSA ABLOY
Entrance Systems



Experience a safer
and more open world



TITELTHEMA

Effizienz und Sicherheit auf kleinstem Raum

Kompakte Sicherheitslösungen in der industriellen Automatisierung

Seite 60



PRO-4-PRO
für 2024/2025



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

Produkt- und Lead-Plattform
für Sicherheit



8 Branka Bernges



18 Peter Lauwe



20 Dr. Daniela Lesmeister



28 Bernhard Klinger

MANAGEMENT

VERBÄNDE

8 Gemeinsam Lösungen finden

Unternehmen brauchen ganzheitliche Sicherheitsstrategien – für physische wie digitale Bedrohungen

12 Innovationen in der Sicherheitstechnik

Zum zweiten Mal: Fachkongress BSW SecTec

MESSEN

14 Zivil und militärisch

Euro Defence Expo (Eudex) und NATO Joint Air Power Competence Centre (JAPCC) parallel zur Security 2026 in Essen

SICHERHEITSDIENSTLEISTUNGEN

16 „Deutschland braucht Kurswechsel in der Wirtschaftspolitik“

Kötter Unternehmensgruppe:
Umsatz wächst auf 722 Millionen Euro

HEFT IM HEFT | KRITIS

BEVÖLKERUNGSSCHUTZ

18 Die Lebensadern der Gesellschaft

Zur Stärkung der Resilienz Kritischer Infrastrukturen

INNERE SICHERHEIT

20 Das Rückgrat unseres Alltags

Kritische Infrastruktur und das neue Kritische Infrastruktur-Dachgesetz

RATGEBER

22 Viele kann man jetzt schon machen!

Neue Realität für Unternehmen: KRITIS-Dachgesetz und NIS-2

NIS2

24 Cyberresilienz brennt im Topmanagement

NIS2 - Steigende Nachfrage am Personalmarkt

EINSATZKRITISCHE KOMMUNIKATION

28 Einsatz- und geschäftskritische Kommunikation

Politische Forderungen des Bundesverbandes Professioneller Mobilfunk für die kommende Legislaturperiode

30 Hightech auf den Gleisen

Frequentis digitalisiert Schienennetz der Schweizer Bundesbahn

CYBER SECURITY

32 Schutzschild gegen Manipulation und Sabotage

Cybersicherheit: Zum Schutz von KRITIS und industriellen Anlagen – Teil 1: Gesetzliche Grundlagen und Anforderungen

ÜBERTRAGUNGSTECHNIK

35 Ohne Strom kein Alarm

Sichere Übertragungstechnik: Vom Schutz der sicherheitstechnischen Gewerke bis zur sicheren Übertragung von Alarmmeldungen

PERIMETERSCHUTZ

38 Nach Art der Zwiebel

Perimetersicherung für ein Umspannwerk



Stephan Holzem & Daniel Kaumanns



Emmanuel Harir-Forouch



Benjamin Schmid



SECURITY

PERIMETERSCHUTZ

40 Solider Zaun gehört dazu

Trends in der Sicherung von Investitions- und Gewerbeobjekten im Jahr 2025

SMART HOME

42 Froschblaues Wunder

Frogblue International Partner Conference 2025: Innovationen und Zukunftsvisionen im Fokus

ZUTRITT

46 Gut aufbewahren!

Schutz wertvoller Dinge vor Diebstahl, Feuer und unbefugtem Zugriff

DISTRIBUTION

50 Durchstarten im Zentrum Europas

Globaler Distributor kommt nach Deutschland

VIDEO

52 Therapie per KI

Britisches Krankenhaus erweitert Kameras durch KI-Funktionen

BRANDSCHUTZ

RICHTLINIEN

54 Auf gemeinsamen Nenner gebracht

Brandschutz und Digitalisierung im Gebäude: VdS-Merkblatt 6024 wird zur VdS-Richtlinie

GERÄTEINTEGRIERTER BRANDSCHUTZ

56 Auf dem Schirm

Geräteintegrierter Brandschutz am Flughafen Berlin Brandenburg

ALARMIERUNG

58 Damit die Feuerwache nicht selbst zum Brandopfer wird...

Kooperation für Rund-um-Brandschutz

SAFETY

TITELTHEMA

60 Effizienz und Sicherheit auf kleinstem Raum

Kompakte Sicherheitslösungen in der industriellen Automatisierung

62 Minimale Größe, maximale Sicherheit

Sicherheits-Laserscanner von Leuze

MASCHINEN- UND ANLAGENSICHERHEIT

64 Maschinensicherheit im Kontext von KI und Security

Künstliche Intelligenz und ihre Auswirkung auf die Risikobeurteilung von Maschinen

66 „Vom Exoten hin zu einem Problemlöser“

Im Gespräch: Helmut Schmid, Vorstand des DRV und Geschäftsführer HS Auxsilium

LITHIUM-IONEN-AKKU LAGERSCHRÄNKE

68 VDMA-Einheitsblatt 24994

Erster einheitlicher Prüfstandard für die Zertifizierung von Lager-/Ladeschränken für Lithium-Ionen-Akkus

PSA

70 Für alle Fälle gerüstet

Zertifizierte Multinorm-Schutzkleidung aus nachhaltiger Produktion

STEIGTECHNIK

72 Kurze Wege sind sichere Wege

Überstiege, Treppen, ortsfeste Leitern und Laufstege beschleunigen die Abläufe

74 Ortschafte Überstiege

Produktvergleich

RUBRIKEN

76 GIT BusinessPartner

82 VIP Interview

83 Impressum

INDEX

QUICK-FINDER

ORGANISATIONEN, INSTITUTIONEN UND UNTERNEHMEN IM HEFT

3-core	22
ADI Global	7, 50
Advancis	45
AG Neovo	31
Assa Abloy	33, 44
Aug. Winkhaus	27
Axis	13, 32, 49
Barox	45
BDSW	13
BHE	26
Blakläder	70
Bosch	27
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe	18
Butterfly	24
BVSW	12
Cubos	58
Dahua	26
Dallmeier	48
Deutscher Robotik Verband	66
Dom Sicherheitstechnik	36
Dormakaba	39
Düperthal	68
e* Message	21
Easyfairs	63
Elatec	6
Frogblue	42, U4
Fiera Milano	17
Flir	48
Frequentis	30
Genetec	45
Gloria	55
Gretsch-Unitas	45
Gunnebo	46
Hailo	71
i-Pro	52
Job	56
Johnson Controls	6
K. A. Schmersal	63
Koelnmesse	6
Kötter	16, 37
Krause-Werk	71
Ksenia Security	U2
Landesmesse Stuttgart	6
Leuze	60, Titelseite
Liveye	7
Lupus	49, 59
Mesago Messe Frankfurt	63
Messe Essen	14
Ministerium des Innern des Landes NRW	20
Mobotix	26
Motorola Solutions	57, 7
Munk	72
Novar	59
Nürnberg Messe	57
Paxton	11
PMeV Professioneller Mobilfunk	28
Record Türautomation	3
Rohde & Schwarz	11
Salto Systems	21, 25, 53
Schwarzwald Dogs	45
Securiton	38
Slat	41
Telefonbau	35
Telenot Electronic GmbH	26, Beilage
VDMA	57, 64
VdS Schadenverhütung	54, 59
Vereinigung für die Sicherheit der Wirtschaft (VSW)	8
Videor	11
Volkswagen	82
Western Digital	13
Winkhaus	25
Wisniowski	40
Zvei	13, 6

Eltefa 2025: Angebote für die Fachkräfte von morgen

Nach dem Erfolg von 2023 kehrte die Eltefa 2025 mit ihren maßgeschneiderten Formaten für junge Talente zurück. Die Young Talent Area, der Eltefa-thon und der Azubi Power Check gehörten erneut zum Programm, das um neue Akzente wie HerTechStories ergänzt wurde. Mit diesen Angeboten spricht die größte Fachmesse für Elektro, Energie, Gebäude und Industrie im Süden gezielt junge Fachkräfte an und stärkt ihre Position als Anlaufstelle für die nächste Generation der Branche. Besonders erfreulich: 2023 konnte der Anteil der Fachbesucher unter 30 Jahren deutlich gesteigert werden – ein klares Zeichen für die Attraktivität der Eltefa für junge Fachkräfte. Die Young Talent Area diente in diesem Jahr wieder als zentraler Treffpunkt für Auszubildende und Nachwuchskräfte. Neben kostenfreier Verpflegung und einer Fotobox lud der Bereich zu lockeren Begegnungen und zum Austausch ein.



Junge Talente aus Handwerk und IT traten beim Eltefa-thon an, um gemeinsam Lösungen für reale Herausforderungen der Elektrobranche zu entwickeln

www.messe-stuttgart.de

Johnson Controls: Joakim Weidemanis folgt auf George R. Oliver

Joakim Weidemanis wird Geschäftsführer von Johnson Controls. Mitte März tritt er die Nachfolge von George R. Oliver an. Als CEO wird Joakim Weidemanis, der zuletzt bei der Danaher Corporation als Executive Vice President und Corporate Officer wirkte, das Unternehmenswachstum vorantreiben. In seiner 13-jährigen Laufbahn bei der Danaher Corporation sammelte Joakim Weidemanis in verschiedenen Führungspositionen umfangreiche Erfahrungen in der Skalierung globaler Unternehmen hinsichtlich Kundenorientierung, Innovation und Effizienz. Als Executive Vice President, Diagnostics and China, war er bei Danaher zuletzt für die operative Konzernleitung von acht globalen Technologieunternehmen mit einem Umsatz von rund 15 Milliarden Euro verantwortlich. Durch Akquisitionen und organisches Wachstum stieg der Umsatz des Diagnostikgeschäfts des Konzerns in den vier Jahren unter seiner Leitung erheblich an.



Als CEO bei Johnson Controls wird Joakim Weidemanis maßgeblich das Unternehmenswachstum vorantreiben

www.johnsoncontrols.de

Elatec stärkt globale Präsenz mit regionalem Hub in Dubai

Elatec beginnt das Jahr 2025 mit der Eröffnung eines neuen Standorts in Dubai. Dies ist ein bedeutender Schritt für die globale Expansionsstrategie des Unternehmens. Der neue Standort wird unter dem Namen Elatec Middle East Trading FZE agieren und als zentraler Knotenpunkt für die Betreuung des wachsenden Kundenstamms und der Partner des Unternehmens im gesamten Nahen Osten dienen. Unter der Leitung von Managing Director Carsten Hoersch sollen sichere und maßgeschneiderte Zugangskontrolllösungen in der Region vorangetrieben werden. „Unsere neue Präsenz im Golf-Kooperationsrat (Gulf Cooperation Council, GCC) zeigt unser Bestreben, die Beziehungen zu den regionalen Partnern zu stärken und auf die marktspezifischen Bedürfnisse einzugehen. Dieser Schritt fügt sich nahtlos in unser Ziel ein, sichere, flexible und zukunftsichere Zugangslösungen anzubieten“, so Gerhard Burits, CEO der Elatec Gruppe. www.elatec.com



Carsten Hoersch, Managing Director von Elatec Middle East Trading FZE

Koelnmesse trotz der Wirtschaftsflaute

Die Koelnmesse hat 2024, dem Jahr ihres 100-jährigen Bestehens, auf Basis vorläufiger Zahlen einen Umsatz von rund 365 Millionen Euro und einen Gewinn von rund 20 Millionen Euro erzielt und bleibt auf einem stabilen Kurs. „Unser 100-jähriges Jubiläum war ein außergewöhnliches Jahr, das uns an unsere Ursprünge erinnert und in dem wir gleichzeitig den Blick nach vorne gerichtet haben“, sagt Gerald Böse, CEO der Koelnmesse GmbH. „Unsere Ergebnisse zeigen eindrucksvoll Stabilität und Resilienz in einem herausfordernden Marktumfeld.“ www.koelnmesse.de



ZVEI: Q-Trainerausbildung geprüfte Fachkraft für Rauchwarnmelder

Der ZVEI veranstaltet am 13. November 2025 das Online-Seminar „Q-Trainerausbildung für die geprüfte Fachkraft für Rauchwarnmelder“. In diesem Online-Seminar lernt der Teilnehmer, selbst Trainer für „Q-geprüfte Fachkräfte für Rauchwarnmelder“ nach DIN 14676 Teil 2 zu werden, und kann seine Lizenz verlängern. Er erhält umfassende Kenntnisse zur Planung, Installation, Prüfung und Zertifizierung von Rauchwarnmeldern und wird optimal auf die Prüfung vorbereitet. Diese Veranstaltung dient sowohl der erstmaligen Q-Trainer-Zertifizierung als auch dem Kompetenznachweis zur Lizenzverlängerung. Der Teilnehmer erhält einen fundierten Überblick über Planung und Einbau von Rauchwarnmeldern, die Prüfung und Zertifizierung von Q-Fachkräften. www.zvei-services.de



Das Dortmunder Team steht in den Startlöchern. (v. l. n. r.): Annemieke Wilken, Andreas Valtin, Hakan Gültekin, Francisco de Ranca, Luize Tahirukaj, Halil Ayaz

LivEye eröffnet neuen Standort in Dortmund

Beim Föhrener Sicherheitsunternehmen LivEye stehen alle Zeichen auf Wachstum: Im neuen Büro in Dortmund baut Standortleiter Andreas Valtin auf rund 220 Quadratmetern ein Sales Office auf. Der Vertriebsleiter Bau, Industrie, Energie, Brandfrüherkennung und NSTR bezog im Januar gemeinsam mit Sales-Profi und Teamleiter Halil Ayaz und Windenergie-Vertriebsleiter Hakan Gültekin die neuen Räumlichkeiten. Bereits jetzt begrüßt das Führungstrio drei Talente. Insgesamt sechs großzügige Räume stehen den Neuankömmlingen zur Verfügung. Andreas Valtin betont die Bedeutung des Standorts: „Mit unserem neuen Büro im Herzen von NRW bündeln wir unsere Sales Power, um unser Wachstum in der DACH-Region und Europa voranzutreiben.“ Um das Engagement in Europa erfolgreich auszubauen, plant das Unternehmen bis Ende des Jahres zehn weitere Stellen zu besetzen. www.liveye.com

Einzelhändler Poundland nutzt Motorola Solutions VT100 Bodycams

Motorola Solutions hat den erfolgreichen Einsatz seiner VT100 Bodycams in den Poundland-Filialen in Großbritannien bekannt gegeben. Seit dem Pilotprojekt meldet der britische Einzelhändler einen deutlichen Rückgang von Ladendiebstählen sowie 11 % weniger Gewalt gegen Mitarbeiter in den Filialen. „Ein sicheres Umfeld für Beschäftigte und Kunden ist die Grundlage für alles“, so Neil Thomas, Corporate Vice President of Enterprise Sales bei Motorola Solutions. „Unsere VT100 Bodycams helfen Poundland, Mitarbeiter, Kunden und Geschäfte zu schützen.“ Neben den Mitarbeitern auf der Fläche profitieren auch die Sicherheitsteams von Poundland von einer objektiven Aufzeichnung der Ereignisse, die bei etwaigen Ermittlungen hilft. Poundland nutzt die Software VideoManager von Motorola Solutions zur Verwaltung digitaler Beweismittel. www.motorolasolutions.com



ADI bringt dich auf die Überholspur!

Gewinnen Sie einen
VW Caddy Cargo Maxi als
Hauptpreis für ihr Unternehmen



ADI Global Germany ist ein führender Distributor von Sicherheitslösungen und -technologien. Das Unternehmen bietet eine breite Palette an Produkten, darunter Videoüberwachung, Zutrittskontrolle und Alarmsystemen. ADI Global ist Teil des internationalen ADI Global Distribution Netzwerks und beliefert Fachhändler, Integratoren und Sicherheitsunternehmen mit innovativen und hochwertigen Lösungen für den Schutz von Unternehmen und Privatpersonen.



Mehr erfahren unter
www.adiglobal.de/win-a-van



VERBÄNDE

Gemeinsam Lösungen finden

Unternehmen brauchen ganzheitliche Sicherheitsstrategien – für physische wie digitale Bedrohungen

Als die Vereinigung für die Sicherheit der Wirtschaft (VSW) 1968 gegründet wurde, ging es darum, eine Brücke zwischen der Wirtschaft und den Sicherheitsbehörden zu schlagen. Vor allem klassische Sicherheitsfragen standen im Mittelpunkt, etwa der Schutz vor Einbruch, Diebstahl oder Industriesabotage. Seitdem hat sich die Sicherheitslandschaft grundlegend verändert – und auch das Selbstverständnis des Verbands. Er versteht sich heute vor allem als strategischer Partner der Mitglieder in einer zunehmend komplexen und vernetzten Welt – sagt VSW-Geschäftsführerin Branka Bernges im Gespräch mit GIT SICHERHEIT.



Branka Bernges,
Geschäftsführerin VSW, Mainz

■ GIT SICHERHEIT: Frau Bernges, wir möchten heute ein wenig über aktuelle Sicherheitsthemen sprechen, die in der VSW auf vielfältige Weise behandelt werden. Sie sind Geschäftsführerin des Verbands. Könnten Sie uns zunächst einmal ein wenig Background über Sie selbst und Ihren professionellen Hintergrund geben?

Branka Bernges: Vielen Dank für die Gelegenheit, mit Ihnen über Sicherheitsthemen zu sprechen, die uns alle betreffen! Ich bin seit 2013 Teil der VSW und begann meine Tätigkeit im Bereich Aus- und Weiterbildungsmanagement sowie in der Mitgliederbetreuung. In dieser Funktion lag mein Fokus darauf, die Bedürfnisse unserer Mitglieder zu verstehen und sicherzustellen, dass sie von zielgerichteten Schulungen und Qualifizierungsprogrammen profitieren können. Ich übernahm zunehmend strategische Aufgaben, was schließlich zu meiner heutigen Position als Geschäftsführerin im Jahr 2022 führte. Daher liegt nun mein Fokus darauf, unseren Mitgliedern praxisnahe Unterstützung zu bieten, Netzwerke zu stärken und innovative Ansätze für die Sicherheitsbranche zu fördern. Mein Ziel ist es, sowohl die Bewältigung aktueller Herausforderungen zu unterstützen als auch auf die Entwicklungen in der Sicherheitslandschaft einzugehen.

Die VSW gibt es ja bereits seit 1968 – gegründet seinerzeit als Schnittstelle zwischen Wirtschaft und Sicherheitsbehörden. Wie hat sich das Selbstverständnis bis heute entwickelt – und worin vor allem sehen Sie die Bedeutung des VSW für die Mitglieder heute?

Branka Bernges: Unsere Bedeutung für die Mitglieder liegt heute insbesondere in drei zentralen Bereichen: Zunächst einmal geht es uns um ganzheitliche Sicherheitslösungen. Die Herausforderungen reichen hier von physischer Sicherheit über Cybersecurity bis hin zu internationaler Krisenvorsorge. Die VSW unterstützt ihre Mitglieder dabei, diese Themen ganzheitlich zu betrachten und aufeinander abgestimmte Strategien zu entwickeln.

Zum zweiten bieten wir unseren Mitgliedern Zugang zu einem starken Netzwerk aus Unternehmen, Sicherheitsbehörden, Wissenschaft und spezialisierten Dienstleistern. Dieser Austausch ist essenziell, um Best Practices zu teilen und voneinander zu lernen.

Drittens vertreten wir als Verband die Interessen unserer Mitglieder gegenüber der Politik und den Behörden. Gleichzeitig fungieren wir als Plattform, um aktuelle Entwicklungen und Risiken frühzeitig zu kommunizieren – sei es durch Veranstal-

tungen, Schulungen oder Informationsmaterialien.

Zusammengefasst hat sich die VSW von einer reinen Schnittstelle hin zu einem umfassenden Partner für Sicherheitsfragen entwickelt. Wir bieten Orientierung, Unterstützung und Innovation in einer Zeit, in der die Herausforderungen nicht nur zahlreicher, sondern auch vielschichtiger geworden sind.

Geben Sie uns einen Überblick über Ihre Mitgliederstruktur?

Branka Bernges: Unsere Mitgliederstruktur spiegelt die Breite der deutschen Wirtschaft wider. Sie umfasst Unternehmen unterschiedlicher Größen: Von großen, international tätigen Konzernen bis hin zu kleinen und mittelständischen Unternehmen (KMU). Wir vertreten Unternehmen aus nahezu allen Wirtschaftssektoren, darunter Industrie, Handel, Technologie, Finanzwesen und Dienstleistung. Dazu gehören auch spezialisierte Sicherheitsunternehmen, Berater und Experten, die mit ihrem Fachwissen zur Sicherheit der Wirtschaft beitragen. Dazu kommen Hochschulen und Institute, die sich mit Sicherheitsforschung und -technologie beschäftigen. Diese vielfältige Zusammensetzung ermöglicht einen breiten Erfahrungsaustausch

und bietet unseren Mitgliedern Zugang zu unterschiedlichen Perspektiven und Lösungen in Sicherheitsfragen.

Die Sicherheit von Unternehmen sieht sich heute einer ganzen Reihe besonderer Herausforderungen gegenüber – vom physischen bis zum Cyberraum. Wir sprechen von KI und Drohnen, von Cyberangriffen, Spionage, etc. Wie schätzen Sie die Situation diesbezüglich ein?

Branka Berges: Die Sicherheitslage für Unternehmen hat sich in den letzten Jahren stark verändert. Die Herausforderungen sind vielfältig, und Unternehmen müssen sich heute sowohl physischen als auch digitalen Bedrohungen stellen. Die zunehmende Nutzung von Künstlicher Intelligenz und Drohnen sowie die wachsende Bedrohung durch Cyberangriffe und Wirtschaftsspionage stellen besonders große Risiken dar.

Künstliche Intelligenz wird sowohl von Unternehmen zur Verbesserung der Sicherheit als auch von Angreifern zur Automatisierung und Optimierung von Angriffen eingesetzt. KI-basierte Angriffe können gezielt und schnell ausgeführt werden, was die Verteidigung erschwert. Drohnen stellen eine neue Bedrohung dar, insbesondere für kritische Infrastrukturen. Sie können zur Überwachung, Datensammlung oder sogar für physische Angriffe genutzt werden, was neue Sicherheitsstrategien erforderlich macht.

Cyberangriffe sind weiterhin eine der größten Bedrohungen. Die zunehmende Vernetzung und Digitalisierung schaffen mehr Angriffsflächen, von Ransomware bis zu ausgeklügelten Phishing-Attacken. Die Bedrohungen entwickeln sich schneller, so dass Unternehmen ständig ihre Sicherheitsvorkehrungen anpassen müssen. Spionage – sowohl durch Cybermethoden als auch durch physische Infiltration – bleibt ein bedeutendes Thema. Unternehmen müssen ihre sensiblen Daten und Betriebsgeheimnisse besser schützen, um wirtschaftlichen Schaden zu vermeiden.

Zusammenfassend lässt sich sagen, dass Unternehmen heute eine ganzheitliche Sicherheitsstrategie benötigen, die sowohl physische als auch digitale Bedrohungen umfasst. Es ist wichtig, dass sie nicht nur in technische Lösungen investieren, sondern auch ihre Mitarbeitende regelmäßig schulen und ein robustes Krisenmanagement entwickeln.

Die VSW unterstützt ihre Mitglieder, sich auf diese Herausforderungen vorzubereiten, indem wir praxisorientierte Schulungen, Beratungen und den Austausch von Best Practices fördern.

Wie schlagen sich in Ihrer Wahrnehmung die deutschen Unternehmen im Umgang mit diesen Themen?

Branka Berges: In meiner Wahrnehmung machen viele deutsche Unternehmen deutliche Fortschritte im Umgang mit modernen Sicherheits Herausforderungen, insbesondere in den Bereichen Cybersecurity und Technologieintegration. Große Unternehmen haben bereits umfassende Sicherheitsstrategien etabliert und investieren in fortschrittliche Schutzmaßnahmen, etwa KI-basierte Systeme zur Bedrohungserkennung oder in robuste Krisenmanagementprozesse.

Allerdings zeigt sich, dass vor allem kleinere und mittelständische Unternehmen (KMU) teils noch hinter den größeren Unternehmen zurückbleiben. Diese kämpfen häufig mit Ressourcenmangel, unzureichendem Know-how oder fehlendem Bewusstsein für die Dringlichkeit von Sicherheitsinvestitionen. Für viele KMUs ist es eine Herausforderung, mit den sich ständig weiterentwickelnden Bedrohungen, insbesondere im Cyberbereich, Schritt zu halten.

Ein weiteres Problem bleibt die Sensibilisierung der Mitarbeitenden. Trotz fortschreitender Digitalisierung sind menschliche Fehler nach wie vor eine der größten Sicherheitslücken, und viele Unternehmen sind sich noch nicht bewusst, wie wichtig kontinuierliche Schulungen und Awareness-Programme sind.

Zusammenfassend lässt sich sagen, dass die deutschen Unternehmen insgesamt ein wachsendes Bewusstsein für Sicherheitsrisiken entwickelt haben, aber noch einen langen Weg vor sich haben, um auf allen Ebenen von Technologie über Mitarbeiterschulung bis hin zu organisatorischen Strukturen optimal gerüstet zu sein. Die Zusammenarbeit und der Austausch, etwa über Netzwerke wie die VSW, sind hier ein wichtiger Schritt, um voneinander zu lernen und gemeinsam Lösungen zu finden.

Das Bundesministerium des Inneren und für Heimat erarbeitet in Zusammenarbeit u.a. mit der Wirtschaft eine nationale Wirtschaftsschutzstrategie. Ziel ist es, die Resilienz unserer Wirtschaft und Wissenschaft vor illegitimer Einflussnahme von außen zu stärken. Welche Haltung nehmen Sie als VSW hier ein – und welche Rolle spielen Sie hier als Verband?

Branka Berges: Die VSW begrüßt die nationale Wirtschaftsschutzstrategie des Bundesministeriums des Inneren und für Heimat ausdrücklich. Wir sehen diese Initiative als einen wichtigen Schritt, um die Resilienz der deutschen Wirtschaft und

Wissenschaft gegenüber immer komplexeren Bedrohungen, insbesondere aus dem Cyberraum und durch illegitime Einflussnahme von außen, zu stärken.

Unsere Haltung ist klar: Wirtschaftsschutz ist eine gesamtgesellschaftliche Aufgabe, die nur durch enge Zusammenarbeit zwischen der Wirtschaft, der Politik und den Sicherheitsbehörden erfolgreich umgesetzt werden kann. Insgesamt spielen wir als VSW eine unterstützende Rolle, die den ASW-Bundesverband (Akteur) in seiner zentralen Funktion stärkt, um eine erfolgreiche und resiliente Wirtschaftsschutzstrategie für Deutschland zu fördern.

Die „illegitime Einflussnahme von außen“ geschieht dank unserer weitgehend digitalisierten Prozesse vor allem im Cyberraum. Durch Künstliche Intelligenz werden Angriffe gar noch optimiert. Welche Fragen kommen hier seitens der Mitglieder in erster Linie auf, als wie angespannt sehen sie die Lage diesbezüglich – und welche Antworten kann die VSW hier bieten?

Branka Berges: Die Bedrohung durch illegitime Einflussnahme im Cyberraum ist für unsere Mitglieder ein wachsendes Thema, insbesondere durch den Einsatz von Künstlicher Intelligenz, die Angriffe effizienter macht. Fragen sind unter anderem: Wie schützen wir uns vor gezielten, KI-unterstützten Angriffen? Wie sichern wir sensible Daten vor Diebstahl? Wie erhöhen wir die Resilienz unseres Unternehmens bei Cyberangriffen? Die Lage ist angespannt, da Angreifer immer raffinierter werden und Unternehmen schneller reagieren müssen.

Unsere Antworten hierauf sind zunächst einmal Schulungen und Awareness, also die Sensibilisierung der Mitarbeiter für neue Bedrohungen. Dazu kommen Beratung und Sicherheitslösungen in Form von maßgeschneiderten Konzepten zur Abwehr von Cyberangriffen sowie Best Practices und Krisenmanagement, insbesondere der Austausch von Sicherheitsstrategien und Unterstützung bei Notfallplänen.

Viel besprochen ist der Schutz vor Drohnenangriffen – hier ist sowohl technisch als auch im Dienstleistungsbereich einiges in Bewegung. Wie sehen Sie die Gefährdungslage hier?

Branka Berges: Die Gefährdungslage durch Drohnen hat in den letzten Jahren erheblich an Bedeutung gewonnen. Drohnen sind mittlerweile leicht zugänglich, relativ kostengünstig und vielseitig einsetzbar. Sie können sowohl für legitime Zwecke als auch für böswillige Absichten genutzt

werden, was sie zu einer zunehmenden Herausforderung für die Sicherheit macht.

Die Lage wird sich in den kommenden Jahren vermutlich weiter verschärfen, insbesondere durch den zunehmenden Einsatz von künstlicher Intelligenz in Drohnen, die ihnen mehr Autonomie und Präzision verleihen. Gleichzeitig werden aber auch die Abwehrmaßnahmen immer raffinierter, was einen Wettlauf zwischen Angriffs- und Verteidigungstechnologien erwarten lässt.

Eine proaktive Auseinandersetzung mit der Thematik – sowohl technisch als auch regulatorisch – ist essenziell, um die Sicherheit vor Drohnenangriffen zu gewährleisten.

Frau Berges, Kritische Infrastrukturen, um ein weiteres aktuelles Themenschwergewicht anzusprechen, sind schon von der Definition her besonders resilienzbedürftig – in unser aller Interesse. Das KRITIS-DACH-Gesetz ist auf dem Weg. Wie setzen Sie sich damit verbandsseitig damit auseinander?

Branka Berges: Das KRITIS-DACH-Gesetz ist ein wichtiger Schritt zur Stärkung der Resilienz kritischer Infrastrukturen. Als VSW setzen wir uns damit auseinander, indem wir unsere Mitglieder über die Anforderungen des Gesetzes auf dem Laufenden halten. Wir bieten aber auch Unterstützung bei der Umsetzung der neuen Sicherheitsanforderungen und fördern den Austausch von Lösungen und Erfahrungen zwischen den Mitgliedern.

Zu allen angesprochenen Themen und darüber hinaus betreiben Sie ein umfassendes Aus- und Weiterbildungsprogramm. Könnten Sie dazu bitte noch etwas sagen?

Branka Berges: Gerne. Wir bieten ein strukturiertes Aus- und Weiterbildungsprogramm, das Unternehmen in die Lage versetzt, auf die wachsenden Herausforderungen der Unternehmenssicherheit zu reagieren. Das Angebot reicht von grundlegenden Schulungen für neue Mitarbeitende bis hin zu spezialisierten Weiterbildungen für erfahrene Sicherheits- und Führungskräfte. Darin geht es uns um die Vermittlung von Kompetenzen, um Bedrohungen effektiv zu erkennen und abzuwehren. Dabei passen wir die Inhalte an die spezifischen Bedürfnisse der Unternehmen an. Wir stellen sicher, dass Mitarbeiter aller Ebenen optimal auf Sicherheitsanforderungen vorbereitet sind – und zwar unter Berücksichtigung neuer Technologien und Trends.

Welche Themen sind hier besonders nachgefragt derzeit?

Branka Berges: Für die Sachkundeprüfung gemäß § 34a GewO bieten wir beispielsweise speziell zugeschnittene Vorbereitungskurse an, die die Teilnehmer optimal auf die Prüfung vorbereiten. Diese umfassen alle relevanten rechtlichen, praktischen und kommunikativen Inhalte, um sicherzustellen, dass sie nicht nur die Prüfung bestehen, sondern auch im Berufsalltag gut gerüstet sind.

Für den Koordinator Betrieblicher Ermittlungen konzentrieren wir uns auf praxisorientierte Inhalte, die von der Durchführung interner Ermittlungen über die rechtssichere Dokumentation bis hin zur Zusammenarbeit mit externen Behörden reichen. Hier spielt auch die Schulung in Befragungstechniken und der Umgang mit sensiblen Daten eine zentrale Rolle.

Die Geprüfte Schutz- und Sicherheitskraft (IHK) richtet sich an Sicherheitskräfte, die eine vertiefte Qualifikation anstreben. Hier setzen wir auf eine Kombination aus theoretischer Wissensvermittlung und praxisnahen Übungen, die Themen wie Arbeitsschutz, Notfallmanagement und rechtliche Befugnisse behandeln.

Themen wie Wirtschaftskriminalität und Cyber-Security spiegeln die aktuellen Herausforderungen wider, mit denen Unternehmen zunehmend konfrontiert sind. Unser Fokus liegt auf der Sensibilisierung für Bedrohungen, der Prävention von Angriffen und der Vermittlung von Grundlagen in IT-Sicherheit und Cyber-Forensik. Damit geben wir unseren Teilnehmenden die Werkzeuge an die Hand, um wirtschaftliche Schäden zu verhindern und Sicherheit in digitalen und physischen Bereichen zu gewährleisten.

Dies ist nur ein kleiner Auszug unseres Programms. Mit diesem modularen Ansatz bieten wir Schulungen, die von der Basisqualifikation bis zur Expertenstufe reichen, und orientieren uns dabei stets an den Bedürfnissen der Unternehmen und der Praxis.

Vielfach wird die Notwendigkeit gesehen, das Image der Sicherheit als Feld der beruflichen Betätigung allgemein zu stärken. Wie sehen Sie das bei der VSW?

Branka Berges: Die VSW sieht die Notwendigkeit, das Image der Sicherheitsbranche als Berufsfeld zu stärken, ebenfalls als sehr wichtig an. Sicherheit ist heute ein zentrales Thema, das weit über traditionelle Sicherheitsberufe hinausgeht. Die fortschreitende Digitalisierung und die zunehmenden Bedrohungen im Cyberraum machen Sicherheitsfachkräfte zu unverzichtbaren Experten, deren Aufgaben immer komplexer und vielfältiger werden.

Unsere Ansätze zur Stärkung des Images umfassen beispielsweise Aufklärung und Öffentlichkeitsarbeit: Wir setzen uns dafür ein, das Berufsbild von Sicherheitsexperten als hochqualifizierte, zukunftssträchtige Tätigkeit in der breiten Öffentlichkeit stärker zu positionieren. Durch unser Aus- und Weiterbildungsprogramm tragen wir dazu bei, dass Sicherheitsberufe als hochqualifizierte und innovative Berufsfelder wahrgenommen werden. Die VSW engagiert sich aktiv, das Bewusstsein für die Bedeutung der Sicherheitsbranche zu steigern und qualifizierte Fachkräfte zu fördern. **GIT**

Newsletter abonnieren Jetzt

inklusive e-Ausgabe!

Ihre Nummer 1 seit mehr als 30 Jahren

WILEY

Nachrichten für Entscheider und Führungskräfte in Sachen Sicherheit

WILEY


**Vereinigung für die Sicherheit
 der Wirtschaft e.V.**
 Hessen, Rheinland-Pfalz, Saarland
www.vsw.de

Fraport setzt Walk-Through-Scanner von Rohde & Schwarz ein

Als erster Flughafen weltweit setzt Fraport zukünftig Walk-Through-Scanner von Rohde & Schwarz an den Sicherheitskontrollen für Passagiere im Regelbetrieb ein. Nach einer rund einjährigen Testphase im operativen Einsatz an der Sicherheitskontrolle im Terminal 1, Halle A, hat die Bundespolizei den QPS Walk2000 nun für den dauerhaften Einsatz als Luftsicherheitskontrolltechnik zertifiziert und zugelassen. Pro Tag passieren bis zu 18.000 Fluggäste die hochfrequentierte Kontrollstelle. Perspektivisch ist der Einsatz an weiteren Kontrollstellen im Terminal 1 und im zukünftigen Terminal 3 geplant. „Mit dem 360°-Durchgangsscanner setzen wir als erster Airport weltweit einen neuen Standard bei den Passagierkontrollen im Luftverkehr“, betont Alexander Laukenmann, Geschäftsbereichsleiter Aviation der Fraport AG.



Nun im Regelbetrieb am Flughafen Frankfurt im Einsatz: der R&S QPSWalk2000

www.rohde-schwarz.com



Paxton eröffnet US-Zentrale in Greenville

Paxton hat die Eröffnung seiner neuen US-Zentrale bekannt gegeben. Das Unternehmen beabsichtigt, seine Präsenz in den USA zu erweitern, indem es zehn Millionen Dollar in das Projekt in Greenville, SC investiert. „Die neue US-Zentrale von Paxton wurde nach Weltklasse-Standards gebaut. Sie spiegelt das Ausmaß unserer Ambitionen und unseren Glauben an Greenville als fantastischen Hub wider, um talentierte Menschen zu rekrutieren und das Geschäftswachstum auf dem nordamerikanischen Markt zu unterstützen. Wir erwarten eine schnelle Erweiterung unserer Technologieherstellungskapazitäten und die Bereitstellung zugehöriger Dienstleistungen, wodurch Arbeitsplätze in der lokalen Gemeinschaft geschaffen werden“, so Adam Stroud, CEO von Paxton. Das neue Gebäude mit einer Fläche von 2.700 Quadratmetern wurde für die sich ändernden Bedürfnisse und Erwartungen von Kunden und Mitarbeitern konzipiert. www.paxton-access.com/de



Feiern Sie mit uns und lernen Sie uns kennen auf der

VIDEOR InfoTour 2025

05.06. | Frankfurt | Klassikstadt

28.08. | Dresden | Gläserne Manufaktur

04.09. | Oberhausen | TopGolf

Seit 50 Jahren vertrauen Facherrichter und Sicherheitsverantwortliche auf VIDEOR. Warum, das können Sie auf unserer Jubiläums-Roadshow live erleben.

Freuen Sie sich auf anregende Keynotes, persönliche Gespräche mit Top-Herstellern und profitieren Sie von neuen Impulsen für Ihr Geschäft – wir freuen uns auf Sie!

Jetzt kostenfrei anmelden!

wp.videor.com/infotour-2025





VERBÄNDE

Innovationen in der Sicherheitstechnik

Zum zweiten Mal: Fachkongress BVS SecTec



Am 5. und 6. Juni 2025 lädt der Bayerische Verband für Sicherheit in der Wirtschaft (BVS) zur BVS SecTec ein. Dieser Fachkongress bietet eine einzigartige Plattform rund um aktuelle Entwicklungen, Regularien und Trends im Bereich der Sicherheitstechnik.

Nach dem erfolgreichen Auftakt im vergangenen Jahr geht der Fachkongress SecTec in die zweite Runde: „Unternehmen müssen sich gegen eine Vielzahl von Bedrohungen schützen, gleichzeitig kommen technische Innovationen auf den Markt, die sich für die Sicherheit nutzen lassen. Die BVS SecTec fungiert hier als Treffpunkt für Expertinnen und Experten und bietet eine erstklassige Plattform für den Austausch von Know-how sowie den Aufbau von geschäftlichen Verbindungen“, sagt BVS-Geschäftsführerin Caroline Eder.

Sicherheitstechnik und rechtliche Rahmenbedingungen

Die Vorträge auf der Veranstaltung bieten den Besuchern ein breit gefächertes Themenspektrum. Auf der Agenda stehen Präsentationen zu aktuellen Herausforderungen in der Sicherheit, sowie mögliche Lösungsansätze, die auf den neusten Entwicklungen der Sicherheitstechnik basieren.



BVS-Geschäftsführerin Caroline Eder (Mitte) und ihr Team freuen sich auf die SecTec 2025. V.l.n.r.: Elisabeth Lindemeyer, Referentin Grundsatzangelegenheiten und Verbandsmanagement; Caroline Eder, Geschäftsführerin; Sandra Sicheneder, Referentin Projekt- und Medienmanagement

Zudem wird auch ein Augenmerk auf die Bedrohungen aus dem Cyberraum gerichtet: Die Digitalisierung hat dafür gesorgt, dass immer mehr Dinge mit dem Internet verbunden sind. Daher stehen nicht nur die IT-Systeme aktuell im Fokus von Cyberkriminellen. Auch die Betriebstechnologie (Operational Technologie, kurz: OT) bietet durch den immer höheren Vernetzungsgrad eine stetig wachsende Angriffsfläche. Die künstliche Intelligenz (KI) verschärft die Lage zusätzlich, denn damit haben Angreifer die Möglichkeit, die vernetzten Systeme automatisiert auf Schwachstellen zu durchsuchen und die passende Schadsoftware programmieren zu lassen.

Informationen zu den rechtlichen Rahmenbedingungen dürfen auf einem Fachkongress für Sicherheitstechnik nicht fehlen: Von der NIS2- Richtlinie über den Cyber Resilience Act bis hin zur EU-Maschinenverordnung gibt es immer

Veranstaltungsort:

NH München Ost Conference Center,
Einsteinring 20, 85609 Aschheim bei
München



Anmeldung und
Teilnahme unter:
[www.bvsw.de/
bvsw-sectec](http://www.bvsw.de/bvsw-sectec)

mehr Vorschriften, bei deren Umsetzung Sicherheitstechnik eine wichtige Rolle spielen kann.

Ganzheitliches Ausstellungskonzept

Die räumliche Gestaltung der Veranstaltung ist darauf ausgerichtet, den Austausch zwischen Besuchern und Ausstellern zu fördern. Die Ausstellungsfläche ist strategisch zwischen Catering-Bereichen und Vortrags-

räumen platziert, um eine dynamische Atmosphäre zu schaffen. Unternehmen haben hier die Möglichkeit, ihre innovativen Lösungen einem hochkarätigen Fachpublikum zu präsentieren und Kontakte zu knüpfen. Diese besondere Anordnung schafft Synergien zwischen Vorträgen, Networking und Produktpräsentationen und trägt zur einzigartigen Atmosphäre der SecTec bei, so die Veranstalter.

Die BVSW stellt eine limitierte Anzahl an exklusiven Ausstellungsflächen zur Verfügung, die eine optimale Sichtbarkeit garantieren und den interaktiven Charakter der SecTec unterstützen.



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

© Bilder: BVSW

ZVEI: Arge Errichter und Planer wählt neuen Vorstand

Christian Kühn, Klemens Siebers und Percy Görgens sind in den Vorstand der Arge Errichter und Planer des ZVEI gewählt worden. Christian Kühn (Schlentzek & Kühn GmbH) ist weiterhin Vorsitzender des Vorstands. Außerdem wurden Klemens Siebers (Wisag Sicherheitstechnik GmbH & Co. KG) als Stellvertreter und Percy Görgens (Percy Görgens UG) als weiteres Mitglied des Vorstands gewählt. Der Vorstand wird sich auf die strategische Ausrichtung der Arbeitsgemeinschaft konzentrieren. „Der deutschen Sicherheitstechnik-Branche stehen spannende Jahre bevor. Vernetzung und Digitalisierung sind zugleich Herausforderung und Chance“, so Christian Kühn. „Als Vorstand möchten wir uns gemeinsam mit unseren Mitgliedern für hohe Qualitätsstandards und Zusammenarbeit in der Branche einsetzen. Durch einen nachhaltigen Erfahrungsaustausch stellen wir zudem die Handlungsfähigkeit unserer Mitglieder sicher.“

www.zvei.org

BDSW fordert bessere Rahmenbedingungen

Der Bundesverband der Sicherheitswirtschaft (BDSW) präsentiert sein Positions- und Forderungspapier zur Bundestagswahl 2025 und fordert eine Stärkung der Sicherheitswirtschaft als elementaren Bestandteil der nationalen Sicherheitsarchitektur. Angesichts zunehmender Bedrohungen durch Kriminalität, Cyberangriffe, Extremismus und geopolitische Spannungen fordert der Verband politische und regulatorische Maßnahmen, um die Sicherheitswirtschaft als zuverlässigen Partner u. a. für den Schutz kritischer Infrastrukturen (KRITIS) weiterzuentwickeln. Der BDSW sieht zur Stärkung der Sicherheitswirtschaft dringenden Handlungsbedarf in mehreren Kernbereichen und die Politik sei gefordert, bessere Rahmenbedingungen zu schaffen. Der Verband hebt hervor, dass die Sicherheitswirtschaft mit ihren rund 290.000 Beschäftigten einen unverzichtbaren Beitrag zur inneren Sicherheit leistet. Dennoch fehlen politische Weichenstellungen, um die Branche nachhaltig zu unterstützen und weiterzuentwickeln.

www.bdsw.de

OPEN – Eventkonzept von Axis Communications

Axis Communications richtet in diesem Jahr zum ersten Mal in der DACH-Region das Event OPEN aus. Die Eventreihe OPEN hat das Unternehmen im Jahr 2023 ins Leben gerufen. Seitdem fand die Veranstaltung bereits in den Städten Paris, Madrid, London, Oslo, Helsinki, Lissabon, Mailand und Malmö mit insgesamt über 3.500 Teilnehmern statt. Jetzt kommt das Event erstmals auch in die DACH-Region. Die Veranstaltung findet am 20. Mai 2025 von 09:30 bis 17 Uhr in der Lokhalle in Göttingen statt. Ziel der Veranstaltung ist es, Partnern und Endkunden von Axis eine gemeinsame Plattform zu bieten, um sich über aktuelle Entwicklungen und Zukunftsperspektiven in der Sicherheitslandschaft und darüber hinaus auszutauschen. Teilnehmer erwarten Updates zum Produktportfolio, Keynotes, eine Podiumsdiskussion und intensive Breakout-Sessions zu Themen, die die Tech-Welt bewegen: digitale Transformation, künstliche Intelligenz, Cloud und Cybersicherheit.

www.axis.com

Western Digital stellt Zukunftsstrategie vor

Der designierte CEO Irving Tan präsentierte die Vision und strategische Ausrichtung von Western Digital sowie Wachstumsprognosen für den KI-Markt auf dem Investor Day 2025 in New York. Außerdem kündigte er die Erprobung der HAMR-Technologie mit Hyperscale-Kunden an. Der designierte CEO Irving Tan bekräftigte Western Digitals führende Rolle als Anbieter erstklassiger, nachhaltiger Speicherlösungen für große Datenmengen. Mit langjähriger Erfahrung in HDD-Technologien und -Innovationen liefert das Unternehmen weiterhin modernste Speicherlösungen, die niedrige Gesamtbetriebskosten (TCO) für die weltweit größten Hyperscaler, CSPs (Cloud-Service-Provider) und OEMs (Original Equipment Manufacturer) ermöglichen. Von heliumgefüllten Laufwerken über branchenführende ePMR CMR-HDDs bis hin zur hochentwickelten UltraSMR-Technologie: Das Unternehmen treibt kontinuierlich Innovationen in der Branche voran – immer mit dem Kunden im Blick.

www.westerndigital.com

Zwei Veranstaltungen, ein gemeinsames Ziel: Die Euro Defence Expo (EUDEx) und die jährliche Konferenz des NATO Joint Air Power Competence Centre (JAPCC) finden 2026 parallel statt



MESSEN

Zivil und militärisch

Euro Defence Expo (Eudex) und NATO Joint Air Power Competence Centre (JAPCC) parallel zur Security 2026 in Essen

Vom 22. bis 25. September 2026 wird die Euro Defence Expo (Eudex) ihre Premiere in der Messe Essen begehen – gleichzeitig mit der jährlichen Konferenz des NATO Joint Air Power Competence Centre (JAPCC) sowie der Security Essen (22. bis 25. September 2026). Während die NATO-Veranstaltung hochrangige Militärvertreter aus den 32 Mitgliedsnationen versammelt, präsentiert die neue Verteidigungsmesse innovative Technologien für Sicherheit und Verteidigung.

Die Euro Defence Expo ist konzipiert als umfassende Plattform für Entscheidungsträger, Experten und Innovatoren, um sich über Neuheiten rund um Sicherheits- und Verteidigungstechnologien zu informieren und auszutauschen. Oliver P. Kuhrt, Geschäftsführer der Messe Essen: „Angesichts der aktuellen Bedrohungslage müssen wir Schutz und Sicherheit neu denken. Daher haben wir mit der Kombination aus Euro Defence Expo und Security Essen ein einzigartiges, hochspannendes Messeformat aus militärischer und ziviler Leistungsschau plus begleitender Konferenz entwickelt. Damit kann sich unsere Gesellschaft stark für die Herausforderungen der Zukunft aufstellen.“

Die Euro Defence Expo (EUDEx) setzt auf den Total-Defence-Ansatz: Dieses Konzept, so die Veranstalter, integriert alle ge-



Während die NATO-Veranstaltung hochrangige Militärvertreter aus den 32 Mitgliedsnationen versammelt, präsentiert die neue Verteidigungsmesse innovative Technologien für Sicherheit und Verteidigung



Auftaktveranstaltung der Euro Defence Expo 2026

sellschaftlichen Akteure, um Demokratie, Sicherheit und Freiheit gegen jegliche Bedrohung zu schützen – von hybriden Aktivitäten über Cyber-Attacken bis hin zur offenen militärischen Konfrontation. Geplant sind daher verschiedene Möglichkeiten und Foren für den Austausch zwischen Politik, Industrie und dem militärischen Nutzer von Sicherheits- und Verteidigungstechnologien.

Die enge Verzahnung von Eudex und JAPCC soll zusätzliche Gelegenheiten für direkte Gespräche zwischen Industrie und Militär schaffen. Bisher geplant sind unter anderem eine gemeinsame Abendveranstaltung sowie Möglichkeiten zum gegenseitigen Besuch beider Veranstaltungen. Oberstleutnant André Haider vom Joint Air Power Competence Centre (JAPCC): „Mit dieser Zusammenarbeit fördern wir den Dialog zwischen Militär und Industrie. Wir freuen uns auf die Gelegenheit, mit relevanten Partnern ins Gespräch zu kommen, innovative Lösungen schneller zu identifizieren und zu integrieren.“

Für Julia Jacob, Projektleiterin der EUDEx, ist die JAPCC-Konferenz „ein weiterer wichtiger Baustein für unseren Ansatz, Sicherheit aus einer ganzheitlichen Perspektive zu betrachten.“ Mit der Kombination aus Fachmessen, Konferenz und Networking-Möglichkeiten wolle man „gemeinsam ein Must-have Event für Unternehmen“ schaffen, „die die Zukunft der Verteidigungs- und Sicherheitsbranche aktiv prägen wollen.“

Eudex: von Land bis Cyberraum

Deutschlands Sicherheits- und Verteidigungsindustrie ist ein wesentlicher Stützpfiler der Sicherheitsvorsorge und innovativer Vorreiter bei der Ausrüstung von Landstreitkräften. Die Euro Defence Expo fokussiert sich daher auf die neuesten Trends und Entwicklungen in der Dimension Land über alle Fähigkeitsdomänen

hinweg. Einen weiteren Schwerpunkt wird das Thema Cybersicherheit und die Abwehr von Bedrohungen aus dem Cyber- und Informationsraum bilden.

Das Format der neuen Verteidigungsmesse überzeugt die Branche, wie die Veranstalter berichten. Zu den bereits angemeldeten Ausstellern gehören unter anderem Heckler & Koch und die Deutsche Risikoberatung. Andreas Schnautz, von Heckler & Koch: „Die Messe Essen setzt mit der Euro Defence Expo das richtige Zeichen für unsere Zeit. Die deutsche Rüstungsindustrie ist fest verankert in der Weltspitze, sie ist leistungsfähig und hochinnovativ. Der russische Angriffskrieg hat noch einmal vor Augen geführt, dass die deutsche wehrtechnische Industrie Teil der Sicherheitsarchitektur unseres Landes sein muss“.

Für Entscheider der Branche

Mit ihrem Konzept und ihren Ausstellern richtet sich die Euro Defence Expo unter anderem an Angehörige der Bundeswehr und verbündeter Streitkräfte, Entscheidungsträger aus den nationalen und internationalen Beschaffungsorganisationen, Vertreter von Verteidigungsministerien, Regierungs- und Ministerialvertreter, Politiker, Vertreter von Polizei und weiteren relevanten Sicherheits- und Strafverfolgungsbehörden sowie Institute und Technologieunternehmen. Ganz gezielt werden dabei die Entscheider angesprochen. **GIT**



Messe Essen
www.eurodefenceexpo.de

JAPCC
www.japcc.org/conference

Jetzt

Newsletter abonnieren



Ihre
Nummer 1
seit mehr als
30 Jahren

Nachrichten für
Entscheider und
Führungskräfte in
Sachen Sicherheit

inklusive
e-Ausgabe!



WILEY

SICHERHEITSDIENSTLEISTUNGEN

„Deutschland braucht Kurswechsel in der Wirtschaftspolitik“

Kötter Unternehmensgruppe: Umsatz wächst auf 722 Millionen Euro



© Kötter

Die Mitarbeiterzahl der Kötter Unternehmensgruppe hat sich im vergangenen Jahr um 8,1 % erhöht, der Umsatz um mehr als 15 %

Die Kötter Unternehmensgruppe hat sich im vergangenen Geschäftsjahr am Markt behauptet. Der Umsatz stieg um 15,2% auf 722 Millionen Euro, die Mitarbeiterzahl erhöhte sich auf 16.000 Beschäftigte (+ 8,1%). Diese Entwicklung gab die Dienstleistungsgruppe, die zu den Top 10 der Facility-Service-Anbieter in Deutschland zählt und mit der Sparte Security zudem größtes Familienunternehmen der Sicherheitsbranche ist, bekannt.

„Ich bin stolz darauf, dass unsere Gruppe in schwierigstem Fahrwasser Kurs gehalten hat und durch den Dreiklang aus riesigem Mannschaftsgeist, Branchen-Diversifizierung sowie ganzheitlichen Qualitätslösungen dieses für unsere stabile wirtschaftliche Entwicklung wichtige Umsatzwachstum erzielen konnte“, sagte Verwaltungsrat Friedrich P. Kötter. Der Familienunternehmer warnte gleichzeitig vor überzogenen Erwartungen. „Unsere im vergangenen Jahr mit organischem und anorganischem Wachstum erzielte Entwicklung ist kein Selbstläufer, im Gegenteil: Weil für 2025 das dritte Rezessionsjahr in Folge droht und parallel die De-Industrialisierung ungebremsst voranschreitet, bleibt das Umfeld für Anbieter unternehmensnaher Dienstleistungen äußerst angespannt. Denn: Gibt es immer weniger Neuinvestitionen in

Deutschland oder hält die Insolvenzswelle mit fortlaufend neuen Rekordwerten an, sind auch unsere Leistungen immer weniger gefragt.“

Zertifizierung für KRITIS-Schutz

Die Gruppe will ihr Geschäftsmodell der integrativen und zunehmend digitalisierten Facility Services weiter ausbauen. „Bei der Digitalisierung liegt unser Fokus auf zwei Kernbereichen: Zum einen wird die Zusammenarbeit mit unseren Kunden und Beschäftigten durch weitere digitale Lösungen schneller und einfacher“, so Friedrich P. Kötter. „Gleichzeitig nutzen wir die Digitalisierung und KI für den Ausbau bestehender bzw. die Entwicklung neuer Leistungen. Genannt seien z. B. der zunehmend umfangreichere Einsatz von Reinigungsrobotern oder Hightech-Lösungen zur Überwachung der immer wichtiger werdenden Cybersicherheit von Unternehmen“.

Entscheidenden Rückenwind, so das Unternehmen, steuere insbesondere die Beteiligung am Luxemburger Cyber Security-Spezialisten G.I.P bei, mit der sich Kötter Security als einer der ersten Anbieter für in Eigenregie erbrachte 360-Grad-Unter-

nehmenssicherheit in Europa positionierte. Last, but not least konnte Kötter Security durch die Zertifizierung gemäß DIN EN 17483 (Private Sicherheitsdienstleistungen – Schutz kritischer Infrastrukturen) jüngst die Kompetenzen für hochqualitativen KRITIS-Schutz weiter stärken. Dabei, so das Unternehmen, unterstreiche die parallele Auditierung für die Komplett-Stufen 1–3 die führende Rolle im Sicherheitssektor: Denn als einer von europaweit nur ganz wenigen Anbietern sei das Familienunternehmen damit gleichermaßen für den Teil 1 „Allgemeine Anforderungen“ als auch für die sektorspezifischen Teile 2 „Flughafen- und Luftsicherheitsdienstleistungen“ bzw. 3 „Sicherheitsdienstleistungen für Seeschifffahrt und Seehäfen“ zertifiziert.

Kritik an „überbordender Bürokratisierung“

Angesichts der anhaltenden wirtschaftlichen Schwäche Deutschlands mahnt der Familienunternehmer nach der Bundestagswahl eine strikte und umgehende Neuausrichtung in der Wirtschaftspolitik sowie höchstes Reformtempo an. Im Fokus stehe dabei neben der Senkung der Steuer-

und Abgabenlast sowie Investitionen in die analoge und digitale Infrastruktur vor allem die drastische Reduzierung der Bürokratie. „Die ungebremste Bürokratisierung hat nahezu alle Wirtschaftsbereiche erfasst und ist zu einem Hemmschuh und eine riesige Belastung für jedes Unternehmen geworden. Allein unsere Gruppe kosten die Folgen der überbordenden Bürokratisierung jährlich mindestens sieben Millionen Euro – Tendenz steigend. Geld, das wir sinnvoller in die Aus- und Weiterbildung unserer Beschäftigten oder neue digitale Angebote für die Kunden investieren könnten“, stellte Friedrich P. Kötter heraus. „Dies zeigt die doppelte Handlungserfordernis: Das Regelungsdickicht muss gelichtet werden und eine Digitalisierungsoffensive bei der öffentlichen Hand erfolgen, um z. B. endlich für die konsequente Schaffung von digitalen Schnittstellen zu den Unternehmens-EDV-Systemen sowie Datenaustausch zwischen den Behörden zu sorgen.“ **GIT**



Kötter GmbH & Co. KG
www.koetter.de



SiCUREZZA

INTERNATIONAL SECURITY & FIRE EXHIBITION

19 – 21 NOVEMBER 2025 | fieramilano

www.sicurezza.it

f X @ in

MIBA

MILAN INTERNATIONAL BUILDING ALLIANCE

ASSOCIATED TO



INTERNATIONAL NETWORK



www.exposec.com.br



www.fireshow.com.br



GEE GLOBAL ELEVATOR EXHIBITION

MADE EXPO

SMART BUILDING EXPO

SiCUREZZA



FIERA MILANO



© Peter Lauwe

BEVÖLKERUNGSSCHUTZ

Die Lebensadern der Gesellschaft

Zur Stärkung der Resilienz Kritischer Infrastrukturen

Vor mehr als zwei Jahrzehnten gegründet, ist das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) die Zentrale Stelle des Bundes für den Bevölkerungsschutz in Deutschland. Die aktuelle politische Lage rückt insbesondere das Thema der Zivilen Verteidigung verstärkt in den Fokus der Aufmerksamkeit. Dazu gehört auch die Resilienz der Kritischen Infrastrukturen. GIT SICHERHEIT sprach darüber mit Peter Lauwe, Leiter der Referatsgruppe Infrastrukturschutz beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.

■ GIT SICHERHEIT: Herr Lauwe, das BBK gibt es seit 2004 und dient seitdem als zentrale Stelle des Bundes für den Bevölkerungsschutz in Deutschland. Könnten Sie bitte zunächst einmal den Begriff der Zivilen Sicherheitsvorsorge eingrenzen, um den es hier geht?

Peter Lauwe: Im Kern geht es um den Schutz der Gesellschaft und ihrer Lebensgrundlagen. Wir im Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) arbeiten an nicht-militärischen Maßnahmen, die darauf abzielen, die Gesellschaft vor Krisen, Katastrophen und militärischen Bedrohungen zu schützen und sie gegenüber diesen resilienter zu machen. Darunter fällt beispielsweise die Warnung der Bevölkerung vor Gefahrenlagen, die Förderung der Selbsthilfefähigkeit der Bürgerinnen und Bürger sowie die Stärkung eines effizienten Risiko- und Krisenmanagements von staatlichen und privaten Akteuren. Angesichts der vergangenen und aktuellen sicherheitspolitischen Veränderungen steht insbesondere die Zivile Verteidigung im Mittelpunkt unseres Handelns. All das gehört zu einer gesamtgesellschaftlichen Sicherheitsvorsorge, die den Schutz der Bevölkerung sowie die staatliche Handlungsfähigkeit gewährleisten muss. Einer meiner Arbeitsschwerpunkte ist dabei die Resilienz von Kritischen Infrastrukturen zu stärken.

Das passt in der Tat gut zusammen, denn die Bevölkerung braucht Wasser, Strom, Verkehrswege, etc. ...

Peter Lauwe: Richtig – Kritische Infrastrukturen sind die Lebensadern unserer modernen Gesellschaft. Die Energie- und Wasserversorgung, der Transport von Gütern oder z.B. auch die medizinische Versorgung sind lebensnotwendig für das Funktionieren des öffentlichen Lebens. Kommt es zu Störungen oder Ausfällen, kann das weitreichende Folgen für die Sicherheit der Bevölkerung haben. Der Schutz Kritischer Infrastrukturen ist insofern ein wichtiger Bestandteil des Bevölkerungsschutzes.

Ihre Zuständigkeit für Kritische Infrastruktur besteht demnach auch unabhängig davon, ob das KRITIS-Dachgesetz verabschiedet wird oder nicht?

Peter Lauwe: Grundsätzlich tragen viele Akteure zum Schutz Kritischer Infrastrukturen bei. Die gesetzliche Grundlage für unsere Arbeit in diesem Bereich ist das Zivilschutz- und Katastrophenhilfegesetz (ZSKG). Dort wird geregelt unter welchen Umständen das BBK Daten erheben und verarbeiten darf, unter anderem über Infrastrukturen, bei deren Ausfall die Versorgung der Bevölkerung erheblich beeinträchtigt wird. Darüber hinaus darf der Bund die

Bundesländer beim Schutz Kritischer Infrastrukturen beraten und unterstützend tätig werden. Zudem wurde 2009 mit der Verabschiedung einer nationalen Strategie zum Schutz Kritischer Infrastrukturen eine gemeinsame Grundlage und strategische Zielvorstellung zum Schutz Kritischer Infrastrukturen in Deutschland geschaffen.

Die Umsetzung der dem KRITIS-Dachgesetz zugrundeliegenden EU-Richtlinie hat sich ja nun durch die vorgezogenen Neuwahlen des Deutschen Bundestags erst mal verschoben. Lassen Sie uns mal annehmen, dass es inhaltlich im Wesentlichen beim Referentenentwurf mit seinem All-Gefahren-Ansatz und der koordinierenden Rolle des BBK bleibt: Welche neuen Aufgaben kommen dann auf Ihre Behörde zu?

Peter Lauwe: Bei Umsetzung der EU-Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie) ist viel in Bewegung und das Gesetzgebungsverfahren muss zunächst abgeschlossen werden, bevor wir uns näher dazu äußern können. Die Umsetzung der Richtlinie bleibt weiter vordringlich.

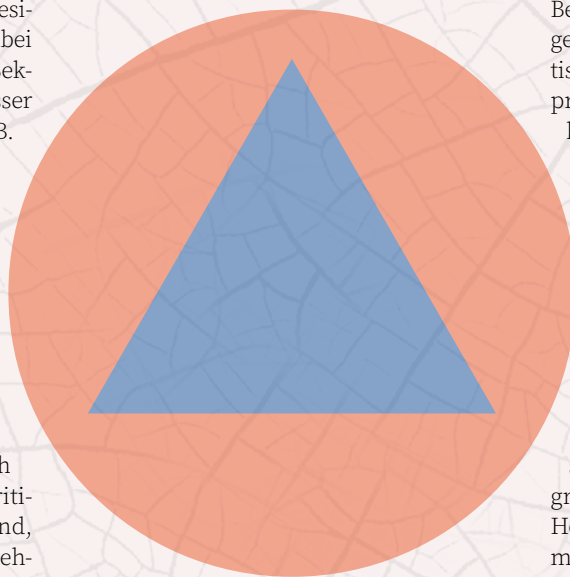
Könnten Sie dennoch anhand dieses Bereichs KRITIS einmal generell die Arbeitsweise des BBK skizzieren?

Peter Lauwe: Allgemein ist zu betonen, dass der Schutz von Kritischen Infrastrukturen nicht an „einer“ Stelle erfolgt, sondern eine gesamtgesellschaftliche Aufgabe mit vielen Schnittstellen ist. Zwischen Staat und Wirtschaft existieren enge Kooperationen, um die Versorgungssicherheit für die Bevölkerung zu gewährleisten. Grundsätzlich ist es Aufgabe der Betreiber Kritischer Infrastrukturen für einen sicheren und zuverlässigen Betrieb ihrer Anlagen zu sorgen. Das BBK berät, unterstützt, plant, schult und vernetzt zur Steigerung der Resilienz von Kritischen Infrastrukturen. Dabei arbeiten wir sowohl in den jeweiligen Sektoren (z.B. Ernährung, Gesundheit, Wasser etc.) als auch sektorübergreifend wie z.B. zu grundsätzlichen Fragestellungen des Risiko- und Krisenmanagements. Wir entwickeln Schutzkonzepte und methodische Grundlagen, arbeiten an der Erstellung von Regelwerken mit und begleiten Forschungsvorhaben. In unserer länderübergreifenden Krisenmanagementübung „LÜKEX“ proben wir auch regelmäßig den Ernstfall auf strategischer Ebene. All das wird flankiert von einem intensiven Austausch mit Akteuren, die mit dem Schutz Kritischer Infrastrukturen betraut sind: Bund, Bundesländer, Kommunen und Unternehmen. Beispielsweise ist seit 2012 eine Bundesländer Arbeitsgruppe etabliert: die Koordinierungsstelle für den Schutz Kritischer Infrastrukturen in Bund und Ländern (AG KOST KRITIS). Auch die Zusammenarbeit zwischen Betreibern Kritischer Infrastrukturen, deren Verbänden und den zuständigen staatlichen Stellen in der sogenannten UP KRITIS (Unabhängige Partnerschaft KRITIS) ist eine wichtige Schnittstelle für das BBK und seine Arbeit.

Ist die Aufsichtsfunktion Ihrer Behörde auch deshalb erforderlich, weil die Kritischen Infrastrukturen nicht isoliert zu sehen sind, sondern es Interdependenzen gibt? Probleme beim Strom etwa führen zu Problemen in Krankenhäusern und im Verkehr, etc...?

Peter Lauwe: Viele Kritische Infrastrukturen sind abhängig voneinander. Diese Interdependenzen zwischen Sektoren und Branchen können das Ausfallrisiko erhöhen. In besonderen Fällen kann das zu Domino- oder Kaskadeneffekten führen, das ist z.B. bei der Abhängigkeit von der Energieversorgung und von Informations- und Telekommunikationstechnik besonders relevant. Kein moderner KRITIS-Betreiber kann heute ohne Strom und Informationstechnik arbeiten. Auch

hier gilt es, einen Überblick zu bewahren und diese Abhängigkeiten und Risiken im Vorfeld in den Blick zu nehmen. Das muss sowohl beim KRITIS-Betreiber selbst als auch durch staatliche Stellen, z.B. durch die Kommune passieren. Im BBK versuchen wir beispielweise über den Ansatz des Integrierten Risikomanagements die staatlichen Akteure mit Betreibern Kritischer Infrastrukturen zu vernetzen und einen strukturierten Austausch zu fördern.



Parallel zum KRITIS-Dachgesetz läuft ja die Umsetzung der NIS2-Richtlinie zur Gewährleistung von Mindeststandards in der Cybersicherheit – und hier übernimmt das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Aufsicht. Das ist sicherlich eine nahe-liegende Aufgabenverteilung?

Peter Lauwe: Das BBK und das Bundesamt in der Sicherheit in der Informationstechnik (BSI) arbeiten seit Jahren beim Schutz Kritischer Infrastrukturen zusammen. Es bestehen institutionalisierte Schnittstellen über das Nationale Cyber-Abwehrzentrum und die UP KRITIS. Darüber hinaus gibt es regelmäßige Austauschformate auf Arbeitsebene in den jeweiligen Sektoren sowie sektorübergreifend.

Herr Lauwe, Kritische Infrastrukturen müssen resilient gemacht werden gegen Gefahren – das ist der Sinn des ganzen EU-weiten normativen Unterfangens. Wie schätzen Sie eigentlich die Gefahren ein? Nehmen sie tatsächlich zu?

Peter Lauwe: In den letzten Jahren erleben wir eine Häufung von Krisen, deren

Auslöser oft vielfältig und komplex sind. Sie reichen von sicherheitspolitischen Entwicklungen wie dem Angriffskrieg Russlands gegen die Ukraine, über extreme Wetterereignisse als Folge des Klimawandels oder auch einer zunehmenden weltweiten Vernetzung, wie uns etwa während der Covid-19 Pandemie vor Augen geführt wurde. Kritische Infrastrukturen können gezielt angegriffen werden. In dieser Hinsicht ist ihr Schutz ein wichtiger Bestandteil der Verteidigungsfähigkeit eines Landes. Seit Beginn des Angriffskriegs von Russland gegen die Ukraine sehen wir besonders drastisch, dass Kritische Infrastrukturen häufig primäre militärische Ziele sind. Darüber hinaus sind sie im Fokus von Cyberangriffen oder Sabotageakten. Aber auch Gefahren wie Unfälle oder technische Störungen, können zu erheblichen Schäden und Beeinträchtigungen führen. Insofern gehen wir beim Schutz Kritischer Infrastrukturen von einem sehr breiten Gefahrenspektrum aus. Diese Herangehensweise bezeichnen wir als All-Gefahren-Ansatz. Einzelne, gefahrenspezifische Maßnahmen sollen sich diesem Ansatz folgend in ein übergreifendes Schutzkonzept einfügen. Die Herausforderung ist, dass Schutzmaßnahmen natürlich nie „abgeschlossen“ sind. Risikoanalysen und Übungen müssen regelmäßig durchgeführt und Notfallplanungen kontinuierlich angepasst werden.

Glauben Sie, dass wir auf dem richtigen Weg sind?

Peter Lauwe: In den letzten Jahren ist hier vieles auf den Weg gebracht worden wie z.B. höhere Standards oder eine stärkere Vernetzung zur frühzeitigen Erkennung von Bedrohungen. Für die Zukunft steht aber auch fest, dass wir uns noch resilienter aufstellen müssen – nicht nur Betreiber Kritischer Infrastrukturen wie Behörden und Unternehmen, sondern auch auf gesamtgesellschaftlicher Ebene. **GIT**



Bundesamt für Bevölkerungsschutz
und Katastrophenhilfe
www.bbk.bund.de

Das Rückgrat unseres Alltags

Kritische Infrastruktur und das neue Kritische Infrastruktur-Dachgesetz

Haben wir noch in den 1980er Jahren aufgrund des Gefühls des Friedens und der Sicherheit den Zivil- und Katastrophenschutz nahezu in die Bedeutungslosigkeit heruntergefahren, so befinden wir uns nunmehr in einer gegenläufigen Entwicklung. Unsere Welt ist zunehmend komplexer, vernetzter und digitaler geworden.

Ob Strom- und Wasserversorgung, Energieversorgung, Gesundheitsversorgung oder auch im Bereich des Transport- und Verkehrswesens: unsere Welt funktioniert nur, wenn diese kritischen Infrastrukturen (KRITIS) stabil sind und bleiben. Ein Beitrag von Dr. Daniela Lesmeister, Staatssekretärin beim nordrhein-westfälischen Ministerium des Inneren.



© Ministerium des Inneren NRW

Dr. Daniela Lesmeister,
Staatssekretärin Ministerium des Innern NRW

Wir sehen uns gegenwärtig einer immer stärker wachsenden Bedrohung ausgesetzt – sei es durch technisches Versagen, Cyberangriffe oder Sabotagen. In unserer digitalisierten Welt können Hackerangriffe oder gezielte Desinformationskampagnen ganze Systeme lahmlegen. Auch hat die aktuelle weltpolitische Lage, insbesondere der anhaltende Konflikt zwischen Russland und der Ukraine, direkte Auswirkungen auf die Sicherheitsarchitektur Europas und Deutschlands. Die jüngsten Entwicklungen im Zusammenspiel mit den USA zeigen eine sehr dynamische und für viele recht unerwartete Entwicklung, mithin eine Verschiebung in den internationalen Beziehungen. Diese geopolitischen Veränderungen erfordern eine kontinuierliche Anpassung und Stärkung der nationalen Sicherheitsstrategien, insbesondere im Bereich des Schutzes Kritischer Infrastrukturen.

Auswirkung auf unser tägliches Leben

Kritische Infrastrukturen sind jene Systeme, deren Ausfall oder Beeinträchtigung gravierende Auswirkungen auf die öffentliche Sicherheit, die Wirtschaft und das tägliche Leben der Bürgerinnen und Bürger haben können. Man stelle sich nur einmal die Auswirkungen eines mehrtägigen Stromausfalls vor. Krankenhäuser, Unternehmen, Lebensmittelzufuhr, der öffentliche Perso-

nennahverkehr wären sofort betroffen. Auswirkungen auf die Sicherheitslage würde es unmittelbar geben. Das Gleiche gilt für einen Cyberangriff auf wichtige digitale Netze. Der Zusammenbruch von Datenverkehren und Finanzsystemen wäre nur die Spitze des Eisbergs.

Daher ist es von größter Wichtigkeit, dass wir in Deutschland diese Infrastrukturen nicht nur allesamt identifizieren, sondern dass sie auch umfassend geschützt werden. Und zwar durch diejenigen, die jeweils für die KRITIS verantwortlich zeichnen. Geschäftsführer, Vorstände, Aufsichtsräte, Behördenleitungen – abhängig von der Art der jeweiligen KRITIS. Bislang besteht hier noch das Problem, dass noch nicht bei allen Verantwortungsträger die Notwendigkeit von entsprechenden Schutzmaßnahmen tatsächlich gesehen wird. Es ist Aufgabe des Staates, hier noch nachdrücklicher zu sensibilisieren.

Prävention, Resilienz und Krisenvorsorge

Der Schutz von KRITIS ist mindestens genauso komplex wie KRITIS selber und sollte mindestens aus den drei Säulen Prävention, Resilienz und Krisenvorsorge bestehen. Im Bereich der Prävention muss in moderne Schutzmaßnahmen investiert werden

und gleichzeitig damit das Bewusstsein einhergehen, dass es keine „unnützen“ Kosten sind, sondern letztendlich diese Schutzmaßnahmen sich bezahlt machen können. Eine Vernetzung von Staat, Wirtschaft und Wissenschaft gehört ebenso zum Bereich der Prävention.

Resilienz wird dadurch erreicht, dass Systeme Störungen bestmöglich verhindern und gleichzeitig im Bedarfsfall dann schnell bewältigen können.

Die Krisenvorsorge schließlich beinhaltet das große Thema Notfallpläne. Bevölkerung, Unternehmen und Behörden müssen sich für potentielle Ausfälle wappnen. Wichtige Prozesse sind dafür zu identifizieren und entsprechende Gegenmaßnahmen einzuleiten. So lagert z.B. die Polizei in Nordrhein-Westfalen bereits seit dem Jahr 2022 ihre eigenen Treibstoffdepots dezentral an gut erreichbaren Örtlichkeiten.

Das „Kritische Infrastruktur-Dachgesetz“

Die Notwendigkeit, den Schutz von KRITIS auch gesetzlich zu verankern, wurde bereits in der vergangenen Legislaturperiode auf Bundesebene erkannt. Leider ist der Gesetzesentwurf zum sogenannten KRITIS-Dachgesetz der Diskontinuität zum Opfer gefallen. Hier gilt es für die neue Bundesregie-

rung, schnellstmöglich daran anzuknüpfen und das Gesetz in Kraft treten zu lassen.

Denn dieses Gesetz verfolgt genau den richtigen Schutzzweck. Erstmals soll hier ein einheitlicher bundesrechtlicher Rahmen für den Schutz dieser Infrastrukturen geschaffen werden. Es soll die bereits bestehenden Regelungen des BSI-Gesetzes zur IT-Sicherheit um weitere zentrale Aspekte ergänzen. Kernpunkte des Gesetzes sind unter anderem die Festlegung bundeseinheitlicher Mindeststandards für Resilienz Maßnahmen, Meldepflichten für Stärkungen sowie Anforderungen an das Krisenmanagement und die physische Sicherheit.

Das Dachgesetz verfolgt mehrere zentrale Ziele:

1. Einheitliche Standards: Es schafft einheitliche Sicherheitsstandards für alle Betreiber kritischer Infrastrukturen, um ein hohes Schutzniveau zu gewährleisten. Dies umfasst sowohl physische als auch digitale Sicherheitsmaßnahmen.

2. Risikomanagement: Betreiber kritischer Infrastrukturen sind verpflichtet, ein umfassendes Risikomanagement zu implementieren. Dies beinhaltet die Identifikation von Risiken, die Bewertung ihrer Auswirkungen und die Entwicklung von Maßnahmen zur Risikominderung.

3. Meldesysteme: Das Gesetz sieht die Einrichtung von Meldesystemen vor, die es den Betreibern ermöglichen, Sicherheitsvorfälle schnell und effizient zu melden. Dies fördert eine schnellere Reaktion auf Bedrohungen und verbessert die Zusammenarbeit zwischen den verschiedenen Akteuren.

4. Schulung und Sensibilisierung: Ein weiterer wichtiger Aspekt des Gesetzes ist die Förderung von Schulungs- und Sensibilisierungsmaßnahmen für Mitarbeiter in kritischen Infrastrukturen. Nur durch gut ausgebildete und informierte Mitarbeiter kann die Sicherheit nachhaltig gewährleistet werden.

5. Zusammenarbeit zwischen Staat und Wirtschaft: Das Dachgesetz betont die Notwendigkeit einer engen Zusammenarbeit zwischen staatlichen Stellen und privaten Betreibern kritischer Infrastrukturen. Diese Kooperation ist entscheidend, um ein umfassendes Sicherheitsnetz zu schaffen.

Die Rolle der Digitalisierung

Ein zentraler Aspekt, der im Kontext kritischer Infrastrukturen nicht vernachlässigt werden darf, ist die fortschreitende Digitalisierung. Die Integration digitaler Technologien in die Betriebsabläufe kritischer Infrastrukturen bietet zahlreiche Vorteile, birgt jedoch auch erhebliche Risiken. Cyberangriffe auf kritische Systeme können verheerende Folgen haben, weshalb der Schutz vor solchen Bedrohungen eine der obersten Prioritäten sein muss.

Das Dachgesetz soll daher die Implementierung von Cyber-Sicherheitsmaßnahmen und die Entwicklung von Notfallplänen fördern, um im Falle eines Angriffs schnell und effektiv reagieren zu können.

Öffentlich-private Partnerschaften

Ein weiterer wichtiger Aspekt des neuen Gesetzes ist die Förderung von öffentlich-privaten Partnerschaften. Die Zusammenarbeit zwischen staatlichen Stellen und privaten Betreibern kritischer Infrastrukturen ist entscheidend, um ein umfassendes Sicherheitsnetz zu schaffen. Durch den Austausch von Informationen und Best Practices können beide Seiten voneinander lernen und ihre Sicherheitsstrategien optimieren. Zudem ermöglicht eine enge Kooperation eine schnellere Reaktion auf Bedrohungen und eine bessere Koordination im Krisenfall.

Schulung und Sensibilisierung

Die Schulung und Sensibilisierung der Mitarbeiter in kritischen Infrastrukturen ist ein weiterer zentraler Punkt des Dachgesetzes. Nur durch gut ausgebildete und informierte Mitarbeiter kann die Sicherheit nachhaltig gewährleistet werden. Regelmäßige Schulungen und Übungen helfen, das Bewusstsein für potenzielle Risiken zu schärfen und die Reaktionsfähigkeit im Ernstfall zu verbessern. Zudem sollten auch die Bürgerinnen und Bürger in die Sensibilisierungsmaßnahmen einbezogen werden.

Fazit und Ausblick

Zusammenfassend lässt sich sagen, dass die Umsetzung des KRITIS-Dachgesetzes einen wichtigen Schritt in Richtung eines umfassenden Schutzes kritischer Infrastrukturen darstellt. Es schafft einen einheitlichen rechtlichen Rahmen, der die Sicherheit und Resilienz dieser Infrastrukturen erhöht. Dennoch müssen wir uns der Herausforderungen bewusst sein, die mit der fortschreitenden Digitalisierung und den sich wandelnden Bedrohungen einhergehen.

Die kontinuierliche Anpassung unserer Sicherheitsstrategien, die Förderung von öffentlich-privaten Partnerschaften sowie die Schulung und Sensibilisierung aller Beteiligten sind entscheidend, um die Sicherheit kritischer Infrastrukturen langfristig zu gewährleisten. Nur durch eine gemeinsame Anstrengung von Staat, Wirtschaft und Gesellschaft können wir die Herausforderungen der Zukunft meistern und die Sicherheit unserer kritischen Infrastrukturen nachhaltig sichern. **GIT**



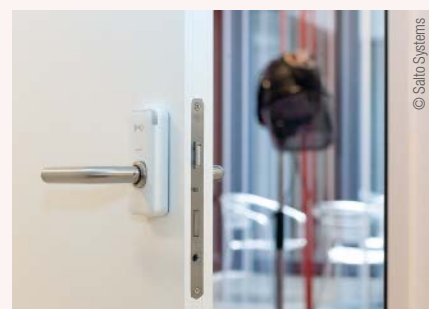
Dr. Daniela Lesmeister, Staatssekretärin
Ministerium des Innern NRW
www.im.nrw

Remote-Support-Lösung

Die e*Message W.I.S. Deutschland GmbH hat mit e*xpertview eine DSGVO-konforme Remote-Support-Lösung zur Steigerung von Ressourceneffizienz, Nachhaltigkeit und Kundenzufriedenheit auf den Markt gebracht. Mit e*xpertview profitieren Unternehmen und Organisationen von einer rechtssicheren, komfortablen Lösung für das Krisenmanagement sowie für Servicefälle in Branchen wie Energie- und Wasserwirtschaft, Werkschutz, Facility-Management, industrieller Fertigung und Instandhaltung, Bauwirtschaft, Versicherungen und medizinischen Notdiensten. Ursprünglich von der Corevas GmbH & Co. KG für Notrufe entwickelt, wurde die Software in Zusammenarbeit mit e*Message weiter optimiert, um ein breiteres Anwendungsspektrum zu eröffnen. Mit e*xpertview profitieren Unternehmen von einer webbasierten Lösung, die ratsuchende Personen effektiv aus der Ferne unterstützt. www.emessage.de

Intelligente Zutrittskontrolle auf der Altenpflege 2025

Aktuelle Entwicklungen, Produkte und Dienstleistungen rund um die stationäre und ambulante Pflege erwarteten die Besucher der Altenpflege 2025. Auch Salto war wieder mit seinen vielseitigen Zutrittslösungen vertreten. Die Pflegemesse in Nürnberg stellte in diesem Jahr Themen wie Nachhaltigkeit, Energie, Digitalisierung oder vernetztes Wohnen in den Mittelpunkt. Bei Salto profitieren Pflegedienstleister von den umfangreichen Integrationsmöglichkeiten der elektronischen Zutrittskontrolle, durch die sich viele tägliche Abläufe automatisieren und damit die Effizienz bei der Gebäudebewirtschaftung steigern lassen. Die Lösungen des Herstellers integrieren sich nahtlos in Management- und IT-Systeme sowie in die Gebäudetechnik. Die Bandbreite reicht hier von ERP-Systemen für den Stammdatenaustausch über die Einbindung einer Wäscherei zur automatisierten Ausgabe von Dienstkleidung bis hin zur Verknüpfung mit der Licht-, Heizungs- und Jalousiensteuerung. www.saltosystems.de



RATGEBER

Vieles kann man jetzt schon machen!

Neue Realität für Unternehmen: KRITIS-Dachgesetz und NIS-2

Der Ukraine-Krieg, die immer häufiger auftretenden Sabotageakte in Deutschland, die Zeitenwende in der Europäischen Sicherheitsarchitektur – all das sind gegenwärtige Themen, die den Schutzbedarf der Kritischen Infrastrukturen in den Fokus rücken. Die Bedrohungslage hat sich deutlich verschärft, und was früher als unwahrscheinliches Worst-Case-Szenario galt, ist heute bittere Realität. Angriffe auf Versorgungsnetze, Kommunikationsinfrastrukturen oder logistische Knotenpunkte können massive Auswirkungen auf unsere Volkswirtschaft sowie auf die innere Stabilität des Staates haben. Ein Beitrag von Stefan Erdweg, Geschäftsführer der Unternehmensberatung 3-core in Bonn.

■ Mit der bevorstehenden Einführung des KRITIS-DachG und der NIS-2-Richtlinie stehen viele Unternehmen, die bislang nicht unter die Klassifizierung als KRITIS-Betreiber fielen, vor völlig neuen Herausforderungen. Diese Gesetze fordern nicht nur klassische KRITIS-Sektoren wie z.B. die Energieerzeugung, Wasserversorgung oder Telekommunikation zu umfassenden Anpassungen ihrer Sicherheitsstrategien, sondern erweitern den Geltungsbereich auf eine Vielzahl von Branchen. Was bisher oft intrinsisch motiviert oder oberflächlich durchgeführt wurde – nämlich die systematische und integrale Implementierung und Überprüfung von Business Continuity Management (BCM), Krisenmanagement und physischen Sicherheitsstrukturen – wird bald verpflichtend. Unternehmen, die diese Anforderungen nicht rechtzeitig umsetzen, riskieren nicht nur regulatorische Strafen, sondern auch massive Sicherheitslücken,

die im Krisenfall schnell zu unkontrollierbaren Situationen führen können.

Bereits jetzt ist klar: Wenn diese Regulierungen in Kraft treten, wird der Bedarf an qualifizierten Fachkräften im Bereich BCM, Krisenmanagement und physischer Sicherheit massiv steigen. Unternehmen, die erst dann mit der Implementierung beginnen, könnten feststellen, dass sie zu spät kommen. Doch es gibt gute Nachrichten: Es ist nicht notwendig, auf den letzten Moment zu warten. Bereits heute können Unternehmen viele der nötigen Schritte einleiten, um den künftigen Anforderungen gerecht zu werden – und zwar ohne den Druck eines unmittelbar bevorstehenden Gesetzes. Das bedeutet: Strukturen und Prozesse können in Ruhe aufgebaut und getestet werden, anstatt unter dem Zwang der kurzfristigen Umsetzung.

Ein kluger Ansatz, der uns immer wieder im Beratungsalltag begegnet, ist die frühzei-

tige Etablierung von Sicherheitsstrukturen und Notfallplänen. Schon jetzt kann vieles erledigt werden, und wer dies vorausschauend erledigt, spart sich später nicht nur Stress, sondern auch erhebliche Kosten.

Regulierungen erweitern den Geltungsbereich deutlich

Das KRITIS-DachG und die NIS-2-Richtlinie erweitern den Geltungsbereich der Klassifizierung als kritische Infrastruktur deutlich. Bislang galten die strengsten Anforderungen vor allem für große Unternehmen in klassischen Sektoren wie Energie, Wasser oder Telekommunikation. Mit den neuen Regulierungen werden mehr Unternehmen in verschiedenen Branchen, einschließlich Gesundheitswesen, Logistik und IT, als KRITIS klassifiziert. Dies bringt eine neue Ebene von Verantwortlichkeiten mit sich. Unternehmen müssen nicht nur ihre physischen Sicherheitsmaßnahmen verbessern, sondern auch umfassende Krisenmanagement- und BCM-Prozesse etablieren. Die Harmonisierung der Europäischen Standards stellt eine besondere Herausforderung dar, da Unternehmen nun länderübergreifend agieren müssen.

Trügerische Sicherheit

Eine häufige Aussage, die wir in unserem Beratungsalltag immer wieder hören, lautet: „Hier ist noch nie etwas passiert.“ Oder: „Unsere Sicherheitsvorkehrungen sind solide, wir sind gut vorbereitet.“ Doch diese Aussagen beruhen oft auf Annahmen, die genauer Prüfung nicht standhalten. Gerade im Bereich der physischen Sicherheit und des Krisenmanagements verlassen sich viele auf Maßnahmen, die nie wirklich

auf die Probe gestellt wurden. Sicherheit und Krisenmanagement werden in vielen Unternehmen als lästige Pflichtübungen betrachtet, die im Alltag wenig Relevanz haben – bis es zu spät ist.

Ein zentrales Problem, das wir immer wieder beobachten, ist die unzureichende Prüfung von Notfall- und Krisenplänen. Unternehmen neigen dazu, auf dem Papier gutaussiehende Strukturen zu haben, die in der Praxis jedoch nie getestet wurden. Die Frage, die sich jeder Manager stellen sollte, lautet: Haben Sie Ihre Sicherheitsmaßnahmen jemals unter realen Bedingungen getestet? Sind Ihre Alarmprozesse tatsächlich effizient, und wie gut ist die Zusammenarbeit zwischen den verschiedenen Abteilungen in einem Notfall? Wenn die Antwort auf diese Fragen unklar ist, wird es höchste Zeit, das zu ändern. Denn: Wer sich keine Prävention leistet, muss sich die Krisen leisten können.

Engpässe bei Fachkräften und Sicherheitssystemen

Wir beobachten immer wieder, dass Unternehmen die Zeit unterschätzen, die es braucht, um belastbare BCM-Strukturen aufzubauen oder ein professionelles Sicherheitskonzept zu implementieren. Diese Prozesse erfordern nicht nur den Zugang zu den richtigen Fachkräften, sondern auch umfassende Planungs- und Umsetzungsphasen. Oft wird davon ausgegangen, dass solche Strukturen schnell implementiert werden können, doch in der Praxis sind mehrere Monate nötig, um diese Maßnahmen effektiv umzusetzen und zu testen. Wer erst mit der Umsetzung beginnt, wenn die gesetzlichen Anforderungen greifen, läuft Gefahr, wertvolle Zeit zu verlieren und dadurch die eigene Krisenresilienz zu gefährden.

In unserem Beratungsalltag haben wir immer wieder beobachtet, dass Unternehmen die Zeit unterschätzen, die benötigt wird, um nicht nur die richtigen Fachkräfte mit der entsprechenden Expertise und Know-how zu finden, sondern auch die passende Infrastruktur aufzubauen. Besonders im Bereich der physischen Sicherheit gibt es lange Bestellzeiten für Technologien, die für die Absicherung von Kritischen Infrastrukturen unerlässlich sind. Professionelle Sicherheitszäune und Überwachungstechnologien, die derartige Anlagen absichern, sind nicht nur teuer, sondern auch in der Beschaffung zeitintensiv. Dies führt zu einem weiteren Problem: Wenn der Bedarf gleichzeitig in vielen Unternehmen entsteht, werden die ohnehin langen Lieferzeiten noch weiter ansteigen.

Frühe Vorbereitung schafft Resilienz

Unternehmen, die vorausschauend handeln, können bereits jetzt viele Maßnahmen

ergreifen, um den kommenden Anforderungen gerecht zu werden. Ein wichtiger Schritt ist der Aufbau von Governance-Strukturen und klaren Prozessabläufen. Dies betrifft nicht nur das Business Continuity Management (BCM) und Krisenmanagement, sondern auch die Integration von Alarm- und Notfallplänen, die reibungslos ineinandergreifen müssen. Besonders entscheidend ist es, bestehende Strukturen nicht nur zu evaluieren, sondern auch regelmäßig zu testen – unangekündigt und praxisnah. Nur so kann sichergestellt werden, dass diese Strukturen im Ernstfall tatsächlich greifen.

Stellen Sie sich vor, ein Unternehmen vertraut auf seine Krisenplanung und ist überzeugt, gut vorbereitet zu sein. Die Sicherheitspläne sind ausgearbeitet, und es gibt regelmäßige Schulungen für das Personal. Doch bei Eintritt einer realen Krise – sei es ein Cyberangriff oder ein großflächiger Stromausfall – scheitern die Prozesse. Notfallmaßnahmen greifen nicht, weil sie nie unter realen Bedingungen getestet wurden.

In unserer Beratungspraxis stoßen wir oft auf ungetestete Sicherheitsstrukturen. Unangekündigte Übungen, bei denen nicht nur die physischen Sicherheitssysteme, sondern auch die Alarmprozesse, das Notfallmanagement, das Krisenmanagement und die BCM-Prozesse überprüft werden, sind unerlässlich. Diese Tests müssen in der Praxis zeigen, ob alle theoretischen Annahmen wirklich funktionieren.

Ablauf und Herausforderungen

Wir führen regelmäßig Stresstests mit Krisenstäben und Notfallstäben durch, die weit über theoretische Überprüfungen hinausgehen und oft unerwartete Schwachstellen aufzeigen. Bei einem typischen Stresstest werden reale Krisenszenarien und Notfallszenarien simuliert – zum Beispiel ein Cyberangriff, Brände, Sabotagen, Demonstrationen oder ein physisches Eindringen. Häufig zeigen sich dabei organisatorische und technische Optimierungspotenziale: Alarmanlagen lösen nicht korrekt aus, oder Mitarbeiter wissen nicht, wie Systeme genau bedient werden sollen.

Besonders in Stresssituationen zeigt sich oft, dass Prozesse und Interaktionen in der Praxis anders ablaufen als geplant. Ein Stolperstein ist teilweise auch die Alarmierung externer Einsatzkräfte wie der Polizei. Auf großen, weitverzweigten Geländen kommt es oft zu Missverständnissen darüber, wo genau die Polizei eintreffen soll, was wertvolle Zeit kosten kann. Da solche Szenarien in theoretischen Übungen selten Beachtung finden, kommt es hier immer wieder zu spannenden Erkenntnissen auf allen Seiten.



Stefan Erdweg, Geschäftsführer der Unternehmensberatung 3-core in Bonn

In einem unserer Tests führte beispielsweise eine Alarmierung zu Verzögerungen, weil unstimmig war, wer wen alarmieren bzw. weiter alarmieren soll. Eine kleine Änderung im Kommunikationsablauf konnte dieses Problem beheben. Ein weiteres Beispiel betraf Zutrittsprozesse, die bei einem Test nicht funktionierten, da solche Prozesse selten unter Stressbedingungen geprüft werden. Diese und ähnliche Schwächen können durch zusätzliche Schulungen und technische Anpassungen schnell behoben werden.

Fazit

Die neuen Regelungen des KRITIS-DachG und der NIS-2-Richtlinie sind ein Appell an viele Unternehmen, die sich bislang in Bezug auf Business Continuity Management, Krisenmanagement und physische Sicherheit weniger proaktiv vorbereitet haben. Es ist keine Frage mehr, ob, sondern wann die Implementierung der organisatorischen Resilienz startet. Unternehmen, die frühzeitig die notwendigen Schritte einleiten, werden nicht nur die gesetzlichen Anforderungen erfüllen, sondern auch ihre Krisenresilienz und Sicherheit erheblich verbessern und Schäden verschiedenster Art reduzieren. Wer sich keine Prävention leistet, muss sich die Krisen leisten können – das lässt sich heute noch vermeiden. **GIT**



3-core GmbH
www.3-core.de

NIS2

Cyberresilienz brennt im Topmanagement

NIS2 – Steigende Nachfrage am Personalmarkt

Mit Inkrafttreten der Anti-Hacker-Richtlinie NIS2 sei der Chief Information Security Officer die gefragteste Person auf der obersten Führungsebene, so Dr. Harald Schönfeld, Geschäftsführer der Personalberatung von Butterflymanager. Cyberresilienz sei derzeit eines der Hauptthemen im Topmanagement. Dies macht er an einer „stark steigenden Nachfrage nach Chief Information Security Officers auf Zeit“ am Personalmarkt fest.

Die Personalberatung Butterflymanager ist auf die Vermittlung von Interimmanagern, also Führungskräften auf Zeit, spezialisiert. Dort hatte man „noch nie so eine hohe Nachfrage nach Managern, die sich in Projekten auf Vorstands- oder Geschäftsleitungsebene um die Cyberresilienz von Unternehmen kümmern sollen“, sagt Geschäftsführer Harald Schönfeld.

Haftung auf Vorstands-, Geschäftsleitungs- und Aufsichtsratsebene

Das Gros der Nachfrage komme von mittelständischen Firmen, die nicht selbst eine sogenannte Kritische Infrastruktur (KRITIS) betreiben, aber KRITIS-Unternehmen im Kundenstamm haben, hat Schönfeld in zahlreichen Gesprächen festgestellt.

Der Hintergrund ist nach seiner Ansicht offensichtlich: Nach Umsetzung der EU-Cybersicherheitsrichtlinie NIS2 (Network & Information Security) in deutsches Recht haften die Firmen bei Hackerangriffen. „Diese Haftung greift nach oben durch bis auf Vorstands- und Geschäftsleitungsebene“, erklärt Dr. Harald Schönfeld, warum Cyberresilienz plötzlich zum Topthema auf der obersten Führungsebene aufgestiegen ist: „Verletzt das Topmanagement seine Pflicht oder unterlässt die Einführung von Maßnahmen zur Minimierung von Cyber Risiken, drohen hohe Bußgelder sowie rechtliche Konsequenzen für die Führungskräfte. Auch die Mitglieder der Überwachungs- und Kontrollorgane des Unternehmens stehen persönlich in der Haftung, insbe-

sondere der Aufsichtsrat.“ Die Anpassung an die neuen rechtlichen Vorgaben erfordere nicht nur technologische Investitionen, sondern ebenso sehr eine Stärkung der Governance-Strukturen. „Governance ist im Grunde immer ein Thema für die oberste Führungsebene und den Aufsichtsrat. Deshalb suchen die Unternehmen einen Chief Information Security Officer und keinen bloßen Cybersicherheitsexperten“, berichtet Harald Schönfeld aus Gesprächen mit Vorständen, Geschäftsführern und Aufsichtsräten.

Die NIS-2-Richtlinie setzt erhöhte Cybersicherheitsstandards für Unternehmen ab 50 Mitarbeitern und 10 Millionen Euro Umsatz in 18 festgelegten Sektoren, die als kritisch für die Aufrechterhaltung wichtiger

Infrastrukturen eingestuft werden. Dazu gehören die Branchen Energie, Transport, Bankwesen, Finanzmarktinфраstruktur, Gesundheit, Trinkwasser, Abwässer, digitale Infrastruktur, IKT-Dienstleistungsmanagement, Öffentliche Verwaltung, Weltraum, Post- und Kurierdienste, Abfallwirtschaft, Herstellung, Produktion und Vertrieb von Chemikalien, Lebensmittelproduktion, -verarbeitung und -vertrieb, Produktion, Herstellung von Medizinprodukten, Maschinen, Fahrzeugen sowie elektrischen/elektronischen Geräten, digitale Anbieter und Forschung.

Haftung umfasst die gesamte KRITIS-Wertschöpfungskette

„Vielen Führungskräften im Mittelstand ist offenbar erst spät klargeworden, dass NIS2 nicht nur für die Betreiber kritischer Infrastrukturen gilt, sondern für die gesamte KRITIS-Wertschöpfungskette, also auch alle Zulieferer“, hat Managementexperte Dr. Harald Schönfeld festgestellt. „Deshalb ist Cyberresilienz in vielen Firmen beinahe über Nacht von der IT-Abteilung auf die Agenda der obersten Führungsebene und auch des Aufsichtsrates als Überwachungs- und Kontrollgremium gesetzt worden. Daher sucht man nun auf Topebene einen schnell verfügbaren Interim Manager, der das Unternehmen in der Rolle des Chief Information Security Officer auf die neuen NIS2-Anforderungen einstellt.“

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) rechnet mit knapp 30.000 von NIS2 betroffenen Firmen in Deutschland, andere Zählungen kommen auf rund 40.000 Unternehmen über die gesamte Wertschöpfungskette hinweg. „Die hohe Nachfrage nach Interimsmanagern zur Stärkung der Cyberresilienz auf Topebene ist auch die Folge eines leergefegten Personalmarktes mit entsprechend qualifizierten Personen“, sagt Schönfeld: „Immer häufiger erhalten wir einen Doppelauftrag: einen Interimsmanager zu finden, der praktisch sofort als Chief Information Security Officer einspringt, und parallel dazu einen Manager zu suchen, der diese Funktion in dauerhafter Festanstellung antreten will. Der erste gelingt uns immer kurzfristig, aber für die zweite Aufgabe gehen unter Umständen Monate dahin, bis sich eine geeignete Führungskraft findet.“ 



Butterflymanager GmbH
www.butterflymanager.com

Salto erhält EPD für XS4 Original+ Beschläge

Salto hat für seine elektronischen XS4 Original+ Schmalschildbeschläge die Umwelt-Produktdeklaration (Environmental Product Declaration – kurz: EPD) des Instituts Bauen und Umwelt e. V. (IBU) erhalten. Mit der EPD für den elektronischen Beschlag XS4 Original+ setzt Salto ein klares Zeichen für Transparenz und Verantwortung. Eine EPD beschreibt die Umweltauswirkungen von Baustoffen, Bauprodukten oder Baukomponenten über den gesamten Lebenszyklus und bildet damit eine wichtige Grundlage für die Nachhaltigkeitsbewertung von Bauwerken. Dies bietet den Kunden eine solide Datenbasis für fundierte Entscheidungen und unterstreicht den Anspruch des Unternehmens, nachhaltige Lösungen weiter voranzubringen und dabei besonders auf umweltbewusste Produktion zu achten. Die Bewertung erfolgt nach internationalen Normen wie ISO 14025 und EN 15804. Die XS4 Original+ Modellreihe kombiniert intelligente Zutrittskontrolltechnologie mit einem schlanken, modernen Design.

www.saltosystems.com

www.GIT-SICHERHEIT.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**

Sichere Alarmübertragung auch nach 2G-Abschaltung

Telenot bietet ein vollumfängliches Programm an zukunftsfähigen Übertragungseinrichtungen und damit zukunftsfähigen Lösungen für die anstehende Migration. Die geplante Abschaltung der 2G-Mobilfunknetze bis 2028 stellt Betreiber von Gefahrenmeldeanlagen vor große Herausforderungen: Die Systeme müssen umgerüstet werden, um weiterhin zuverlässig Notrufe und Alarmsignale von Einbruch- und Brandmeldeanlagen übertragen zu können. Eine rechtzeitige Migration auf moderne Übertragungstechnik ist unerlässlich. Nachdem im Jahr 2021 die 3G-Mobilfunknetze in Deutschland abgeschaltet wurden, steht bis 2028 der Ausstieg aus dem 2G-Netz (GSM und GPRS) bevor. Dieses ältere Netz wurde bislang beibehalten, da es essenzielle Dienste wie Sprachtelefonie, SMS sowie Notruf- und Alarmsysteme (z. B. in Aufzügen) unterstützt. Mit der bevorstehenden Abschaltung des 2G-Netzes wird jedoch keine Alarmübertragung mehr über diese Technologie möglich sein – weder per Sprache noch via IP-Übertragung. Alle Sprach- und Datendienste (einschließlich des CSD-Protokolls) sowie SMS werden funktionslos.



www.telenot.com



Smarte Retail-Lösungen auf der Eurocis

Dahua stellte seine intelligenten Einzelhandelslösungen auf der Messe Eurocis in Düsseldorf aus. Wenn Einzelhandelsgeschäfte hinter ihren Umsatzerwartungen zurückbleiben, kann das viele Ursachen haben. Während z. B. die falsche Standortwahl ein nur schwer zu korrigierender Kardinalfehler ist, lassen sich andere Ursachen für schlechte Geschäfte durch eine intelligente Analyse des Käuferverhaltens oft erstaunlich effizient beheben. Aber auch gut laufende Shops können durchaus noch optimiert werden und mehr Umsatz generieren. Die Business Intelligence-Lösungen mit KI von Dahua unterstützen Shopbetreiber bei der Transformation ihres Einzelhandelsgeschäfts. Daten sind der Schlüssel zur Zukunft. Unter Wahrung der Privatsphäre der Kunden bietet das Unternehmen seinen Partnern professionelle und intelligente Big-Data-Analysetools und -lösungen, darunter: Kundenverkehrsanalyse, demografische Kundenanalyse, Heatmap-Analyse und Schadensvermeidung.

www.dahuasecurity.de



„Navigating Tomorrow“ – Mobotix Partner Conference 2025

Unter dem Motto „Navigating Tomorrow“ nahmen mehr als hundert Mobotix Partner, Videotechnologieexperten sowie Interessierte an der diesjährigen Mobotix Partnerkonferenz im rheinland-pfälzischen Langmeil teil. Ein beeindruckendes Branchentreffen, bei dem sich die Mobotix Partner über Trends und Entwicklungen in der Videotechnologie austauschen und die neuesten Lösungen des Unternehmens zum Teil noch vor Markteinführung kennenlernen konnten. Schon zuvor fand im mexikanischen Cancún die MPC für den lateinamerikanischen Markt statt. Im März trafen sich alle anderen europäischen und internationalen Partner auf der englischsprachigen MPC in Amsterdam (Niederlande). Für April und Mai sind zwei weitere Konferenzen in Jakarta, Indonesien, sowie Melbourne, Australien, geplant mit Fokus auf den asiatischen und pazifischen Markt. „An den zwei Konferenztage haben wir unseren Partnern in erster Linie demonstriert, wie Mobotix Lösungen ihnen entscheidende Wettbewerbsvorteile und einen strategischen Mehrwert bieten können. Überdies konnten wieder einmal wertvolle Kontakte mit Branchenkollegen geknüpft und berufliche Netzwerke ausgebaut werden“, so Thomas Lausten, CEO der Mobotix AG.

www.mobotix.com

Digitaler BHE-Thementag: KRITIS-Sicherheit im Fokus

Die grundlegenden Anforderungen an die physische Sicherheit im KRITIS-Bereich sowie aktuelle sicherheitstechnische Entwicklungen präsentierte der BHE Bundesverband Sicherheitstechnik e. V. in Kooperation mit dem Bundesverband für den Schutz Kritischer Infrastrukturen e. V. (BSKI) beim ersten digitalen BHE-Thementag „Sicherheit in KRITIS“. Trotz der jüngsten Verzögerungen bei der Umsetzung der NIS2-Richtlinie und des KRITIS-Dachgesetzes bleibt der Schutz Kritischer Infrastrukturen eine zentrale Aufgabe. Durch die Kombination aus physischer Sicherheit und Cybersecurity wird die Funktionsfähigkeit lebenswichtiger Einrichtungen und Dienste (z. B. Energie- und Wasserversorgung, Gesundheitswesen, Kommunikations- und Verkehrssysteme) sichergestellt. Entsprechende Mindestanforderungen sind in der EU-Richtlinie über die Resilienz kritischer Infrastrukturen (CER-Richtlinie) sowie der europäischen NIS2-Richtlinie festgelegt.

Die Online-Veranstaltung bot unter anderem Sicherheitsverantwortlichen von KRITIS, Anbietern und Planern von Sicherheitslösungen sowie Versicherern und Behörden die Möglichkeit, sich über aktuelle Entwicklungen und innovative Lösungen zum Schutz Kritischer Infrastrukturen zu informieren. Die Teilnehmer erwartete ein spannendes, neutrales Vortragsprogramm mit interaktiven Fragerunden, das per Video-Stream übertragen wird. Den Auftakt bildete ein Vortrag von Holger Berens, Vorstandsvorsitzender des BSKI, zur aktuellen Gesetzeslage.

Darüber hinaus wurden am Praxisbeispiel eines Umspannwerks in mehreren Beiträgen die Anforderungen eines Sicherheitskonzepts und dessen Umsetzung veranschaulicht sowie intelligente sicherheitstechnische Lösungen und die damit einhergehenden Vorgaben und Mindest-Standards im KRITIS-Bereich beleuchtet.

www.bhe.de



BOSCH



Der Schutz kritischer Infrastrukturen braucht mehr als Instinkt.

Sicherheit liegt in unserer Natur.

Als Experten für den Schutz kritischer Infrastruktur entwickeln wir für Sie Maßnahmen zur Stärkung der physischen Resilienz. Von der Konzeption und Beratung bis zur Umsetzung.

Mehr erfahren Sie unter: go-to-bosch.com/kritis



EINSATZKRITISCHE KOMMUNIKATION

Einsatz- und geschäftskritische Kommunikation

Politische Forderungen des Bundesverbandes Professioneller Mobilfunk für die kommende Legislaturperiode

Deutschland hat am 23. Februar 2024 einen neuen Bundestag gewählt. Wann es einen Bundeshaushalt 2025 geben wird, ist offen. Mangels Bundeshaushalts hängt auch so manches Sicherheitsprojekt in der Schwebe. Speziell zur Zukunft der einsatz- und geschäftskritischen Kommunikation äußert sich der Bundesverband Professioneller Mobilfunk (PMeV) mit sieben politischen Forderungen, die er in einem Impulsprogramm zusammengefasst hat. GIT SICHERHEIT sprach darüber mit Bernhard Klinger, Vorsitzender des Vorstands beim PMeV.

■ **GIT SICHERHEIT:** Herr Klinger, der PMeV weist regelmäßig auf die Notwendigkeit sicherer einsatz- und geschäftskritischer Kommunikation hin – vor allem vor dem Hintergrund der fortschreitenden Digitalisierung und zunehmender Bedrohungen. Zunächst einmal zur Situation in Deutschland: Wie dringlich ist die Lage?

Bernhard Klinger: Die Entwicklungen der letzten Monate und vor allen Dingen der letzten Wochen lassen keinen Zweifel daran: Wir stehen inmitten einer Zeit politischer Umbrüche und sicherheitspolitischer Herausforderungen. Die angespannte Sicherheits- und Wirtschaftslage verlangt eine Anpassung bestehender Regulierung und des Finanzierungsrahmens für sichere Kommunikation. Das gilt für die Industrie, staatliche Institutionen und Behörden, Kritische Infrastrukturen sowie das Einsatz- und Rettungswesen. Die Zeit drängt. Denn der Bedarf an einsatzkritischer Breitbandkommunikation wird in den kommenden Jahren weiter steigen und für die Sicherheit, Versorgung und Wettbewerbsfähigkeit Deutschlands essenziell sein.

Am 23. Februar hat das Land neu gewählt. Sie haben aus diesem Anlass ein Impulspapier für die kommende Legislaturperiode vorgestellt. Welche der darin genannten Punkte sind aus Ihrer Sicht besonders zeitkritisch?

Bernhard Klinger: Für die Umsetzung der notwendigen Maßnahmen für ein BOS-Breitbandnetz fehlen derzeit ausreichend finanzielle Mittel sowie verfügbare dedizierte Frequenzen. Dieses Vorhaben ist jedoch dringend nötig, denn einsatzkritische Kommunikation ist eine der Grundlagen für unsere innere Sicherheit. Hier braucht es zügig einen langfristigen Finanzierungsrahmen und ein klares Bekenntnis aller Ressorts, um das Projekt erfolgreich umzusetzen. Wir begrüßen deshalb ausdrücklich das 4-Phasen-Modell der Breitbandstrategie von Bund und Ländern zur Errichtung eines eigenbeherrschten Breitbandnetzes der BOS, also der Behörden und Organisationen mit Sicherheitsaufgaben.

Ein weiterer dringlicher Punkt: Durch europäische und deutsche Gesetzgebung steigt die Anzahl notwendiger Zertifizierungen für Hersteller und Anwender im

Bereich Cybersicherheit. Das Bundesamt für Sicherheit in der Informationstechnik als zentraler Zertifizierer muss deshalb mit ausreichenden finanziellen und personellen Ressourcen ausgestattet werden, um die gesetzlichen Zielvorgaben erfüllen zu können. Nur dann kann die Cybersicherheit in Deutschland effektiv gestärkt und die Position Deutschlands als wichtiger Standort für IT-Sicherheit in Europa gefestigt werden.

Besonders viel Aufmerksamkeit gilt natürlich den Kritischen Infrastrukturen. Das Dachgesetz konnte nicht mehr verabschiedet werden. Könnten Sie einmal anschaulich machen, welchen Anteil hochverfügbare und sichere Kommunikationsnetze an der Sicherheit solcher Infrastrukturen haben?

Bernhard Klinger: Kritische Infrastrukturen funktionieren heutzutage nicht mehr ohne Funknetze und sind zunehmend auch von Breitbandfunkdiensten abhängig. Ein hochverfügbares und sicheres Kommunikationsnetz sorgt also zunächst für die Sicherstellung eines ordnungsgemäßen

Betriebsablaufes. Darüber hinaus ist bei Großschadenslagen oder Sabotageakten eine sichere und hochverfügbare Kommunikation zur Aufrechterhaltung oder Wiederherstellung der Funktionsfähigkeit der Kritischen Infrastrukturen von größter Bedeutung. Es lässt sich nicht leugnen, dass die Sicherheitslage in Deutschland äußerst angespannt ist. Laut einer aktuellen Umfrage haben sowohl Cyberangriffe als auch physische Angriffe auf Wirtschaftsunternehmen zugenommen. Deutsche Geheimdienste befürchten für die Zukunft noch mehr physische Sabotageakte. Damit erhöht sich auch die Notwendigkeit einer sicheren und hochverfügbaren Kommunikation für kritische Infrastrukturen.

Was sind insoweit Ihre Forderungen?

Bernhard Klinger: Kritische Infrastrukturen sollten dedizierte Funknetze mit speziell zugewiesenen Frequenzen nutzen müssen. Diese Netze können für die hohen Anforderungen an Sicherheit und Verfügbarkeit ausgelegt werden. Die Nutzung eines eigenen dedizierten Netzes gewährleistet zudem die Netzsicherheit und Datensouveränität und reduziert in hohem Maße die Abhängigkeit von Dritten. Um die Transition der Kommunikation in Richtung Breitband auch für die Kritischen Infrastrukturen zu ermöglichen, die eine Versorgung in der Fläche sicherstellen, sind dedizierte Breitbandfrequenzen für eine großflächige Funkversorgung erforderlich. Hier müssen entsprechende regulatorische Schritte unternommen werden.

Die kleinen und mittleren Unternehmen (KMU) sehen sich ebenfalls neuen Risiken ausgesetzt. Auch zur Reduzierung von Risiken setzt der PMeV auf private 5G-Campuslösungen, wie wir es hier in der GIT SICHERHEIT auch schon verschiedentlich thematisiert haben. Könnten Sie die Hintergründe dazu noch einmal zusammenfassen?

Bernhard Klinger: Private 5G-Campusnetze erfüllen die individuellen Anforderungen der Unternehmen hinsichtlich Datenschutz und Latenz, der Zuverlässigkeit, Datensicherheit sowie der Verfügbarkeit. Mit einem solchen Netz kann die digitale Kommunikationsinfrastruktur also autonom und flexibel gestaltet werden, maßgeschneidert für die spezifischen Anforderungen von Unternehmen. Private 5G-Campusnetze garantieren zudem Sicherheit und Datensouveränität. Darüber hinaus bieten Sie eine langfristige Perspektive für die globalen Herausforderungen, denen sich Unternehmen am Wirtschaftsstandort Deutschland stellen müssen. Sie unterstüt-

7 Forderungen des PMeV

1. Mehr finanzielle Unterstützung und politischer Rückhalt für ein sicheres und hochverfügbares BOS-Breitbandnetz
2. Förderprogramme für den Aufbau von privaten 5G-Campuslösungen für kleine und mittelständische Unternehmen (KMU)
3. Verbindliche Nutzung von sicheren und hochverfügbaren Kommunikationsnetzen für Kritische Infrastrukturen
4. Zuteilung von dedizierten Breitbandfrequenzen für Anwender in der Fläche
5. Bundesamt für Sicherheit in der Informationstechnik mit ausreichend finanziellen und personellen Ressourcen ausstatten
6. Beschleunigung von Exportgenehmigungsverfahren in Deutschland
7. Förderung von Aus- und Weiterbildungsprogrammen im einsatz- und geschäftskritischen Mobilfunk

Das vollständige
Impuls-Papier finden
Sie hier:



zen und beschleunigen die digitale Transformation der Wirtschaft und tragen damit zur internationalen Wettbewerbsfähigkeit der Unternehmen bei.

Sie fordern hier staatliche Förderprogramme. Könnte das die Wirtschaft nicht aus eigener Kraft stemmen?

Bernhard Klinger: Aktuell werden die Potentiale von 5G vornehmlich von größeren Unternehmen getestet und evaluiert. Die finanziellen Mittel und das erforderliche Know-how für die Implementierung eines 5G-Netzes ist dort eher als bei kleinen und mittelständischen Unternehmen vorhanden. KMU sind derzeit noch zurückhaltend, 5G-Campusnetze zu testen und unter Realitätsbedingungen einzusetzen. Die hohen Kosten für die Errichtung einer 5G-Testumgebung mit dem Ziel der anschließenden realen Nutzung ist ein wesentliches Hemmnis für 5G im Kontext von Campusnetzen. Um jedoch die hohen Anschubfinanzierungen für 5G-Campusnetze leisten zu können, sind für kleine und mittlere Unternehmen bundesweite Anreize durch Förderprogramme notwendig. Die KMU können das in der Regel nicht alleine stemmen – erst recht nicht in der derzeitig angespannten Wirtschaftslage. Führt man sich jedoch die Vielzahl und Bran-

chenvielfalt der KMU in Deutschland vor Augen und besinnt sich gleichzeitig auf die Tatsache, dass diese seit jeher der Garant für die Vielfalt und Wettbewerbsfähigkeit der deutschen Wirtschaft sind, so kommt man zu dem Schluss, dass Investitionen in 5G-Campusnetze, insbesondere wegen der durch den Einsatz dieser Technik erzielten Mehrwerte, ein notwendiger Schritt sind, um den aktuellen und zukünftigen wirtschaftlichen Herausforderungen in Deutschland und Europa zu begegnen. Eine gezielte Förderung ist folglich eine Investition in die Digitalisierung unserer KMU und damit eine unverzichtbare Investition in die Zukunftsfähigkeit unserer Wirtschaft.

Die Parteien, die nun eine Bundesregierung bilden können, haben sich ja zu diesen Themen bereits positioniert. Welche Hoffnungen haben Sie bezüglich Ihrer Forderungen angesichts des Ausgangs der Wahl?

Bernhard Klinger: Die Parteien, die Koalitionsverhandlungen zur Bildung einer neuen Bundesregierung aufgenommen haben, müssen der multiplen Gefahren- und Bedrohungslage Rechnung tragen: Gefährdung der inneren und äußeren Sicherheit, eine militärische Kriegsgefahr inklusive hybride Kriege durch Cyberangriffe, Sabotageakte und Desinformationskampagnen. Und natürlich auch die nicht zu leugnende Zunahme von Naturkatastrophen im In- und Ausland. Der PMeV hofft, dass die Politik schnellstmöglich mit finanziellen und regulatorischen Verbesserungen für die Kritische Kommunikation reagiert. Andernfalls verschlechtert sich die Sicherheit für die Menschen in Deutschland rapide. Es geht um Menschenleben und die Resilienz von Staat und Wirtschaft. Nichts zu unternehmen ist moralisch schwerwiegend und letztendlich – wenn die multiplen Krisen kumulieren – teurer als jetzt schnell zu entscheiden, Gesetze zu verabschieden und zu investieren. Die ersten Ergebnisse der Sondierungen zwischen CDU/CSU und SPD bezüglich zukünftiger Investitionen in die Infrastruktur mittels eines Sondervermögens stimmen zunächst zuversichtlich. Bei der Umsetzung muss jedoch sichergestellt werden, dass die sichere hochverfügbare, einsatz- und geschäftskritische Kommunikation, insbesondere im Rahmen der Transition in Richtung Breitband nicht auf der Strecke bleibt. **GIT**



Bundesverband Professioneller
Mobilfunk (PMeV)
www.PMeV.de

EINSATZKRITISCHE
KOMMUNIKATION

Hightech auf den Gleisen

Frequentis digitalisiert Schienennetz der Schweizer Bundesbahn

Ein im September 2024 von der Schweizer Bundesbahn (SBB) erteilter Auftrag an das Unternehmen Frequentis ist ein wichtiger Meilenstein im Geschäft mit digitalisierten Kommunikationssystemen für Eisenbahnen. Das Wiener Unternehmen Frequentis implementiert und wartet dabei eine neue Systemplattform mit dem Namen IMS Service BTA.

Die Systemplattform IMS Service ist so konzipiert, dass sie bis weit ins nächste Jahrzehnt im Übergang zur einsatzkritischen Hochgeschwindigkeits-Datenübertragung (MCX) auf 5G-Mobilfunkstandard eingesetzt werden kann. Implementiert wird IMS Service BTA als rein softwarebasiertes System. Die dabei angewandte Technologie ersetzt die bisherigen Dispatcher-Systeme in den Leitzentralen, indem sie die Kommunikation zwischen den Leitstellen, den Zügen, dem Bahnpersonal und den Notfallteams miteinander vernetzt.

MissionX – Schlüsseltechnologie von Frequentis

Im Rahmen von „MissionX“, seiner Ende-zu-Ende-Systemlösung für einsatzkritische Breitbandkommunikation, hat Frequentis ein Konzept entwickelt, mit dem alle Funknetzwerke unabhängig von ihren technologischen Standards verknüpft werden können. Der Ansatz der „Bearer Independent Communication“ wird konsequent weiterge-

führt. Die Anwendungen für Endbenutzer sind dabei von den Übertragungssystemen entkoppelt. Für die Bedienung benötigt das Personal keine zusätzlichen Spezialendgeräte. Die Daten sind auf den Bildschirmen der Kontrollzentren genauso abrufbar wie auch auf Tablets und Smartphones.

Mit seiner neuen Produktgeneration auf Basis der digitalen Plattform FTS 3020 adressiert Frequentis einen Markt, der in den nächsten Jahrzehnten kontinuierlich wachsen wird, ebenso wie der Bedarf an Bandbreite. So erfordern die Technologien des automatisierten Fahrens (Automatic Train Operation) und das Europäische Zug-sicherungssystem ETCS schnell getaktete Steuerinformationen. Zugleich müssen die von Sensoren und Kameras gesammelten Daten zeitnah verarbeitet werden. Darüber hinaus dienen die Systeme zur Vorbeugung und zum Management von Störungen mit geringen Latenzzeiten. Neben dem exponentiellen Wachstum der Datenmengen im Bahnverkehr werden

auch personelle Engpässe bei den Eisenbahnen die Digitalisierung der Kommunikation beschleunigen.

Das Future Railway Mobile Communication System, kurz FRMCS, bildet hier die System-Architektur für das künftige 5G-basierte Kommunikationssystem der europäischen Bahnen. Entwickelt wird es durch den internationalen Eisenbahnverband UIC und die Unternehmen der Eisenbahnindustrie, mitfinanziert durch die Europäische Union. Frequentis, erläutert Thomas Karl, im Unternehmen Vice President Public Transport, habe hier bei MCX in den letzten Jahren den Sprung in die Produktphase geschafft: „Wir haben den Beweis erbracht, Kommunikationssysteme auf Basis von MissionX, unsere Systemlösung für die sicherheitskritische Kommunikation über 4G- und 5G-Mobilfunknetze, zu kommerzialisieren.“ Die ersten Aufträge auch im Bahnbereich konnte Frequentis sich bereits sichern, einen von der ÖBB und zuletzt im September einen weiteren vom Privatbahnbetreiber NÖVOG im österreichischen Bundesland Niederösterreich.

Standardisierung der 5G-Kommunikationssysteme im Schienenverkehr

Mit ersten öffentlichen Ausschreibungen rechnet Frequentis-Experte Karl in den nächsten Jahren. „2027 oder 2028 wird das Marktfenster für die großen Investitionen aufgehen.“ Bis dahin soll die Standardisierung der 5G-Kommunikationssysteme

im Schienenverkehr abgeschlossen sein. Zielkunden sind staatsnahe Eisenbahnen in Europa, wo in den nächsten Jahrzehnten eine Hochleistungs-Infrastruktur entstehen soll. Um die bestehenden Kommunikationssysteme umzurüsten, ist der Investitionshorizont der Eisenbahnen in Richtung FRMCS auf zehn bis 15 Jahre angelegt, erläutert Karl. „Alle unsere Kunden befinden sich in einer Migrationsphase, in der sie Bestandstechnologie erhalten müssen und zugleich Lösungen benötigen, mit denen sie die neue Technologie ausrollen können.“

Für Frequentis bedeutet das auch, das Produktportfolio ständig mit neuen Lösungen für den nahtlosen Übergang zwischen den Systemen zu ergänzen. Beispielsweise mit Modulen, die es ermöglichen, dass herkömmliche GSM-R- und 5G-Mobilfunknetze gemeinsam einen Notruf absetzen können. Und weil die Eisenbahngesellschaften ihre Budgets effektiv einsetzen müssen, entwickelt Frequentis investitionsschonende Anwendungen für die betriebliche Kommunikation auf Basis öffentlicher Mobilfunknetze. Im Rahmen der Bearer-Independence-Technologie für die Kommunikation über offene mobile Netzwerke hat Frequentis 2023 eine Lösung bei SNCF in Frankreich platziert.

Potenzial KI-basierte Drohnen

Der künftige Einsatz von Künstlicher Intelligenz ist ein weiterer potenzieller Zukunftsmarkt in der Digitalisierung der Eisenbahn. Einer der Einsatzbereiche ist die Instandhaltung von Schienenstrecken mit Hilfe von Drohnen. Branchenexperten beziffern die jährlichen Instandhaltungskosten auf bis zu 10 000 Euro pro Kilometer Bahnschiene.

Niederschwellige Lösungen mit Hilfe von Drohnen-Überwachungsflügen könnten enorme Kosteneinsparungen bewirken.

Im Teststatus sind die autonom fliegenden Drohnen, die Frequentis in Kooperation mit der ÖBB von Hangars aus startet, um bestimmte Streckenabschnitte und

Softwareplattform sind für den Betrieb in Fahrzeugen zugelassen. Als nächsten Schritt plant Frequentis hier, eine Eisenbahngesellschaft für das erste Projekt zu gewinnen.

Das Bahngeschäft ist dem Geschäftsbereich Public Safety & Transport zugeordnet, der zuletzt rund 30 Prozent am



Ende-zu-Ende-Systemlösung für einsatzkritische Breitbandkommunikation: alle Funk-Netzwerke unabhängig von ihren technologischen Standards verknüpft

Bahn-Infrastrukturen zu überwachen. Als nächste technologische Schritte hat Frequentis die vollautomatische Auswertung der von den Drohnen aufgezeichneten Videobilder sowie die KI-basierte Vollüberwachung einzelner Strecken einschließlich der Weiterleitung der Bilder an eine Zentrale im Blick.

Nach drei Forschungsprojekten im Rahmen des 2020 gestarteten „Harmony“-Programms - inhaltlich aufgeteilt in Datensammlung, Entwicklung der Plattform und dem Anlernen der Datenanalyse per KI - hat Frequentis den Status der Vorproduktreife für eine fahrzeuggestützte Lösung erreicht. In der Praxis bedeutet das: Hardware und

Gesamtumsatz stellte. Weil die Abnehmer überwiegend Behörden und staatliche Betriebe sind, macht Frequentis in der Regel keine Angaben zu den Auftragsvolumina. Die über einen mehrjährigen Zeitraum gestaffelten Erlöse sorgen für langfristig kalkulierbare Einnahmen. Auf lange Sicht eröffnet sich mit der Digitalisierung der Eisenbahnen für Frequentis ein Geschäftsfeld, das in der Sparte Public Safety & Transport Umsatz und Margen weiter in die Höhe schieben kann. **GIT**



Frequentis AG
www.frequentis.com

AG neovo

RUND UM DIE UHR IM DIENST

AG Neovo Displays mit NeoV™ Glasstechnologie -> 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

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



Elektronische
Zugangskontrolle

CYBER SECURITY

Schutzschild gegen Manipulation und Sabotage

Cybersicherheit: Zum Schutz von KRITIS und industriellen Anlagen – Teil 1: Gesetzliche Grundlagen und Anforderungen

Manipulation und Sabotage betrieblicher Anlagen kommen von den verschiedensten Seiten. Sollen Schutzkonzepte effektiv sein, müssen sie viele Faktoren berücksichtigen, um eine angemessene Absicherung gegen unberechtigte Eingriffe zu gewährleisten. In einem zweiteiligen Beitrag befassen sich Dr. Kai Nürnberger von Fraunhofer FKIE, Jochen Sauer von Axis Communications und Jörg Brasas von Phoenix Contact mit den normativen Grundlagen und Anforderungen sowie der Firmware als potentieller Schwachstelle. Der folgende erste Teil behandelt die gesetzlichen Regelungen sowie die zukünftigen Anforderungen, die sich aus ihnen ergeben.

„There must be fifty ways to leave your lover“, heißt es in einem bekannten Ohrwurm von Paul Simon. In Anlehnung daran könnte man sagen, dass es vermutlich ebenso viele Möglichkeiten gibt, unberechtigt in betriebliche Anlagen einzudringen, auf sensible Bereiche zuzugreifen, diese zu manipulieren oder zu sabotieren. Vorgehen und Zielsetzung hängen maßgeblich von den Interessen, Intentionen und Fähigkeiten der Tätergruppen ab. Das Spektrum der

Angriffsvektoren ist breit und kann die Lieferkette, die physische Infrastruktur, technische Systemkomponenten, das Personal oder die IT-Systeme betreffen.

Anlagen und Dienstleistungen mit kritischer Bedeutung für die Aufrechterhaltung des öffentlichen Lebens müssen naturgemäß ein besonders hohes Sicherheitsniveau erfüllen. Die entsprechenden Anforderungen sind daher in einer europäischen Richtlinie (EU 2022/2557) geregelt und werden

in der nationalen Gesetzgebung (KRITIS-Dachgesetz) implementiert. Aufgrund der zunehmenden Bedeutung der Cybersicherheit gibt es mit EU NIS2 (= Network and Information Security) eine zusätzliche europäische Richtlinie, die Mindeststandards der IT-Sicherheit für Betreiber kritischer Infrastrukturen verbindlich festlegt. Sie ist in nationales Recht umzusetzen (NIS2 Umsetzungsgesetz).

Bitte umblättern ►



© Fraunhofer FKIE

Dr. Kai Nürnberger, Leiter Strategie & Markterschließung beim Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE



© Axis Communications

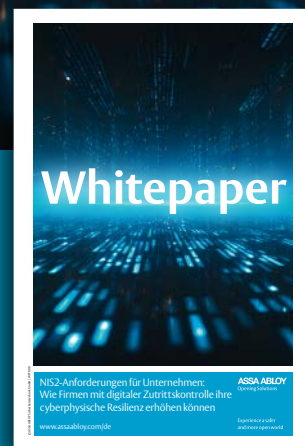
Jochen Sauer, Architect & Engineering Manager bei Axis Communications



© Phoenix Contact

Jörg Brasas, Strategic Product Marketing Manager bei Phoenix Contact

Verstehen und Umsetzen der NIS2-Richtlinie: Was Sie jetzt wissen müssen.

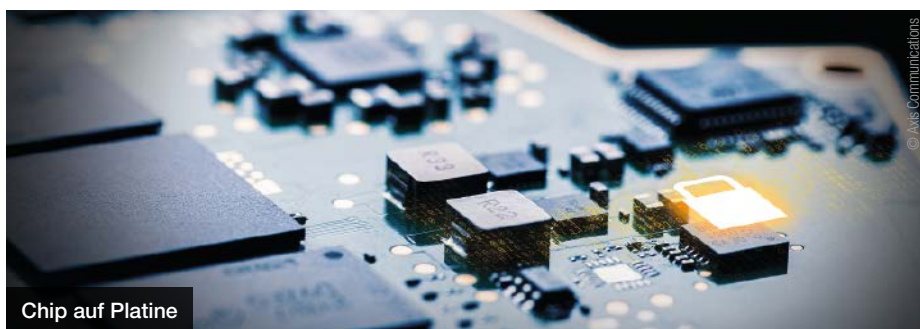


Whitepaper jetzt downloaden!



ASSA ABLOY
Opening Solutions

Experience a safer
and more open world



Vertrieb von Lebensmitteln und Chemikalien oder Produktion von elektrischen Geräten, Maschinen und Fahrzeugen).

Cyber Resilience Act (CRA)

Der CRA liegt bislang als Entwurf vor. Er nimmt nach Inkrafttreten die Hersteller in die Pflicht, Security-by-Design-Produkte zu entwickeln, um eine CE-Kennzeichnung zu erhalten. Dazu werden Mindestanforderungen an die Cybersicherheit definiert, die je nach Produktklasse durch eine Konformitätsprüfung oder durch die nachweisliche Anwendung der Normvorgaben bei der Herstellung dokumentiert werden müssen. Hersteller sind verpflichtet, innerhalb einer vorgegebenen Frist entsprechende Anpassungen vorzunehmen, um konforme Produkte auf dem Unionsmarkt in Verkehr bringen zu können.

Die essenziellen Anforderungen des CRA zielen auf einen sicheren Wertschöpfungsprozess, von der Konzeption über die Entwicklung bis hin zur Produktion, ab. Zusätzliche Bestandteile sind das Schwachstellenmanagement und Regelungen für die Dauer der Bereitstellung von Sicherheitsupdates. Um die Anforderungen an das Schwachstellenmanagement zu erfüllen, ist es wichtig, dass für alle Produkte eine standardisierte Software Bill of Material (SBOM) zur Verfügung steht. Dabei handelt es sich faktisch um eine Liste, die alle Software-Komponenten eines Produkts beschreibt. Zusätzlich müssen bekannte Schwachstellen in einem standardisierten digitalen Format wie dem Common Security Advisory Framework (CSAF) dokumentiert sein. Dadurch soll sichergestellt werden, dass die Fristen für die Meldung und Behebung von Schwachstellen eingehalten werden.

Betrachtet man die Komplexität der oben skizzierten Normen und Gesetze, so wird deutlich, dass sowohl für Hersteller als auch Systemintegratoren und Betreiber Handlungsbedarf besteht. Die Umsetzung der entsprechenden Regelungen muss einem strikten Vorgehensmodell folgen. **GIT**

Demnächst in GIT SICHERHEIT lesen Sie den zweiten und abschließenden Teil dieses Beitrags. Er wird sich mit dem Risikofaktor Firmware beschäftigen.

Eine klare Regelung der Pflichten und der damit einhergehenden technischen Anforderungen ist wichtig. Das kann einen Innovationsschub auslösen. In einem sehr dynamischen Umfeld ist jedoch zu befürchten, dass gesetzliche Vorgaben schnell von der Realität überholt werden, da sich diese vor allem auf bekannte Bedrohungen beziehen. Regelmäßige Überprüfungen und Novellierungen sind daher essenziell. Weiterhin hängt die Durchschlagskraft jeglicher Gesetzgebung von der konkreten Umsetzung und eigenverantwortlichen Aufrechterhaltung eines hohen Sicherheitsniveaus in einer komplexen Infrastruktur durch den Betreiber ab. Das erfordert differenzierte, flexible und aktualisierbare Konzepte, die schnell auf neue Täterwerkzeuge und veränderte Angriffsmethoden reagieren können.

Relevante gesetzliche Regelungen

Die zunehmende Digitalisierung und Vernetzung vergrößern die Angriffsflächen für Cyber-Attacken. Darüber hinaus werden die Täter und ihre Methoden immer professioneller. Verbesserte Cybersicherheit ist daher für Unternehmen existenziell, um das Wissen (z. B. Patente, Konstruktionspläne, Verfahren), sensible Daten (z. B. Kundendaten, Vertragskonditionen) und Wertschöpfungsprozesse zu schützen. Darüber hinaus können Cybervorfälle das Vertrauen der Kunden, Partner und Investoren in ein Unternehmen beeinträchtigen – hier gilt es also vorzuzugreifen.

Unternehmen sind grundsätzlich zur Einhaltung gesetzlicher Vorschriften zum Datenschutz verpflichtet. Für kritische Infrastrukturen gelten weitergehende gesetzliche Vorgaben zur Umsetzung der Cybersicherheit, die durch die NIS2-Richtlinie der EU zukünftig auf viele weitere Unternehmen ausgedehnt werden. Prinzipiell betreffen die erforderlichen Maßnahmen zwei Domänen:

- Information Technology (IT)
- Operational Technology (OT)

Zum Schutz beider Bereiche wird in der IT ein Informationssicherheits-Management-System (ISMS) eingeführt (ISO 27001/2), das in Richtung der OT erweitert werden soll. Die Anforderungen an ein ISMS umfassen

sowohl technische als auch organisatorische Aspekte. Die technischen Anforderungen können mit Hilfe der Norm IEC 62443-2-1 für Industrial Automation and Control Systems (IACS) auf Maßnahmen in der OT übertragen werden. Konkrete Anforderungen dieser Normenreihe sind unter anderem:

- Konfiguration und Segmentierung von Netzwerken
- Schutz der Daten bei der Speicherung und Übertragung
- Authentifizierung der Benutzerinnen und Benutzer
- Überwachung und Protokollierung von Benutzer- und Systemaktionen
- Sicherheitshärtung der eingesetzten Geräte
- Konfiguration, Updates, Backup und Restore
- Organisatorische Anforderungen an den Betrieb des Systems

Gemeinsam bieten die beiden Normen einen ganzheitlichen Ansatz zum Schutz vor Cyber-Bedrohungen. Dieses Maßnahmenpaket war bisher nur für kritische Infrastrukturen gesetzlich vorgeschrieben. Mit der neuen EU-Richtlinie NIS2 ändert sich das grundlegend.

EU NIS2-Richtlinie

Um Systeme vor Cyber-Attacken zu schützen, verpflichtet die NIS2-Richtlinie die Betreiber öffentlicher oder privater Einrichtungen zur Einführung geeigneter Sicherheitsinstrumente. Im Vergleich zur bestehenden NIS1 weitet sie die Regelungen auf mittelgroße Unternehmen mit mehr als 50 Mitarbeitenden und einem Umsatz von mehr als zehn Millionen Euro aus und gilt damit für viele ‚wesentliche und wichtige Einrichtungen‘ in der EU. Unter dem Begriff ‚wesentliche Einrichtungen‘ versteht man Unternehmen, die in kritischen Infrastrukturen tätig sind, z. B. in den Bereichen Erzeugung, Speicherung und Übertragung von Strom und Gas, Transport auf Wasser, Straße und Schiene, Betrieb von Anlagen für Trinkwasserversorgung und Abwasserentsorgung sowie von Anlagen der digitalen Infrastruktur. Die ‚wichtigen Einrichtungen‘ werden aus einer Liste von sieben Sektoren nach ihrer Kritikalität und Art der Dienstleistung ausgewählt (z. B. Herstellung und



**Fraunhofer-Institut für
Kommunikation, Informations-
verarbeitung und Ergonomie FKIE**
www.fkie.fraunhofer.de

Axis Communications
www.axis.com

Phoenix Contact
www.phoenixcontact.com



Stephan Holzem, Geschäftsführer
TAS Telefonbau Arthur Schwabe

ÜBERTRAGUNGSTECHNIK

Ohne Strom kein Alarm

**Sichere
Übertragungstechnik:
Vom Schutz der
sicherheitstechnischen
Gewerke bis zur
sicheren Übertragung
von Alarmmeldungen**



Daniel Kaumanns, Leiter Produktmanagement
TAS Telefonbau Arthur Schwabe

Die europäischen Anforderungen des künftigen KRITIS-Dachgesetzes sowie des NIS2-Umsetzungsgesetzes sind bereits festgelegt: Cyber- und physische Risiken müssen bewertet werden und entsprechende Schutzmaßnahmen sollen dem Stand der Technik entsprechen. Daher ist man gut beraten, Sicherheitssysteme dem neuesten technischen Standard entsprechend zu planen, sagen Stephan Holzem, Geschäftsführer, und Daniel Kaumanns, Leiter Produktmanagement von TAS Telefonbau Arthur Schwabe im Gespräch mit GIT SICHERHEIT.

Herr Holzem, Herr Kaumanns, wie wichtig umfassende Sicherheitskonzepte für unsere Kritischen Infrastrukturen sind, steckt schon in dieser Bezeichnung: Sie sind eben „kritisch“ – sprich, sie sind von prioritärer Wichtigkeit für uns alle. Ohne Strom, Wasser und Verkehr läuft nichts – und es gibt Interdependenzen und Dominoeffekte wenn auch nur eine Einrichtung größere Probleme macht. Wie hoch schätzen Sie die Gefahr von Ihrer Warte aus gesehen eigentlich ein?

Stephan Holzem: Kritische Infrastrukturen sind auf unterschiedliche Art und Weise bedroht, durch Naturkatastrophen, technisches Versagen oder durch Gefahren, die der Mensch verursacht. Zu letzterem, den sogenannten anthropogenen Gefahren, gehören z. B. Unfälle, Cyberangriffe und

Sabotage. Die Gefahren sind also vielfältig. Die zunehmende Digitalisierung verstärkt darüber hinaus die Interdependenzen der Kritischen Infrastruktur untereinander wie beispielsweise bei den intelligenten Stromnetzen, den Smart Grids. Hier sind neue Energietechnologien mit der Informationstechnik vernetzt. Ein Ausfall in einem Sektor kann zu Ausfällen in anderen Sektoren führen bis hin zum Kaskadeneffekt. Die Gefahren sind hoch und die Betreiber von Anlagen der Kritischen Infrastruktur müssen im Rahmen des Risiko- und Krisenmanagements alle Gefahrenarten berücksichtigen. Dies bezeichnet man als All-Gefahren-Ansatz. Für den Schutz der Kritischen Infrastruktur bedeutet das: Ganzheitlich denken im Sinne von Cyber-Sicherheit, physischen Schutz z. B. durch Einbruch- und Überfallmeldeanlagen und den Einsatz sicherer Produkte.

Zu Ihren Themen zählt in diesem Zusammenhang vor allem die Übertragungstechnik – hier reden wir etwa von der sicheren Übertragung von Alarmmeldungen über Netzwerke, wie sie die DIN EN 50136 regelt. Ist das richtig?

Stephan Holzem: Es muss gewährleistet sein, dass Einbruch- und Brandmeldeanlagen sowie Zutrittskontrollsysteme ihre Alarmmeldungen zu den Alarmempfangszentralen, z. B. zu einer Leitstelle, sicher übertragen können. Sie müssen zudem resilient sein gegen Cyberangriffe, technische Störungen und Netzwerk-Überlastungen. Die Anforderungen dafür regelt die DIN EN 50136. Das Ziel ist eine sichere und hochverfügbare Übertragungsstrecke aufzubauen, Übertragungszeiten gemäß den geltenden Normen und Richtlinien einzuhalten und die Übertragungswege zu überwachen. Die

Normenreihe der EN 50136 regelt dabei sowohl die Übertragung der Alarmmeldungen zu den Leitstellen als auch den sicheren Remote Access, also sämtliche weitere Verbindungen zu sicherheitstechnischen Gewerken, die für „Remote Services“ verwendet werden.

Auf die Sicherheit von Routern und Netzen kommt es hier an. Welche Störungen sind es vor allem, gegen die sie resilient sein müssen?

Daniel Kaumanns: Potenzielle Risiken können ein Ausfall der Spannungsversorgung oder ein Blitzeinschlag sein. Ein erhöhtes Risiko ergibt sich zudem aus der signifikant gestiegenen Anzahl an Cyberangriffen. Eine Sabotage auf die Stromversorgung ist sehr einfach möglich. Fallen Übertragungswege oder sogar komplette Übertragungsnetze aus, können Alarmer nicht mehr übertragen werden. Das zwingt Hersteller von Netzwerkkomponenten zum Handeln! Als Hersteller von Übertragungseinrichtungen, welche die Schnittstelle zum öffentlichen Netz darstellen, ist es unser Anspruch, den Schutz der sicherheitstechnischen Gewerke sowie eine sichere Übertragung von Alarmmeldungen und aller weiteren Verbindungen zu den sicherheitstechnischen Gewerken zu gewährleisten.

Geben Sie uns ein paar Beispiele?

Daniel Kaumanns: Die Richtlinien und Normen geben uns klare Vorgaben zur unterbrechungsfreien Stromversorgung, um vor Stromausfällen zu schützen. Dazu gehören redundante Übertragungswege, z. B. ein leitungsgebundener IP-Übertragungsweg (DSL) und ein funkbasierter IP-Übertragungsweg (Mobilfunk). Sie gewährleisten nicht nur den Schutz vor einem Ausfall des Übertragungsnetzes, sondern verhindern auch das Blockieren der Meldungsübertragung durch DoS-Angriffe. Angriffe, die auf

weitverbreitete Betriebssysteme ausgelegt sind, laufen bei unseren Übertragungseinrichtungen ins Leere, durch das eigens entwickelte und gehärtete Betriebssystem. Durch Security by Design und Security by Default werden die Angriffsmöglichkeiten reduziert. Sicherheit fängt schon bei der Übertragungstechnik an.

Welche Mindeststandards gibt es diesbezüglich bei Kritischen Infrastrukturen?

Stephan Holzem: Die Übertragungstechnik muss gegen Spannungseinbrüche und Stromausfälle abgesichert sein. Die unterbrechungsfreie Stromversorgung wird hierbei mittels Akkumulatoren gewährleistet. Darüber hinaus sollte die Energieversorgungseinheit der Übertragungseinrichtung kontinuierlich überwacht werden, sodass Störungen an eine ständig besetzte Stelle gemeldet werden. Eine solche Energieversorgungseinheit sollte den Anforderungen der DIN EN 50131 Grad 4 entsprechen. Neben Spannungseinbrüchen gibt es auch Überspannungen, dagegen ist ein zusätzlicher Schutz sinnvoll. Die redundanten Übertragungswege müssen zumindest objektseitig vollständig notstromversorgt sein und über eine Ende-zu-Ende-Überwachung zur Alarmempfangszentrale verfügen. Zudem muss die Übertragungstechnik adäquat gegen mechanische Beschädigung oder Sabotage geschützt werden, bspw. durch die Installation im Überwachungsbereich einer Einbruchmeldeanlage, durch ein robustes Gehäuse, Deckelkontakt, Durchbohrungsschutz oder Abreißschutz. Höchste Priorität hat die Cybersicherheit. Für die Alarmübertragung sind ausschließlich speziell dafür vorgesehene Protokolle wie zum Beispiel VdS SecurIP zu verwenden, die dem aktuellen Stand der Technik entsprechen. Und das eingesetzte Gerät sollte nach den geltenden Cyber-Sicherheitsanforderungen (z. B. VdS 3836) zertifiziert sein.

Ein besonderes Sicherheitsrisiko entsteht beim Fernzugriff – Stichwort Remote-Access und Remote-Services. Hier gibt es die TS 50136-10. Könnten Sie dazu etwas Näheres sagen?

Daniel Kaumanns: In der Vergangenheit wurden Remote Access und Remote Services häufig nicht in die Risikoanalyse einbezogen. Standardrouter mit offenen Ports wurden direkt mit dem Internet verbunden, um Fernzugriffe zu ermöglichen. Diese Art des Fernzugriffs stellt jedoch ein erhebliches Sicherheitsrisiko dar. Diese Problemstellung haben die Branchenverbände und Normungsgremien erkannt und 2021 entsprechende Normen und technische Spezifikationen veröffentlicht. Die Norm EN 50710 beschreibt die Anforderungen des Remote Services und die technische Spezifikation TS 50136-10 beschreibt die Anforderungen des Remote Access. Durch diese Maßnahmen wurde erstmalig eine einheitliche Struktur erarbeitet und für die Branche rechtssicher definiert. Welchen Stellenwert diese Normierung hat, sieht man schon allein daran, dass die TS 50136-10 derzeit bereits überarbeitet wird und in eine Norm umgewandelt werden soll. Kernaussagen dieser Normung sind die Anforderungen an das Verbindungsmanagement aller Verbindungen, die Remote-User-Authentifizierung, Datenintegrität, Vertraulichkeit, Authentifizierung der Endgeräte, Authentifizierung von automatisierten Systemen sowie das Logging aller Zugriffe. Zudem werden klare Verantwortlichkeiten mit dem jeweiligen Remote Access Infrastructure Service Provider definiert. Dieser verantwortet genau die genannten Anforderungen an die gesamte Remote Access Infrastructure. Ohne Berücksichtigung dieser Vorgaben ist ein Fernzugriff nicht mehr vertretbar und führt zwangsläufig zu einem Cyberisiko.

Pro V2 mit Rutschkupplung von Dom

Dom Sicherheitstechnik hat eine Rutschkupplung entwickelt, die beispielsweise in Schulen oder Altenheimen eingesetzt werden kann. Die Pro V2 Rutschkupplung ermöglicht es, dass Türen von innen ohne Schlüssel verriegelt werden können – beispielsweise in Situationen, bei denen das unverzügliche Verschließen der Klassenräume von innen lebensrettend sein kann.

Jeder, ob Schüler oder Lehrer, kann die Tür bei Gefahr von innen verriegeln. Das ist schnell und ohne Schlüssel mit einem Drehknopf möglich. Die so verriegelte Tür lässt sich von außen nur mit einem Schlüssel öffnen, den ausschließlich berechnete Personen besitzen. Blockiert z. B. ein Schüler im Alltag aus Spaß von innen die Tür, so kann sie der Lehrer dennoch von außen mit dem Schlüssel öffnen. Möglich macht dies ein spezieller Knopfzylinder, der die vorhandenen Schließzylinder ersetzt. Das speziell für diese Anforderung entwickelte Kupplungssystem, Pro V2 mit Rutschkupplung, steuert die Schließfunktion bei blockierendem Innenknopf. Das System funktioniert ohne Elektronik, also rein mechanisch.

www.dom-security.com/de



Wie erkennt man Produkte, die den erforderlichen Sicherheitsstandards entsprechen? Kürzlich wurde ja der Cyber Resilience Act, eine EU-Verordnung, veröffentlicht?

Stephan Holzem: Der Cyber Resilience Act (CRA) beschreibt erstmals branchenübergreifend die Anforderungen an die Cybersicherheit vernetzbarer Produkte. Dies umfasst sowohl die Hardware als auch die Software. Hersteller müssen sicherstellen, dass ihre Produkte den neuen Standards entsprechen. Ohne die Anforderungen, die ab Dezember 2027 gelten, dürfen die Produkte im EU-Binnenmarkt nicht mehr verkauft werden, weder die Hersteller selbst noch Händler und Importeure. Kurz gesagt, legt der CRA fest, dass die Informationssicherheit eines Produkts über dessen gesamten Lebenszyklus hinweg gewährleistet sein muss, durch Prinzipien wie „Security by Design“ und „Security by Default“ sowie die Sicherstellung der Vertraulichkeit und Integrität der verarbeiteten Daten. Hersteller sind verpflichtet, entdeckte Schwachstellen zu melden und durch Sicherheitsupdates zu beheben. Zudem muss in einer Software Bill of Materials (SBOM) dokumentiert werden, welche kommerziellen und freien Software-Bestandteile in Software-Produkten enthalten sind.

Viel ist von Komponenten etwa von chinesischen Herstellern die Rede, die hinsichtlich ihrer Sicherheit als problematisch angesehen werden. Gerade bei der Übertragungstechnik sollte man ja wohl keine Luft reinlassen...?

Stephan Holzem: Insbesondere chinesische Firmen geraten zunehmend unter Druck. In den USA sind bereits einige chinesische Produkte für den Einsatz in kritischen Bereichen gesperrt. Das Risiko für den Einsatz fraglicher Produkte muss im Rahmen des Sicherheitskonzeptes zumindest bewertet werden. Denn: Sowohl über die eingesetzte Hardware als auch über die Software können Hintertüren in die Produkte eingeschleust werden. Die gesamte Vernetzung der sicherheitstechnischen Anlagen ist durch eine fragliche Komponente gefährdet, wenn über diese eine Backdoor geschaffen wird, über die Dritte Zugriff erlangen und funktionsrelevante Komponenten unerkannt außer Betrieb nehmen können. Dabei ist es zum Teil schwierig nachzuweisen, ob das Gerät „nach Hause telefoniert“. Dies erfordert ein kontinuierliches Monitoring aller Komponenten. Systeme müssen auf aktuellem Software-Stand gehalten werden. Es müssen Verfahren etabliert und dokumentiert werden, die Sicherheitslücken erkennen. Auf Sicherheitslücken muss teils innerhalb weniger Stunden reagiert werden. Hier gibt es abhängig vom Risiko erhebliche Anforderungen durch NIS2.

Sicherheit und Herkunft müssen ja entlang der gesamten Lieferkette transparent sein...?

Stephan Holzem: Ja, denn ist nur eine Komponente unsicher und schafft ein Einfallstor für Angriffe, ist die Gesamtsicherheit nicht mehr gewährleistet. Einheitliche Standards in der EU sollen die Zuverlässigkeit der verwendeten Komponenten gewährleisten. Labels wie „Made in Germany bzw. Europe“ erhalten damit zunehmend eine höhere Bedeutung. 



TAS Telefonbau
Arthur Schwabe
GmbH & Co.KG
www.tas.de

STATE OF SECURITY

Die Sicherheitskonferenz
am Brandenburger Tor 2025



Verpassen Sie nicht den Pflichttermin für alle Sicherheitsverantwortlichen. Renommierte Referenten informieren Entscheider aus Wirtschaft, Politik und Sicherheitsbehörden zum Thema

Digitale und physische Sicherheit im Zusammenspiel

Unternehmensschutz ganzheitlich betrachtet

am 3. Juni 2025
im Allianz Forum am Pariser Platz

Referenten u. a.:

Dr. Dirk Häger

Abteilungsleiter Operative Cyber-Sicherheit beim Bundesamt für Sicherheit in der Informationstechnik (BSI)

Markus Horschig

Leitung KRITIS bei der Hamburg Port Authority

Heimo Krum

Chief Information Officer der FUNKE Mediengruppe

Dr. Carolin Schilling-Schulz

Rechtsanwältin / Partnerin bei ARNECKE SIBETH DABELSTEIN

Jetzt informieren und kostenlos anmelden unter:
koetter.de/state-of-security

KÖTTER Security
Wilhelm-Beckmann-Straße 7
45307 Essen

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



Nach Art der Zwiebel

Perimetersicherung für ein Umspannwerk



Videoanalyse oder eine Kombination z. B. mit einem Laserscanner sind eine gute Möglichkeit, eine sichere und falschalarmfreie Detektion des Übertritts zu erzielen

Im Rahmen der Absicherung von Kritischen Infrastrukturen wird der Perimetersicherung vermehrt eine hohe Bedeutung zugesprochen. Ein wichtiger Grund hierfür ist sicherlich die Lage und die Größe vieler Objekte. Sie sind über ganz Deutschland verteilt und haben in der Regel auch einen größeren Flächenbedarf. Eine Absicherung nach dem Zwiebelschalenmodell ist daher das Mittel der Wahl, um eine möglichst große Interventionszeit zu erlauben. Thomas Hermes, Leiter Geschäftsfeld Energie bei Securiton Deutschland, sprach darüber kürzlich auf dem BHE-Thementag „Sicherheit in KRITIS“ – und fasst seinen Vortrag im folgenden Beitrag für GIT SICHERHEIT zusammen.



Thomas Hermes, Leiter Geschäftsfeld Energie bei Securiton Deutschland.

Es gibt in Deutschland circa 300 Umspannwerke in der höchsten Spannungskategorie. In diesen Umspannwerken finden sich Transformatoren, Hochleistungsschalter, Portalkonstruktionen und natürlich auch Gebäude und Nebenanlagen, die für den Betrieb erforderlich sind. Bei einer mittleren Größe von ca. 20.000 bis 30.000 Quadratmetern – es gibt auch deutlich größere Anlagen – müssen jeweils ca. 500 Meter Perimeter abgesichert werden.

Gehen wir davon aus, dass die Risikoanalyse Schwachstellen im Sabotageschutz

aufzeigt. Es kann nicht sichergestellt werden, dass der Zaun unverletzt ist. Daher kann auch nicht ausgeschlossen werden, dass es unverhältnismäßig lange Aufenthalte von Personen auf dem Gelände gibt, die unbemerkt bleiben.

Nach den Zwiebelschalen wird die Perimetersicherung in einem solchen Fall die Schicht 0 (außerhalb des Zaunes), die Schicht 1 (die mechanische Absicherung selbst) und die Schicht 2 (das Gelände innerhalb) unterscheiden.

Schicht 0: Tatvorbereitung

Eine effiziente Absicherung der Außengrenze mit Kamerasystemen kann bereits alarmieren, wenn eine Person sich außergewöhnlich lange vor dem Zaun aufhält. Dieses sogenannte „Loitering“ (Herumlungern) ermöglicht eine Alarmierung, wenn eine Manipulation des Zaunes oder gar ein Unterkriechen vorbereitet wird.

Schicht 1: Überwindung des Zaunes

Leider muss immer wieder festgestellt werden, dass die mechanische Barriere mithilfe

von falsch abgestellten Containern oder Gerüsten relativ leicht überwunden werden kann. Auch Bäume in unmittelbarer Nähe können hier den Überstieg erleichtern. In der Schicht 1 ist daher häufig ein Volumendetektionssystem wie z. B. die Videoanalyse oder eine Kombination z. B. mit einem Laserscanner eine gute Möglichkeit, eine sichere und falschalarmfreie Detektion des Übertritts zu erzielen.

Schicht 2: Täterverfolgung

Die Norm sieht für hochgradige Perimetersicherungssysteme (PSS) der Kategorie z. B. 4D eine Täterverfolgung vor. Ziel dieses „Trackings“ ist eine klare Aussage, in welchen Bereichen des Umspannwerks der Täter sich aufgehalten hat. Dies bietet in der Nachverfolgung des Tathergangs eine gute Möglichkeit, wo nach versteckten Sabotagehandlungen gesucht werden muss.

Einteilung nach DIN

Es gibt eine grobe Einteilung von Systemen, die in den Betriebsanforderungen auch in der DIN VDE V 0826-20 festgelegt sind. Diese ist zweiteilig. Auf der einen Seite der PSS-Eigenschutz der Anlage (1-4). Dieser ist vergleichbar mit den VDS-Klassen einer Einbruchmeldeanlage. Daneben gibt es die PSS-Leistungskategorie. Sie ist abhängig davon, wieviel Gebäude auf dem Gelände sind. Auch die Form des Perimeters spielt eine Rolle, also ob sie beispielsweise gradlinig ist oder viele Kurven und Ecken hat. Die Frage ist auch, ob es Straßen, Wege, Plätze und Orte mit höherem Sicherheitsbedarf



Perimeterschutz für ein Umspannwerk: Eine Absicherung nach dem Zwiebelschalenmodell ist daher das Mittel der Wahl

gibt. Dies fordert von dem PSS eine entsprechende höhere Leistungskategorie (A-D).

Wir empfehlen bei einer kritischen Infrastruktur immer von der höchsten Eigenschutzkategorie auszugehen. Das heißt, wir liegen hier immer bei einem PSS-Eigenschutz 4. Je nachdem, ob es sich um ein kleines Gelände oder ein komplexeres handelt, wird die Perimeter-Sicherheitskategorie 4B bis 4D sein. Eine Anforderung für ein solches Objekt kann zum Beispiel sein, dass nicht nur ein Detektionssystem, sondern mehrere Detektionssysteme eingesetzt werden sollten, um sicher vor etwaigen Sabotagehandlungen zu sein. Eines kann z. B. eine Detektion unmittelbar am Zaun oder ein 2D-LIDAR-System in Kombination mit einer Videoanalyse sein.

Drohnen

Neben der eigentlichen Zaunüberwachung sollte auch das Thema Drohnensicherheit

betrachtet werden. Inwieweit muss ein Täterszenario unter Einsatz von Drohnen ebenfalls detektiert werden? Es gibt heute sehr effektive Systeme, die es ermöglichen, Drohnen effektiv zu detektieren und auch zu bekämpfen, also zu übernehmen und in einer gesicherten Zone zu landen. Das Ziel ist, dass eine „Dome-Security“ in der Art einer virtuellen Kuppel über Anlagen der kritischen Infrastruktur gespannt wird. Dies bedeutet Sicherheit von der bodennahen Detektion an der juristischen Grenze bis zur Überwachung und Sicherung des bodennahen Luftraumes. **GIT**



Securiton Deutschland
www.securiton.de

BHE
www.bhe.de

MotionIQ – Klimaschutz an der Eingangstür

Dormakaba zeigte auf der Messe BAU 2025 in München mit seiner Technologie MotionIQ eine Lösung, die den Energieverlust bei Automa-tiktüren erheblich reduziert. Durch eine präzise Türsteuerung minimiert MotionIQ die Offenhaltezeit und ermöglicht Energieeinsparungen von bis zu 50 % im Vergleich zu Standardlösungen. Dadurch wird der CO₂-Fußabdruck eines Gebäudes reduziert. Ermöglicht wird die Bewertung des Einsparpotenzials für jeden Anwendungsfall durch den Door Efficiency Calculator von Dormakaba, ein wissenschaftlich validiertes Tool, das Architekten und Bauplanern fundierte Daten für nachhaltige Entscheidungen liefert. Das Herzstück der neuen Technologie ist ein intelligentes System, das die Türbewegungen in Echtzeit analysiert und steuert. Das System passt die Türbewegung präzise an die Annäherungsgeschwindigkeit der Nutzer an. Dadurch öffnen sich die Türen nicht früher als nötig und schließen so schnell wie möglich. **www.dormakaba.com**



Neben KI, Drohnen und Biometrie gehört nach wie vor der physische Perimeterschutz zu den effektiven Sicherheitsvorkehrungen

PERIMETERSCHUTZ

Solider Zaun gehört dazu

Trends in der Sicherung von Investitions- und Gewerbeobjekten im Jahr 2025

Immer häufiger sprechen wir über digitale Sicherheitsmaßnahmen, fortschrittliche Videoüberwachung oder CCTV-Systeme sowie Alarmsysteme, die fernüberwacht mit Apps und unseren Smartphones verbunden sind. Dabei zählt nach wie vor ein verstärkter Zaun mit einem soliden Verschluss zu den effektivsten Sicherheitsvorkehrungen für ein Gelände. Wisniewski Deutschland macht sieben Trends aus, die den Sicherheitsmarkt dieses Jahr dominieren werden.

■ Die Sicherung von Investitionsobjekten spielt eine äußerst wichtige Rolle beim Schutz von Infrastruktur, Daten und materiellen Werten. Im Jahr 2025 werden sich die Technologien in diesem Bereich dynamisch weiterentwickeln, um zunehmend komplexeren und vielfältigeren Bedrohungen gerecht zu werden.

Eine Branchenanalyse, die allein Daten aus Polen umfasst, zeigt zum Beispiel, dass der Schutz von Eigentum auf Baustellen eine große Herausforderung darstellt. Seit 2021, als 225 000 Häuser und Wohnungen fertiggestellt wurden, gab es auch einen Anstieg der Diebstähle auf den Baustellen. Am häufigsten wurden hochwertige Baumaterialien wie Betonstahl, elektrische Leitungen und Dachziegel gestohlen, aber auch Fenster- und Türbeschläge. Dieser besorgniserregende Trend macht deutlich, wie wichtig es ist, moderne Überwachungslösungen,

Sicherheits- und Alarmsysteme zu implementieren, die finanzielle und zeitliche Verluste während der Investitionsphase wirksam minimieren können.

Hier sind die wichtigsten Trends, die den Sicherheitsmarkt dominieren werden:

1. Integration von Künstlicher Intelligenz (KI)

Die KI revolutioniert die Art und Weise, wie man Bedrohungen überwacht und auf sie reagiert. Im Jahr 2025 werden Sicherheitssysteme, die mit Algorithmen des maschinellen Lernens ausgestattet sind, in der Lage sein, Daten von Kameras, Sensoren und anderen Geräten automatisch zu analysieren – zum Beispiel an bestimmten Tagen oder zur richtigen Tages- und Nachtzeit. KI wird eine frühzeitige Erkennung verdächtiger Aktivitäten ermöglichen, wie

etwa unbefugtes Betreten oder ungewöhnliches Verhalten auf dem Gelände.

2. Biometrie und Verhaltensidentifikation im Rahmen von CCTV

Die zunehmende Beliebtheit biometrischer Lösungen wie Gesichtserkennung, Iriserkennung oder Ganganalyse verändert die Standards für die Identitätsprüfung. Im Jahr 2025 werden diese Systeme noch präziser sein und in größerem Umfang eingesetzt werden, um sicherzustellen, dass nur berechnete Personen Zugang haben. Dies wird durch fortschrittliche Technologien von Überwachungskameras und CCTV-Systemen ermöglicht.

3. Perimetersicherung der nächsten Generation

Investitionsgelände erfordern eine effektive physische Perimetersicherung. Im Jahr 2025 wird jedoch der Fernzugang

liche Überwachung, ohne dass zahlreiche Mitarbeiter erforderlich sind.

5. Verstärkung von Materialien für Perimeterschutz

Zaunsysteme sind dann effektiv, wenn sie schwer zu durchdringen und verstärkt sind. Je länger sie haltbar und widerstandsfähig gegen Witterungseinflüsse oder Beschädigungen sind, desto länger werden sie ihre Funktion erfüllen. Es lohnt sich also, nach professionellen feuerverzinkten und pulverbeschichteten Zäunen Ausschau zu halten, die nicht nach ein paar Jahren ausgetauscht werden müssen.

6. Zusammenarbeit mit intelligenten Städten (Smart Cities)

Die Sicherheitslösungen für Investitionsobjekte werden zunehmend in die Infrastruktur intelligenter Städte integriert. Überwachungssysteme, Verkehrsmanagement und Krisenkommunikation werden miteinander

7. Design, der mit dem gesamten Objekt harmonisiert

Das Jahr 2025 bringt uns einem ganzheitlichen Ansatz zur Ästhetik von Grundstücken näher. Früher wurden Investitionsprojekte mit den günstigsten Gitterpaneelen oder Drahtzäunen umzäunt. Heute wählen Investoren schon in der Planungsphase Zäune, die die Attraktivität des gesamten Projekts erhöhen und eine Visitenkarte des Objekts werden können. Bereits während der Bauphase soll das Zaun nicht nur das Gelände sichern, sondern auch den Standort aufwerten und den Charakter des entstehenden Gebäudes unterstreichen.

Im Jahr 2025 werden Technologien wie künstliche Intelligenz, Biometrie und Drohnen die Zukunft der Sicherheitslösungen prägen. Dank eines integrierten Ansatzes und innovativer Lösungen können wir ein höheres Maß an Sicherheit und Effizienz im Risikomanagement erwarten. **GIT**



zum Gelände, beispielsweise durch das Öffnen von Zufahrtstoren über eine App, von großer Bedeutung sein. Moderne Lösungen ermöglichen es, anderen Personen, Investoren oder Subunternehmern Zugang zu gewähren, ohne dass beispielsweise der Bauleiter oder der Sicherheitsdienst vor Ort erscheinen muss. In Verbindung mit KI bieten diese Lösungen eine schnelle Reaktion auf Bedrohungen in Echtzeit. Ein Beispiel dafür ist die polnische Lösung Wiśniowski Connected, die 2024 im Bereich von Garagentorprodukten ihre Premiere hatte.

4. Drohnen und Patrouillenroboter

Die Automatisierung physischer Schutzprozesse wird 2025 einen weiteren Schritt zur Sicherung von Investitionsflächen darstellen. Drohnen mit Wärmebildkameras und Bewegungssensoren überwachen bereits große Areale, während Bodenroboter in besonders wertvollen Investitionsbereichen wie Solarparks eingesetzt werden. Solche Lösungen gewährleisten eine kontinuier-

interagieren, was eine schnellere Reaktion in Notfällen und eine bessere Planung des Schutzes ermöglicht. Auch die Anzahl der städtischen Kameras wird zunehmen, was zur Verbesserung der Sicherheit in städtischen Bereichen beitragen wird.



Wisniowski Deutschland GmbH
www.wisniowski.de

© Bilder: Wisniowski



Smart-City-Lösungen für 24/7 Videoüberwachung

Outdoor-Gehäuse mit managed Layer 2 Switch. Anschluss mehrerer Objekte über PoE/PoE+/HiPoE & Glasfaser. Echtzeitkontrolle und Fernwartung.

SMART HOME

Froschblaues Wunder

**Frogblue International Partner Conference 2025:
Innovationen und Zukunftsvisionen im Fokus**

Vom 23. bis 25. Februar 2025 fand die International Partner Conference (IPC) der Kaiserslauterer Technologie-Pioniere Frogblue statt. Die Veranstaltung bot eine Plattform für den Austausch von Innovationen, Strategien und Zukunftsvisionen im Bereich der Gebäudeautomation und Zutrittskontrolle bis hin zu Einblicken in Kamertechnik. Mit Keynotes, technischen Präsentationen und interaktiven Workshops gewährte das Team um die Unternehmensgründer Dr. Ralf Hinkel und René Hinkel den Teilnehmern einen umfassenden Einblick in die neuesten Entwicklungen und Produkte.



René Hinkel mit frogTerminal

Frogblue bietet Lösungen für die Steuerung von Beleuchtung, Heizung, Jalousien, Türen und mehr. Die Made-in-Germany-Produkte des Unternehmens aus dem pfäl-

zischen Kaiserslautern basieren auf der Bluetooth-Technologie und ermöglichen eine einfache und flexible Installation ohne zentrale Steuerungseinheiten. Zu den

Kunden zählen sowohl private Haushalte als auch gewerbliche und industrielle Anwender, „die Wert auf zuverlässige und sichere Automatisierungslösungen legen“, so Gründer Dr. Ralf Hinkel, der vor Frogblue bereits weitere erfolgreiche Unternehmen aufgebaut hatte – darunter der mittlerweile zur japanischen Konica Minolta Gruppe gehörige IP-Videosystem-Anbieter Mobotix.



International Partner Conference 2025

Vom 23. bis 25. Februar 2025 lud Frogblue zur International Partner Conference ein, um die neuesten Entwicklungen und Innovationen im Bereich der Gebäudeautomation und Zutrittskontrolle vorzustellen. Die Veranstaltung begann mit einer Vorstellung einiger der wichtigsten Akteure des Unternehmens, darunter die CEOs Dr. Ralf Hinkel und René Hinkel, Julian Lenser-Hobbs und Alexander Fuksik, beide Development Project Manager. Der Vertrieb wird geleitet von Christian Heller.

Der offizielle Part des Events startete mit Dr. Ralf Hinkel. In seiner Keynote stellt er die Highlights des neuen frogTerminals vor. Dieses Gerät bietet eine dezentrale Zu-

trittskontrolle und Gebäudeautomation, basierend auf dem internationalen Standard SIP. Es ermöglicht die Kommunikation mit verschiedenen Telefonsystemen und bietet hohe Sicherheit durch die Integration von Smartphone-Steuerungen.

Das frogTerminal – am Rande der Veranstaltung mit einem der begehrten GIT SICHERHEIT AWARDS 2025 ausgezeichnet – ist eine SIP-Video-Türstation mit einer hemisphärischen 180°-Kamera und einer Auflösung von 8 MP. Es verfügt über ein integriertes 3,5"-Touch-Display, das flexibel mehrere Klingeltasten oder Funktionen anzeigen kann und für Mehrparteien-Szenarien geeignet ist. Die Zugangskontrolle erfolgt über PIN und/oder RFID-Schnittstelle (Mifare DesFire EV2). Die Verbindung und Stromversorgung erfolgt über Netzwerk-kabel (PoE) oder über Klingeldraht und WLAN.

Weitere spannende Präsentationen folgten, darunter das Vertriebskonzept und Marketing sowie eine Partner-Präsentation zur kundenspezifischen SaaS-Schnittstelle mit RFID-Integration. Technische Einblicke gab es von Julien Lenser-Hobbs, der noch einmal weitere Vorteile und Funktionen des frogTerminals detailliert erläuterte.

Immer steht bei Events dieser Art auch das Konzept der „Frogs“ im Mittelpunkt, kleine Bluetooth-Steuerungsmodule, die eine dezentrale und flexible Gebäudeautomation ermöglichen. Diese Module kommunizieren untereinander und sorgen für eine zuverlässige und sichere Steuerung aller angeschlossenen Geräte. Nebenbei sind sie auch die Namensgeber des Unternehmens: Signale hüpfen von Gerät zu Gerät, wie Frösche, englisch Frogs – das Ganze via Bluetooth – daraus ergibt sich der Name Frogblue.

Wie genau funktionieren nochmals die Frogs?

Für alle, die nicht in vergangenen Ausgaben der GIT SICHERHEIT stöbern wollen, sei es nochmals gerne erläutert: Die kleinen, leistungsstarke Bluetooth-Steuerungsmodule, die zum Beispiel hinter Standard-Lichtschaltern oder Steckdosen installiert werden und nur 230V benötigen, sind das Herzstück des Frogblue-Systems und ermöglichen eine drahtlose Verbindung und Steuerung von Beleuchtung, Jalousien, Lüftern, Fenstern, Türen, Heizungen, Gegensprechanlagen und Standard-Lichtschaltern.

Die Frogs kommunizieren untereinander über ein Bluetooth-Mesh-Netzwerk, das eine zuverlässige und sichere Steuerung aller angeschlossenen Geräte gewährleistet. Jedes Modul kann Schalt- und Dimmfunktionen ausführen, Messungen vornehmen, Türen öffnen und noch viel mehr. Die Kom-

munikation erfolgt blitzschnell und die Nachrichten werden realtime und – wichtig zu erwähnen – verschlüsselt weitergeleitet, um die Reichweite zu erhöhen.

Ein großer Vorteil der Frogs ist auch ihre einfache Installation und Flexibilität. Da keine zentralen Steuerungseinheiten oder Server benötigt werden, können die Module problemlos in bestehenden Gebäuden nachgerüstet werden. Die Konfiguration erfolgt über eine App, die es ermöglicht,

ges- und zeitgesteuerte Programme optimieren den Energieverbrauch raumweise.

■ **Alarmanlage:** Benachrichtigungen über das Öffnen von Fenstern und Türen oder das Drücken von Lichtschaltern auf einem Smartphone. Push-Benachrichtigungen per Nachricht, E-Mail oder Anruf.

■ **Zugang und Kommunikation:** Dezentrale Zutrittskontrolle und Kommunikation über das frogTerminal. Integration von SIP-Telefonie und direkter Verbindung zu



Führungsstark auf der IPC 2025 (v.l.n.r.): Julien Lenser-Hobbs, Sabine Hinkel, Gründer Dr. Ralf Hinkel und René Hinkel, Alexander Fuksik. CSO Christian Heller konnte krankheitsbedingt leider nicht teilnehmen.

Schalterfunktionen, Wechselschaltungen und Zentralbefehle später anzupassen.

Produktportfolio von Frogblue

Auf der IPC gab es für alle Teilnehmerinnen und Teilnehmer genügend Gelegenheit, sich noch einmal das Komplettprogramm der Innovatoren aus der Pfalz anzusehen oder erläutern zu lassen. So bietet Frogblue eine breite Palette von Produkten, die alle Aspekte der Gebäudeautomation abdecken.

Einige der wichtigsten Funktionen und Produkte von Frogblue umfassen:

■ **Beleuchtung:** Steuerung aller Beleuchtungsquellen, einschließlich variabler Dimmkurven und DALI 2-Kompatibilität. Premises-weite LED-Steuerung und Farbsynchronisation über alle Räume.

■ **Verschattung:** Zeit- und wettergesteuerte Verschattung mit zentralen und Zonenfunktionen. Integration von verschiedenen Wind- und Tageslichtsensoren.

■ **Heizung:** Heizungssteuerungssystem, das die richtige Temperatur in jedem Raum gewährleistet, sei es Fußbodenheizung, Heizkörper oder elektrische Heizung. Ta-

Endgeräten ohne zusätzliche Hardware.

■ **Fernsteuerung:** Steuerung aller Funktionen von überall auf der Welt über ein Smartphone mit aktiviertem Cloud-Service.

Nicht ganz uninteressant zu erwähnen ist der noch dezent gegebene Hinweis, dass ab 2026 Frogblue wohl sogar IP-Kameras anbieten wird, mit Funktionen wie Gesichtserkennung, Nummernschilderkennung und Objekterkennung.

Zusammenfassung: Was können die Frogblue-Produkte?

Frogblue bietet eine Vielzahl von Vorteilen, die ihre Produkte zu einer attraktiven Wahl für die Gebäudeautomation machen können. Hier einige der wichtigsten Vorteile in der Übersicht:

Einfache Installation und Flexibilität:

■ Die Produkte von Frogblue basieren auf der Bluetooth-Technologie, was eine drahtlose Verbindung von Beleuchtung, Jalousien, Lüftern, Fenstern, Türen, Heizungen, Gegensprechanlagen und Standard-Lichtschaltern ermöglicht.

Bitte umblättern ►

■ Die Installation ist einfach und erfordert keine zentrale Steuerungseinheit oder Server. Die Module können hinter Standard-Lichtschaltern oder Steckdosen installiert werden und benötigen nur 230V.

Die Konfiguration erfolgt über eine App, die es ermöglicht, Schalterfunktionen, Wechselschaltungen und Zentralbefehle später anzupassen.

Kosteneffizienz:

■ Frogblue-Produkte sind sehr kosteneffektiv, da sie keine teuren Steuerungskabel oder zentrale Steuerungseinheiten benötigen.

■ Die innovative Heizungssteuerung spart Energiekosten, indem sie die richtige Temperatur in jedem Raum gewährleistet und tages- und zeitgesteuerte Programme zur Optimierung des Energieverbrauchs bietet.

Zuverlässigkeit und Sicherheit:

■ Frogblue-Systeme sind hoch zuverlässig und haben keinen zentralen Ausfallpunkt. Die parallele Übertragung über Bluetooth und WLAN-Mesh sorgt für eine stabile Verbindung.

■ Im Falle eines Stromausfalls stellt das System den Zustand vor dem Ausfall in weniger als einer Sekunde wieder her.

■ Alle Daten bleiben im Haus und die Funktionen können ohne Cloud-Abonnement oder IT-Infrastruktur genutzt werden.

Vielseitige

Steuerungsmöglichkeiten:

■ Die Steuerung aller Funktionen kann lokal über Bluetooth oder weltweit über

ein Smartphone mit aktiviertem Cloud-Service erfolgen.

■ Zeit- und wettergesteuerte Verschattung mit zentralen und Zonenfunktionen sowie die Steuerung aller Beleuchtungsquellen, einschließlich variabler Dimmkurven und DALI 2-Kompatibilität, sind möglich.

■ Das System umfasst auch eine Alarmanlage, die Benachrichtigungen über das Öffnen von Fenstern und Türen oder das Drücken von Lichtschaltern auf einem Smartphone sendet.

Innovative Funktionen:

■ Frogblue bietet eine Vielzahl innovativer Funktionen, wie z.B. die Warmfeet-Funktion, die mehr Komfort bietet und gleichzeitig Energie spart.

■ Die Produkte sind zukunftssicher und können an die Anforderungen der Benutzer auch Jahre später angepasst werden.

Benutzerfreundlichkeit:

■ Die Konfiguration und Bedienung der Frogblue-Produkte ist lizenzfrei und beinhaltet kostenlose Updates.

■ Jede technisch versierte Person kann die Schalterfunktionen, Wechselschaltungen und Zentralbefehle selbst über die App konfigurieren, ohne Kabel verlegen zu müssen.

Fazit der IPC 2025

Die Konferenz gab einen guten Einblick in die aktuellen und neuen Systeme sowie Funktionen der Frogblue-Systeme – und bot den Teilnehmerinnen und Teilnehmern zudem die Möglichkeit, an interaktiven

Workshops teilzunehmen oder sich in Feedback-Runden und Q&A-Sessions aktiv einzubringen. Zur Auswahl standen auch technische Trainings und die Besichtigung eines Musterhauses, um die praktischen Anwendungen der Frogblue-Technologien hautnah zu erleben.

Innovative Lösungen und eine echte Vision für die Zukunft der Gebäudeautomation: Auf der IPC konnte jede und jeder sein frogblaues Wunder erleben, was die Produkte dieser deutschen Unternehmer- und Erfinderfamilie Hinkel & Co. alles leisten, bewegen und in Häusern, Gewerbeimmobilien steuern können. **GIT**



Frogblue Technology GmbH
www.frogblue.com

© Frogblue Technology GmbH

Durch die Kippfalle bleibt die Leichtgängigkeit von Drücker sowie Zylinder auch bei mehreren Verriegelungspunkten erhalten und erfüllt damit durchgängig die Vorgaben für Panik- und Notausgangsschlüsse nach EN179/EN1125



Solution Locks: Neue Schlossgeneration von Assa Abloy

Assa Abloy hat das komplette Programm von Vollblattschlössern für Holz- und Stahlblechtüren überarbeitet. Die neue Schlosslinie „Solution Locks“ bietet ein umfangreiches Lösungsportfolio für den Einsatz in zahlreichen Türsystemen. Das Angebot reicht von Schlössern für Basisanforderungen mit verbesserten einbruchhemmenden Eigenschaften über Panikschlösser und -gegenkästen sowie selbstverriegelnde Sicherheitsschlösser mit Kippfallentechnologie bis hin zum mechatronischen Hochsicherheitsschloss.

Der Kippfallen-Mechanismus stellt sicher, dass sämtliche durch Vorlast an der Tür auftretenden Kräfte kompensiert werden – sei es aufgrund von Dichtungsdruck oder eines verzogenen Türblatts. Unabhängig von der Anzahl der Verriegelungspunkte sowie etwaigen thermisch bedingten Druckunterschieden bleibt dadurch die Leichtgängigkeit von Drücker sowie Zylinder erhalten. Die Vorgaben für Panik- und Notausgangsschlüsse nach EN179/EN1125 werden durchgängig erfüllt. www.assaabloy.com



Die neuen Sicherheitsschlösser mit Kippfallentechnologie können hohe Vorlast-Kräfte an der Tür kompensieren

© Assa Abloy Sicherheitstechnik GmbH

Sicher, smart, vernetzt: BKS elektrisiert die BAU 2025

Unter dem Motto „Systemlösungen aus einer Hand“ präsentierte die BKS GmbH auf der BAU 2025 ihre umfangreiche Produktpalette. Besonders großes Interesse weckten die neuesten elektronischen Zutrittskontrolllösungen des Traditionsunternehmens. Mit einem breiten Angebot an Innovationen in den Bereichen Bau- und Gebäudetechnik bot die Veranstaltung die ideale Bühne für die BKS GmbH, um ihre zukunftsweisenden Zutrittskontrolllösungen zu präsentieren. Davon gab es am zweistöckigen Messestand reichlich zu entdecken.

Ein Highlight war die Vorstellung des Ixalo Doppelknauflzylinders, der nach den neuesten Sicherheitsstandards entwickelt wurde. Dank modernster Verschlüsselungs- und Kommunikationstechnik bietet er höchste Cybersicherheit. Die Intelligenz des Systems, die bisher teilweise im Knäuf integriert war, wurde vollständig in den Zylinder verlagert. Dies sorgt für zusätzliche Sicherheit und Zuverlässigkeit.

www.bks.de

Datenträgerspürhunde unterstützen Ermittlungsarbeit

Schwarzwald Dogs bietet maßgeschneiderte Lösungen für Unternehmen, Regierungs- und Strafverfolgungsbehörden, private Ermittler und Sicherheitsdienste. Die ausgebildeten Datenträgerspürhunde sind ein unverzichtbares Hilfsmittel in der modernen Ermittlungsarbeit. Sie bieten eine einzigartige Fähigkeit, elektronische Beweismittel schnell und effizient aufzuspüren, und ergänzen menschliche und technische Suchmethoden optimal. Besonders in Zeiten zunehmender Digitalisierung leisten sie einen wesentlichen Beitrag zur Sicherheit und Strafverfolgung. Datenträgerspürhunde (auch „Cyberdogs“ genannt) sind speziell ausgebildete Hunde, die elektronische Datenträger wie USB-Sticks, Festplatten, SD-Karten, Mikro-Sim, Mikro-Kamera, Tonaufnahme-Geräte (z. B. in Form eines Stiftes, Autoschlüssels, Adapters usw.), GPS-Tracker, Burner Phones und Smartphones aufspüren können.

www.schwarzwald dogs.de

Security Center SaaS um Einbruchsmangement erweitert

Genetec erweitert Security Center SaaS um Einbruchsmangement. Die einheitliche physische Sicherheitslösung des Unternehmens, die in der Cloud oder als Hybridlösung eingesetzt werden kann, kombiniert Einbruchserkennung mit Videoüberwachung, Zutrittskontrolle, Identitäts- sowie Besuchermanagement. Damit bietet sie eine vollständig vereinheitlichte, offene, Cloud-verwaltete Plattform, die von der Genetec Cloudlink-Produktlinie unterstützt wird. Security Center SaaS ist mit einer Vielzahl von Einbruchmeldeanlagen verschiedener Hersteller kompatibel, angefangen mit Bosch Intrusion Panels. Das automatisierte Einbruchsmangement beseitigt die Abhängigkeit von manuellen Prozessen, reduziert Fehler und stellt sicher, dass Systeme bei Bedarf automatisch aktiviert werden.

www.genetec.de

Erfolgreicher Abschluss des Forschungsprojekts SPELL

Nach dreijähriger Projektdauer geht das Forschungsprojekt SPELL (Semantische Plattform zur intelligenten Entscheidungs- und Einsatzunterstützung in Leitstellen und Lagezentren) ab 2025 in die konkrete Anwendung. Die Advancis Software & Services GmbH spielte als einer der zentralen Projektpartner eine maßgebliche Rolle bei der Entwicklung und Umsetzung der Projektziele. Der Fokus von Advancis lag dabei auf der Integration, Harmonisierung und Nutzbarmachung von Sensordaten aus Sicherheits-, Gebäudemanagement- sowie Kommunikations- und Informationstechnik in nahezu Echtzeit. Das vom Bundesministerium für Wirtschaft und Klimaschutz geförderte Projekt zielte darauf ab, mithilfe von Künstlicher Intelligenz (KI) und modernen Datentechnologien die Reaktionsfähigkeit und Effizienz in Krisensituationen zu verbessern. Gerade bei Notfällen wie Naturkatastrophen oder Blackouts ermöglicht dies einen entscheidenden Informations- und Zeitgewinn bei der Lagebewältigung.



**David Teppe, Head of
Strategic Alliances
Advancis.**

<https://advancis.ne>

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

ZUTRITT

Gut aufbewahren!

Schutz wertvoller Dinge vor Diebstahl, Feuer und unbefugtem Zugriff

Gunnebo hat eine breite Palette von Produkten im Portfolio, die dazu dienen, wertvolle Gegenstände vor Feuer, Diebstahl und Beschädigung zu schützen. Sie werden kontinuierlich weiterentwickelt, um neuen Bedrohungen zu begegnen, und finden weltweit in verschiedenen Wirtschaftszweigen Anwendung. Emmanuel Harir-Forough, Product Line Manager bei Gunnebo Safe Storage, sprach darüber mit GIT SICHERHEIT.

■ GIT SICHERHEIT: Herr Harir-Forough, für alle, die Ihr Unternehmen noch nicht kennen, könnten Sie es bitte kurz vorstellen?

Emmanuel Harir-Forough: Gunnebo Safe Storage ist ein weltweit führendes Unternehmen für sichere Aufbewahrungslösungen und bietet hochwertige Tresore, Tresorräume und Sicherheitsschränke führender Marken an, die für den Schutz von Wertsachen, Bargeld und sensiblen Dokumenten konzipiert sind. Zu den Marken gehört u.a. Chubb Safes, ein Unternehmen das in diesem Jahr sein 190-jähriges Bestehen feiert. Gunnebo Safe Storage blickt auf eine lange Tradition im Bereich der Sicherheitsinnovation zurück und bietet maßgeschneiderte Lösungen, die den höchsten Industriestandards entsprechen. Unser Know-how hat sich weiterentwickelt und weltweit auf nachhaltige Geldautomatensafes, feuerfeste Schränke sowie Tresortüren und -räume ausgedehnt, die Technologie mit langlebiger Handwerkskunst kombinieren. Gunnebo Safe Storage setzt auf Zuverlässigkeit und kundenorientiertes Design und bietet durch geprüfte und zertifizierte Lösungen den Schutz von Vermögenswerten vor Diebstahl, Feuer und unbefugtem Zugriff.

Können Sie bitte etwas zu Ihrem beruflichen Hintergrund in der Branche und Ihrer derzeitigen Rolle sagen?

Emmanuel Harir-Forough: Ich verfüge über mehr als zwei Jahrzehnte Erfahrung in der globalen Geschäfts- und Produktentwicklung. Meine Aufgabe bei Gunnebo ist es, die Verantwortung für die technische Entwicklung und innovative Antworten auf

den Bedarf an Sicherheitslösungen zu übernehmen. Dies gilt strategisch für die Regionen EMEA, APAC und Nord- und Südamerika. Seit ich 2002 zu Gunnebo gekommen bin, habe ich eine entscheidende Rolle bei der Weiterentwicklung von sicheren Aufbewahrungslösungen gespielt. Als Produktlinienmanager für SafeStore Auto habe ich Innovationen bei automatischen, elektronischen und mechanischen Tresorraumsystemen vorangetrieben. Mein Fachwissen erstreckt sich auch auf Tresorraumlösungen und Strategien zur Geschäftsexpansion. Zuvor war ich als Vertriebsleiter für den Geschäftsbereich Banken tätig. In der Industrie war ich Präsident von Eurosafe und bin derzeit Präsident des französischen Herstellerverbands Syfraco.

Können Sie uns Ihre Produkt- und Lösungskategorien bei Gunnebo Safe Storage beschreiben: Ihre Hochsicherheitslösungen, Schlösser, Tresore und Schränke sowie Software?

Emmanuel Harir-Forough: Sicherheit ist keine pauschale Größe. Jedes Unternehmen hat seine eigenen Herausforderungen, ob es um den Schutz von Bargeld, Wertgegenständen, Vermögenswerten oder sensiblen Dokumenten geht. Deshalb arbeiten wir eng mit unseren Kunden zusammen, um Hochsicherheits-

Emmanuel Harir-Forough,
Product Line Manager bei
Gunnebo Safe Storage

lösungen zu entwickeln, die das richtige Gleichgewicht zwischen Schutz, Komfort, Compliance und Innovation bieten. Für Banken und Finanzinstitute geht es bei der Sicherheit darum, nahtlose, automatisierte Erfahrungen für Kunden zu schaffen und gleichzeitig sicherzustellen, dass Vermögenswerte geschützt bleiben. Unsere Tresore und Schließfächer sind so konzipiert, dass sie eine sichere und dennoch zugängliche Aufbewahrung ermöglichen und modernste Automatisierungs- und elektronische Schließsysteme enthalten. Einzelhändler und Unternehmen, die mit Bargeld umgehen, benötigen Lösungen, die nicht nur Wertsachen schützen, sondern auch die täglichen Abläufe optimieren. Unsere Einzahltresore und intelligenten Aufbewahrungssysteme tragen dazu bei, die zunehmende Gefahr von Diebstahl zu verhindern und gleichzeitig ein effizientes Cashflow-Management zu gewährleisten. Neben der physischen Sicherheit erkennen wir auch die wachsende Nachfrage nach digitaler Integration. Unsere Softwarelösungen ermöglichen es Unternehmen, den Zugang aus der Ferne zu überwachen und zu kontrollieren, so dass sie die Sicherheit immer im Blick haben.

In welchen Sektoren und Branchen sind Ihre wichtigsten Kunden zu finden?

Emmanuel Harir-Forouch: Gunnebo Safe Storage bedient ein breites Spektrum von Branchen, die jeweils unterschiedliche Sicherheits- und Betriebsanforderungen haben. Im Bankensektor beispielsweise helfen wir dabei, Bargeld, Wertgegenstände und sensible Dokumente zu schützen und gleichzeitig die Einhaltung strenger Vorschriften zu gewährleisten. Einzelhändler, von Luxusmarken bis hin zu Einzelhandelsketten, verlassen sich auf unser Fachwissen, um ihre Vermögenswerte zu schützen, insbesondere angesichts der zunehmenden Bedrohung durch Einbrüche. Die pharmazeutische Industrie verlangt eine sichere Lagerung von kontrollierten Substanzen, medizinischer Forschung und geistigem Eigentum und benötigt daher Lösungen, die strenge Sicherheits- und Compliance-Anforderungen erfüllen. Verteidigungsorganisationen vertrauen uns bei der Sicherung von Verschlusssachen, kritischen Infrastrukturen und hochriskanten Materialien. Darüber hinaus arbeiten wir mit Unternehmen jeder Größe zusammen, von agilen Start-ups bis hin zu großen Unternehmen mit mehreren Standorten, und entwickeln maßgeschneiderte Strategien, die sich an die sich verändernden Sicherheitsanforderungen anpassen. Anstatt vordefinierte Produkte aufzudrängen, hören wir zu, bewerten die Herausforderungen und

Gunnebo Safe Storage: sichere Aufbewahrungslösungen wie Tresore, Tresorräume und Sicherheitsschränke zum Schutz von Wertsachen, Bargeld und sensiblen Dokumenten



entwickeln zukunftsichere, nachhaltige Lösungen, die den Schutz, die Effizienz und die Einhaltung von Vorschriften verbessern. Der Schlüssel zu jeder Branche liegt in der partnerschaftlichen Zusammenarbeit vom ersten Entwurf an, so dass wir die Hauptanliegen der Kunden verstehen und ihnen zuhören können. So stellen wir sicher, dass wir die richtige Lösung entwickeln, die sowohl skalierbar als auch zukunftsicher ist, um den sich ändernden Anforderungen gerecht zu werden.

Was sind die wichtigsten Treiber von Innovation und Entwicklung bei Gunnebo Safe Storage?

Emmanuel Harir-Forouch: Die Kundenbedürfnisse sind die treibende Kraft hinter unserer Innovation. Da sich die Sicherheitsanforderungen weiterentwickeln, benötigen Unternehmen Lösungen, die einen hohen Schutz bieten und gleichzeitig Effizienz, Komfort und digitale Integration gewährleisten. Finanzinstitute suchen zunehmend nach automatisierten, selbstbedienten Tresoren, die den Kunden einen sicheren Zugang ohne Personaleinsatz ermöglichen. Einzelhändler benötigen intelligente Tresore, die nicht nur Bargeld und Vermögenswerte schützen, sondern auch den Bargeldfluss optimieren und die Handhabungsrisiken über interne und externe Bedrohungen hinaus reduzieren. Die Nachfrage nach vernetzter Sicherheit hat uns

auch dazu veranlasst, Softwarelösungen zu entwickeln, die Echtzeitüberwachung, Fernzugriffskontrolle und nahtlose Systemintegration ermöglichen. Durch die Nähe zu unseren Kunden und das Verständnis ihrer Herausforderungen schon bei der Spezifikation können wir maßgeschneiderte Sicherheitslösungen entwickeln, die sich mit den Anforderungen moderner Unternehmen weiterentwickeln. Die Module Guard Tresortüren und Tresorräume sind ein wichtiges Beispiel dafür, dass sie bei Bedarf noch mehr Sicherheit bieten, indem sie neben der BRE-Zertifizierung und der FRE-Einstufung auch ballistischen Widerstand gegen Angriffe bieten. Die Türen und Paneele sind nach der Norm EN 1522 klassifiziert und verfügen über eine FB2-Einstufung für ballistische Widerstandsfähigkeit - sie sind so konzipiert, dass sie dem Beschuss mit einer 9-mm-Pistole standhalten.

Wie arbeiten Sie bei der Entwicklung neuer Lösungen mit Kunden und Partnern zusammen?

Emmanuel Harir-Forouch: Die Zusammenarbeit mit Kunden und Partnern ist der Schlüssel zur Entwicklung von Lösungen, die den höchsten Anforderungen und gesetzlichen Vorschriften entsprechen. Bei der Sicherheit geht es nicht nur um den Schutz, sondern auch darum, dass Unternehmen die strengen Branchenrichtlinien

Bitte umblättern ►

einhalten und gleichzeitig die Effizienz und Benutzerfreundlichkeit aufrechterhalten. Wir arbeiten eng mit unseren Kundenpartnern zusammen, um sicherzustellen, dass unsere Produkte den globalen und regionalen Vorschriften entsprechen, von der EN 1143-1-Zertifizierung für Tresore und Tresorräume bis hin zu Datenschutzgesetzen für digitale Zugangslösungen. Regelmäßige Feedback-Sitzungen, Audits und Pilotprogramme ermöglichen es uns, unsere Lösungen an die sich entwickelnden gesetzlichen und betrieblichen Anforderungen anzupassen. Durch Partnerschaften mit Branchenverbänden und Technologieanbietern können wir die neuesten Sicherheitsentwicklungen integrieren und gleichzeitig die Einhaltung gesetzlicher Vorschriften gewährleisten. Dank dieses proaktiven Ansatzes können sich unsere Kunden darauf verlassen, dass ihre Sicherheitslösungen nicht nur innovativ und robust sind, sondern auch den für ihre Branche geltenden rechtlichen Rahmenbedingungen voll und ganz entsprechen.

Was wird aus Ihrer Sicht die Zukunft von Hochsicherheitslösungen wie Tresorräumen, Tresortüren und Schließfachsystemen bestimmen?

Emmanuel Harir-Forouch: Die Zukunft liegt in der intelligenten Sicherheitsintegration, bei der digitaler Zugang, biometrische Authentifizierung und Echtzeitüberwachung einen nahtlosen, hochsicheren Betrieb gewährleisten. Da Cyber- und physische Bedrohungen immer ausgefeilter werden, werden hybride Sicherheitslösungen – die physischen Schutz mit KI-gesteuerter Überwachung und cloudbasierter Zugangskontrolle kombinieren – die nächste Generation von Tresorräumen definieren. Sie können das ausgeklügeltste, internetfähige biometrische Scansystem der Welt haben, aber wenn der Kern schlecht konstruiert und von schlechter Qualität ist, wird die Sicherheit schnell durchbrochen. Die Branche wird weiterhin innovative Lösungen entwickeln, um allen Risiken voraus zu sein und gleichzeitig sicherzustellen, dass die Sicherheit benutzerfreundlich und effizient bleibt.

Könnten Sie ein paar wichtige aktuelle Projekte beschreiben?

Emmanuel Harir-Forouch: Viele der Projekte von Gunnebo Safe Storage werden aus Sicherheitsgründen vertraulich behandelt, aber zwei bemerkenswerte Kooperationen unterstreichen unsere Kompetenz im Be-

reich sicherer Aufbewahrungslösungen. Ein wichtiges Projekt ist die Zusammenarbeit mit Svensk Värdeförvaring, dem ersten bankenunabhängigen Anbieter von Schließfachdienstleistungen in den nordischen Ländern. Svensk Värdeförvaring hat die Infrastruktur der Banken übernommen und die Safe Control-Software von Gunnebo, elektronische 2000C-Schließfächer und Kartenlesegeräte in Stockholm und Göteborg implementiert, wobei eine Erweiterung in Malmö geplant ist. Dadurch wird ein nahtloser Übergang für die Kunden gewährleistet und gleichzeitig die Nachhaltigkeit gefördert. Ein weiteres Großprojekt sind private Tresorräume für Safes im City Walk von Dubai, wo Gunnebo Safe Storage in Zusammenarbeit mit Axon das SafeStore Auto und ein elektronisches Schließfachsystem installiert hat. Das System ist rund um die Uhr verfügbar und verbindet Sicherheit mit Komfort. Beide Projekte zeigen das Engagement von Gunnebo für Innovation, langfristige Partnerschaften und zukunftssichere Sicherheitslösungen, die auf die sich wandelnden Kundenbedürfnisse zugeschnitten sind. **GIT**



Gunnebo Safe Storage
www.gunneboselfstorage.com

© Bilder: Gunnebo

Smarte Sicherheitslösungen in Casinos

Der deutsche Videotechnikhersteller Dallmeier zeigte auf der WGPC 2025 (World Game Protection Conference) in Las Vegas als Exclusive Platinum Sponsor seine intelligenten Videolösungen für Casinos. Zu den Highlights gehörten die Kameraserie „Picoline“, die CAT Casino Automation Technologie sowie das Videomanagementsystem Hemisphere SeMSy. Die Picoline vereint hohe Bildqualität mit bis zu fünf MP Auflösung, einer Vielzahl von Cybersecurity-Vorkehrungen und KI-Analysefunktionen in einem kompakten Aufputzgehäuse. Der kleine Formfaktor ermöglicht die Montage auf engstem Raum an Decken oder Wänden. Die Stromversorgung wird über PoE realisiert.

www.dallmeier.com

Scout Pro Wärmebild-Monokular

Flir stellt mit dem Scout Pro ein Wärmebild-Monokular der nächsten Generation vor, das für die hohen Anforderungen von Strafverfolgungs- und Sicherheitsexperten entwickelt wurde. Das Scout Pro bietet mit seinem 32-Grad-Sichtfeld einen außergewöhnlich guten Überblick über die Situation. Der Benutzer kann Menschen in bis zu 500 Metern Entfernung erkennen und gleichzeitig ein sehr breites Umfeld überwachen. Diese Ausgewogenheit von breiter Abdeckung und praxisgerechtem Erfassungsbereich liefert die entscheidenden Informationen und Erkenntnisse, die sowohl für sicheres Patrouillieren als auch für das schnelle Auffinden vermisster oder verletzter Personen erforderlich sind. Das in Zusammenarbeit mit Strafverfolgungsbehörden und Sicherheitsexperten entwickelte Scout Pro kombiniert das weite Sichtfeld mit einer 640 x 480 Wärmebildauflösung und liefert klare, hochwertige Bilder. Das Handheld-Infrarotmonokular ermöglicht einen zwei-, vier-, sechs- und achtfachen Zoom zur Vergrößerung.



www.flir.co.uk

GIT SICHERHEIT

Die GIT SICHERHEIT ist für mich wichtig, weil sie sich meinem Eindruck nach durch eine große Nähe zu den verschiedenen Akteuren der Sicherheitsbranche auszeichnet. Es ist wahrscheinlich diesem Vertrauen zu verdanken, dass man immer wieder Informationen aus erster Hand und für die Branche selten offene Einblicke erhält.



Dr. Alexandra Forster,
Leiterin Konzernsicherheit
bei der Bayer AG



Mobilfunk Notruftaster – schnelle und flexible Sicherheit

Der Mobilfunk Notruftaster von Lupus-Electronics sorgt auf Knopfdruck für schnelle Hilfe und bietet dank IoT-Technologie und Cloud-Anbindung permanente Sicherheit und Flexibilität. Das handliche Gerät ist bereits für die Stadtritter Notrufleitstelle vorkonfiguriert und sendet bei Aktivierung einen stillen Alarm. Durch die einfache Plug-and-Play-Funktionalität ist keine Installationshilfe notwendig, und die Mobilfunk-basierte Übertragung gewährleistet stabile Verbindungen, selbst in abgelegenen Räumen.

Das Produkt ist geeignet für den Einzelhandel, Büro- und Praxisbetriebe, Behörden, Alleinarbeitende, Senioren und Menschen mit erhöhtem Sicherheitsbedürfnis. Ein stiller Alarm wird über Mobilfunk direkt an die Leitstelle übertragen, die sofort geeignete Maßnahmen ergreift. Das System ist unbegrenzt skalierbar und wird im Preismodell Hardware plus monatliches Stadtritter Abo angeboten, sodass Kunden flexibel bleiben.

Dank der drahtlosen Funktionalität ist der Notruftaster besonders leicht bedienbar. Die Lupus App bietet den Nutzern volle Einsicht in das Alarmsystem. Push-Benachrichtigungen und Meldungen über die Cloud informieren in Echtzeit über potenzielle Gefahren. Zusätzlich können weitere Sicherheitsfunktionen wie Videoüberwachung, Bewegungs- und Rauchmelder in das Cloud-System integriert werden. So wird der Notruftaster Teil eines umfassenden Smarthome-Sicherheitskonzepts, das sich problemlos und individuell erweitern lässt.

Man stelle sich folgendes Szenario in einem Einzelhandelsgeschäft vor: Eine Angestellte arbeitet allein in den Abendstunden, als sie plötzlich einen verdächtigen Kunden bemerkt, der sich ungewöhnlich lange im hinteren Bereich des Ladens aufhält und sich auf Ansprache aggressiv zeigt. Um keine unnötige Aufmerksamkeit zu erregen, drückt sie unauffällig auf den Lupus Mobilfunk Notruftaster, den sie diskret unter der Theke platziert hat.

Durch die Aktivierung des Tasters wird ein stiller Alarm über die integrierte IoT-Verbindung an die Stadtritter Notrufleitstelle gesendet. Die Leitstelle erhält die Benachrichtigung sofort über die Lupus Cloud und informiert umgehend den Wachschutz sowie die Polizei, ohne dass die Angestellte ihr Handy oder das Geschäftstelefon nutzen muss.

Zusätzlich hat die Filialleitung über die Lupus App jederzeit Einsicht in die Alarmmeldungen und kann sicherstellen, dass der Vorfall dokumentiert wird. Dieser Einsatz des Notruftasters stellt sicher, dass die Angestellten jederzeit geschützt sind, ohne selbst auf ein Telefon angewiesen zu sein, und dass die Sicherheit im Laden auch bei unvorhergesehenen Ereignissen gewährleistet ist.

www.lupus-electronics.de



Das handliche Gerät ist bereits für die Stadtritter Notrufleitstelle vorkonfiguriert und sendet bei Aktivierung einen stillen Alarm

Schutzengel als Button: Der Lupus Mobilfunk Notruftaster ermöglicht eine sofortige Benachrichtigung im Notfall

9. Generation des Arptec System-on-Chip

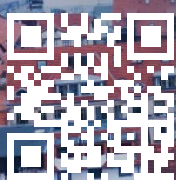
Axis Communications bringt die 9. Generation seines System-on-Chip (SoC) für Netzwerk-Video heraus. Der Arptec-9 bietet eine hochwertige Bildverarbeitung, erhöhte Cybersicherheit, verbesserte Funktionen für die KI-basierte Videoanalyse und eine niedrige Bitrate. Er unterstützt den AV1-Video codec der Alliance for Open Media (AOM), einen quelloffenen Standard für die Codierung digitaler Videos. Der Arptec System-on-Chip bildet die Basis für grundlegende Funktionen wie Bildqualität, Codierleistung oder leistungsfähige Analyseanwendungen auf der Grundlage von Deep Learning „on the edge“. Der Arptec-9 baut auf den Funktionen seines Vorgängers, Arptec-8, auf und wurde eigens von Axis für die Anforderungen der Sicherheitsbranche weiterentwickelt. www.axis.com

OPEN

20
05
25

LOKHALLE GÖTTINGEN

OPPORTUNITY.
CONNECTION.
DISCOVERY.



Jetzt QR-Code
scannen &
registrieren!

AXIS
COMMUNICATIONS



DISTRIBUTION

Durchstarten im Zentrum Europas

Globaler Distributor kommt nach Deutschland

ADI Global Distribution gehört weltweit zu den größten Distributoren für Sicherheitstechnik. Seit letztem Jahr ist das Unternehmen auch in Deutschland präsent. GIT SICHERHEIT sprach mit Daniel Grossbach, Key Account Manager bei ADI Global Distribution.

■ GIT SICHERHEIT: Herr Grossbach, seit letztem Jahr ist ADI Global Distribution auch in Deutschland präsent. Viele unserer Leser werden Sie auf der letzten Security in Essen kennengelernt haben. Wie vielversprechend ist für Sie der deutsche Markt?

Daniel Grossbach: Unser Einstieg in Deutschland ist ein strategischer Schritt, den wir mit viel Vorfreude und Engagement angegangen sind. Deutschland ist ein Schlüsselmarkt in Europa, mit einer starken Nachfrage nach modernen Sicherheitslösungen. Der Technologie- und Innovationsgrad hier ist hoch, und wir sehen ein großes Potenzial, mit unseren maßgeschneiderten Lösungen und unserem breiten Produktportfolio einen echten Mehrwert zu bieten. Die Security in Essen hat uns eine großartige Gelegenheit gegeben, direkt mit potenziellen Kunden und Part-

nern in Kontakt zu treten. Wir haben dort die enorme Resonanz und das Interesse an unseren Produkten und Dienstleistungen gespürt. Das bestätigt uns in der Überzeugung, dass unser Angebot hier sehr gut ankommt. Wir sind überzeugt, dass wir durch unsere breite Produktpalette, unsere starke Partnerschaft mit führenden Herstellern und unseren umfassenden Support eine wertvolle Ergänzung für den deutschen Markt darstellen. Es wird spannend, aber wir sind mehr als zuversichtlich, dass wir hier weiterhin stark wachsen können.

Wie setzt sich Ihr Team in Düsseldorf zusammen?

Daniel Grossbach: Unser Team steht – und wir sind bereit! Wir haben alle wichtigen Funktionen besetzt, um erfolgreich durchzustarten. Unser Innendienst ist

immer ansprechbar und unterstützt unsere Kunden mit kompetenten Lösungen. Unser technischer Support steht bereit, um auch bei komplexen Fragen weiterzuhelfen. Damit der Webshop reibungslos läuft, kümmert sich ein Kollege um alles rund um das Online-Bestellwesen. Unser Marketing Manager setzt kreative Konzepte um – darunter auch die „Win a Van“-Kampagne. Zudem sorgt unsere Business Analystin für wertvolle Einblicke und strategische Weitsicht. Auch wenn nicht alle Teammitglieder in Düsseldorf sitzen, sind unsere Außendienstkollegen fester Bestandteil unseres Erfolgs. Sie stehen im direkten Austausch mit unseren Kunden und zeigen, was ADI besonders macht.

Ihr Portfolio ist ausgesprochen umfassend – damit grenzen Sie sich teils auch von Wettbewerbern ab. Welche Gewerke decken Sie ab?

Düsseldorfer Office-Gebäude von Frank Ghery – hier hat auch ADI Global Distribution ihren Sitz



Daniel Grossbach: Wir decken eine Vielzahl von Gewerken ab und verstehen uns als verlässlicher Partner für Sicherheits- und Gebäudetechnik. Unser Sortiment umfasst unter anderem die Videoüberwachung – von Kameras über Rekorder bis hin zu intelligenten Analyselösungen –, den Bereich Einbruch- und Brandmeldetechnik für umfassenden Schutz in privaten, gewerblichen und industriellen Bereichen. Und in der Zutrittskontrolle decken wir alles von klassischen Schließsystemen bis hin zu modernen biometrischen Lösungen ab. Durch diese breite Abdeckung ermöglichen wir unseren Kunden, verschiedene Systeme nahtlos miteinander zu verbinden – alles aus einer Hand, mit kompetenter Beratung und zuverlässigem Service.

Mit welchen Herstellern arbeiten Sie hauptsächlich zusammen?

Daniel Grossbach: Unser breites Sortiment basiert auf einer engen Zusammenarbeit mit renommierten und führenden Herstellern aus verschiedenen Gewerken der Sicherheits- und Gebäudetechnik. Dabei legen wir besonderen Wert auf Qualität, Innovation und langfristige Verfügbarkeit. Im Bereich Videoüberwachung arbeiten wir unter anderem mit Bosch, Pelco, Axis und Hanwha zusammen. Diese Hersteller bieten ein breites Spektrum an Lösungen. Für Einbruchmeldetechnik setzen wir auf bewährte Systeme von beispielsweise Honeywell, und in der Zutrittskontrolle kooperieren wir mit Anbietern wie Paxton, HID und CDVI, die Lösungen für unterschiedliche Anforderungen bieten – von kleinen Unternehmen bis hin zu großen Industrieanlagen. Durch diese Vielfalt ermöglichen wir unseren Kunden, aus einer großen Auswahl an Technologien genau die passenden Produkte für ihre individuellen Anforderungen zu finden. Gleichzeitig garantieren wir durch unsere enge Zusammenarbeit mit den Herstellern eine kompetente Beratung sowie eine zuverlässige und nachhaltige Lieferkette.

Sie haben aber auch Eigenmarken?

Daniel Grossbach: Ja, neben unserem umfangreichen Markenportfolio bieten wir auch Eigenmarken an, die speziell auf die Anforderungen unserer Kunden zugeschnitten sind. Unsere Eigenmarken zeichnen sich durch ein attraktives Preis-Leistungs-Verhältnis aus, ohne Kompromisse bei Qualität und Zuverlässigkeit einzugehen. Sie wurden entwickelt, um eine optimale Ergänzung zu den etablierten Herstellermarken zu bieten und gleichzeitig den wachsenden Anforderungen des Marktes gerecht zu werden. Durch diese Kom-

bination aus führenden Herstellermarken und Eigenmarken können wir flexibel auf die Bedürfnisse unserer Kunden eingehen und maßgeschneiderte Lösungen für unterschiedlichste Anwendungen bieten.

Geliefert wird von Ihrem Lager in den Niederlanden aus. Sie haben aber auch weitere Lager in Europa. Profitieren auch Ihre deutschen Kunden von Ihrer internationalen Präsenz?

Daniel Grossbach: Ja, absolut. Unsere internationale Präsenz bringt auch für unsere deutschen Kunden spürbare Vorteile. Auch wenn unser Hauptlager für Deutschland in den Niederlanden liegt, greifen wir auf ein leistungsfähiges europäisches Logistiknetzwerk mit mehreren Standorten zurück. Das bedeutet für unsere Kunden vor allem eins: höhere Verfügbarkeit und schnellere Lieferzeiten. Wenn ein Produkt an einem Standort knapp wird, können wir flexibel auf andere Lager zugreifen, um Engpässe zu vermeiden. Gleichzeitig eröffnet unser internationales Netzwerk Zugang zu einer noch breiteren Produktpalette – oft mit kürzeren Wartezeiten als bei rein national agierenden Anbietern. Kurz gesagt: Unsere deutsche Kundschaft profitiert nicht nur von unserer lokalen Präsenz, sondern auch von der Stärke eines globalen Distributors. Wir verbinden die Verlässlichkeit eines bewährten Logistiksystems mit der Flexibilität, die der Markt heute erfordert.

Sie erwähnten schon Ihre technischen Support-Mitarbeiter. Welchen Service bieten Sie Ihren Kunden, also Integratoren von Sicherheitstechnik, im Einzelnen an?

Daniel Grossbach: Unser technischer Support ist für uns mehr als nur eine Serviceleistung – wir sind ein echter Partner für unsere Kunden. Für Integratoren bieten wir umfassende Unterstützung, die weit über den klassischen Support hinausgeht. Schon bei der Produktberatung und Planung stehen wir beratend zur Seite, helfen dabei, die richtigen Systeme und Komponenten auszuwählen und maßgeschneiderte Lösungen zu entwickeln. Bei der Inbetriebnahme und Konfiguration sind unsere Experten immer ansprechbar, um bei technischen Fragen oder Problemen schnell zu helfen. Zudem bieten wir regelmäßig Schulungen und Webinare, um sicherzustellen, dass unsere Partner immer auf dem neuesten Stand sind und Best Practices in der Sicherheitsbranche kennen. Und wenn es einmal besonders komplex wird, bieten wir in vielen Fällen auch Vor-Ort-Unterstützung an, um sicherzustellen, dass alles reibungslos läuft. Unser Ziel ist klar: Wir möchten nicht nur Produkte liefern, sondern Integratoren in jeder Phase ihrer Projekte unterstützen – so können sie ihre Arbeit effizient und erfolgreich umsetzen. **GIT**

Hier gelangen Sie zum Gewinnspiel von ADI Global Distribution:



ADI Global Distribution
www.adiglobal.com

Newsletter
abonnieren



Ihre Nummer 1
seit mehr als 30 Jahren

Jetzt

inklusive e-Ausgabe!



Nachrichten für Entscheider und Führungskräfte in Sachen Sicherheit

WILEY

Mit der Installation von nur 25 Kameras von i-Pro konnte ein britisches Krankenhaus insgesamt 100 Kameras mit KI-Funktionen aufrüsten

VIDEO

Therapie per KI

Britisches Krankenhaus erweitert Kameras durch KI-Funktionen

Mit Kameras der X-Serie von i-Pro hat ein Lehrkrankenhaus im Nordosten Englands seine Sicherheitsinfrastruktur aufgerüstet. Sie wurden dabei in die Videomanagement-Software XProtect von Milestone integriert.

Das Krankenhaus ist Teil des National Health Service (NHS) Trust im Nordosten Großbritanniens. Während der letzten zehn Jahre hat das Krankenhaus seine Sicherheitsinfrastruktur grundlegend modernisiert und ist von analogen Videosystemen auf ein vollständig IP-basiertes System umgestiegen. Im Zuge dieser Umstellung installierte das Krankenhaus kürzlich 25 Edge-Processing-Kameras der X-Serie von i-Pro. Ziel dieser Maßnahmen ist es, die Sicherheit des weitläufigen Krankenhauses durch den Einsatz neuester KI-gestützter Kameratechnologie zu erhöhen und gleichzeitig die Betriebsabläufe zu optimieren. Durch den Einsatz der neuen Kameras sollten also keine Patienten therapiert werden, wohl aber das Sicherheitssystem.

Im laufenden Betrieb

Die größte Herausforderung für das Krankenhaus war, Teile des vorhandenen Sicherheitssystems mit hochmodernen, KI-gestützten Kameras aufzurüsten, ohne dabei die strengen Budgetvorgaben für den öffentlichen Sektor zu überschreiten oder den täglichen Betrieb des stark ausgelasteten Krankenhauses zu stören. Aufgrund des weitläufigen Geländes und der zahlreichen Gefahrenquellen benötigte das Krankenhaus außerdem eine Lösung, die die Funktionalität der vorhandenen, nicht-KI-gestützten Kameras erweitert und gleichzeitig die Überwachungsfunktionen verbessert.

„Die größte Herausforderung bestand darin, das System innerhalb des begrenz-

ten Budgets aufzurüsten und gleichzeitig ein hohes Maß an Sicherheit und betrieblicher Effizienz aufrecht zu erhalten“, so Chris Lakin, Direktor von Oracle Vision, dem leitenden Systemintegrator in diesem Projekt. „Der Kunde wollte eine Lösung, die sich in seine aktuelle Infrastruktur integrieren lässt, fortschrittliche KI-Funktionen für einen besseren Schutz von Patienten, Personal und Vermögenswerten des Krankenhauses bietet und gleichzeitig an zukünftige Anforderungen anpassbar ist.“

KI für Kameras ohne KI

Nach eingehender Prüfung entschied sich das Krankenhaus für die Installation von Edge-Processing-Kameras der i-Pro X-Serie, die sich nahtlos in die VMS-Plattform XPro-

tect von Milestone einfügt. Das Wichtigste: Diese Kameras ermöglichen es dem Krankenhaus, seine bestehenden, nicht KI-gestützten Kameras um KI-Funktionalität zu erweitern. Dank dieser Innovation konnte das Potenzial der vorhandenen Kameras maximiert werden, ohne sie komplett zu ersetzen.

Die KI-Kameras der X-Serie nutzen dazu die AI Processing Relay App, durch die nicht KI-fähige Kameras – auch die anderer Hersteller – um KI-Funktionen ergänzt werden. Dieser Ansatz maximiert nicht nur die Lebensdauer der bestehenden Überwachungssysteme, sondern reduziert auch die Zahl der Fehlalarme erheblich. Durch die Installation von 25 KI-Kameras der i-Pro X-Serie und deren Verknüpfung mit den vorhandenen Modellen ohne KI konnte das Krankenhaus 100 Kameras mit neuen KI-Funktionen ausstatten und so seine videogestützten Sicherheitsfunktionen verbessern.

„Für das Krankenhaus lag die Entscheidung quasi auf der Hand. Mit i-Pro mussten sie nicht ihren gesamten Kamerabestand ersetzen, um wichtige neue Funktionen zu erhalten. Stattdessen rüsteten wir das bestehende System auf, indem wir 75 vorhandene Kameras um KI-Funktionen erweiterten. So maximierten wir deren Wert, ohne das Budget zu sprengen“, sagt Lakin. „Die Flexibilität der AI Processing Relay App von i-Pro ist beeindruckend. Sie verwandelt jede verbundene Kamera in eine KI-gestützte Lösung. Mit diesem System erreicht das Krankenhaus jetzt ein Maß an Sicherheit und operativer Transparenz, das mit den älteren Systemen bislang unmöglich war.“

Fortschrittliche KI-Funktionen

Die KI-Kameras der i-Pro X-Serie verfügen über Lernfunktionen, mit denen das Sicherheitsteam des Krankenhauses vor Ort festlegen kann, was die Kameras erkennen und überwachen sollen. So können die Bediener den Kameras beispielsweise beibringen, bestimmte Objekte wie Fahrzeuge oder Personen zu erkennen und Warnmeldungen auszugeben, wenn bestimmte Verhaltensweisen oder Aktivitäten in sensiblen Bereichen wie der Zufahrt zur Notaufnahme auftreten.

Darüber hinaus erhält das Krankenhaus KI-gestützte Analysen. Diese helfen dem Sicherheitspersonal nicht nur bei der Organisation der Besucherströme und der Erkennung verdächtigen Verhaltens, die Daten lassen sich auch problemlos in das Zutrittskontrollsystem von Paxton integrieren.

Alle Kameras sind mit der XProtect Smart Wall des Krankenhauses verbunden, wo durch KI-Analysen oder Zutrittskontrollen ausgelöste Ereignisse, wie z. B. Sicherheitsverletzungen oder abnormales Verhalten, automatisch auf dem Bildschirm angezeigt werden, sodass das Personal in Echtzeit auf diese reagieren kann.

Leistungsstarkes Edge-Computing

Die Kameras der i-Pro X-Serie nutzen den Chip AI SoC (CV52) von Ambarella für ein leistungsstarkes Edge Computing, welches das Krankenhaus in die Lage versetzt, komplexe Analysen lokal auszuführen, ohne das Netzwerk zu belasten. Es besteht die Möglichkeit, neun verschiedene KI-Anwendungen auszuführen, wie z. B. Privacy Guard von i-Pro, das die Gesichter oder den gesamten Körper von Patienten unkenntlich macht, um deren Privatsphäre zu schützen. Das Krankenhaus kann mit den neuen Kameras also sowohl seine Sicherheit verbessern als auch operative Daten erfassen, zum Beispiel indem es die Bewegung von bestimmten Geräten oder Mitarbeitenden auf dem Gelände verfolgt.

Dank ihres großen Dynamikbereichs (Wide Dynamic Range, WDR) von bis zu 144 dB liefern die Kameras zudem eine sehr gute Bildqualität selbst bei schwierigen Lichtverhältnissen wie z.B. bei Gegenlicht. Mit einer Auflösung von bis zu 6 MP und einer IR-Beleuchtung von bis zu 70 Metern sind hochauflösende Videos in jeder Umgebung möglich.

Ergebnisse

Durch die Implementierung von KI-Kameras der i-Pro X-Serie konnte das Krankenhaus seine Sicherheitsinfrastruktur verbessern und gleichzeitig die engen Budgetvorgaben einhalten. Dank der fortschrittlichen KI-Funktionen profitiert das Krankenhaus von Echtzeitwarnungen und Automatisierungen, die seine Sicherheitsabläufe verbessern. Besonders bemerkenswert ist, dass das Krankenhaus dank der Flexibilität der Kameras mit der Installation von nur 25 i-Pro Kameras insgesamt 100 Kameras mit KI-Funktionen aufrüsten konnte – ein enormer Vorteil und zugleich eine zukunftsichere Investition. 



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



Mehr zu den Vorteilen und zum Funktionsumfang unserer Systemplattformen.



i-Pro
www.i-pro-com
www.milestonesys.com

RICHTLINIEN

Auf gemeinsamen Nenner gebracht

**Brandschutz und Digitalisierung im Gebäude:
VdS-Merkblatt 6024 wird zur VdS-Richtlinie**



Digitale Haustafeln und Infoscreens in sensiblen Gebäudebereichen wie Fluchtwegen erfordern einen vorbeugenden, geräteintegrierten Brandschutz

Im Zuge der Digitalisierung werden auch in sensiblen Gebäudebereichen, die gleichzeitig auch oft als Fluchtweg dienen, immer mehr elektrische Verbraucher aufgestellt. Digitale Kommunikations- und Informationssysteme in Form großer Displays, die Flug- oder Bahnverbindungen anzeigen, sind nur ein Beispiel dafür. Als Hindernis erwies sich dabei in der Vergangenheit, dass zum Einbringen von elektrischen Geräten in sensiblen Gebäudebereichen kaum klare Handlungsanweisungen, Richtlinien oder Verordnungen vorlagen. Im Ergebnis führte dies zu einer aufwendigen und zudem uneinheitlichen Prüf- und Genehmigungspraxis von Baubehörden und Entscheidern.

Das VdS Merkblatt 6024, das seit 2022 durch eine unabhängige Arbeitsgemeinschaft (ARGE) unter der Schirmherrschaft der VdS Schadenverhütung erstellt wurde, hat erstmals standardisierte Voraussetzungen definiert. Vertreter von Seiten der Versicherungen, Baubehörden, Planer, Prüfstel-

len, Hersteller und Anwender haben ihre jeweilige Expertise eingebracht und neben den Anforderungen an elektrische Geräte auch eine praxistaugliche, unabhängige Prüfbarkeit der Wirksamkeit und Zuverlässigkeit definiert. Dadurch ist es gelungen, zum einen vermehrt Aufmerksamkeit auf dieses wichtige Thema zu lenken und zum anderen Akzeptanz für vereinheitlichte Standards im Markt zu finden.

Viel Akzeptanz in kurzer Zeit

Seit der Veröffentlichung am 1. September 2023 hat sich das VdS-Merkblatt als wichtiger Wegweiser in Planungs- und Prüfprozessen erwiesen. Auch ist es den Marktteilnehmern mit gemeinsamen Anstrengungen gelungen, kontinuierlich die Bekanntheit des Merkblatts zu steigern und gleichzeitig Hersteller zu ermutigen, ihre Produkte konform zu den Vorgaben anzubieten – eine zentrale Voraussetzung, um Projekte auf Basis der formulierten Stan-

Wie lässt sich die Nutzung von Digital-Signage-Systemen, Automaten, Ticketdruckern und anderen elektrischen Geräten in sensiblen Gebäudebereichen mit den hohen Anforderungen des Brandschutzes in Einklang bringen? Zu mehr Orientierung und bundesweiten Standards trägt seit über einem Jahr das VdS Merkblatt 6024 „Brandschutz elektrischer Geräte in sensiblen Bereichen“ bei. Aufgrund der positiven Resonanz aus der Praxis folgt nun der nächste Schritt: Aus dem Merkblatt wird voraussichtlich noch im ersten Quartal 2025 eine VdS Richtlinie mit nochmals verbindlicherem Charakter abgeleitet – als einheitlicher Maßstab für zukünftige Projekte. Ein Beitrag von Heike Siefkes, VdS Schadenverhütung in Köln.

dards planen und realisieren zu können. Bereits jetzt verfügbare Datenbanken mit VdS 6024-konformen Produkten sowie erste Ausschreibungen für größere Projekte etwa von Flughafenbetreibern, die auf Basis des Merkblatts erfolgt sind, spiegeln diese erfreuliche Entwicklung wider.

Gleichzeitig ist festzustellen, dass ein Merkblatt nur der erste Schritt auf dem Weg zu einer Standardisierung sein kann. So können beispielsweise Ausschreiber und Behörden nur bedingt auf ein Merkblatt referenzieren. Daher ist es der folgerichtige nächste Schritt, auf Basis der Praxiserprobungen eine verbindlichere VdS-Richtlinie zu erarbeiten. Vielfältige Erfahrungswerte aus dem ersten Jahr sind in den aktualisierten und überarbeiteten Richtlinien-Entwurf eingeflossen, der sich in Kürze in der öffentlichen Konsultation befindet. Somit können wir zuversichtlich sein, dass die VdS-Richtlinie 6024 bis zum Ende des ersten Quartals 2025 veröffentlicht werden kann.

Mehr Klarheit zu normativen Anforderungen

Dies kann nach der Erwartung aller Beteiligten dazu dienen, die Anforderungen an den Brandschutz elektrischer Geräte in sensiblen Gebäudebereichen weiter zu vereinheitlichen, für Genehmigungsbehörden, Ausschreiber und Anwender eine Vergleichbarkeit zu ermöglichen und insgesamt zu mehr Transparenz im Markt beizutragen. Gleichzeitig dürfte die Richtlinie nochmals mehr Verbindlichkeit schaffen und aktuell teilweise festzustellenden Missverständnissen entgegenwirken.

So ist aktuell eine gewisse Begriffsverwirrung zu beobachten, wenn es etwa um die Angabe der Brandschutzklassifizierung von Produkten geht. Viele Marktteilnehmer haben dabei zuvorderst die Nationale Klassifizierung DIN 4102-1 im Blick, mit nicht-brennbaren Baustoffen Klassen A1 und A2 sowie Baustoffen der Klassen B1, B2 und B3. Tatsächlich bezieht sich aber die VdS 6024 seit der Erstveröffentlichung auf die europäische Klassifizierung nach DIN EN 13501-1. Diese EU-Norm kennt die Brandverhaltensklasse A bis F. Auch hier gibt es also die Klasse A – nur meint dies etwas anderes als die „A1“ der DIN 4102-1. Anders ausgedrückt: Wenn Hersteller angeben, dass ihr Produkt nach B1 klassifiziert wird, ist zu hinterfragen, ob wirklich die DIN oder die europäische Norm gemeint ist. Darüber hinaus umfasst die VdS 6024 zwei Brandszenarien: „Brand von außen“ sowie „Brand von innen“. Häufig wurde bislang nur das Brandszenario von außen betrachtet, die VdS 6024 stellt somit eine ganzheitliche Weiterentwicklung dar.

Unabhängige Produktprüfung und Zertifizierung

Im Interesse aller Marktbeteiligten ist es ohne Zweifel, dass nicht mit Angaben geworben wird, die unter Umständen gar

nicht erfüllt werden. Deshalb sollte allen Beteiligten klar sein, dass die VdS-Richtlinie 6024 die europäische Norm fordert. Auch bei Formulierungen wie „angelehnt an Brandschutzklasse A“ ist ein gewisses Maß an Skepsis geboten – bedeutet dies, dass tatsächlich eine externe Zertifizierung erfolgt ist? Die Richtlinie wird dieses Thema lösen, indem eindeutig verlangt wird, dass eine Zertifizierung durch eine unabhängige Stelle erfolgt sein muss. Dieser wichtige Schritt wird nochmals mehr Planungssicherheit für alle Beteiligten und mehr Standardisierung schaffen.

Brandgefahren von außen oder von innen

Zugleich bleibt es eine zentrale Aufgabe, nach Veröffentlichung der VdS-Richtlinie den Kenntnisstand bei Behörden, Feuerwehren, Ausschreibern und Anwendern kontinuierlich weiter zu steigern und für die Anforderungen zu sensibilisieren. Dies gilt unter anderem für eine detaillierte Risikobetrachtung, speziell die Unterscheidung der Brandgefahren von außen sowie von innen. Bei der Risikoabwehr von Brandgefahren von außen steht die Wahl geeigneter Materialien mit Eigenschaften wie nicht brennbar, schwer entflammbar oder eine geringe Rauchentwicklung im Vordergrund. Diese Eigenschaften sind von den Herstellern entsprechend der europäischen Norm mit unabhängigen Versuchen und Zertifizierungen nachzuweisen.

Elektrizität und Defekte an elektronischen Bauteilen stellen hingegen ein Brandrisiko von innen dar, indem sie durch Fehlfunktionen einen Brand verursachen können. Sollte es aufgrund von technischen Defekten zu einem Brand innerhalb eines Gerätes kommen, ist ohne zusätzliche Maßnahmen mit einer starken Rauchentwicklung und einem erheblichen Brandverlauf zu rechnen, was die Nutzbarkeit der betrof-

fenen Flucht- und Rettungswege wesentlich beeinträchtigen kann. Auch dieses Risiko ist von Seiten der Hersteller zu prüfen und entsprechend zu behandeln.

Vorteile eines geräteintegrierten Brandschutzes

Vielfach werden zu diesem Zweck heute bereits Lösungen des geräteintegrierten Brandschutzes genutzt. Ein Brand oder eine Überhitzung kann durch diese automatischen Mini-Feuerlöscher direkt im elektrischen Gerät detektiert und gemeldet werden. Gleichzeitig wird der Brand schon in seiner frühzeitigen Entstehungsphase gelöscht, die Stromzufuhr unterbrochen und so eine Wiederentzündung verhindert. Somit wird eine Brandausbreitung unterbunden und – das Wichtigste – es bestehen keine Gefahren mehr für die Menschen, die sich in diesem sensiblen Gebäudebereich aufhalten.

Fazit

Die kommende VdS-Richtlinie 6024 stellt einen maßgeblichen weiteren Schritt dar, um die fortschreitende Digitalisierung im Gebäude und Anforderungen des Brandschutzes auf einen gemeinsamen Nenner zu bringen. Anforderungen an Produkteigenschaften, deren Überprüfung und Zertifizierung schaffen Klarheit für alle Beteiligten. Nun kommt es darauf an, die Bekanntheit der neuen Richtlinie kontinuierlich zu steigern sowie Hersteller, Inverkehrbringer, Planer und nicht zuletzt die Genehmigungsbehörden bei allen damit verbundenen Fragen zu unterstützen. **GIT**



VdS Schadenverhütung GmbH
www.vds.de



Mehr Infos

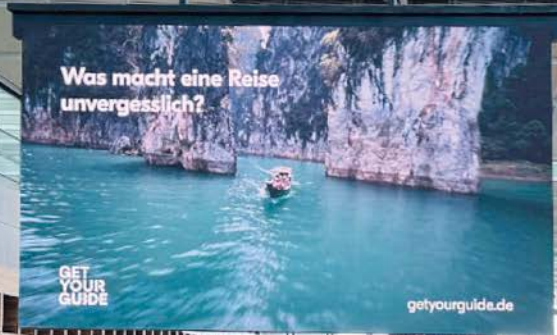
80 JAHRE GLORIA GMBH
Ihr Experte für vorbeugenden Brandschutz

GLORIA®

80 JAHRE GLORIA®



Die E-Bulb von Job schützt 576 LED-Cabinets der vier LED-Wände im Marktplatz im Sicherheitsbereich des Flughafens Berlin Brandenburg



GERÄTEINTEGRIERTER BRANDSCHUTZ

Auf dem Schirm

Geräteintegrierter Brandschutz am Flughafen Berlin Brandenburg

Der Flughafen Berlin Brandenburg (BER) ist mit seinen rund 23,1 Millionen Fluggästen (2023) und 176.649 Flugbewegungen (2023) der drittgrößte Flughafen Deutschlands. In seinen LED-Wänden im Shoppingbereich nutzt er geräteintegrierte Brandschutzlösungen von Job.

Flughäfen sind aufgrund der großen Anzahl an Menschen, die täglich den Flughafen nutzen, kritische Infrastrukturen, zum anderen aber ein wichtiger Ort für Werbetreibende. Werbeeinnahmen stellen eine wichtige Einnahmequelle für die Flughafenbetreiber dar. Allerdings müssen die Werbeträger – insbesondere LED-Wände, Monitore und Bildschirme – den hohen Anforderungen u.a. an Brandschutz an Flughäfen erfüllen.

Über dem Marktplatz – dem Shoppingbereich des BER hinter den Sicherheitskontrollen – wurden vier neue LED-Wände installiert. Dank integrierter Brandschutzlösung von Job erfüllen sie die neuesten Sicherheits- und Brandschutzbestimmun-

gen. Auf den LED-Screens, die in Zweierpaaren von der Decke hängen, werden nun Werbung und Informationen des Flughafens gezeigt. Durch die beeindruckende Größe gelten die Screens als spektakulärste Werbefläche des gesamten Flughafengeländes. „Durch geräteintegrierten Brandschutz“, so Werner Green vom BER, „konnten wir dieses Projekt leichter realisieren“.

Schont die Elektronik

Die vier LED-Wände bestehen aus insgesamt 576 LED-Cabinets. Diese sind mit Job E-Bulbs ausgestattet, wodurch sie bestmöglich vor einer Brandentstehung im Inneren der Cabinets geschützt sind. Der E-Bulb löst bei einer festgelegten Temperatur aus und löscht so entstehende Brände.

Dank der rückstandsfreien Löschflüssigkeit bleibt die restliche Elektronik verschont. Dadurch werden Ressourcen sowie Zeit und Kosten für die Reparatur gespart. Zudem ermöglicht dieser integrierte Brandschutz (gegen Brände von innen) im Zusammenspiel mit äußeren Gerätemaßnahmen (gegen Brände von außen) die Installation von elektrischen Geräten auch in sensiblen Bereichen. Dazu zählen beispielsweise Flucht- und Rettungswege mit viel Personenverkehr. **GIT**



Job GmbH
www.job-group.com

VDMA-Symposium: Gebäude im Brandfall richtig sichern

Der VDMA Fachverband Allgemeine Lufttechnik hat das überarbeitete Grundlagenpapier Entrauchung und Rauchfreihaltung veröffentlicht und wird am 6. Mai 2025 Inhalte der Publikation auf dem 7. VDMA-Symposium Brandschutz und Entrauchung präsentieren. Die vorgestellten Maßnahmen zur Entrauchung und Druckbelüftung verhindern die unkontrollierte Ausbreitung des Rauchs und sind eine wesentliche Voraussetzung für die Selbst- und Fremddrettung, die Brandbekämpfung und den Sachschutz. Zudem unterstützt die gezielte Rauchableitung die Feuerwehr bei der Durchführung wirksamer Löschmaßnahmen. Die Freisetzung von Rauch ist stark vom Material und den Verbrennungsbedingungen abhängig. So entstehen zum Beispiel Rauchgase in hohen Mengen bei der Verbrennung von Papier, Pappe, Holz, Kunst- oder Schaumstoff. Rauch beeinträchtigt innerhalb kurzer Zeit massiv die Sicht und verhindert die Möglichkeit der Orientierung.

www.vdma.org



© Motorola Solutions | Oliver Lang

Motorola stattet die Fregatte Sachsen mit Digitalfunk aus

Motorola Solutions hat das Marineschiff F124 Sachsen mit einer Tetra-Digitalfunklösung ausgestattet. Die neue Kommunikationsinfrastruktur an Bord der Fregatte dient der zuverlässigen Kommunikation der Schiffssicherungstrupps, der Schadensabwehrkräfte und der Einsatzleitung des Schiffssicherungspersonals zur Führung des Schadensabwehr- und Gefechtsdienstes (SAGD). Ihre Aufgabe ist es, die Sicherheit der Soldaten und die Bereitschaftsfähigkeit des Marineschiffes zu jedem Zeitpunkt zu gewährleisten. Die Digitalfunklösung basiert auf dem Dimetra X Core Deployable System von Motorola Solutions, einem sicheren Funksystem, das für die besonderen Anforderungen von Militär-, Verteidigungs- und Sicherheitsorganisationen entwickelt wurde. Neben der Installation der Tetra-Lösung auf der F124 Sachsen hat das Unternehmen die Lösung bereits erfolgreich als Test- und Ausbildungssysteme für die Marine in Betrieb genommen.

www.motorolasolutions.com

FeuerTrutz 2025

Internationale Fachmesse mit Kongress für vorbeugenden Brandschutz

BRANDSCHUTZ ERLEBEN

Nürnberg, 25. – 26. Juni 2025



SCAN ME

feuertrutz-messe.de/dabei-sein

ALARMIERUNG

Damit die Feuerwache nicht selbst zum Brandopfer wird...

Kooperation für Rund-um-Brandschutz

Erst Anfang letzten Jahres wurde die neue Feuerwache in Stadtallendorf als modernster Feuerwehrstützpunkt im Landkreis Marburg-Biedenkopf eingeweiht. Nur wenige Monate später zerstörte ein Brand große Teile des Gebäudes und verursachte einen zweistelligen Millionenschaden. Ganz besonders folgenschwer: Die Feuerwache selbst besaß keine Brandmeldeanlage. Viele Verantwortliche fragten sich daraufhin: Wie können Unternehmen und kritische Infrastrukturen besser vor Bränden geschützt werden?



Lupus-Brandmelder in einem Feuerwehr-Einsatzwagen – mit Groupalarm-App auf dem Smartphone im Vordergrund

Die Alarmierungslösung Groupalarm und der Rauchmelder-Hersteller Lupus-Electronics bieten neuerdings gemeinsam eine Lösung an, die effektive Alarmierung und modernste Brandmelde-Technik durch einfache Integration miteinander vereint. Lupus hat mit seinem Mobilfunkrauchmelder ein Produkt entwickelt, dass nach eigenen Angaben eine Weltneuheit darstellt.

Der autarke, smarte Mobilfunk-Rauchmelder ist direkt mit dem Narrowband-IoT-Mobilfunknetz der Deutschen Telekom verbunden. Und er erfordert weder Gateway noch lokale Internet- oder Stromversorgung. Dank der eingebauten SIM-Karte und einer zehnjährigen Batterielaufzeit ist er zudem äußerst flexibel einsetzbar. Die vollautomatische Fernwartung sowie die einfache Aktivierung durch QR-Code-Scan machen ihn zu einer bequemen Lösung für den sicheren und sorgenfreien Betrieb von Einrichtungen, Institutionen und Unternehmen. Besonders wichtig ist dabei vor allem die unbegrenzte Skalierbarkeit des Systems. Von kleinen Gebäuden bis hin zu großflächigen Anlagen können beliebig viele Sensoren zentral verwaltet werden.

Sofortige Alarmierung

Ergänzt wird die smarte Lösung jetzt durch die Alarmierungsplattform Groupalarm. Sobald ein Rauchmelder Alarm schlägt, wird über die Plattform automatisch eine direkte Benachrichtigung an alle relevanten Einsatzkräfte und Verantwortlichen verschickt. In Sekundenschnelle läuft der Alarm über verschiedene Kommunikationskanäle wie App, SMS oder Sprachanruf. Passend für größere Einrichtungen erlaubt die Plattform zudem die individuelle Konfiguration von Eskalationsstufen und Alarmgruppen. So wird sichergestellt, dass immer die richtigen Personen erreicht werden.

Das Ergebnis ist ein Rund-um-Schutz, der verheerende Brand-Szenarien verhindern soll. Durch die Integration der Lupus-Technologie in Groupalarm entsteht ein nahtloses System, das Brandmeldungen nicht nur erkennt, sondern unmittelbar reagiert – ein Vorteil sowohl für Feuerwehren als auch für kritische Infrastrukturen und Unternehmen.

Ein Beispiel, das Schule machen sollte

Der Fall Stadtallendorf zeigt, wie wichtig Vorbeugung im Brandschutz ist. Brandmel-

deanlagen sind vielerorts zwar gesetzlich nicht vorgeschrieben, doch ihre Bedeutung für den Schutz von Gebäuden und Einsatzkräften ist unbestreitbar. Der Einsatz smarter Mobilfunkrauchmelder in Kombination mit einer leistungsstarken Alarmierungsplattform bietet nun eine ganzheitliche Lösung für den modernen Brandschutz, die sogar weit über gesetzliche Anforderungen hinausgeht. Für Stadtallendorf und viele andere Orte könnte diese Technologie ein entscheidender Schritt sein, um ähnliche Tragödien in Zukunft zu verhindern. Denn eines sei klar, so die Anbieter: Es sei Zeit, dass Gemeinden und Organisationen über den gesetzlichen Mindestschutz hinausgehen. Mit cleveren, innovativen Lösungen gelinge das schnell, einfach und effektiv. **GIT**



cubos Internet GmbH
www.groupalarm.com

OMS-Rauchwarnmelder

Lupus-Electronics stellte auf der E-world in Essen seinen OMS-Rauchwarnmelder vor. Der OMS-Rauchwarnmelder eröffnet Messdienstleistern und Messsystemanbietern die Möglichkeit, einen günstigen, fern-inspizierbaren Rauchmelder zertifiziert nach DIN 14676-1C mit zehn Jahren Batterielaufzeit einzusetzen. Damit leistet er einen entscheidenden Beitrag zur Digitalisierung und ressourcensparenden Effizienzsteigerung.

In Deutschland sind Rauchwarnmelder gesetzlich vorgeschrieben, da sie Brandrauch frühzeitig erkennen und einen lokalen Alarm auslösen. Um ihre Funktionalität sicherzustellen, ist jedoch eine jährliche Inspektion verpflichtend. Diese bringt nicht nur hohen Verwaltungsaufwand und Kosten mit sich, sondern erfordert auch wiederholte Anfahrten zu den Objekten – insbesondere für größere Immobilienportfolios eine ressourcenintensive Herausforderung.

Der OMS-Rauchwarnmelder setzt hier an: Mit einer zehnjährigen Batterielaufzeit und vollautomatischer Ferninspektion nach DIN SPEC 91388 sowie DIN 14676 1-C ist er ein echter Gamechanger. Das Inspektionsprotokoll wird per OMS/Wireless M-Bus übertragen, wodurch eine Vor-Ort-Kontrolle nur noch bei der Installation notwendig ist. Darüber hinaus ist der Rauchwarnmelder kompatibel mit allen gängigen OMS-basierten Messsystemen, Walk-by-Empfängern und dem Lupus OMS-Gateway.

Die Lupus Cloud ist ein modular aufgebautes Service-Angebot je nach Bedarf: Die Service-Module starten mit der OMS-Geräteverwaltung und ARGE-Datenverteilung, optional erweiterbar mit den Modulen Datenplattform- und Visualisierung, Mieterverwaltung/Mieter-App sowie der automatischen Verbrauchs- und Gebäudeabrechnung. Diese bietet eine transparente Darstellung der unterjährigen Verbrauchswerte, ist modular aufgebaut und vollständig EED-konform.

www.lupus-electronics.de



© Lupus-Electronics

VdS: Lehrgänge zu Sprinkleranlagen nach FM Standards



Das VdS-Bildungszentrum bietet fundierte Lehrgänge zur Auslegung und Installation von Sprinkleranlagen nach FM Standards an

In Kooperation mit FM starten im April 2025 die VdS-Lehrgänge „Sprinkleranlagen nach FM – Teil 1: Auslegung von Sprinkleranlagen“ und „Sprinkleranlagen nach FM – Teil 2: Installation von Sprinkleranlagen“ in Köln. In Kooperation mit FM bietet VdS die beiden aufeinander aufbauenden, jeweils zweitägigen Lehrgänge an. Beide Lehrgänge finden in Köln statt, Teil 1 zum ersten Mal am 23. und 24. April 2025, Teil 2 am 27. und 28. Mai 2025.

Beide Teile des Lehrgangs bieten neben der Vermittlung fundierten Fachwissens auch Workshops mit praktischen Übungen zur Auslegung bzw. zur Installation der Sprinkleranlagen. Somit können sich Interessierte im VdS-Bildungszentrum

zu allen wesentlichen Regelwerken für Sprinkleranlagen fortbilden. Neben den neuen FM-Lehrgängen sind schon seit vielen Jahren fundierte Lehrgänge zu VdS- und NFPA-Richtlinien Teil des Programms.

Die Lehrgänge „Sprinkleranlagen nach FM“, Teil 1 und 2, sind interessant für Firmen, die Anlagen nach FM Standards installieren möchten. So können die beiden Lehrgänge von VdS-anerkannten Errichtern als Vorbereitung auf die Zusatzqualifikation für Anlagen nach FM Standards besucht werden. Daneben sind die Fortbildungen zum Beispiel auch für Mitarbeitende von Planungsbüros der Gebäudetechnik, Brandschutzdienststellen, Baubehörden oder Versicherungsunternehmen sowie für Sachverständige interessant.

Technisches Grundwissen über die generellen Anforderungen an die Installation von Sprinkleranlagen wird für die Teilnahme vorausgesetzt.

Die neuen Lehrgänge finden in Kooperation mit FM statt. Dabei kommen unter anderem die Inhalte der VdS 2132, „VdS-Richtlinien für die Anerkennung von Errichterfirmen für Feuerlöschanlagen“, zur Anwendung, deren aktuelle Fassung vom November 2024 neben der VdS-Anerkennung auch die Möglichkeit einer Zusatzqualifikation für Anlagen nach FM Standards beinhaltet. Hintergrund: Immer mehr Errichterunternehmen installieren Anlagen nach verschiedenen Standards, sodass das Interesse an einer Zusatzqualifikation steigt.

www.vds.de

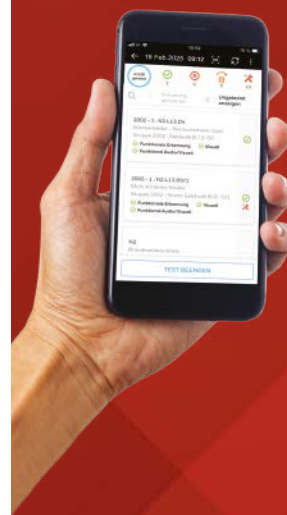
Revolution im Brandschutz: IQ8Quad-Brandmelder mit Selbsttest-Technologie



- **Normgerechte 1-Mann-Prüfung: weniger Systemausfallzeit, keine Brandwachen erforderlich**

- **Minimale Unterbrechung: geringer Eingriff in den laufenden Betrieb**

- **Höhere Effizienz: schnelle Identifizierung notwendiger Korrekturmaßnahmen und Fehlerbehebung**



Mehr Infos QR-Code scannen
oder unsere Website besuchen:

www.esser-systems.com

ESSER

by Honeywell



Der drehbare Anschluss erlaubt eine flexible Kabelführung und somit eine platzsparende Montage



Mit der eigens für den RSL 200 entwickelten Halterung lässt sich der Sicherheits-Laserscanner horizontal und vertikal ausrichten, im Servicefall kann er mit nur vier Schrauben schnell ausgetauscht werden

TITELTHEMA

Effizienz und Sicherheit auf kleinstem Raum

Kompakte Sicherheitslösungen in der industriellen Automatisierung

In der automatisierten Industrie müssen Effizienz und Sicherheit Hand in Hand gehen: Doch in engen Fertigungsstraßen, an fahrerlosen Transportsystemen oder Robotern ist der Platz oft begrenzt. Hier punkten ultra-kompakte Sicherheits-Laserscanner. Dr. Albrecht von Pfeil, Director Business Area Safety bei Leuze erläutert, worauf Anlagenbetreiber bei der Wahl eines passenden Laserscanners achten sollten. Außerdem im Interview mit GIT SICHERHEIT zu diesem Thema: Benjamin Schmid, Chief Innovation Officer bei Leuze.



Der RSL 200 sichert bei minimalen Abmessungen Maschinen, fahrerlose Transportsysteme und Roboter



Kommunikationswege über USB und Bluetooth, hier zusätzlich über TCP / IP, ermöglichen eine flexible Konfiguration und Diagnose



Mit der wechselbaren Speicherkarte wird die Konfiguration auf das neue Gerät übertragen

— Sicherheits-Laserscanner stehen in vielen Branchen zunehmend im Fokus. Die Geräte sind oft unverzichtbar, wenn es gilt, hohe Sicherheitsstandards für den Schutz von Personen zu gewährleisten. Sie lassen sich durch konfigurierbarer Schutz- und Warnfelder flexibel zur Gefahrenbereichs- und Zugangssicherung einsetzen, sowohl für stationäre als auch für mobile Anwendungen. Ein typischer Einsatzbereich ist die Absicherung gefährlicher Arbeitsbereiche einer Maschine gegen den Zutritt und die Anwesenheit von Personen. Ebenso eignen sich Laser-Sicherheitsscanner zur Sicherung autonomer mobiler Roboter (AMRs) und fahrerloser Transportsysteme (FTS), auch als Automated Guided Vehicle bezeichnet (AGV).

Sicherheit, die wenig Platz braucht

Moderne Sicherheits-Laserscanner müssen mehrere Anforderungen erfüllen: Neben der Hauptaufgabe, Maschinen oder Anlagen sicher abzuschalten, dürfen sie die Maschinenverfügbarkeit nicht beeinträchtigen und zu unnötigen Stillstandzeiten führen. Darüber hinaus sollen Laserscanner über Reichweite und Scanwinkel verfügen, während Sicherheitsklassifizierungen gemäß Typ 3, SIL 2 und PLd gewährleistet sein sollen. Auch muss sich der Anlagenbetreiber auf eine einfache Konfiguration und Diagnose verlassen können, die über verschiedene Schnittstellen wie Bluetooth, USB oder Ethernet-TCP/IP intuitiv erfolgen. Zu guter Letzt entscheidet die Gerätegröße. Denn mit zunehmender Automatisierung gewinnt räumliche Effizienz an Bedeu-

tung. Anlagen werden komplexer, zugleich schwindet der verfügbare Platz für die Sicherheitstechnik, vor allem im mobilen Einsatz am FTS.

Der Sicherheits-Laserscanner RSL 200 von Leuze arbeitet mit LiDar-Technologie auf einem Raum von nur 80 x 80 x 86 Millimetern. Dadurch ist seine Integration selbst bei beengten Platzverhältnissen möglich.

Installation und Wartung

Leuze hat für den Scanner eine eigene Halterung entwickelt, womit sich die Scanebene horizontal und vertikal ausrichten lässt. Im Servicefall kann der Scanner schnell getauscht und die Sensorparameter können über eine Speicherkarte vom alten auf den neuen Sensor übertragen werden.

Drehbare M12-Anschlüsse des Scanners erlauben eine flexible Kabelführung für I/Os und Stromversorgung sowie zur Datenübertragung. Dies ist wichtig für den Einsatz an kleinen FTS. Mithilfe einer mobilen Diagnose-App bietet Leuze dem Anwender zudem Unterstützung bei schwer zugänglichen Installationsorten des Laserscanners an.

Auf alle Anforderungen ausgerichtet

Damit ein-Laserscanner die anwendungsspezifische Sicherungsaufgabe zuverlässig erfüllen kann, muss sein Scanwinkel groß genug sein. Etwa, um tote Winkel oder schwer einsehbare Zonen hinter Maschinen oder Förderbändern lückenlos abzudecken. Aber auch, um kleine omnidirektionale FTS/AMR in alle Richtungen abzusichern. Der Laserscanner von Leuze bietet einen

275-Grad-Scanwinkel bei drei Meter Reichweite. Dieser erlaubt eine Rundumsicherung mit nur zwei diagonal positionierten Geräten, selbst mit Montagetoleranzen.

32 umschaltbare Sets aus Schutz- und Warnfeldern ermöglichen dem Anwender des FTS/AMR eine permanente Anpassung an Fahrtrichtung und Geschwindigkeit. Die überwachten Bereiche können so bei Kurvenfahrten, unterschiedliche Geschwindigkeiten und verschiedene Beladungszustände angepasst werden. **GIT**



Autor:
Dr. Albrecht von Pfeil
Director Business Area
Safety bei Leuze

Lesen Sie auf der nächsten Seite das Interview mit Benjamin Schmid, Chief Innovation Officer bei Leuze ▶



**Leuze electronic
GmbH + Co. KG**
www.leuze.com



Minimale Größe, maximale Sicherheit

Sicherheits-Laserscanner von Leuze

Sicherheits-Laserscanner haben sich in automatisierten Anlagen und Produktionsumgebungen als effiziente Lösungen für den Schutz von Mensch und Maschine etabliert. Benjamin Schmid, Chief Innovation Officer bei Leuze, erläutert im Gespräch die Vorteile dieser Technik und weshalb ultra-kompakte Modelle im Kommen sind.

— GIT SICHERHEIT: Herr Schmid, weshalb spielen Sicherheits-Laserscanner für viele Anwendungen in der Industrie eine wichtige Rolle?

Benjamin Schmid: Sicherheits-Laserscanner sind ein Schlüsselwerkzeug, um Mensch und Maschine in der Industrie 4.0 zuverlässig zu schützen. Mit ihren frei konfigurierbaren Sicherheitszonen, lassen sie sich dynamisch anpassen. Ein Beispiel ist die Absicherung von fahrerlosen Transportsystemen in der Logistik: Hier müssen die Scanner nicht nur Hindernisse erkennen, sondern die Sicherheitszonen jederzeit an die Bewegungsrichtung des Fahrzeugs anpassen. Ebenso eignen sie sich zur Zugangsüberwachung an Fertigungsanlagen, etwa bei Roboterschweißzellen. Der Scanner erkennt, wenn jemand in die Gefahrenzone eintritt und kann die Maschine sofort anhalten. Diese Technik ist auch bei kollaborativen Robotern unverzichtbar, hier können Laserscanner flexibel die Arbeitsumgebung überwachen. Und dann bei Annäherung einer Person die Robotergerätschwindigkeit reduzieren oder diesen stoppen. All das macht die Geräte in der industriellen Automation aus meiner Sicht unverzichtbar.

In den vergangenen Jahren haben kompakte Geräte an Bedeutung gewonnen. Warum sind die Abmessungen eines Sicherheits-Laserscanners und dessen Integration immer öfter ein entscheidender Faktor für Anlagenbetreiber?

Benjamin Schmid: Um es zugespitzt zu formulieren: In der Industrie zählt heute jeder Millimeter. Produktions- und Lo-

gistikumgebungen werden immer dichter gepackt, dadurch bleibt häufig auch weniger Fläche für die Sicherheitslösungen. Deshalb lässt sich ein Sicherheits-Laserscanner mit kleinen Abmessungen leichter integrieren. Hinzu kommt das Gewicht: Jedes zusätzliche Gramm zählt. Ob an Maschinenfronten und Robotern, engen Förderstrecken oder am FTS, wo der Platz ohnehin begrenzt ist. Auch ein wichtiger Aspekt: Ausgeklügelte Installationsmethodik senkt die Installationskosten, weil man einfachere Halterungen nutzen kann und keine oder nur kleinere Gehäusekonstruktionen für die Sicherheitskomponente braucht. Manchmal bleibt es dem Betreiber sogar erspart, eine bestehende Anlage umzubauen, wenn der neue Scanner kompakter ist als der alte. Das reduziert die Komplexität, den Aufwand und damit die Kosten.

Aber können diese ultra-kompakten Scanner bei der Leistung auch mit größeren Modellen mithalten?

Benjamin Schmid: Absolut. Dank moderner Technologien stehen kompakte Modelle ihren größeren Pendanten in nichts nach. Die Leistung hängt nicht von der Größe ab, sondern von der zugrundeliegenden Technologie. So sind ultra-kompakte Geräte wie unser RSL 200 optimal für den Einsatz an FTS und AMR geeignet. Derzeit ist er der kleinste Sicherheits-Laserscanner auf dem Markt, kann aber dank drei Meter Reichweite und einem 275 Grad breiten Scanwinkel zur Bereichssicherung an Maschinen und Anlagen verwendet werden. Natürlich sind je nach Anlage manchmal

größere Reichweiten erforderlich. In dem Fall lohnt sich dann ein Sicherheits-Laserscanner wie der große Bruder RSL 400 mit bis zu 8,25 Meter Reichweite. Dieser arbeitet mit bis zu zwei unabhängigen Schutzfunktionen und kann so zwei Scanner ersetzen – das macht wiederum die größeren Abmessungen wett.

Worauf sollten Anlagenbetreiber bei Sicherheits-Laserscannern noch achten?

Benjamin Schmid: Es ist wichtig, die spezifischen Anforderungen der Anlage zu analysieren. Soll der Scanner stationär oder mobil eingesetzt werden? Welche Reichweite und Auflösung werden benötigt? Faktoren wie Schnittstellen und Flexibilität bei der Konfiguration beziehungsweise Diagnose spielen ebenso eine Rolle. Für unseren Laserscanner bieten wir eine passende Service-App an, um auf Statusinformationen und Diagnosedaten zuzugreifen. Per Bluetooth lassen sich alle Informationen aus der Entfernung erfassen. Das ist von Vorteil, wenn der Laserscanner in schwer einsehbaren Bereichen einer Anlage montiert ist. Oder wenn der Zugang zum Gerät eingeschränkt ist. Für das Auslesen der Informationen muss das Schutzfeld nicht betreten werden, die Maschine kann also unterbrechungsfrei weiterarbeiten. Nicht zu vergessen: Seit Januar 2025 gilt die neue ISO 13855, die Berechnungsgrundlage für den Sicherheitsabstand hat sich geändert. Deshalb sollte jeder Anlagenbetreiber seine Anlagen und die Positionierung von Schutzeinrichtungen diesbezüglich überprüfen lassen – Leuze unterstützt bei Fragen dazu gerne. **GIT**

Finale Analyse bestätigt Relevanz der SPS 2024

Mitte November 2024 wurde die fränkische Stadt Nürnberg für 51.291 Besucher und 1.114 ausstellende Unternehmen wieder zum jährlichen Meetingpoint der smarten und digitalen Automation. Auf einer Fläche von insgesamt 125.000 m² präsentierten die Automatisierer einem durchweg zufriedenen Publikum ein umfassendes Angebot an Produkten, Innovationen und Lösungen. Die Fachmesse ist das Highlight der Branche, bei dem sich seit über 30 Jahren ausstellende Unternehmen, von Start-ups bis zu Keyplayern, und hochqualifizierte Besucher treffen, um sich persönlich auszutauschen, Geschäftsbeziehungen zu pflegen und neue Kooperationen einzugehen. Insgesamt

87 % der Aussteller haben bereits mehrfach an der SPS teilgenommen und 94 % bewerten die SPS als wichtig oder sehr wichtig für ihr Unternehmen.

Die internationale Beteiligung auf Ausstellerseite lag bei 40 % und somit etwas höher als im Vorjahr. Nach Deutschland sind die Top 5 Ausstellernationen: China, Italien und die USA, den 4. Platz teilen sich die Schweiz und Österreich und an fünf-

ter Stelle stehen Taiwan, die Niederlande sowie Großbritannien. Besucherseitig gab es ebenfalls einen Anstieg im Vergleich zur SPS 2023. Die am zahlreichsten vertretenen ausländischen Nationen sind hier Österreich, Italien und die Schweiz.

Die Umfrage unter den Besuchern ergab, dass 92 % erneut auf die Messe kommen und 95 % sie an Kollegen und Kunden weiterempfehlen würden. 91 % bewerteten die SPS als wichtig oder sehr wichtig für ihr Unternehmen und insgesamt waren 98 % mit ihrem Besuch sehr zufrieden oder zufrieden. Die Vortragsprogrammzahlen 2024 zeigen deutlich, dass der Wissensaustausch eine bedeutende Rolle auf der Fachmesse spielt: Insgesamt nahmen 5.610 Teilnehmer an 172 Beiträgen auf den Messeforen teil. Bei spannenden Fachvorträgen, innovationsstarken Produktvorstellungen oder praxisorientierten Podiumsdiskussionen konnten die Teilnehmer auf insgesamt vier Messeforen ihre Kenntnisse erweitern und sich über aktuelle Trends und Innovationen informieren.

www.mesago.com

Flexibel einsetzbare Lichtgitter mit höheren Reichweiten

Schmersal bringt neue Ausführungen von Sicherheitslichtvorhängen und Sicherheitslichtgittern der Baureihe SLC440COM-H/ SLG440COM-H auf den Markt. Mit Reichweiten von bis zu 30 Metern (SLC440COM) bzw. 60 Metern (SLG440COM) bieten

sie zuverlässigen Hand- oder Körperschutz und ermöglichen so eine Überwachung über große Entfernungen mit minimalem Installationsaufwand. Zusätzlich sind die Sicherheitslichtvorhänge und -lichtgitter mit einer Bluetooth-LE-Schnittstelle ausgestattet, die mit der von Schmersal entwickelten App „SLC Assist“ eine Statusmeldung der Geräte abbildet und umfassende Diagnosedaten

liefert. Die neue Version der „SLC Assist“-App bietet mehr Funktionalität, unter anderem kann mithilfe der App nun auch der erforderliche Sicherheitsabstand zur Gefahrstelle berechnet werden.

www.schmersal.com



 all about automation



Heilbronn
14. + 15. Mai 2025

Industrieautomation, Robotik,
Digitalisierung: Kommen Sie
mit auf den Weg zur flexiblen
Automation und smarten
Produktion.

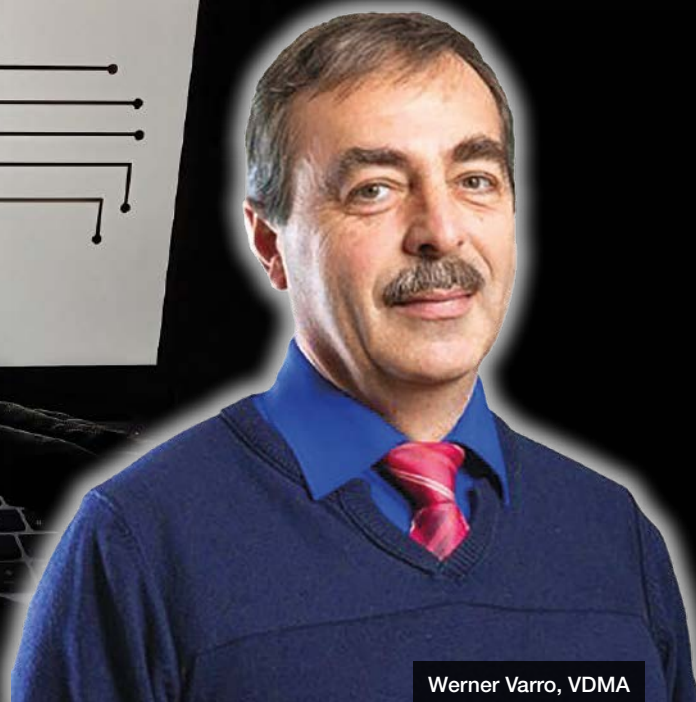
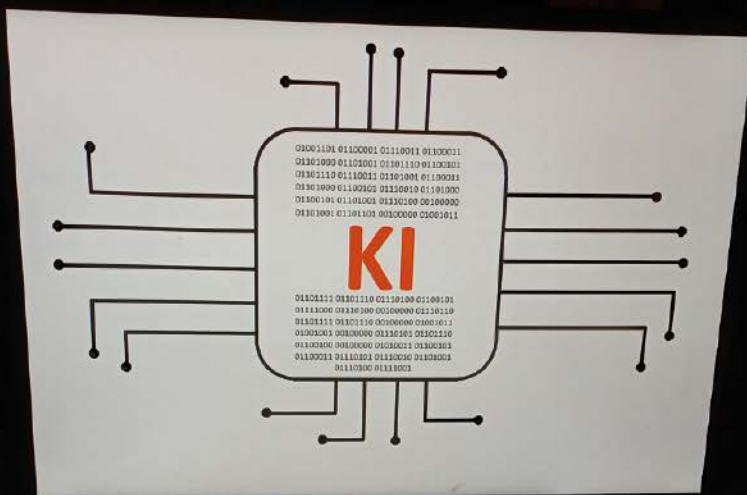
www.automation-heilbronn.de

Weitere
Messestandorte 2025:

- Friedrichshafen
- Hamburg • Wetzlar
- Düsseldorf • Chemnitz



by
EASYFAIRS



Werner Varro, VDMA

© Neura Robotics GmbH

Die digitale Vernetzung und die Verwendung neuer Technologien wie Künstliche Intelligenz (KI) stellen den Maschinen- und Anlagenbau, seine Komponentenzulieferer und Maschinenbetreiber in Sachen Funktionale Sicherheit vor neue Herausforderungen. Maschinen und Anlagen werden deutlich flexibler und bieten neue Möglichkeiten. Gleichzeitig wächst die Komplexität der Applikationen. Cybersecurity-Bedrohungen und neue Regularien stellen erhöhte Anforderungen. Wie können wir dem begegnen?

Eine Artikel-Serie in Kooperation von VDMA, ZVEI und GIT SICHERHEIT.

Die Ansprechpartner: Birgit Sellmaier betreut im VDMA-Fachverband Elektrische Automation Technik- und Technologiethemen wie Steuerungstechnik und Funktionale Sicherheit in der Anwendung im Maschinenbau. Dr. Markus Winzenick ist zuständig für den Fachbereich Schaltgeräte, Schaltanlagen, Industriesteuerungen im ZVEI Fachverband Automation.

MASCHINEN- UND ANLAGENSICHERHEIT

Maschinensicherheit im Kontext von KI und Security

Künstliche Intelligenz und ihre Auswirkung auf die Risikobeurteilung von Maschinen

Bis vor wenigen Jahren galt es vorrangig den Menschen vor der Maschine zu schützen (Safety), um Arbeitsunfälle zu vermeiden. Im Zeitalter weitreichender Erfassung und Auswertung von Maschinendaten und der Verschränkung von Informationstechnologie (IT) und Operativer Technologie (OT) gilt dies aber auch zunehmend umgekehrt. Nun heißt es, die Maschine vor dem Menschen bzw. vor einem nicht autorisierten Zugriff zu schützen (Security). Durch den Einsatz Künstlicher Intelligenz (KI) ist es nun zunehmend möglich, weitere Potentiale in der Fertigung zu heben. Zugleich ergeben sich dadurch weitreichende Konsequenzen für die Risikobeurteilung von Maschinen und Betriebsmittel. Welche das sind, erläutert Werner Varro, Consultant Safety & Certification bei Neura Robotics GmbH, im Interview mit GIT SICHERHEIT.



Elektrische Automation

electrifying
ideas

■ GIT SICHERHEIT: Herr Varro, inwiefern verändert sich der Umgang mit Maschinen und Anlagen durch die immer stärkere Vernetzung aller Komponenten?

Werner Varro: Der Umgang mit Maschinen verändert sich rasant, da mehrere Ereignisse gleichzeitig eintreffen. Die zunehmende Vernetzung führt zu erhöhter Kommunikation und großen Datenmengen, die erzeugt, transportiert, verarbeitet und gespeichert werden. Gleichzeitig wird eine sehr hohe Rechenleistung bereitgestellt, was die steigende Komplexität, Modularität und Flexibilität der Maschinen unterstützt.

Die Mobilität der Maschinen und ihre Fähigkeit zur eigenständigen Erkennung der Umgebung erhöhen ihre „Selbstständigkeit“. Neue Geschäftsmodelle wie Equipment-as-a-Service (EaaS), Robotics-as-a-Service (RaaS) und Pay-per-Use (PpU) bringen neue Teilnehmer und Stakeholder in den Lebenszyklus der Maschinen ein. Diese Änderungen setzen den Einsatz neuer Mensch-Maschinen-Schnittstellen voraus und ermöglichen es, bestehende Schnittstellen für einen größeren „Benutzerkreis“ zu öffnen.

Dadurch findet sozusagen eine Erweiterung der Grenzen der Maschine statt, von der Maschine an sich über die Kommunikationswege bis hin zur Applikation in der Cloud (Navigation, Machine Learning, ...) und verändert zwangsläufig auch den Umgang mit Maschinen. Durch diese Interaktionsformen der Menschen mit hochvernetzten Technologien entstehen sogenannte „soziotechnische Systeme“, die neue und zusätzliche Anforderungen an die Technik, aber auch an die Qualifizierung der Menschen stellen.

Welchen Einfluss hat der zunehmende Einsatz von KI auf die Sicherheit von Maschinen und Anlagen im Allgemeinen?

Werner Varro: Der Einfluss ist im Moment schwer abzuschätzen und hängt sehr stark mit der Applikation zusammen. Der Einsatz von KI bedeutet in der Regel eine Öffnung der Schnittstellen der Maschine nach außen, um die notwendigen Kommunikationsmöglichkeiten bereitzustellen. Dadurch erhöhen sich auch die Möglichkeiten, die Maschine von außen zu beeinflussen, z. B. durch Cyber-Angriffe oder durch die Bereitstellung ausgewählter falscher Datensätze für Machine Learning (ML). Wir stehen also wie bisher vor der Aufgabe, die Menschen vor der Maschine zu schützen (Safety), aber nun auch die Maschine vor den Menschen zu schützen (Security). Im Zusammenhang mit KI muss der Schutz des Menschen vor der Maschine in einen größeren Kontext (soziotechnisches System) gestellt werden. Nicht nur der Schutz vor physischen Gefahren, sondern auch psychische Gefahren (Vermenschlichung, Mobbing, Manipulation) und die Einhaltung geltender Gesetze – z. B. Erfassung persönlicher Daten (biometrische Daten, Stimmerkennung, Emotionenerken-

nung) – spielen in diesem Zusammenhang eine Rolle.

Einerseits kann also der Einsatz von KI eine Erleichterung sein, z. B. als Unterstützung bei der Bedienung der Maschinen oder bei der Entscheidungsfindung auf Basis großer Datenmengen. Andererseits wissen wir aber auch, dass der Mensch dazu neigt, die Maschine zu vermenschlichen. D. h. er überträgt ihr bestimmte menschliche Eigenschaften, vertraut ihren Entscheidungen und generiert dadurch zusätzliche Risiken.

Wieso bedarf es Ihrer Ansicht nach Regulierungen z. B. in Form einer erweiterten Risikobeurteilung?

Werner Varro: Bereits heute müssen zum Konformitätsnachweis Risikobeurteilungen und -analysen durchgeführt werden, z. B. gemäß Maschinenrichtlinie, Niederspannungsrichtlinie, EMV-Richtlinie sowie Cyber Security Act und AI Act der EU. Die Beurteilungen und Analysen werden dabei getrennt adressiert und in den Unternehmen in der Regel auch so umgesetzt. Durch diese Betrachtungsweise besteht die Gefahr, gegenseitige Beeinflussungen nicht vollständig oder zu spät zu erfassen, z. B. der Einfluss der KI auf die Funktion oder der Einfluss der Abläufe auf die KI.

Die erweiterte Risikobeurteilung ist also keine neue Regulierung. Sie ist vielmehr eine konsequente Erweiterung der bestehenden Methode (ISO 12100), um Risiken, die in einem soziotechnischen System durch die Kommunikation, Human Machine Interface und Cloud entstehen, systematisch zu bewerten. Des Weiteren geht es darum, die gegenseitige Beeinflussung von Safety, Security und KI zu erfassen, bzw. zu analysieren und quasi als Nebenergebnis transparent darzustellen. Damit bleibt die Risikobeurteilung Dreh- und Angelpunkt der Sicherheit und Datensicherheit und weiterhin der wichtigste Nachweis der Produktkonformität! Gleichzeitig ist sie aber auch die Basis, um Vertrauen in die neue Methode zu schaffen.

Wie sollte eine erweiterte Risikobeurteilung, Ihrer Meinung nach, gestaltet sein?

Werner Varro: In die erweiterte Risikobeurteilung müssen zusätzliche Aspekte einfließen und systematisch bewertet werden: Dazu gehören z. B. erweiterte Grenzen, die vom Sensor bis zur Cloud reichen, aber auch die Nutzer selbst, die im Lebenszyklus mit der Maschine interagieren. Des Weiteren gilt es ethische, soziale und gesetzliche Aspekte (ELSI), wie die Erfassung persönlicher Daten und Diskriminierung, zu berücksichtigen. Und natürlich sind die Generierung, Bearbeitung und Nutzung von Daten, die Daten- und Cybersicherheit, Rückfallstrategien und KI-Algorithmen wichtige Bestandteile. D. h. die erweiterte Risikobeurteilung muss all

diese Aspekte adressieren und identifizieren, die wechselseitigen Möglichkeiten zur Beeinflussung analysieren und abgestimmte Maßnahmen definieren und umsetzen.

So ausgestaltet, bleibt die Risikobeurteilung weiterhin das Basisdokument für die Konformität einer Maschine. Ein interessantes Beispiel zu dieser Entwicklung ist der Entwurf der Norm „BS 8611 Robots and robotic devices. Guide to the ethical design and application of robots and robotic systems“, die Hilfestellungen zur Identifizierung ethischer Gefährdungen gibt.

Die Gefahr von Cyber-Attacken hat in den letzten Jahren extrem zugenommen. Da auch eine künstliche Intelligenz durch eine Cyber-Attacke korrumpiert werden könnte, stellt sich natürlich die Frage, wie die Sicherheit von Maschinen in diesem Zusammenhang zu bewerten ist.

Werner Varro: Security, also Daten- und Cybersicherheit ist eine Voraussetzung für eine funktionierende KI und muss im gesamten Lebenszyklus berücksichtigt werden. D. h. für jede Lebensphase der Maschine müssen die richtigen Securitymaßnahmen definiert und ihre Wirksamkeit in regelmäßigen Abständen überprüft und neu justiert werden.

Zum Abschluss wäre es noch interessant zu erfahren, welche sozialen Interaktionsprobleme zwischen Mensch und Maschine beim zunehmenden Einsatz von KI entstehen können und ob auch hier eine Regulierung hilfreich sein kann.

Werner Varro: Das Gebiet der sozialen Interaktionsprobleme zwischen Mensch und Maschine beim zunehmenden Einsatz von KI ist weit und zum Teil noch unerforscht. In diesem Zusammenhang ist z. B. noch einmal die Vermenschlichung zu nennen, wodurch Vertrauen in die Maschine und deren Entscheidungen entsteht, was wiederum das Risiko erhöht, persönliche Daten preiszugeben. Ein weiteres Problem ist die Manipulation, sowohl der Maschine durch den Menschen, indem das Verhalten angepasst und „geschönt“ Daten verwendet werden, als auch des Menschen durch die Maschine, beispielsweise durch gezielte Abfrage persönlicher Daten. Ethik spielt ebenfalls eine Rolle, etwa ob die Maschine den Gesundheitszustand des Menschen erkennen muss. Zudem stellt sich die Frage, ob Sprach- und Gestikbefehle immer ausgeführt oder auch abgelehnt werden sollten und wenn ja, welche und wie. Eine Regulierung wird daher nicht vermeidbar sein, um die Schutzziele der geltenden Gesetze und Richtlinien zu erreichen. **GIT**



Neura Robotics GmbH
https://neura-robotics.com/de

„Vom Exoten hin zu einem Problemlöser“

**Im Gespräch: Helmut Schmid,
Vorstand des DRV und
Geschäftsführer HS Auxsilium**

Bis 2030 fehlen uns voraussichtlich sechs Millionen Fachkräfte. Deshalb haben wir bei Helmut Schmid vom Deutschen Robotik Verband nachgefragt, ob Roboter diese Lücke wirklich schließen und deutsche Robotik-Unternehmen von diesem Boom profitieren können? Auch spannend ist die Frage, wie ich Roboter problemlos in bestehende Arbeitsprozesse integriere.



© Deutscher Robotik Verband

■ In einer Pressemeldung vom 1. September 2022 schreiben Sie, dass mehr als 1.000.000 Roboter bis 2030 den Personalmangel deutlich reduzieren können. Wo stehen wir heute 2,5 Jahre später und ist das Ziel von 1.000.000 Robotern bis 2030 realistisch?

Helmut Schmid: Die wirtschaftliche Situation in Deutschland hat in den vergangenen beiden Jahren auch in der Robotik Bremsspuren hinterlassen und zu Stagnation beziehungsweise sogar zu einem Rückgang der Roboter-Installationen geführt. Nichtsdestotrotz heißt es gerade jetzt in Deutschland, Aktionen und Maßnahmen zu setzen, um das gesteckte Ziel noch zu erreichen.

Wer profitiert von dem Robotik-Boom – Deutschland, Japan, China, Südkorea....?

Helmut Schmid: Hier gibt es aktuell einen klaren Gewinner und das ist China. Das Land hat gezeigt, dass man mit einer klaren Roboter-Agenda, die man konsequent verfolgt und umsetzt, enorm erfolgreich sein kann. China hat mit Ihrer Agenda in den vergangenen vier Jahren die Roboterichte

auf 470 Roboter je 10.000 Arbeiter verdoppelt, wohingegen wir in Europa bei 219 Robotern je 10.000 Mitarbeiter stagnieren.

Inwieweit nutzt die deutsche Industrie aktuell Roboter, um den Fachkräftemangel zu kompensieren? Und wo sehen Sie weitere (zukünftige) Einsatzgebiete für Roboter?

Helmut Schmid: In Europa ist Deutschland mit 420 Roboter je 10.000 Mitarbeiter noch gut aufgestellt, doch leider stagniert auch hier der Einsatz von Robotern insbesondere durch die schwache Automobilindustrie, der einstige Treiber der Robotik in Deutschland. Der Mittelstand wächst konstant, aber moderat, kann den Rückgang der Automobilindustrie jedoch nicht kompensieren. Zukünftig werden Branchen wie die Landwirtschaft, der Bau aber insbesondere der Servicebereich zu Treibern der Robotik zählen. Auch die Industrie wird bei einem Anspringen der Wirtschaft ebenfalls wieder Fahrt aufnehmen, um die Wettbewerbsfähigkeit am Standort Deutschland aufrecht zu erhalten.

Welche spezifischen Aufgaben können Roboter übernehmen, die derzeit von Fachkräften ausgeführt werden?

Helmut Schmid: Auch Fachkräfte übernehmen in vielen Arbeitsbereichen immer noch zu viele monotone, repetitive oder auch gefährliche Tätigkeiten, für die Roboter einfach besser geeignet sind und eingesetzt werden können. Dies gilt sowohl für den Einsatz von stationären als auch mobilen Robotern. Denken Sie hierbei zum Beispiel an Tätigkeiten wie das Palettieren, wo Gewichte im Tonnenbereich je Tag bewegt oder an den Warentransport, wo Mitarbeiter kilometerweite Wege zurücklegen ohne wirklich produktiv zu sein.

Wie können Unternehmen sicherstellen, dass die Einführung von Robotik nicht zu Arbeitsplatzverlusten führt, sondern vielmehr neue Arbeitsplätze schafft?

Helmut Schmid: Aus meiner Sicht stellt sich diese Frage überhaupt nicht, da genügend Unternehmen Fachkräfte suchen, diese aber leider nicht finden. Daher, Betroffene zu Beteiligten machen und rechtzeitig in die geplanten Veränderungsprozesse mit einbinden, Ängste nehmen und die neuen Chancen aufzeigen. Es ist doch besser die vorhandenen Mitarbeiter weiter zu qualifizieren, ihnen interessantere Tätigkeiten zu geben und Roboter unterstützend als helfende Hand einzusetzen. Das

Arbeiten mit Robotern begeistert doch viele und sollte daher bei diesen keine Ängste schüren, ersetzt zu werden.

Inwieweit bietet der DRV Schulungen und Weiterbildungsmaßnahmen an, um Mitarbeitende auf den Umgang mit Robotern vorzubereiten und Bedenken abzubauen?

Helmut Schmid: Schulungen und Aufklärung sind in der Tat sehr wichtige Treiber, um Vertrauen bei der Einführung von Robotern in den Betrieben zu schaffen. Der DRV erarbeitet gerade einen Roboter-Führerschein, der genau hier ansetzen und unterstützen soll. Es soll hierbei allgemein die Sicherheit, der Einsatz und der Umgang mit Robotern gelehrt werden, um nach Abschluss entsprechend qualifiziert zu sein. Hier wird mit unterschiedlichen Stakeholdern zusammengearbeitet, um eine erfolgreiche Einführung in diesem Jahr sicherzustellen.

Wie hat sich der Einsatz von Robotik in den vergangenen Jahren entwickelt, insbesondere in Bezug auf die Effizienzsteigerung und Kostensenkung?

Helmut Schmid: Der Einsatz von Robotern insbesondere der von Cobots hat erfolgreich Einzug in die Industrie gehalten und sich vom Exoten hin zu einem ernsthaften Produkt und Problemlöser entwickelt. Dies zeigt auch der enorme Wettbewerb von neuen Herstellern und Anbietern, der sich dort mittlerweile eingestellt hat als auch die Erweiterung deren Portfolios hinsichtlich Reichweite und Payload.

Welche Initiativen hat der DRV in diesem Bereich gestartet?

Helmut Schmid: Unsere Mitglieder stehen hier den Unternehmen als kompetente Ansprechpartner, Umsetzer und Inbetriebnehmer zur Seite, um sie mit einem guten PreisLeistungsverhältnis von Automatisierungslösungen zu befähigen, weiterhin wettbewerbsfähige Produkte in Deutschland zu produzieren.

Welche Herausforderungen gibt es bei der Integration von Robotik in bestehende Arbeitsprozesse?

Helmut Schmid: Die größten Herausforderungen liegen im Finden der richtigen Prozesse für die Automatisierung, denn oft wird versucht mit den komplexesten Projekten zu starten oder den Mitarbeiter in einem bestehenden Prozess 1:1 mit einem Roboter zu tauschen. Meist leidet aber dann die Produktivität des Prozesses oder die hohen Er-



**DEUTSCHER
ROBOTIK
VERBAND**

Der Deutsche Robotik Verband deckt zahlreiche Fachbereiche ab und steht als Ansprechpartner unter anderem bei Fragen zu Gesetzlichen Vorgaben, Normung und Sicherheit oder auch zu Förderung und Finanzierung an Ihrer Seite. Ausführliche Informationen finden Sie hier:



wartungshaltungen an eine Automatisierung wird nicht erfüllt. Zudem sorgt das Thema Sicherheit immer für Herausforderungen bei der Integration von Robotern. Gerade Erst-einsteigern empfehlen wir, mit einfachen Prozessen zu starten und diese sukzessive zu erweitern und mit dem wachsenden Erfahrungshintergrund aller Beteiligten die nächste Stufe der Robotik zu zünden.

„Wir haben in Deutschland hervorragende Robotik-Unternehmen, die auf dem Weltmarkt mitspielen [...]. Wir sollten positiver nach vorne schauen, denn die Basis ist enorm stark. Jetzt gilt es, auch am Umfeld und der Infrastruktur zu arbeiten und endlich die Bürokratiebremse zu lösen.“

Wie unterstützt der DRV den Anwender, diese Herausforderungen zu bewältigen?

Helmut Schmid: Der DRV hat eine sehr starke Fachabteilung Normen und Sicherheit, die mit absoluten Branchenexperten besetzt ist und hier tatkräftig unterstützt, um skalierbare Robotik in den KMU in Einsatz zu bekommen. Wir bieten hier eine Vielzahl von Webinaren, Fachvorträgen und Veranstaltungen an, die als Informationsplattform genutzt oder besucht werden können.

Gibt es erfolgreiche Beispiele oder Best Practices von Unternehmen, die Robotik erfolgreich zur Bewältigung des Fachkräftemangels eingesetzt haben?

Helmut Schmid: Es gibt bereits eine Vielzahl von Unternehmen, die sich in den vergangenen Jahren mit der Einführung von Robotern befasst und auch umgesetzt haben. Je nach Unternehmensgröße haben diese meist mit einer Roboter-Applikation

begonnen und bis heute 10, 20 bis hin zu 50 Robotern je Standort im Einsatz.

Welche politischen und wirtschaftlichen Rahmenbedingungen sind notwendig, um den Einsatz von Robotik weiter zu fördern?

Helmut Schmid: Wir benötigen eine klare Agenda zu Robotik & KI, wie diese in den USA beziehungsweise China bereits erfolgreich umgesetzt wird respektive wurde. Zudem muss der Zugang von institutionellem Risikokapital erleichtert werden, damit die vorhandenen Innovationen auch skalierbar ausgerollt und eingesetzt werden können.

Wie schätzen Sie das Potenzial des deutschen Robotik-Unternehmen im Vergleich zu anderen starken Märkten wie Südkorea, China und Japan ein?

Helmut Schmid: Wir haben in Deutschland hervorragende Robotik-Unternehmen, die auf dem Weltmarkt mitspielen beziehungsweise das Potential mitbringen, genau dort

eine entscheidende Rolle zu spielen. Wir sollten positiver nach vorne schauen, denn die Basis ist enorm stark. Jetzt gilt es nur auch am Umfeld und der Infrastruktur zu arbeiten und endlich die Bürokratiebremse zu lösen.

Und eine abschließende Frage: Sehen Sie Robotik als Ausweg aus dem Fachkräftemangel?

Helmut Schmid: Ich bin der starken Überzeugung, dass Robotik und Automatisierung als einer der maßgebenden Ansätze zur Lösung des Fachkräftemangels gelten, denn in nur fünf Jahren (2030) werden uns voraussichtlich an die sechs Millionen Fachkräfte fehlen, die nicht alleine durch Fortbildung und qualitative Einwanderung gelöst werden kann. Daher sieht die Robotik meines Erachtens, trotz einer aktuell schwierigen Lage, rosigen Zeiten entgegen. (agry) 



Deutscher Robotik Verband e.V.
www.robotikverband.de

LITHIUM-IONEN-AKKU LAGERSCHRÄNKE

VDMA-Einheitsblatt 24994

Erster einheitlicher Prüfstandard für die Zertifizierung von Lager-/Ladeschränken für Lithium-Ionen-Akkus



Dr. Andre Horstenkamp, zuständig für das Projektmanagement beim Gefahrgutsspezialisten Düperthal

Mit dem VDMA-Einheitsblatt 24994 gibt es seit August vergangenen Jahres erstmals eine Grundlage für einen einheitlichen Prüfstandard im Bereich von Lager- bzw. Ladeschränken und -einrichtungen für Lithium-Ionen-Akkus. Das soll für mehr Sicherheit auf Seiten der Anwender und Hersteller sorgen. Im ersten Beitrag unserer vierteiligen Reihe zum VDMA-Einheitsblatt 24994, erläutert Dr. Andre Horstenkamp, zuständig für das Projektmanagement beim Gefahrgutsspezialisten Düperthal, die spezifischen Herausforderungen auf Seiten der Hersteller, die Fortschritte im Bereich der Innentests sowie die Auswirkungen auf das Produktportfolio bei Düperthal.

— GIT SICHERHEIT Wie stellt sich gegenwärtig die Situation im Bereich der Prüfung von Lagerschränken/Lagereinrichtungen für Lithium-Ionen-Akkus dar? Schafft das neue VDMA-Einheitsblatt 24994 mehr Transparenz und Klarheit sowohl für Hersteller als auch für Konsumenten?

Dr. Andre Horstenkamp: Obwohl bereits seit annähernd 10 Jahren Lagerschränke für das Laden und Lagern von Lithium-Ionen-Akkus am Markt verfügbar sind gab es bisher keinen einheitlichen Prüfstandard für diese Produkte. Wir von Düperthal haben daher unsere Battery line Sicherheitsschränke bereits frühzeitig in Zusammenarbeit mit dem Fraunhofer ICT mit Lithium-Ionen-Akkus unterschiedlicher Größe getestet.

Das VDMA-Einheitsblatt 24994 bietet den Herstellern die Möglichkeit ihre Produkte nach einheitlichen und vergleichbaren Kriterien prüfen zu lassen. So ist eine Prüfung mit realen Batteriezellen mit einer definierten Zellchemie im vorgegeben. Weiterhin beinhaltet das VDMA-Einheitsblatt grundlegende Konstruktive Vorgaben für den Lagerschrank, wie z. B. den Einbau eines Rauchmelders.

Ein Brandtest von außen wird zwar im VDMA-Einheitsblatt beschrieben, ist jedoch nicht zwingend erforderlich. Hier bleibt es dem Hersteller überlassen, ob er seine Produkte entsprechend zertifizieren und kennzeichnen möchte.



Einrichten der Sensoren für Temperaturüberwachung zur präventiven Früherkennung von Batteriebränden in Düperthal connect

Für den Betreiber bzw. Nutzer schafft das VDMA-Einheitsblatt insofern Transparenz, dass man entsprechend gekennzeichnete Produkte nach objektiven Kriterien miteinander vergleichen kann. Ein weiterer großer Vorteil für den Nutzer ist, dass die maximal Batteriekapazität, die im Schrank bzw. pro Lagerbereich gelagert werden kann, angegeben werden muss.

Welche spezifischen Herausforderungen und Widersprüche sehen Sie bei den aktuellen Prüfscenarien und Normen für Lagerschränke für Lithium-Ionen-Akkus ?

Dr. Andre Horstenkamp: Derzeit findet man viele Produkte am Markt, die nach unterschiedlichen Normen und Standards geprüft wurden. Dazu gehören beispielsweise Prüfungen nach DIN EN 14470-1, der Prüfnorm für Sicherheitsschränke zum Lagern von brennbaren Flüssigkeiten, Brandprüfungen nach DIN EN 1363-1 und auch die von uns in Zusammenarbeit mit dem Fraunhofer ICT durchgeführten Tests mit Lithium-Ionen-Akkus unterschiedlicher Größe. Teilweise finden sich aktuell Produkte, die nur in Anlehnung an einen Prüfstandard oder bereits vor Veröffentli-

chung eines Prüfstandards, wie z. B. dem VDMA-Einheitsblatt, geprüft wurden. Das führt aus unserer Sicht zu einer erhöhten Unsicherheit bei der Produktauswahl beim Kunden, da die Produkte so nur schwer miteinander vergleichbar sind.

Wie bewerten Sie die freiwilligen Außenbrandtests nach VDMA, und welche Fortschritte wurden beim Innenbrandtest erzielt?

Dr. Andre Horstenkamp: Der Thermal-Runaway-Test, wie er in dem VDMA-Einheitsblatt beschrieben ist, ist aus unserer Sicht eine gute Lösung, um die Leistungsfähigkeit eines Lagerschranks unter Beweis zu stellen. Durch die Definition des für den Test zu nutzenden Zellformats (zylindrisch) und der Zellchemie (NMC 8-1-1 oder NMC 9-0,5-0,5) sowie der Ladung (SoC => 98 %) der Zellen werden die Tests untereinander vergleichbar.

Den äußeren Brandschutz des Sicherheitsschranks sehen wir als wichtigen Bestandteil unseres Sicherheitskonzepts. Durch den Brandschutz von außen wird gewährleistet, dass im Falle eines Brandes im Raum die im Sicherheitsschrank gelagerten Batterien das Brandgeschehen nicht zusätzlich verstärken und Personen den Gefahrenbereich sicher verlassen können und Rettungskräfte vor den gelagerten Lithium-Ionen-Batterien geschützt sind.

Welche Schwachstellen sehen Sie im VDMA-Einheitsblatt?

Dr. Andre Horstenkamp: Wir sehen an einigen Stellen des VDMA-Einheitsblatts noch ein gewisses Verbesserungspotential. So kann der Thermal-Runaway-Test auf eine Lagerebene begrenzt werden, wenn die darunter und darüber gelagerten Lithium-Ionen-Akkus nicht propagieren. Eine weitere Aufteilung der jeweiligen Lagerebenen in kleinere Bereiche auf die der Thermal Runaway begrenzt bleibt ist bisher nicht vorgesehen, obwohl dadurch die Sicherheit für den Betreiber und die Nutzer weiter erhöht wird.

Eine weitere Herausforderung stellen die bei einem Thermal Runaway austretenden Gase dar. In der aktuellen Fassung des VDMA Einheitsblatts werden austretende Gase nur am Rande erwähnt, obwohl sie ein erhebliches Gefährdungspotential für die Nutzer darstellen.

Ebenso wird im VDMA Einheitsblatt die elektrische Sicherheit der Lagerschränke bisher nicht betrachtet. Da ein großer Teil der auf dem Markt angebotenen Lagerschränke mit Steckdosen zum Laden von

Akkus ausgestattet ist, sollte die elektrische Sicherheit aus unserer Sicht ein weiteres Prüfkriterium darstellen.

Gibt es Modifikationen an den Produkten von Düperthal, die durch das VDMA-Einheitsblatt bedingt sind?

Dr. Andre Horstenkamp: Ja, es ergeben sich Modifikationen, da das VDMA Einheitsblatt vorsieht, dass der Schrankinnenraum durch einen Temperatursensor und einen Rauchmelder überwacht wird, müssen die nach dem VDMA-Einheitsblatt gekennzeichneten Schränke mit der entsprechenden Sensorik ausgestattet werden. Bisher wurde die Sensorik für den präventiven Brandschutz nur als optionales Zubehör angeboten.

Weiterhin ergeben sich Modifikationen beim Brandschutz von außen. Im Vergleich zur DIN EN 14470-1, der Prüfnorm für Lagerschränke für brennbare Flüssigkeiten, sieht das VDMA Einheitsblatt bei einem Außenbrand eine maximale Temperaturerhöhung um 100 K bzw. 120 K im Schrankinneren vor. Im Vergleich hierzu ist bei der Brandprüfung nach DIN EN 14470-1 eine Temperaturerhöhung um 180 K erlaubt.

Wie sieht es mit dem Thema Explosion aus? Wird dies vom VDMA-Einheitsblatt berücksichtigt und wie wird mit austretenden Gasen umgegangen?

Dr. Andre Horstenkamp: Das Thema Explosionen wird nur am Rande berücksichtigt, da es während des Thermal Runaway Test zu vielen kleinen Explosionen kommen kann. Diesen Explosionen muss der Schrank standhalten.

Ein zusätzlichen Explosionstest mit einer größeren Gasmenge, wie ihn z. B. die neu erschienene UL 1487 vorsieht, ist im VDMA-Einheitsblatt nicht beschrieben. Mit einem solchen Test soll gezeigt werden, dass der Lagerschrank auch dem Explosionsdruck einer größeren Gasmenge standhalten kann. Eine solche Gasmenge kann sich ansammeln, wenn Lithium-Ionen-Batterien nur ausgasen und die Gase nicht direkt gezündet werden.

Welche zukünftigen Entwicklungen und Innovationen planen Sie im Bereich der Akkuaufbewahrung, um auf zukünftige Herausforderungen zu reagieren?



Thermisch isolierte Lagerböden mindern das Risiko, dass Brände innerhalb der Lagerebenen überspringen

Dr. Andre Horstenkamp: Auch zukünftig ist es unser Ziel innovative und nachhaltige Produkte, die dem Stand der Technik entsprechen anzubieten. Dazu bieten wir optimierte Lagerlösungen für die Lagerung und das sichere Laden von Lithium-Ionen-Akkus an. Dabei orientieren wir uns an den Wünschen unserer Kunden. So können wir z. B. Schließfachlösungen mit unterschiedlichen Schließungen oder spezielle Lösungen für den Einbau von Ladesystemen, wie sie viele Batterie-System-Hersteller auf den Markt bringen, anbieten.

Für den präventiven Brandschutz bieten wir auf die Bedürfnisse unserer Kunden angepasste Monitoring Lösungen an. Hier können wir offline Lösungen liefern, wie z. B. die kombinierte Überwachung des Sicherheitsschranks mit einem oder mehreren Temperatursensoren und einem Rauchmelder.

Darüber hinaus können wir auch vernetzte Rauchmelder einbauen und über unsere Düperthal connect Lagermanagementsoftware den Sicherheitsschrank und die integrierte Sensorik online überwachen. **GIT**



Düperthal Sicherheitstechnik
GmbH & Co. KG
<https://dueperthal.com>

PSA

Für alle Fälle gerüstet

Zertifizierte Multinorm-Schutzkleidung aus nachhaltiger Produktion

Arbeitssicherheit ist eine Notwendigkeit – wer in risikoreichen Umfeldern arbeitet, ob im Umgang mit Flammen, Chemikalien oder elektrischen Spannungen, braucht entsprechende Ausstattung, welche sämtliche Gefahren abwehrt. Multinorm-Schutzkleidung, die gleich mehrere Sicherheitsstandards bedient, ist hier das Mittel der Wahl.

Die Multinorm-Produkte von Blåkläder zeichnen sich durch eine Kombination aus Schutz, Komfort und Langlebigkeit aus. Die Kleidungsstücke sind nach internationalen Normen zertifiziert, darunter EN ISO 11612 für Hitzeschutz, EN 1149 für elektrostatische Entladung und EN ISO 20471 für Sichtbarkeit. Die gleichzeitige Abdeckung von mehreren Risiken ist vor allem in Berufen, in denen die Gefahrenlage oft wechselt, ein entscheidender Vorteil.

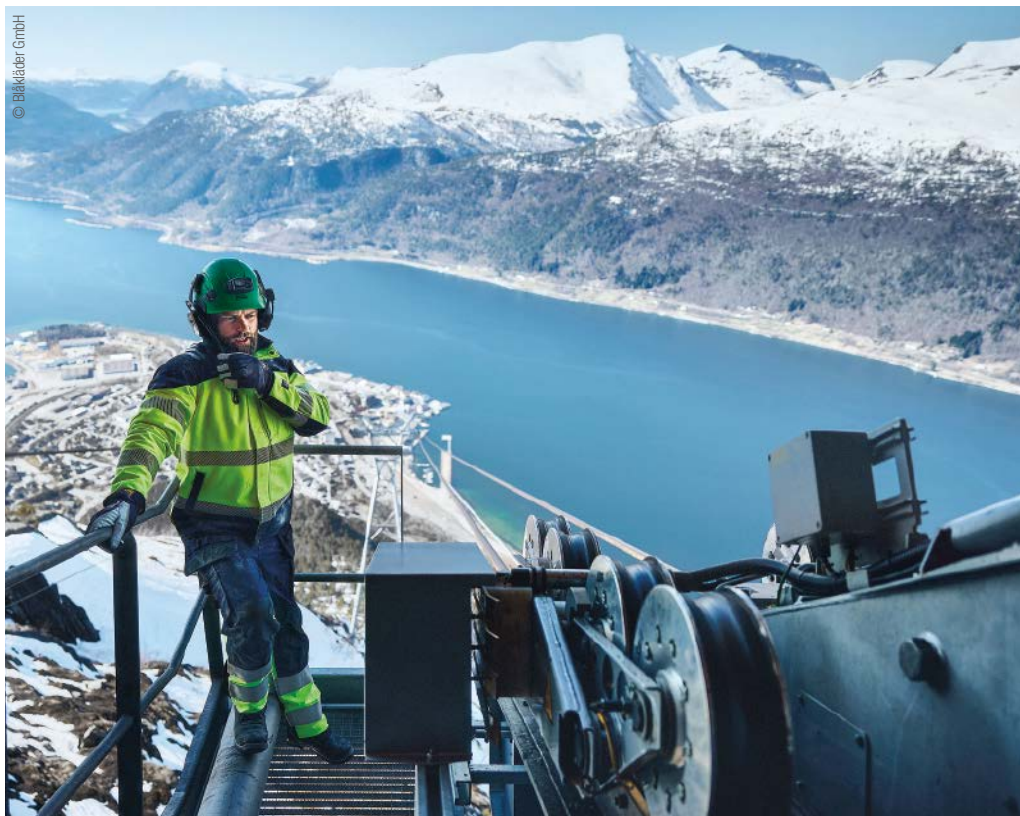
Sicherheit, Komfort und Langlebigkeit

Die beste Schutzausrüstung bringt jedoch wenig, wenn sie unbequem ist und dadurch nicht konsequent genutzt wird. Deshalb setzt Blåkläder auf ergonomische Schnitte, atmungsaktive Materialien und flexible Stretcheinsätze für mehr Bewegungsfreiheit. Die Kleidung muss nicht nur schützen, sondern auch zahlreichen Waschgängen und intensiver Nutzung standhalten. Hochwertige Materialien und verstärkte Nähte tragen dazu bei, dass die Kleidung ihre Schutzfunktion über lange Zeit behält – ein Faktor, der nicht nur die Sicherheit erhöht, sondern auch für Nachhaltigkeit steht. Denn jedes Kleidungsstück, das länger genutzt werden kann, reduziert den Ressourcenverbrauch.

Transparenz in Produktion und Logistik

Nachhaltigkeit beginnt bereits in der Herstellung. In der Textilbranche, die für einen erheblichen Teil der globalen Umweltbelastung verantwortlich ist, gewinnt die Frage nach transparenten und fairen Produktionsbedingungen seit Jahren an Bedeutung.

Viele Marken setzen auf ausgelagerte Fertigung und lange, oft intransparente Lieferketten. Bei Blåkläder findet ein Großteil der Produktion in eigenen Fabriken statt, was die Kontrolle über Arbeitsbedingungen, Materialwahl und Umweltstandards ermöglicht. Wie auch die Produkte selbst, sind die Produktionsstätten nach ökologi-



Die Multinorm-Schutzkleidung von Blåkläder schützt vor extremen Temperaturen, elektrostatischer Entladung und gewährleistet hohe Sichtbarkeit

schen und sozialen Standards zertifiziert – darunter LEED Gold und LEED Platin für nachhaltiges Bauen.

Diese Strategie schafft nicht nur Transparenz, sondern trägt aktiv zur Reduzierung des ökologischen Fußabdrucks bei. Kurze Entscheidungswege ermöglichen es, auf nachhaltige Produktionsmethoden zu setzen und faire Arbeitsbedingungen zu gewährleisten. Diese verantwortungsvolle Vorgehensweise in der Textilbranche ist positiv hervorzuheben.

Sicherheit und Nachhaltigkeit als Zukunftsstandard

Unternehmen und Verbraucher legen Wert auf nachhaltige Beschaffungen, sodass sich ein Blick hinter die Kulissen lohnt. Multi-

norm-Schutzkleidung ist eine essenzielle Investition in die Sicherheit von Arbeitnehmern – doch genauso wichtig ist es, wie und unter welchen Bedingungen sie hergestellt wird.

Die Kombination aus zertifiziertem Schutz, hoher Trageakzeptanz und einer transparenten, nachhaltigen Produktion zeigt, dass Arbeitssicherheit und Umweltbewusstsein Hand in Hand gehen und der Maßstab für die Zukunft der Arbeitskleidung sein können. **GIT**



Blåkläder Deutschland GmbH
www.blaklader.de

Besonders leicht und sicher

HAILO Überstiege

Ob in Lagern, bei Verkehrsbetrieben oder in der Produktion – die Sicherheit der Mitarbeiter hat höchste Priorität. Besonders dort, wo auf den Arbeitswegen Leitungen und Rohre, Produktionsstraßen, maschinelle Anlagen und andere Hindernisse überquert werden müssen. HAILO Professional bietet für diese Fälle ein breites Portfolio an ortsfesten Überstiegen sowie an stationären oder fahrbaren Plattformtreppen aus Aluminium an. Alle Produkte entsprechen den Vorgaben der europäischen Norm EN ISO 14122 und sind in verschiedenen Varianten erhältlich. Sie sind mit 45 oder 60 Grad Neigungswinkel verfügbar und können in Höhe und Breite individuell konfiguriert werden: 3 bis

10 Stufen sind möglich; an Stufenbreiten bietet HAILO 600, 800 oder 1000 mm. Für beengte Verhältnisse gibt es zudem eine Variante mit 75 Grad Neigungswinkel. Treppenstufen und Podest sind für maximale Trittsicherheit rutschhemmend geriffelt. Für industrielle Zwecke und andere besondere Anforderungen können die Stufen optional auch mit einem Anti-Rutsch-Belag ausgestattet werden.

Mehr Informationen unter:



Standardisierte Systemlösungen

Stationäre und mobile Überstiege

Effizienz steigern, Sicherheit gewährleisten: Mit den stationären und mobilen Überstiegen von KRAUSE überwinden Sie alle Hindernisse sicher. Ob stationär montiert oder fahrbar – die Überstiege sind in verschiedenen Neigungswinkeln (45° und 60°) und drei Stufenbreiten erhältlich. Sondermaße und alternative Stufen- und Plattformbeläge sind ebenfalls möglich.

Dank vormontierter Baugruppen ist die Montage schnell und unkompliziert. Kurze Lieferzeiten und die Möglichkeit der individuellen Konfiguration machen die Systemlösungen zur ersten Wahl für Sicherheitsbeauftragte und Verantwortliche in Prozess- und Betriebsplanung.

Typische Einsatzgebiete: Logistik – z. B. zur Überbrückung von Transport- oder Förder-

bändern – sowie Produktion zur sicheren Überquerung von Maschinen und Anlagen. Auch für Kontrollpunkte und Wartungsarbeiten im Energie- und Versorgungssektor bestens geeignet.

www.krause-systems.de



Überzeugen Sie sich selbst:



Die Überstiege von Munk Günstzburger Steigtechnik können individuell an die jeweilige Anforderung angepasst werden. Dabei steigern sie die Effizienz in Produktions- und Transportanlagen und sorgen zugleich für höchste Arbeitssicherheit

STEIGTECHNIK

Kurze Wege sind sichere Wege

Überstiege, Treppen, ortsfeste Leitern und Laufstege beschleunigen die Abläufe

Wer in der Fertigung und in der Logistik sicher, schnell und wirtschaftlich neue Wege gehen will, dem reicht manchmal bereits eine kleine Neuerung. Kurze Wege helfen da ungemein, wie die Überstiege, Treppen, Plattformtreppen und Laufsteganlagen von Munk Günstzburger Steigtechnik zeigen: Sie verkürzen die Wege in der Fertigung, im Lager und in der Logistik, sowie auch im Außenbereich und sorgen so dafür, dass die Produktivität und Sicherheit nicht auf der Strecke bleiben. Die Lösungen des Unternehmens können auch online mit Hilfe von Produktkonfiguratoren individuell und flexibel zusammengestellt werden. Seine Lösungen präsentierte der Hersteller auf der Logimat 2025 in Stuttgart.

„Der richtige Überstieg am richtigen Platz wird schnell zum Schlüsselfaktor für schnellere Betriebsabläufe: Unsere Kunden senken so ihre Produktionskosten, denn sie können voll auf automatisierte Fertigungsabläufe setzen und trotzdem sicher sein, dass das Bedienpersonal schnell und ohne große Umwege von A nach B kommt. Das

spart jede Menge Zeit und Geld und sorgt für ein Höchstmaß an Arbeitssicherheit“, sagt Ferdinand Munk, Inhaber und Geschäftsführer der Munk Group. Er verweist dabei gerne auf Studien, die den großen Nutzen von Prävention am Arbeitsplatz herausstellen: Demnach fließt jeder in Arbeitsschutz investierte Euro in Höhe von 2,2 Euro zurück.

Für die Überstiege, Laufstege, Treppen und fahrbaren Plattformtreppen des Herstellers gilt: Dank ihres modularen Aufbaus können diese bei Bedarf flexibel verändert und erweitert werden und dank Hülsenmuttern, die T-Nuttschrauben ersetzen, klappt auch die Montage so schnell wie nie zuvor. Darüber hinaus sind die Lösungen

Die Beläge für die Tritt- und Standflächen der Treppen, Überstiege und Laufstege aus Günstzburg sind frei wählbar

bereits in der Standardausführung mit Idealstopp-Rollen ausgestattet, sie bieten zusätzliche Mehrwerte und glänzen mit einer neuen, modernen Optik.

Produktkonfiguratoren

Egal, ob Überstiege, Treppen und fahrbare Plattformtreppen, Steigleitern oder seit neustem auch Dachüberstiege: Die zu ihren Anforderungen perfekt passende Lösung können sich Kunden auch rund um die Uhr online und mit nur wenigen Klicks selbst zusammenstellen. Möglich machen das die Produktkonfiguratoren der Hersteller, welche die Kundenbetreuung von Mensch zu Mensch ergänzen. Schritt für Schritt werden die gewünschten Maße, Ausführungen und Zubehörteile eingegeben. Das Ergebnis wird via drehbarem 3D-Modell und Maßzeichnung in Echtzeit dynamisch dargestellt und nach dem Speichern wird sofort ein Angebot samt Zeichnung per E-Mail zugestellt. Die Services sind unter www.munk-group.com/konfigurator verfügbar – hier gibt es auch Demo-Videos, welche die Funktionen der Produktkonfiguratoren vorstellen.

Auf der diesjährigen Logimat konnten die Messebesucher die unterschiedlichen Produktkonfiguratoren testen. Erstmals dabei war der neue Konfigurator für Dachüberstiege, mit dem die Anwender nicht nur die Neigungswinkel und Stufenbeläge ihrer Dachüberstiege anpassen, sondern dabei auch den Dachaufbau sowie Dachhindernisse einbeziehen können. Auch der Steigleiter-Konfigurator war ein besonderes Highlight, denn er ist branchenweit der erste Konfigurator mit realitätsnaher Wandsimulation: Mit ihm entwerfen Planer und Anwender die für sie perfekte Steigleiter direkt an der Zielfassade. Sie können dabei alle Störkonturen wie Fenster, Simse und Rohrungen berücksichtigen.

Überstiege für jede Anforderung

Für jede Anforderung gibt es den passenden Überstieg. Und wie bei Aluminium-Industrietreppen sind auch bei den Überstiegen und Laufsteganlagen die Beläge für Tritt- und Standflächen frei wählbar. Stahl-Gitterroste sind etwa im Außenbereich sinnvoll, weil sie eine hohe Rutschsicherheit bieten und Schmutz und Schnee durchs Raster fallen können. Geriffeltes Aluminium eignet sich dagegen für den Einsatz in Produktions- und Lagerhallen oder etwa Werkstätten. Und Lochbleche und Gitterroste aus Aluminium empfehlen sich bei hohen Hygienestandards, also etwa in Lebensmittellagern. Wie auch die Korundbeschichtung des Unternehmens erfüllen diese den strengen R13-Standard für Rutschhemmung und sorgen somit auch in nassen, överschmierten und staubigen Arbeitsbereichen für einen sicheren Tritt und Stand.



Mit dem Produktkonfigurator der Munk Günzburger Steigtechnik können sich Kunden des Unternehmens Überstiege, Treppen sowie fahrbare Plattformtreppen individuell selbst zusammenstellen

Die Überstiege von Munk Günzburger Steigtechnik sind standardmäßig in der benutzerfreundlichen Version mit einem Steigwinkel von 45 Grad oder in einer steileren Ausführung mit 60-Grad-Winkel erhältlich. Durch die Möglichkeit, die Neigungswinkel und Aufstiegshöhen über den Produktkonfigurator individuell anzupassen, lassen sich die Überstiege zudem besonders flexibel konfigurieren. Auch sehr niedrige Bauhöhen sind ganz einfach per Mausklick realisierbar. Für maximale Flexibilität können auch Geländer und Handläufe getrennt angewählt werden und Stecktaschen sind nicht mehr an die Auswahl eines Geländers gebunden.

Laufsteganlagen in Modulbauweise

Weiteres Plus in der Praxis: Das Unternehmen bietet auch seine Laufsteganlagen in Modulbauweise und im Baukastensystem an, sodass sich Kunden die für sie passenden Systeme besonders komfortabel und kosteneffizient individuell zusammenstellen können. Die Laufstegmodule sind

in drei Längen (1260, 1860 und 3060 mm) erhältlich und lassen sich frei miteinander kombinieren.

Zum kundenfreundlichen Service gehört auch die schnelle Lieferung. Überstiege und Laufsteganlagen, aber auch Treppen und fahrbare Plattformtreppen zählen zum Schnell-Lieferprogramm des Qualitätsherstellers und verlassen innerhalb von zehn Tagen das Werk, Steigleitern sogar innerhalb von ein bis drei Tagen. Außerdem entsprechen alle Produkte des Unternehmens den einschlägigen Normen und Vorschriften und werden ausschließlich am Firmensitz in Günzburg produziert. Sie werden zudem dem zertifizierten Herkunftsnachweis „Made in Germany“ des TÜV Nord gerecht und haben eine Garantie von 15 Jahren. **GIT**



Munk Group
www.munk-group.com

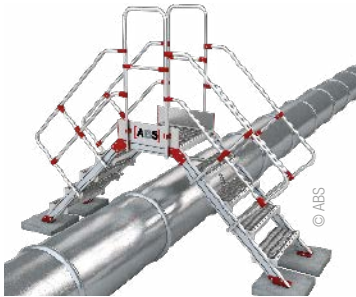


Die Überstiege und Treppen von Munk Gönzburger Steigtechnik: Ihre Montage klappt jetzt so schnell wie nie zuvor

6

PRODUKTVERGLEICH

Ortsfeste Überstiege



Firma	ABS	Hailo	Hymer
Listenpreis (Netto)	Preise auf Anfrage	ab 1.428,00 €	ab 1.903,00 €
Material	leichte, langlebige Aluminium-Konstruktion	Aluminium AlMg3 / AlMgSi 0,5	Aluminium
Lichte Höhe	310 mm, 510 mm, 710 mm, 910 mm, 1110 mm, 1310 mm, 1510 mm	1190 mm	280 mm – 2630 mm
Max. Gesamtbelastung	300 kg	300 kg (2 Personen) / 150 kg pro Stufen	300 kg
Stufenbreite	600 mm	600 mm, 800 mm, 1000 mm	600 mm, 800 mm, 1000 mm
Treppenneigung	45°	45°, 60°, 75°	35°, 40°, 45°, 50°, 55°, 60°, 65°, 70°, 75°
Stufen- und Plattformbelag	- Aluminium-Gitterroststufen (Stufentiefe 225 mm) - Aluminium-Gitterrostpodest (Rutschhemmung R13)"	- geriffelte Aluminiumstufen (optional mit Anti-Rutsch-Belag R13) - Gitterroststufen (Rutschhemmung R12)	- Aluminium geschlossen, gerieft Rutschhemmungsklasse R11 - Aluminium Gitterrost Rutschhemmungsklasse R13 - Stahl Gitterrost Rutschhemmungsklasse R12 - Stahl Gitterrost Rutschhemmungsklasse R13 - Stahl Lochblech Rutschhemmungsklasse R13
Sicherung Plattform Ein- und Ausgang		Zugangs-/Sicherungs-Schranken sind optional erhältlich	wahlweise mit und ohne Durchgangssperren konfigurierbar
Geländer-/Handlaufausführungen	fest montiert, Geländer mit Fußleiste beidseitig am Podest	Handlauf und Geländer einseitig	- fest montiert oder abnehmbar - Handlauf Rot oder Aluminium Natur
Zubehör		zusätzlicher Handlauf	Ablageschale (wahlweise mit 100 mm oder 200 mm Tiefe)
Anwendungsbereiche	- Überquerung von Hindernissen - Fachdach (Kabenkanal, Brandschutzwand, usw.) - in Gebäuden (Kabelkanal, Maschinen, usw.)	- maschinellen Anlagen - Lagereinrichtungen - Verpackungs- und Produktionsstraßen	
Besonderheiten	- freier online Konfigurator - versetzte Höhen sind möglich, dank Baukasten-System - Schnelle Montage durch vormontierte Baugruppen - grundsätzlich mit Geländern/Handlauf auf beiden Seiten ausgeliefert - Geländer mit Fußleiste beidseitig am Podest - verfügt standardmäßig über Gitterroststufen und -podeste der höchsten Rutschhemmungsklasse (R 13) - Standfestigkeit erfolgt mit Gewichten (nicht im Lieferumfang enthalten), keine Dachdurchdringung notwendig	- Modulares Baukastensystem - Schnelle Montage durch vormontierte Baugruppen - entsprechen der europäischen Norm EN ISO 14122, sowie EN 131-7	- freier online Konfigurator - beschichtete, ergonomische Handläufe - Geländerhöhe 1.100 mm - Versand in vormontierten Baugruppen - CE-konform nach DIN EN 1090

Ortsfeste Überstiege sind unverzichtbare Lösungen für die sichere Überquerung von Hindernissen in industriellen und gewerblichen Umgebungen. Hersteller wie ABS, Hailo, Hymer, Krause, Munk und Zarges bieten eine breite Palette an Überstiegen, die den europäischen Normen entsprechen und sich durch ihre modulare Bauweise auszeichnen. Diese Überstiege sind ergonomisch optimiert und ermöglichen einen sicheren und bequemen Auf- und Abstieg. Sie sind in verschiedenen Materialien wie Aluminium und feuerverzinktem Stahl erhältlich und können individuell konfiguriert werden, um den spezifischen Anforderungen und örtlichen Gegebenheiten gerecht zu werden.



© Krause



© Munk



© Zarges

Krause	Munk	Zarges
ab 2.095,00 €	ab 1.935,00 €	ab 2.104,00 €
Aluminium	Aluminium	Aluminium
400 mm – 2.500 mm	225 mm – 2200 mm, Sondermaße gerne auf Anfrage	280 mm – 2.630 mm
300 kg Plattformbelastung im Standard, 150 kg Stufenbelastung im Standard, wahlweise auch andere Belastungshöhen möglich	300 kg	300 kg
600 mm, 800 mm, 1000 mm, Sondermaße gerne auf Anfrage	600 mm, 800 mm, 1000 mm, Sondermaße gerne auf Anfrage	600 mm, 800 mm, 1000 mm
45°, 60°	45°, 60°	45°, 60°
- Aluminium gerieft - Stahl Gitterrost (auf Wunsch R10 oder R12) - Aluminium Gitterrost (auf Wunsch R10 oder R13) - Stahl Lochblech (in R11) - Aluminium Lochblech (in R11)	- Aluminium gerieft R 9, alu und gelb - Aluminium Gitterrost R13 - Stahl Gitterrost R12, Stahl und gelb - Aluminium Lochblech R13 - Korundbelag R13, schwarz und gelb - Stahl Lochblech R13	- Aluminium gerieft (R10) - Stahl Gitterrost (R12) - Aluminium Gitterrost (R13) - Stahl Lochblech verzinkt (R13) - Aluminium gerieft, signalgelb RAL 1003 (R9)
Sicherungsschranke, Pendeltür, Sicherungskette	Sicherungstüre, Sicherungsschranke, Sicherungsseil	Sicherungstür, Fallschranke
- fest montiert oder steckbar - rutschhemmend - pulverbeschichtet - in diversen RAL-Farben erhältlich - Ablageschale • Anprallschutzleiste • Pendeltür - Sicherungsschranke • Sicherungskette - Stufenkantenmarkierung - Schmutzfangblech unterhalb der Stufen	- starre Handlauf- und Geländerbefestigung - steckbare Handlauf und Geländerbefestigung - Haken - Ablageschale	- fest montiert oder abnehmbar - Stoßschutz • Haken • Ablageschale - Werkzeugtasche • optionales Fahrwerk für mobilen Einsatz • umlaufende Geländer
- Überquerung von z. B. Transport-/Förderbänder - Produktionsanlagen und Maschinen - als Zugang zur Kontrollpunkten oder für Wartungsarbeiten im Energie- und Versorgungssektor	- Überquerung von Bauteilen, Förderbändern, etc. - Zugang zu Maschinen und Anlagen - Wartungs- und Inspektionsarbeiten	- Überbrückung von Hindernissen - Arbeitsplattform mit beidseitigem Zugang - ortsfest oder fahrbar
- Individuelle Anpassung gemäß Kundenanforderung in Länge, Breite, Höhe und Farbe - Einbindung in bestehende Systeme - Fahrbare Ausführung möglich - Geländer/Handlauf auch mit vollflächigem Schutz (Plexiglas, Lochblechplatten) erhältlich - Mehrere Auf- und Abgänge auch in verschiedenen Winkeln und Neigungen möglich - Standardplattformtiefe: 625 mm - Stufentiefe 225 mm bei 45° und 175 mm bei 60 ° Neigung - Handläufe sind bei einer Treppenneigung von 45° mit einer Knieleise ausgestattet - Plattformgeländer 1.100 mm hoch mit Knie- und Fußleiste ausgestattet - Mit Bodenbefestigungswinkeln ausgestattet - Schnelle Montage durch vormontierte Baugruppen	- freier online Konfigurator - Vielfalt bei Belag und Breite - Ressourcenschonende Herstellung, - Hochfeste und recyclingfähige Materialien - Höchste Industriequalität - Ortsfeste Ausführung, auch fahrbar erhältlich	- freier online Konfigurator - Unterstützung bei der Lösungsfindung - Schnelle und einfache Montage durch das Zarges Verbindungssystem mit hohem Vormontagegrad - Schnelle Lieferung - Angewandte Normen DIN EN 14122, EN 131-7 - Geprüfte Sicherheit (TÜV) - Überwachte Produktion im Fachbetrieb

Liebe Leserinnen und Leser,

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

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

SICHERHEITS MANAGEMENT

Sicherheitsmanagement



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 6261 3193537
www.adiglobal.de · sales.de@adiglobal.com
Ihre zentrale Anlaufstelle für Sicherheit, Brandschutz und audiovisuelle Produkte.
Autorisierter Händler von über 45 führenden Marken.

Sicherheitsmanagement



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 Videoüberwachungs-, Einbruchmelde-, Brandmelde-, Sprachalarm- und Managementsysteme sowie Zutrittskontrolle, professionelle Audio- und Konferenzsysteme. In ausgewählten Ländern bietet Bosch Lösungen und Dienstleistungen für Gebäudesicherheit, Energieeffizienz und Gebäudeautomation an.

Sicherheitsmanagement



Daitem / Atral Security Deutschland GmbH
Eisleber Str. 4 · D-69469 Weinheim
Tel.: +49(0)6201/6005-0
info@daitem.de · www.daitem.de
www.brandwarnanlage.de
Funk-Einbruch- und Brandschutzlösungen vom Technologieführer. Vertrieb über qualifizierte Sicherheitsfacherrichter.

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



Freihoff Sicherheitsservice GmbH
Herzogstraße 8 · 40764 Langenfeld
Tel.: 02173 106 38-0
info@freihoff.de · www.freihoff-gruppe.de
Einbruchmeldeanlagen, Brandmeldeanlagen, Videoüberwachung, Zutrittskontrolle, Notruf- und Serviceleitstelle

Sicherheitsmanagement



NSC Sicherheitstechnik GmbH
Lange Wand 3 · 33719 Bielefeld
Tel.: +49 (0) 521/13629-0
Fax: +49 (0) 521/13629-29
info@nsc-sicherheit.de · www.nsc-sicherheit.de
Brandmeldetechnik, Videotechnik, Sprach-Alarm-Anlagen

Sicherheitsmanagement



SCHUHEN Consulting GmbH
Dorfstraße 5A · 85778 Haimhausen
Tel.: 08133/4019 660 · Fax: 08133/4019 690
Mobil: 0170 321 3040
info@schuhen-consulting.de
www.schuhen-consulting.de
Ihre Experten für Sicherheitsdienstleistungen
Beratung – Konzepte – Bedarfsermittlung – Beschaffung – Qualitätssicherung



Newsletter abonnieren Jetzt

Nachrichten für
Entscheider und
Führungskräfte in
Sachen Sicherheit

inklusive
e-Ausgabe!



WILEY

Sicherheitsmanagement



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

Gebäudesicherheit



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

PERIMETER SCHUTZ

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 Wirt-
schaft als unabhängige Organisation zur Verfügung.

Gebäudesicherheit



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

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 Freige-
ländesicherung aus einer Hand! Als Qualitätshersteller
für Schiebetore, Drehflügeltore, Zaun-, Zugangs- und
Detektionssysteme haben Sie mit INOVA auf alle Fragen
des Perimeterschutzes die passende Antwort.

GEBÄUDE SICHERHEIT

Ihr Eintrag in der Rubrik



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

Wir beraten Sie gerne!

Perimeterschutz



Raytec Ltd.
Unit 15 Wansbeck Business Park · Rotary Parkway
Ashington, Northumberland · NE63 8QW, UK
Tel: +44 (0) 1670 520055
sales@raytecled.com · www.raytecled.com
Raytec LED-Beleuchtung für Ihre Sicherheit.
Beleuchtungslösungen für die Bereiche Gefahrenzonen,
Industrie, Transport und Sicherheit.

Gebäudesicherheit



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

Gebäudesicherheit



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

VIDEO ÜBERWACHUNG

Gebäudesicherheit



v 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 Torstechnik

Gebäudesicherheit



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

Videoüberwachung



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.

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

Gebäudesicherheit



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

Videoüberwachung



**Ihr Value Added Distributor für
Videosicherheitstechnik „Made in Germany“**

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

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

www.luna-hd.de

High Definition Video

Videoüberwachung • Türsprechanlagen

Zeit + Zutritt



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

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.



Zeit + Zutritt



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

Videoüberwachung



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

Hanwha
Techwin Europe

Zeit + Zutritt



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



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

Videoüberwachung



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

Zeit + Zutritt



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



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.

Videoüberwachung



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

Zeit + Zutritt



Bird Home Automation GmbH
Uhlendstr. 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



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

Videoüberwachung



LivEye GmbH
Europa-Allee 56b
54343 Föhren
liveye.com

Zeit + Zutritt



CDVI GmbH
Dahlweg 105 / Tor 2 · D-48153 Münster
Tel.: +49 (0)251 798 477-0
info@cdvi.de · www.cdvi.de
Zutrittskontrolle, Zutrittskontrollsysteme,
Zutritt mittels Smartphone, Biometrische Systeme,
Türautomation, Komponenten für Türen+Tore

Zeit + Zutritt



FEIG ELECTRONIC GMBH
Industriest. 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 
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

ASSA ABLOY
Entrance Systems

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

BRAND SCHUTZ

Zeit + Zutritt

GUNNEBO®

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

Zeit + Zutritt

salto 
INSPIRED ACCESS

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

Brandschutz

DENIOS®
UMWELTSCHUTZ & SICHERHEIT

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

Ihr Eintrag in der Rubrik

BusinessPartner
Die Einkaufsrubrik für den direkten Kontakt

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

Wir beraten Sie gerne!



TKH
SECURITY

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

Brandschutz

Hertek
Brandschutzsysteme

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

Zeit + Zutritt

pcs

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

NOTRUF SERVICE LEITSTELLE

Brandschutz

seTec

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, Feuerweh
Schlüsseldepots, Feuerweh, Schlüsselmanager,
Feuerwehperipherie, Feststellanlagen, Störmeldezentralen

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, Zeit-
erfassung, BDE, Türkommunikation, Besuchermanagement,
Parksysteme, Zufahrtskontrolle, Vending, ... Terminals,
Einbaumodule, Kartensponder, Tischlesegeräte, Leser für
Markenschalterprogramme, Identifikationsmedien,
... einfach und komfortabel zu integrieren.

Notruf- und Service-Leitstelle

HWS

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



Brandschutz

WAGNER®
DIE BESSERE LÖSUNG IM BRANDSCHUTZ

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

Zeit + Zutritt

primion
AZKOYEN Time & Security Division

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

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
Störungsaufnahme in der Energieversorgung.

Ihr Eintrag in der Rubrik

BusinessPartner
Die Einkaufsrubrik für den direkten Kontakt

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

Wir beraten Sie gerne!

ARBEITS SICHERHEIT

Arbeitssicherheit



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

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

GEFAHRSTOFF MANAGEMENT

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.

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

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, Ar-
beitsschutz, sicherheitsrelevante Betriebsaus-
stattung, Gefahrstoff-Leckage-Warnsystem

Gefahrstoffmanagement



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

GASMESS TECHNIK

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 SICHERHEIT

Maschinen + Anlagen



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

Maschinen + Anlagen



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

Maschinen + Anlagen



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

Maschinen + Anlagen



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

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

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.

Maschinen + Anlagen



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

aus dem Wiley Verlag

NEWSLETTER
GIT-SICHERHEIT.de
Jetzt kostenfrei
registrieren



[www.git-sicherheit.de/
newsletter](http://www.git-sicherheit.de/newsletter)

The collage features several security-related publications and digital content:

- Top Left:** A QR code and the text "www.git-sicherheit.de/newsletter".
- Top Center:** Cover of "GIT CYBER SECURITY" magazine, featuring a blue background with binary code and the text "EIN SPECIAL VON GIT SICHERHEIT".
- Top Right:** Cover of "GIT SMART HOME SECURITY" magazine, featuring two men and the text "EIN SPECIAL VON GIT SICHERHEIT".
- Middle Left:** Cover of "GIT SECURITY INTL" magazine, featuring a circuit board and a shield icon, with the text "MAGAZINE FOR SAFETY AND SECURITY - WORLDWIDE".
- Middle Center:** Cover of "GIT SICHERHEIT" magazine, featuring three men and the text "GIT SPECIAL JVA & FORENSIK".
- Middle Right:** Cover of "GIT SICHERHEIT" magazine, featuring a woman in a blue hard hat and yellow safety vest, with the text "Ihre Nr. 1 seit mehr als 30 Jahren".
- Bottom Left:** Cover of "GIT SECURITY PRO-4-PRO" magazine, featuring a woman in a red jacket and the text "KOMMUNALE SICHERHEIT".
- Bottom Center:** A tablet displaying the "GIT SICHERHEIT" website, showing various articles and a "GIT SICHERHEIT AWARDS 2023" section.
- Bottom Right:** The "WILEY Industry Talks" logo and a QR code for "Ausgabe ONLINE lesen".

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

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

WILEY

DAS **VIP** INTERVIEW



© Volkswagen AG

Andreas Maack

Leiter Konzern Sicherheit & Resilienz
und Chief Security Officer
der Volkswagen AG

- 1991–2010 verschiedene Verwendungen im Bundeskriminalamt
 - u.a. Terrorismus, Schwere & Organisierte Kriminalität, Synthetische Drogen inkl. Rauschgiftlaboratorien, Grundstoffüberwachung, Narco-Terrorismus
 - darunter zahlreiche Projekte mit den Vereinten Nationen, Interpol und Europol sowie befristete Entsendungen im diplomatischen Dienst (Deutsche Botschaft in Duschanbe/Tadschikistan)
- 2010–2018 Sicherheitsleiter bei der Merck KGaA
- 2018–2021 Chief Security Officer der Bayer AG
- Seit 2021 bei der Volkswagen AG

Menschen machen Märkte

In jeder Ausgabe Ihrer GIT SICHERHEIT bitten wir wichtige Personen, Entscheider, Menschen aus der Sicherheitsbranche, zum VIP-Interview.

Ihr Berufswunsch mit 20 war:

Ich wollte (Not-)Arzt werden, hatte aber nach dem Wehrdienst und einem Pflegepraktikum noch ein paar Wartesemester bis zum Medizinstudium zu überbrücken.

Was hat Sie dazu bewogen, eine Aufgabe im Bereich Sicherheit zu übernehmen?

Zur Überbrückung der Wartezeit und aus Neugier hatte ich mich beim Bundeskriminalamt beworben. Kripo und BKA klang sehr attraktiv. Das war dann vom Studium, den Praktika und dem Alltag so vielseitig und interessant, dass ich dabei geblieben bin.

Welche sicherheitspolitische Entscheidung oder welches Projekt sollte Ihrer Meinung nach schon längst umgesetzt sein?

Wir müssen alle dazu bereit sein, mehr für unsere Sicherheit in der Gesellschaft zu tun. Sicherheit ist nicht etwas, das Andere (z.B. die Polizei, die Bundeswehr) für wieder einen selbst „produzieren“. Wir brauchen dringend einen wirkungsvollen „Wirtschaftsschutz“ und damit einen Sicherheitsdialog auf Augenhöhe zwischen Unternehmen und den staatlichen Stellen. Da ich seit Jahren über Deutschland hinaus vor allem auch mit Behörden aus anderen Staaten zusammenarbeite, kann ich sagen: Viele sind da wesentlich weiter.

Ein Erfolg, den Sie kürzlich errungen haben, war:

Ich habe tatsächlich ein paar Kilo abgenommen und wieder angefangen, regelmäßig Sport zu machen. Der Erfolg? Ich brauche neue Anzüge und Hemden.

Welche Reform bewundern Sie am meisten?

Aus beruflicher Sicht bewundere ich den Mut des Volkswagen-Konzerns beim konsequenten Umstieg vom Verbrennungsmotor zur E-Mobilität. Diese ambitionierten Ziele umzusetzen und die dafür notwendigen Investitionen aufzubringen ist alles andere als leicht – dient aber einer wichtigen und notwendigen gesellschaftlichen Ambition.

Wer hat Ihrer Meinung nach eine Auszeichnung verdient?

Meine Frau. Sie hält mir in diesen rasanten Zeiten völlig den Rücken frei.

Worüber können Sie sich freuen?

Dass meine Kinder geradlinig ihre Wege gehen, dass wir alle gesund sind und dass es uns gut geht.

Wobei entspannen Sie?

...wenn ich gelegentlich abends in aller Ruhe mit dem Flugsimulator die digitale Welt erkunde. Steuerhorn, Pedale und VR-Brille sind mit am Start. Geflogen wird auf maximal-realistischen Einstellungen.

Welchen Urlaubsort können Sie empfehlen?

Ganz klar Sizilien, mein Lieblingssort ist nicht weit von Cefalù. Ich mag Land und Leute, italienisches Essen und die Historie der Insel. Wenn es nicht so weit sein soll, dann sind die Regionen in der Mitte Italiens auch sehr schön.

Wie würde ein guter Freund Sie charakterisieren?

Zuverlässig, loyal, humorvoll und als jemanden, der immer ein offenes Ohr hat.

Die GIT SICHERHEIT ist für mich wichtig, weil...

es spannend ist zu sehen, welche Themen Kolleginnen und Kollegen aus unserer Branche so bewegen und voranbringen.

Welches Buch haben Sie zuletzt gelesen?

„Klar zur Wende“ von Karl-Ludwig Kley und aktuell (als Audiobuch) „Freiheit“ von Angela Merkel.

Was motiviert Sie?

Gestaltungsraum, Kreativität, und: wenn ein Plan aufgeht.

Worüber machen Sie sich Sorgen?

Ein Konglomerat aus verschiedenen Themen: Die gesellschaftliche Verrohung, die Zunahme von Gewalt und Aggression, die Meinungsbildung am gesellschaftlichen Rand, Krieg in Europa und dass einige Menschen fast ausschließlich in ihren „Bubbles“ leben und das nicht mehr merken bzw. dass es ihnen egal scheint. Kurzum: Ich sehe unsere Demokratie und unser Wertesystem in Gefahr.

Die beste Erfindung im Bereich Sicherheit ist Ihrer Meinung nach:

Da bin ich ein bisschen exotisch. Ich glaube, dass in der künstlichen Intelligenz (KI) immenses Potential auch für die Sicherheit steckt. Wir haben uns das nur noch nicht umfassend für die Security erschlossen. Aber: Anomalie-Erkennung, Informationsanalysen, Massendatenanalysen, Bilderkennung und vieles andere mehr, da geht noch einiges Nutzbringendes.

Ihre gegenwärtige Geistesverfassung ist:

Ich fühle mich sehr wohl, habe viel Energie und Spaß an dem, was ich tue.

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

Jetzt registrieren!
Hier Produkt oder Lösung für den nächsten
GIT SICHERHEIT AWARD einreichen

Neue Ausgabe jetzt Online!
Die aktuelle Ausgabe von
GIT SICHERHEIT zum Download

Nachrichten per Mail
Nichts mehr verpassen mit dem
Newsletter von GIT SICHERHEIT

Management
**BVSW SecTec 2025: Innovationen
in der Sicherheitstechnik**
Zum zweiten Mal: Fachkongress BVSW SecTec am 5. und 6. Juni 2025 – mit
aktuellen Entwicklungen, Regularien und Trends.

Management
**Strategisches Risikomanagement:
Schutz und Chancen
für Unternehmen**

WIRTSCHAFTS
Kühler-Welding-Bay:
Wissenswertes zu Ursachen und
Vermeidung von Schweißunfällen

ANZEIGE
STREITZ SECURA
SICHERHEITSTECHNIK
→ CP4480ESD

News

GIT SICHERHEIT
VfS fördert 20
Milliarden Euro aus
Sondervermögen

GIT SICHERHEIT
Schmersal Gruppe laut
ihre Präsenz in Asien aus

GIT SICHERHEIT
Adis erhält IT-
Sicherheitskennzeichen
des BSI

GIT SICHERHEIT
Salto Boosts Marke
bei Schließsystemen

GIT SICHERHEIT
TeleTrust fördert
Investitionen aus
Sondervermögen

Themen

**Erfolgsfaktor Cyber Security: IT-Sicherheit
als Kernstrategie für Unternehmen**
Moderne Cyberangriffe erfordern neue Strategien: Var
Group setzt deshalb auf KI, Maschinelles Lernen und
SOC-Standorte in verschiedenen Zeitzeilen.

Newsletter & e-Ausgabe
Nachrichten, Trends und Hintergrund
sowie die neueste Ausgabe der GIT
SICHERHEIT.
Ihre E-Mail-Adresse: ...
Mit Ihrer Anmeldung stimmen Sie
unseren Datenschutz-Bestimmungen
zu.
Abmelden

ANZEIGE
**Ganzheitliche Ansätze
im Identity & Access
Management**
Online Event | 3. April 2025
Jetzt registrieren! **imprivata**

GIT SICHERHEIT
Sick: „Qualität im Service ist
eine Frage des Know-hows“
Was der Kunde heute an Support erwartet und was
Sick an Leistungen bietet, darüber sprechen wir mit
Thorsten Hufnagel, Head of Lifetime Services &
Mitglied der Geschäftsleitung bei Sick in Düsseldorf.

GIT SICHERHEIT
Cybersicherheit: Studie zum Nutzen besserer
Integration von Sicherheitsmaßnahmen
Für die Studie „Capturing the cybersecurity dividend“
wurden von Juli bis September 2024 insgesamt 1.000
Führungskräfte aus 21 Branchen und 18 Ländern
befragt.

GSA 2026

VIP

Corporate Security

GIT SICHERHEIT AWARD 2026
Anmeldeschluss: 31. März
JETZT ANMELDEN!

**VIP-Interview: Dr. Alexandra
Forster, Konzernsicherheit Bayer**
GIT SICHERHEIT im Interview mit Dr.
Alexandra Forster, Leiterin
Konzernsicherheit bei der Bayer AG.

**Zur Strategie der
Konzernsicherheit bei Volkswagen**
Interview mit Andreas Maack, Leiter
Konzern Sicherheit & Resilienz und
Chief Security Officer (CSO) des
Volkswagen-Konzerns.

Produkte

U-Series
U-Series von i-Pro: KI-
Funktionen für alle
Sicherheitskameras

9000 1000
Digital-Beschlag
für Außenstüren
von SimonsVoss

9000 1000
Modulares
Taschenrucksack
erweitert

9000 1000
Denios entwickelt
Musterzug für Merck

9000 1000
Sicherheitsschuh
„Pain“ von Bauk

Beliebte Inhalte

Herausgeber

Wiley-VCH GmbH

Geschäftsführer

Dr. Guido F. Herrmann

Publishing Director

Dipl.-Betriebswirt Steffen Ebert

Wissenschaftliche

Schriftleitung

Dipl.-Verw. Heiner Jerofsky

(1991–2019) †

Anzeigenleitung

Mirjam Reubold

+49 6201 606 127

Sales Director

Jörg Willner

+49 6201 606 748

Redaktion

Dipl.-Betw. Steffen Ebert

+49 6201 606 709

Matthias Eler ass. iur.

+49 160 72 101 21

Dr. Timo Gimbel

+49 6201 606 049

Eva Kukatzki

+49 6201 606 761

Assistenz

Tina Renner

+49 6201 606 021

Textchef

Matthias Eler 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

Mirjam 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

Wiley-VCH GmbH

Boschstr. 12, 69469 Weinheim

Telefon +49 6201 606 0

E-Mail: git-gs@wiley.com

Internet: www.git-sicherheit.de

Verlagsvertretung

Dr. Michael Leising

+49 36 03 89 42 800

Bankkonten

J.P. Morgan AG, Frankfurt

Konto-Nr. 6161517443

BLZ: 501 108 00

BIC: CHAS DE FX

IBAN: DE5501108006161517443

GIT SICHERHEIT

Auflage: s. ivw.de

inkl. GIT Sonderausgabe PRO-4-PRO



Abonnement 2025

10 Ausgaben (inkl. Sonderausgaben)

122,30 €, zzgl. MwSt.

Einzelheft 17 € zzgl. Porto + MwSt.

Schüler und Studenten erhalten unter Vorlage einer gültigen Bescheinigung einen Rabatt von 50 %. Abonnement-Bestellungen gelten bis auf Widerruf; Kündigungen 6 Wochen vor Jahresende. Abonnementbestellungen können innerhalb einer Woche schriftlich widerrufen werden, Versandreklamationen sind nur innerhalb von 4 Wochen nach Erscheinen möglich. Alle Mitglieder der Verbände ASW, BHE, BID, BDSW, BDGW, PMeV, Safety Network International, vfdb und VfS 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 0948-9487



WILEY

DIE NÄCHSTE GENERATION SMARTER GEBÄUDEAUTOMATION

Zukunftssicher. Innovativ. Energieeffizient.

MADE IN GERMANY



**OHNE KABEL.
OHNE LIMITS.
MAXIMAL SICHER.**

Für Projekte jeder Größe!