35. JAHRGANG | Mai 2026 | AUSGABE 5 | 17 €

VSW Bundesverband Offizielles Organ für Verband für Sicherheit in der Wirtschaft e.V.

GIT SICHERHEIT

MAGAZIN FÜR SAFETY UND SECURITY

30 926

Ausgabe ONLINE lesen:

Titelthema Seite 94:

Cyber-Security für industrielle Infrastrukturen

Phoenix Contact: Neue EU-Vorgaben praktisch umgesetzt

35 JAHRE GIT SICHERHEIT JUBILÄUMSHEFT

WILEY

Securitas

„Wenn es um die Umsetzung des KRITIS-Dachgesetz geht, kommt es auf Erfahrung an. Seit über 30 Jahren sind wir in Deutschland am Markt – wir haben wertvolles operatives Wissen aufgebaut, Prozesse optimiert und Innovationen vorangetrieben. Viele tausend erfolgreiche umgesetzte Sicherheitskonzepte für Unternehmen jeder Größenordnung sprechen für sich.“

Björn Hawlitschka
Business Development Manager KRITIS

Das KRITIS-Dachgesetz gilt. Sind Sie bereit?

Profitieren auch Sie von unserer Expertise als Sicherheitspartner für KRITIS-Betreiber. Vereinbaren Sie jetzt einen Termin für Ihre Erstberatung und gehen Sie mit uns gemeinsam die erforderlichen Schritte der neuen KRITIS-Regulierung.

Vereinbaren Sie jetzt
Ihre Erstberatung

securitas.de/KRITIS

Für Sie immer on air: Patricia Reinhard, Dr. Timo Gimbel, Sylvia Heider, Miryam Reubold, Matthias Erler, Steffen Ebert, Claudia Vogel (v. l.). Nicht im Bild, dafür im Home Office und ebenfalls stets leidenschaftlich für Sie am Ball: Tina Renner (Assistenz), Andi Kettenbach (Layout), Dr. Michael Leising (Media) und Dr. Ralf Schlichting (Online)

35 JAHRE GIT SICHERHEIT Leidenschaft Sicherheit

35 Jahre GIT SICHERHEIT – das ist mehr als ein Anlass zum Zurückblicken. Es ist ein Beweis für Kontinuität in einer Branche, die sich ständig neu erfindet. Seit 1991 begleiten wir die Welt der Sicherheit als unabhängiges Fachmedium – mal erklärend, mal einordnend, immer mit dem Anspruch, Relevantes von Beliebigem zu trennen.

Gerade unser Thema Sicherheit hat in diesen 35 Jahren einen bemerkenswerten Wandel erlebt. Mechanik, Melder und Kameras sind längst Teil vernetzter Sicherheitsarchitekturen geworden. Zutrittskontrolle bedeutet heute Identitätsmanagement, Perimeterschutz schließt Drohnenabwehr ein, Videoanalyse denkt in Mustern und Kontexten. Sicherheit ist komplexer geworden – aber auch strategischer, integrierter und wirksamer. Oder anders gesagt: Sie kann heute sehr viel mehr, als nur Alarm auslösen.

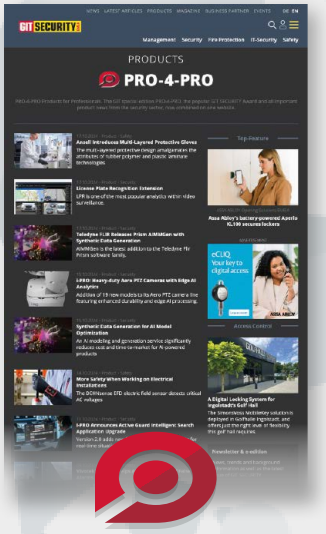
Diese Jubiläumsausgabe greift genau das auf. Im Management-Teil beleuchten wir unter anderem hybride Bedrohungslagen und deren Auswirkungen auf den Wirtschaftsschutz sowie integrierte Sicherheitskonzepte für kritische Infrastrukturen. Lesen Sie dazu auch unser ausführliches Gespräch mit Dr. Patrick Hennies, Chief Security Officer der Deutschen Bahn, über Resilienz, Kooperation und Sicherheit auf Europas Schienen.

Im Security-Ressort stehen konkrete Anwendungen im Fokus – von moderner Zutritts- und Videosicherheit über Drohnen- und Perimeterschutz bis hin zu unabhängigen Tests und Praxisprojekten. Die Titelstory zeigt, warum die Verzahnung von physischer und digitaler Sicherheit kein Trend, sondern Voraussetzung ist. Zentrale Botschaft des CSO-Interviews mit Thomas Tschersich von der Deutschen Telekom: Richtlinien allein halten keine Angreifer auf – Wirkung entsteht durch Risikoorientierung, Integration und konsequente Umsetzung. Brandschutz, Maschinen- und Anlagensicherheit sowie Arbeitsschutz machen deutlich, wie sehr Technik, Organisation und Verantwortung heute zusammenspielen – und warum der Mensch dabei stets im Mittelpunkt bleibt.

Unser Dank gilt Ihnen, den Leserinnen und Lesern, Autorinnen und Autoren, Interviewpartnern sowie Werbepartnern – und all jenen, die diese Jubiläumsausgabe mit Glückwünschen und Beiträgen bereichert haben. Ohne diese Ihre Treue wäre es uns als Team nicht möglich gewesen, seit 35 Jahren Ihr Medium Nummer eins zu werden und zu bleiben. Ihr Vertrauen ist für uns Verpflichtung und Ansporn zugleich, auch künftig beste Arbeit zu leisten.

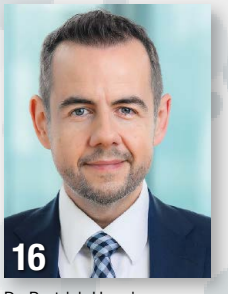
Denn Sicherheit ist für uns – und sicher auch für Sie – das spannendste Thema überhaupt: mal atemberaubend, mal über- oder mindestens herausfordernd, bei gelungenen Projekten auch so sehr zufrieden machend und erfüllend. Mal auch einfach Rock 'n' Roll, großes Tennis oder schlicht nur krass. Und noch so viel mehr. Aber: immer relevant. GIT

Ein Großes Dankeschön an
Sie sagt ganz herzlich
Ihr Team GIT SICHERHEIT



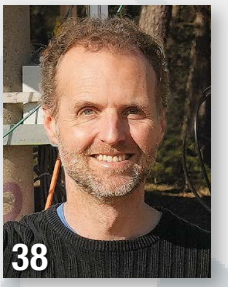
GIT-SICHERHEIT.DE/DE/PRODUKTE
PRODUCTS FOR PROFESSIONALS
Produkt- und Lead-Plattform für Sicherheit

Sven Horstmann



Dr. Partrick Hennies

Johannes Hölzl



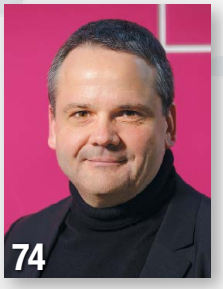
David Sonntag

MANAGEMENT

TRENDBERICHTE

Mario Nolle

Aljona Götter



Thomas Tschersich

SECURITY

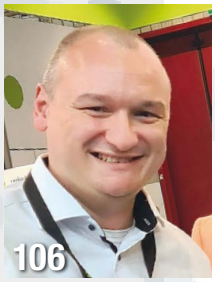
TRENDBERICHTE

CYBER-SECURITY

INDEX

QUICK-FINDER

ORGANISATIONEN, INSTITUTIONEN UND UNTERNEHMEN IM HEFT



Wolfgang Onderka

Franca Hopf

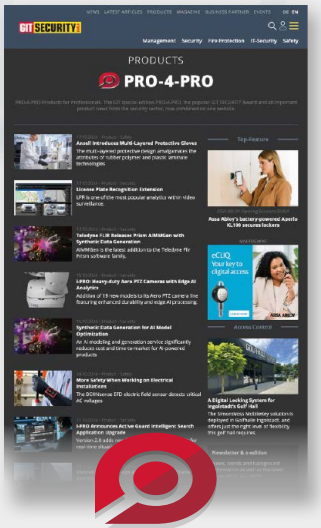
Jan Undermann

Hendrik van Elten

David Bastias

81 INNENTITEL
Who Guards the Guardian

Wie Feuerwehrgerätehäuser technisch wirksam abgesichert werden könne



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

BRANDSCHUTZ

INNENTITEL

BRANDMELDEANLAGEN

81 Who Guards the Guardian
Wie Feuerwehrgerätehäuser technisch wirksam abgesichert werden können

FEUERWEHR

86 Taktgeber Technik
Parlamentarischer Abend des VDMA Feuerwehrtechnik

TRENDBERICHTE

84 Ein dynamischer Markt
Trendbericht von Steffen Springer, Geschäftsführer der Wagner Group

88 Von Compliance zu intelligenter, vernetzter Sicherheit
Brandschutz im Wandel: Trendbericht von Klaus Hirzel, Business Leader Europe Central Region (DACH) bei Honeywell Fire Products

90 Brandschutz im Wandel
Marion Heidrich, Operations Director Gloria, über Trends, Technologie und Zukunft der Branche

SAFETY

TITELTHEMA

94 Pflicht zur Umsetzung nachweisbarer Security-Maßnahmen
Wie industrielle Netzwerke widerstandsfähiger gegen Cyber-Angriffe gestaltet werden

MASCHINEN- UND ANLAGENSICHERHEIT

98 Zukunftssicher mit ASi-5
Warum Anwender von der neuen ASi Generation vielfach profitieren

100 Smarte Schwingungsmessung
Fehler erkennen, bevor sie entstehen

HYGIENEKRITISCHE PRODUKTIONSUMGEBUNGEN

102 Keine Chance für Keime
Wie sich HMI-Systeme und Bedienelemente hygienegerecht und normkonform auslegen lassen.

MASCHINEN- UND ANLAGENSICHERHEIT

106 Cybersecurity in der Praxis: Was Sie jetzt wissen müssen
Bedeutung von MVO und CRA für Risikobeurteilung, OT-Security und Dokumentationsprozesse im Maschinenbau

PSA

110 Workwear, die weiterdenkt
Blåkläder: Von Eigenproduktion, Material-Updates und der Frage, was moderne PSA wirklich leisten muss

SICHERHEITSSCHUHE

112 „Mutig bleiben, ohne leichtfertig zu werden“
Elten im Wandel zwischen Familienwerten und Internationalisierung

PSA

116 Sicherheit mit Hand und Fuß
Wie Ejendals Hand- und Fußschutz unter regulatorischem Druck, Lieferkettenrisiken und Nachhaltigkeitszielen weiterentwickelt

HSE-MANAGEMENT

118 Von Transport bis Recycling
Fünf Wege, wie HSE-Manager nachhaltigere Entscheidungen im Bereich PSA treffen können

EINSATZSTIEFEL

120 Jedes Gramm am Fuß zählt
Warum Komfort, Feuchtigkeitsmanagement und neue Materialien im Defence-Bereich immer wichtiger werden

RUBRIKEN

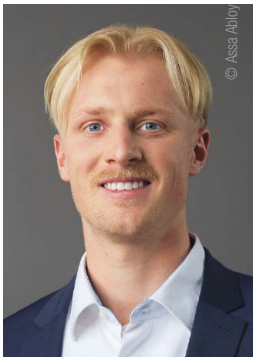
Assa Abloy: Warum zur Cyber-Resilienz auch die Tür gehört

Die Assa Abloy Sicherheitstechnik GmbH nimmt vom 11. bis 13. Mai 2026 erneut am NIS-2-Congress in Frankfurt teil. Im Mittelpunkt des Auftritts steht ein Workshop zur Frage, warum Unternehmen im Zuge von NIS2 nicht nur ihre digitalen Systeme, sondern auch den physischen Zugang zu sensiblen Bereichen konsequent absichern müssen. Der Kongress versteht sich als IT-Security-Dialog für Unternehmen und erwartet in diesem Jahr rund 700 Teilnehmer, mehr als 50 Fach- und Praxisvorträge sowie 16 Workshops.

Der Zeitpunkt der Fachveranstaltung könnte kaum besser gewählt sein, denn seit Ende letzten Jahres ist die EU-Cybersicherheitsrichtlinie NIS2 auch in Deutschland in Kraft. Mehr noch: Anfang März lief beim BSI die Registrierungspflicht für Unternehmen ab, die von dem neuen Gesetz zur Umsetzung der NIS2-Richtlinie betroffen sind.

Seitdem häufen sich Medienbeiträge darüber, dass die Mehrzahl der Unternehmen diesen Schritt verpasst hat – obwohl der rechtliche Schutz für Nachzügler nun weggefallen ist und Bußgelder sowie verschärfte Kontrollen drohen. Das macht deutlich, wie groß der Nachholbedarf bei Umsetzung, Verantwortlichkeiten und Sicherheitsstrategie in vielen Organisationen weiterhin ist.

Miriem Ajouri verantwortet als Business Development Managerin bei Assa Abloy den Bereich Industrie



Business Development Manager Felix Steinhausen betreut gemeinsam mit den Kollegen des Assa Abloy KRITIS-Teams den Bereich Sicherheit Kritischer Infrastrukturen

Der Workshop von Assa Abloy setzt genau dort an und greift einen weiteren wichtigen Aspekt auf, der in Compliance, Cybersecurity und Resilienz oft unterschätzt wird: Sicherheitskonzepte bleiben lückenhaft, wenn sie sich allein auf Netzwerke, Endpunkte und Prozesse konzentrieren, nicht aber auf Türen, Zutritte und reale Infrastrukturen. Entgegen der weitverbreiteten Annahme stellt NIS2 auch starke Anforderungen an die physische Zutrittskontrolle.

Eine isolierte Betrachtung digitaler Risiken greift damit zu kurz. Überall dort, wo Verfügbarkeit, Schutz kritischer Bereiche und nachvollziehbare Zugriffssteuerung entscheidend sind, gilt es ganzheitliche Strategien zu entwickeln, die IT-Sicherheit, Organisation und physische Absicherung zusammendenken.

Am 12. Mai, 11:45 Uhr, demonstrieren die beiden Assa Abloy Business Development Manager Miriem Ajouri und Felix Steinhausen in ihrem Workshop daher, wie sich digitale und physische Sicherheitswelten mit elektronischen Schließanlagen manipulationssicher, skalierbar und regelkonform verbinden lassen. Der Titel bringt es auf den Punkt: „Wenn Angreifer durch die Tür kommen, hilft keine Firewall: Warum physische Sicherheit genauso geschützt sein muss wie Netzwerke."

www.assaabloy.com/de

Frequentis: Starkes Wachstum bei Umsatz, Ergebnis und Jobs

Frequentis verzeichnete 2025 das fünfte Jahr in Folge ein zweistelliges Wachstum. Der Umsatz stieg um 20,8 % auf EUR 580,1 Mio., das Ebit erhöhte sich um fast die Hälfte auf EUR 46,8 Mio. bei einer Ebit-Marge von 8,1 %. Die eingegangenen Aufträge stiegen um 16,5 % oder fast EUR 100 Mio. auf EUR 680,2 Mio. Und die Nachfrage bleibt unverändert hoch: Der Auftragsstand konnte gegenüber dem Wert des Vorjahrs noch einmal um über ein Drittel auf fast EUR 800 Mio. (EUR 794,9 Mio.) gesteigert werden. Mit Blick auf diese starke Auslastung wurde der Personalstand weltweit um mehr als 200 Mitarbeiter erhöht. „Unser Wachstum und die Profitabilität zeigen, dass unser Geschäftsmodell nachhaltig trägt – gerade in herausfordernden Zeiten", sagt Frequentis-CEO Norbert Haslacher. „Vor allem aber sind sie das Ergebnis des außergewöhnlichen Engagements unserer rund 2.600 Mitarbeiter weltweit."

Norbert Haslacher, CEO von Frequentis

www.frequentis.com

35 JAHRE GIT SICHERHEIT

35 Jahre GIT SICHERHEIT – das ist nicht einfach nur ein Jubiläum. Es ist ein Beleg dafür, dass unabhängiger, praxisnaher Fachjournalismus im Sicherheitsbereich unverzichtbar ist. Als Unternehmen, das selbst in diesem Jahr seinen 40. Geburtstag feiert, wissen wir: Wer so lange am Markt besteht, hat immer wieder neu bewiesen, dass er gebraucht wird. Das hat die GIT SICHERHEIT eindrucksvoll getan – als kritische Stimme, als Wissensplattform und als verlässlicher Partner für alle, die Sicherheit nicht als Pflichtübung, sondern als Haltung verstehen.

Wir gratulieren herzlich und freuen uns auf die nächsten gemeinsamen Jahrzehnte.

Horst Rose / Managing Director (CSO) / DENIOS SE / Bad Oeynhausen

Das Geutebrück Management-Team (v.l.n.r.): Dr. Christian Gutzen, Alica Shahino-Hoffmann, Chris Trier-Schürholz und Tobias Hümmerich

Geutebrück richtet Führung neu aus

Die Geutebrück GmbH stellt ihr erweitertes Management-Team vor und setzt damit ein deutliches Signal für strategische Weiterentwicklung, internationalen Ausbau und nachhaltiges Wachstum im Markt für Video- und Sicherheitstechnologie. Neben der weiterhin aus Katharina Geutebrück und Christoph Hoffmann bestehenden Geschäftsführung verantworten vier Führungskräfte zentrale Schlüsselbereiche des Unternehmens. Neu im Führungsteam sind Alica Shahino-Hoffmann (Chief Financial Officer) und Chris Trier-Schürholz (Chief Sales Officer). Alica Shahino-Hoffmann stärkt als CFO die finanzielle Stabilität und strategische Steuerung des Unternehmens. Sie schafft die Grundlage, um Wachstumsvorhaben entschlossen umzusetzen und Investitionen in Zukunftstechnologien zu fördern. Bereits seit einiger Zeit verstärken Tobias Hümmerich (Chief Technology Officer) und Dr. Christian Gutzen (Chief Strategy Officer) das Management-Team. **www.geutebrueck.com**

Nvidia und Milestone Systems intensivieren Zusammenarbeit

Edward Mauser, Director von Project Hafnia bei Milestone Systems

Milestone Systems und Nvidia intensivieren ihre Zusammenarbeit im Bereich Vision AI. Milestone Systems hat neue Erweiterungen seiner KI-Plattform Hafnia vorgestellt – darunter synthetische Trainingsdaten, ein neues Training-as-a-Service-Angebot sowie für den EU-Markt optimierte Visual Language Models für Verkehrsanalysen. Ziel ist es, Entwicklern und Städten den Zugang zu leistungsfähiger Smart-City-KI zu erleichtern. Durch die Kombination aus realen und synthetischen Daten können KI-Modelle künftig auch für seltene oder bislang unbekannte Szenarien trainiert werden – etwa ungewöhnliche Verkehrssituationen oder extreme Wetterlagen. Damit adressieren Milestone Systems und Nvidia eine zentrale Herausforderung vieler KI-Systeme: Trainingsdaten bilden solche Ereignisse oft nur unzureichend ab. Die neuen Modelle werden bereits mit ersten europäischen Städten getestet. **www.milestonesys.com**

Primion Technology GmbH akquiriert die Primion AG Schweiz

Die Primion Technology GmbH mit Sitz in Süddeutschland hat sämtliche Anteile an der Primion AG mit Sitz in Tuggen, Kanton Schwyz, übernommen. Damit wird die seit Jahren bestehende enge Zusammenarbeit innerhalb der Primion Group auf eine neue, konsolidierte Grundlage gestellt. Die Primion AG wurde am 31. Januar 2002 gegründet, um die Lösungen der Primion Group noch näher an die Schweizer Kundschaft heranzutragen. Seither ist das Unternehmen als eigenständiger Anbieter in den Bereichen Zutrittskontrolle, Zeitwirtschaft, Besucherverwaltung und Sicherheitsmanagement tätig und fokussiert auf den Markt der Schweiz und des Fürstentums Liechtenstein. Mit ihrem inhabergeführten, persönlichen Ansatz hat die Primion AG eine starke regionale Verankerung aufgebaut und sich als zuverlässiger Partner für Unternehmen unterschiedlicher Größen und Branchen etabliert. **www.primion.io**

Die GIT SICHERHEIT ist für mich wichtig, weil sie als führende Fachpublikation genau die Entscheider erreicht, die für einen wirksamen Wirtschaftsschutz entscheidend sind – von Unternehmen über Sicherheitsverantwortliche bis hin zu Politik und Verwaltung – und damit eine zentrale Plattform bietet, um sicherheitspolitische Entwicklungen einzuordnen, Bewusstsein zu schaffen und den Dialog zwischen allen relevanten Akteuren im Sinne einer starken gesamtstaatlichen Sicherheitsarchitektur zu fördern.

Johannes Strümpfel, Präsident des Verbands für Sicherheit in der Wirtschaft, Bundesverband e.V. – VSW-Bundesverband

35 JAHRE GIT SICHERHEIT

VISION

Innerhalb der nächsten zehn Jahre werden wir im Bereich der Sicherheit durch die Integration von physischer und Cybersicherheit Angriffe frühzeitig erkennen, schneller reagieren und besser mit neuen Unsicherheiten umgehen können.

Lars Findorff,
Trumpf SE + Co. KG und
ASW-BW Vorstandsmitglied

35 JAHRE GIT SICHERHEIT

VdS-Fachtagung „KRITIS: Wo steht Deutschland?“

Deutschland muss resilienter gegen Angriffe aller Art werden, da sind sich die Experten einig. Was aktuell ansteht, erläutert die neue VdS-Fachtagung am 6. Mai 2026 in Köln und online im Livestream.

Erst Anfang dieses Jahres hat es der Stromausfall in Berlin, ausgelöst durch einen Brandanschlag, deutlich gezeigt: Kritische Infrastruktur in Deutschland ist nicht umfassend geschützt – und sie kann im Zweifel nach einem Vorfall nicht so schnell wieder instandgesetzt werden, wie bisher angenommen. Grund genug, mehr Bewusstsein für die Notwendigkeit zu schaffen, sich mit möglichen Krisen und dem Aufbau von Resilienz zu beschäftigen.

Nachdem die VdS-Fachtagung KRITIS, Teil 1 im vergangenen Herbst den Fokus auf Unternehmen und Service-Leitstellen gelegt hatte, nimmt die „VdS-Fachtagung KRITIS: Wo steht Deutschland?“ am 6. Mai 2026 – in Köln und im Livestream – die Gesamtsituation in den Blick. Sie zeigt: Es ist einiges im Umbruch, viele Fragen müssen neu gestellt und beantwortet werden. Und das geht nicht ohne intensiven Austausch zwischen allen Beteiligten.

Neues KRITIS-Dachgesetz

Die VdS-Fachtagung geht unter anderem auf das neue KRITIS-Dachgesetz ein, dessen Entwurf kürzlich im Bundestag beschlossen wurde. Der Gesetzesentwurf wird aus zahlreichen Perspektiven betrachtet und diskutiert. Dabei kommen Vertreter unterschiedlicher Sektoren zu Wort, zum Beispiel von Versicherungen, KRITIS-Betreibern, Sicherheitsdienstleistern, öffentlichen Institutionen und Herstellern von Sicherungstechnik.

Widerstandsfähige Sicherungsketten

Die Fachtagung geht der Frage nach, wie zeitgemäße Sicherungsketten robuster aufgebaut und betrieben werden können: Welche Chancen und Risiken stecken beispielsweise in Cloud-basierten Ansätzen für die Alarmübertragung und im Plattformvernetzten Gefahrenmanagementsystem? Hat der Begriff des barrierefreien Handlings in der Leitstelle eine praktische Bedeutung, also Rettungskonzepte, die Sicherheit und Barrierefreiheit verbinden? Und wie passt künstliche Intelligenz (KI) in diese Umgebung?

Es wird aufgezeigt, wie sich alle Sicherungsgewerke, wie Einbruchmeldeanlagen, Brandmeldeanlagen, die Zutrittskontrolle und Videoüberwachung, auf einer Plattform zusammenführen lassen und wie dabei echte Mehrwerte für die Gefahrenabwehr entstehen. Auch die Problematik der Cyber-Sicherheit auf der gesamten Sicherungskette wird behandelt und gezeigt, welche Zertifikate wichtig und notwendig sind. Die Fachtagung richtet sich an alle, die sich mit der Sicherheit von Unternehmen und Institutionen beschäftigen, darunter

www.vds.de

EVENT

BVSW Wintertagung 2026

Hybride Bedrohungen, geopolitische Umbrüche und ihre Folgen für Wirtschaft und Sicherheit

Zum 14. Mal hat der Bayerische Verband für Sicherheit in der Wirtschaft (BVSW) Expertinnen und Experten aus Wirtschaft, Wissenschaft und Behörden zum Get-Together am malerischen Spitzingsee geladen. Wie im vergangenen Jahr standen auch im diesen Jahr die geopolitischen Entwicklungen rund um den Globus, die volatile Sicherheitslage im Inneren sowie im Ausland und die Ausweitung hybrider Bedrohungen im Fokus. Sicherheit ist kein isoliertes Fachthema mehr, sondern eine strategische Querschnittsaufgabe für Unternehmen, Staat und Gesellschaft – so der Tenor.

Die internationale Lage und das Verhältnis Europas zu den Großmächten USA, China und Russland bildeten den übergeordneten Rahmen. Zugleich wurde deutlich, dass hybride Angriffe nicht nur auf Infrastrukturen und Unternehmen zielen, sondern auch auf Vertrauen, gesellschaftlichen Zusammenhalt und die Funktionsfähigkeit demokratischer Institutionen.

Innere Sicherheit und Cybercrime als Ausgangspunkt

Zum Auftakt beleuchtete Michael Schwald, Landespolizeipräsident Bayern, die Sicherheitslage im Freistaat. Während die objektive Lage weiterhin als stabil beschrieben wurde, nimmt das subjektive Unsicherheitsgefühl zu. Cybercrime stellte einen Schwerpunkt dar: Ransomware, DDoS Angriffe, Social Engineering und Phishing sind längst betriebliche Risiken und treffen zunehmend auch mittelständische Unternehmen. Schwald verwies auf spezialisierte polizeiliche Anlaufstellen und unterstrich die Bedeutung frühzeitiger Kooperation zwischen Wirtschaft und Sicherheitsbehörden.

Diese Perspektive vertiefte Manfred Hauser, Präsident des Bayerischen Landesamts für Verfassungsschutz. Er ordnete die aktuelle Lage als Multikrise ein, in der kriminelle und staatliche Akteure – insbesondere im Cyberraum – zunehmend ineinandergreifen. Hybride Bedrohungen zielten nicht nur auf wirtschaftlichen Schaden, sondern auf Vertrauen, Ordnung und demokratische Stabilität. Themen wie Spionage, Wissensabfluss, Desinformation und persönliche Bedrohungen exponierter Personen wurden als relevante Risiken für Unternehmen benannt.

Geopolitik und strategische Verschiebungen

Den zweiten Konferenztag eröffnete Prof. Dr. Gunther Schmidt mit einem geopolitischen Überblick. Seine Analyse zeichnete das Bild einer zunehmend instabilen Weltordnung, in der zwischenstaatliche Gewalt an Bedeutung gewinnt und Systemkonflikte offen ausgetragen werden. Handel, Technologie und Abhängigkeiten seien sicherheitspolitisch aufgeladen. Für Unternehmen bedeutet dies, dass Lieferketten, Marktstrategien und Technologiepartnerschaften nicht mehr losgelöst von geopolitischen Risiken betrachtet werden können.

Wie schnell solche Risiken operativ wirksam werden, zeigte Carsten Baeck (DRB Deutsche Risikoberatung) am Beispiel eines Stromausfalls in Berlin. Der Vorfall offenbarte Defizite in Krisenmanagement, Redundanz und Kommunikationsfähigkeit. Besonders deutlich wurde die Trennung zwischen kurzfristiger Wieder¬versorgung und langfristiger Wiederherstellung – ein Hinweis darauf, dass Resilienz langfristig geplant werden muss.

Die strategische Dimension digitaler Abhängigkeiten griff Prof. Timo Kob, Professor für Wirtschaftsschutz und Cybersicherheit, auf. Er plädierte für klare Prioritäten statt breiter Ambitionsprogramme. Digitale Souveränität sei weniger eine Frage perfekter Lösungen als strategischer Entscheidungen und bewusster Abwägungen.

Zukünftige Szenarien hybrider Bedrohungen skizzierte Dr. Konstantinos Tsetsos.

Er beschrieb eine Entwicklung, in der physische und psychokognitive Angriffe zunehmend verschmelzen. Für Unternehmen leitete er daraus die Notwendigkeit ganzheitlicher Resilienz ab – organisatorisch, technisch und kognitiv.

Governance, Ethik und strategische Koordination

Der dritte Konferenztag rückte ordnungspolitische und Governance Fragen in den Mittelpunkt. Christina Moritz griff dabei die Rolle des Nationalen Sicherheitsrats auf, der seit 2025 als ressortübergreifendes Koordinierungsgremium der Bundesregierung besteht. Im Fokus stand nicht seine Existenz, sondern die Frage, wie seine Arbeitsweise effizienter und reaktionsschneller gestaltet werden kann. Diskutiert wurden insbesondere klarere Entscheidungswege, eine stärkere strategische Verzahnung der beteiligten Ressorts sowie eine intensivere Vernetzung mit Wirtschaft und Sicherheitsbehörden.

Einen wirtschaftsethischen Akzent setzte Prof. Dr. Nils Goldschmidt (Weltethos Institut). In seinem Beitrag stellte er die Frage nach Verantwortung und Wettbewerb in einer zunehmend fragmentierten Welt. Sicherheit und Resilienz seien nicht nur technische oder organisatorische Themen, sondern auch normative Fragen, die unternehmerisches Handeln prägen.

Den Zusammenhang zwischen Innovation, Regulierung und Sicherheit beleuchtete PD Dr. habil. M. Britta Stumbaum (The SPEAR Institute) am Beispiel staatlich getriebenen Technologietransfers. Exportkontrollen, Schutz sensibler Schlüsseltechnologien und internationale Kooperationen wurden als Spannungsfelder beschrieben, die für Unternehmen zunehmend sicherheitsrelevant sind.

Michael Schwald, Landespolizeipräsident Bayern, und Manfred Hauser, Präsident des Bayerischen Landesamts für Verfassungsschutz, stehen dem Auditorium am ersten Abend der BVSW-Wintertagung Rede und Antwort

Markus Klaedtke, Vorstandsvorsitzender des Bayerische Verband für Sicherheit in der Wirtschaft, bei der Eröffnung der BVSW-Wintertagung 2026

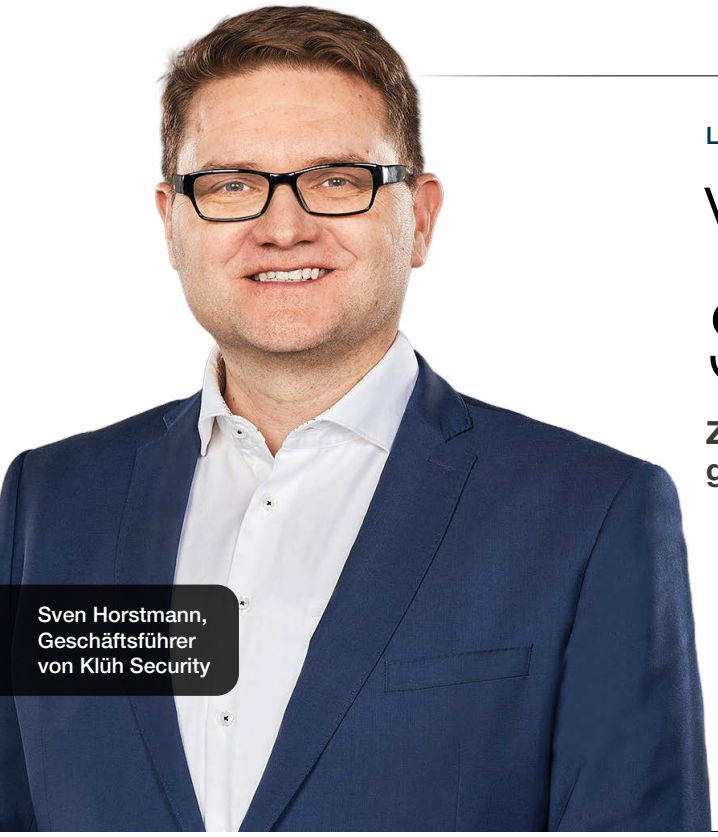
Den inhaltlichen Abschluss der Wintertagung bildete der traditionelle Beitrag von Dr. Benedikt Franke, CEO der Münchner Sicherheitskonferenz. Er ordnete die Diskussionen in den internationalen sicherheitspolitischen Kontext ein und betonte, dass Sicherheit nur als Verbundaufgabe von Staat, Wirtschaft und Wissenschaft tragfähig ist. Entscheidend seien gemeinsame Lagebilder, strategische Vorausschau und schnellere Entscheidungsprozesse über institutionelle Grenzen hinweg.

Bilanz und Ausblick: Sicherheit gemeinsam weiterdenken

Mit Blick auf die kommende BVSW Wintertagung 2027 zeichnet sich ab, dass diese Fragen weiter an Bedeutung gewinnen werden. Die internationale Lage bleibt angespannt, hybride Bedrohungen entwickeln sich dynamisch weiter und die Anforderungen an Vernetzung und Reaktionsgeschwindigkeit steigen. Der Spitzingsee wird damit auch künftig ein zentraler Ort bleiben, um sicherheitsrelevante Entwicklungen einzuordnen, Erfahrungen auszutauschen und gemeinsame Perspektiven zu entwickeln.

Die BVSW Wintertagung hat sich als fester Orientierungspunkt der Sicherheitsbranche etabliert – und lädt auch 2027 dazu ein, Sicherheit gemeinsam weiterzudenken und aktiv mitzugestalten. GIT

Bayerischer Verband für Sicherheit in der Wirtschaft (BVSW) e. V.
www.bvsw.de



Sven Horstmann, Geschäftsführer von Klüh Security

LEITSTELLEN

Validierte Sicherheit

Zertifizierte Leitstelle von Klüh Security gewinnt erste Partner und Kunden

Die integrierte Alarmempfangsstelle (AES) und Notruf- und Serviceleitstelle (NSL) von Klüh Security ist jetzt nach VdS 3138 und VdS 3137/DIN EN 50518, DIN EN 17483-1 (Private Sicherheitsdienstleistungen – Schutz kritischer Infrastrukturen) und ISO 27001 zertifiziert.

Die VdS-Zertifizierung bestätigt die normgerechte Auslegung und den zuverlässigen Betrieb der Alarmempfangsstelle nach VdS 3137/DIN EN 50518 – einschließlich definierter Anforderungen an technische Infrastruktur, organisatorische Abläufe und die strukturierte Verarbeitung von Alarm- und Notrufmeldungen. Die Zertifizierung nach DIN EN 17483-1 belegt, dass die Dienstleistung von Klüh Security auch den speziellen Anforderungen an einen Sicherheitsdienstleister in Zusammenhang mit kritischen Infrastrukturen gerecht wird und für besonders sicherheitskritische Umgebungen eingesetzt werden kann.

Ergänzend dokumentiert die ISO 27001-Zertifizierung, dass das Unternehmen ein umfassendes und auditierbares Informationssicherheitsmanagement etabliert hat, das den Schutz sensibler Daten und Prozesse gewährleistet. Näheres erfuhr GIT SICHERHEIT von Sven Horstmann, Geschäftsführer bei Klüh Security.

Die Zertifizierung bestätigt, dass die Alarmempfangsstelle und Notruf- und Serviceleitstelle höchsten technischen und organisatorischen Anforderungen entsprechen

GIT SICHERHEIT: Herr Horstmann, welche konkreten Vorteile bringt die jetzt zertifizierte AES/NSL Ihren Kunden – insbesondere in hochsensiblen KRITIS-Umgebungen?

Sven Horstmann: Die Zertifizierung bestätigt, dass unsere Alarmempfangsstelle und Notruf- und Serviceleitstelle höchsten technischen und organisatorischen Anforderungen entsprechen. Für Betreiber kritischer Infrastrukturen bedeutet das vor allem operative Verlässlichkeit: Sicherheitsrelevante Ereignisse werden strukturiert bewertet, priorisiert bearbeitet und revisionssicher dokumentiert.

Mit den Zertifizierungen erfüllen wir zentrale Anforderungen an Leitstellenbetrieb, KRITIS-Schutz und Informationssicherheit. Unsere Kunden können sich darauf verlassen, dass Technik und Prozesse regelmäßig geprüft werden und aktuellen regulatorischen Vorgaben entsprechen.

Gleichzeitig bleibt das Modell flexibel: Unternehmen können eigene Leitstellen betreiben, diese durch unsere Infrastruktur erweitern oder Leitstellenleistungen vollständig an uns auslagern.

Welche Rolle spielen moderne Technologien wie KI-gestützte Alarmfilterung, IoT-Anbindung oder Drohnentechnik im operativen Alltag der neuen Leitstelle?

Sven Horstmann: Technologie spielt eine zentrale Rolle, weil sie die strukturierte Verarbeitung der wachsenden Menge sicherheits- und betriebsrelevanter Daten ermöglicht. In modernen Gebäuden entstehen kontinuierlich Meldungen aus unterschiedlichen Systemen – etwa aus Zutrittskontrolle, technischer Sensorik oder Videoanalyse.

Das technologische Fundament unserer Leitstelle bildet die von unserem Partner

Advancis bereitgestellte Plattform WinGuard. Sie führt diese Informationen in einer gemeinsamen Steuerungsumgebung zusammen und stellt sie in einem konsolidierten Lagebild dar. Ereignisse lassen sich so schneller einordnen und Maßnahmen koordiniert einleiten.

Intelligente Alarmfilter helfen, Datenmengen zu priorisieren und Fehlalarme zu reduzieren. Die Bewertung und Eskalation sicherheitsrelevanter Ereignisse bleibt dabei bewusst in der Verantwortung qualifizierter Leitstellenmitarbeitender.

Mit seiner Alarmempfangsstelle (AES) und Notruf- und Serviceleitstelle (NSL) will Klüh Security einen neuen Standard für technologiegestützte Sicherheitslösungen setzen

GIT SICHERHEIT hat Ihr hochvernetztes Leitstellen-Ökosystem bereits ausführlich in Heft 3/26 vorgestellt – inklusive KI-gestützter Alarmfilterung, NIS2-Konformität, DORA-Vorgaben und der engen Kooperation mit TAS. Welche strategischen Schritte planen Sie nun, um dieses Ökosystem in den nächsten zwölf Monaten weiter auszubauen und technologisch wie organisatorisch noch resilienter zu machen?

Sven Horstmann: Resilienz entsteht aus dem Zusammenspiel von Technologie, Organisation und qualifiziertem Personal. Unsere Leitstelle ist redundant ausgelegt und als skalierbares Betriebsmodell konzipiert, sodass wir flexibel auf Störungen und wachsende Anforderungen reagieren können.

Ein Schwerpunkt liegt auf der Auswertung von Ereignis- und Betriebsdaten, um Risiken frühzeitig zu erkennen und Prozesse kontinuierlich zu optimieren. Parallel investieren wir in klare Entscheidungs- und Notfallstrukturen sowie die Qualifizierung unserer Mitarbeitenden. Die Weiterentwicklung der Plattform erfolgt eng mit Partnern, um neue Anforderungen schnell in stabile Betriebsprozesse zu überführen.

Unser Ziel ist eine verlässliche Steuerungsinstanz für Sicherheit und Betriebsprozesse – besonders in komplexen, regulierten Infrastrukturen. GIT

Klüh Service Management GmbH
www.klueh.de

© Bilder: Klüh

35 JAHRE GIT SICHERHEIT STATEMENT

Predictive Security

Von Jürgen Wittmann, Vice President Corporate Security bei der Robert Bosch GmbH und Präsident ASW-BW

© Bild: ASW-BW

Die Sicherheitswelt hat sich von einem Fokus auf physische Sicherheit (z. B. Objektschutz) hin zu einem integrierten Ansatz entwickelt, der Cyber-Angriffe, Desinformationskampagnen und geopolitische Instabilitäten als gleichwertige Risiken betrachtet.

Die einschneidendsten Entwicklungen bestehen in der Zunahme von staatlich gesteuerten Cyberangriffen und gezielten Desinformationskampagnen, die nicht nur auf IT-Systeme, sondern auf die Reputation und das Vertrauen in Unternehmen abzielen.

Die Reise geht klar in Richtung „Predictive Security“. Wir müssen lernen, potenzielle Krisen (z. B. durch Social Media Monitoring und KI-Analysen) frühzeitig zu erkennen. Resilienz wird nicht mehr nur technisch, sondern auch organisatorisch und kulturell im Unternehmen verankert werden müssen (Stichwort: Business Continuity Management 2.0). GIT

ASW Baden-Württemberg
www.asw-bw.com

Keine Sicherheit ohne sichere Kommunikation

Ein Trendbericht von Bernhard Klinger, Vorsitzender des Bundesverbands Professioneller Mobilfunk (PMeV)

Wir stehen vor geopolitischen, sicherheitspolitischen, wirtschaftlichen und klimatischen Herausforderungen, die sich stetig zuspitzen. In diesen Zeiten akuter Bedrohungen durch Cyberangriffe, militärische und wirtschaftliche Kriege und Konflikte sowie Naturkatastrophen ist eine sichere und hochverfügbare Kommunikation wichtiger denn je. Auch Politik, Wirtschaft und Gesellschaft spüren das: Die Akzeptanz von Investitionen in Sicherheit ist gestiegen – und dies gilt auch für sicherheitskritische Kommunikationssysteme. Zunehmend an Bedeutung gewinnt zudem die zivil-militärische Zusammenarbeit im Bereich der Interdisziplinären mobilen Kommunikation.

In der heutigen Situation gilt mehr denn je: Ohne sichere Kommunikation gibt es keine Sicherheit. Ohne verlässliche und hochverfügbare Kommunikationsnetze gibt es keine Resilienz. Und ohne Resilienz gibt es weder einen souveränen und handlungsfähigen Staat noch eine arbeits- und leistungsfähige Wirtschaft. Ohne kritische Kommunikation würde unser Land stillstehen. Wenn sie funktioniert, fällt sie nicht auf. Doch wenn sie ausfällt, fehlt der entscheidende Faktor – für Leben, für Sicherheit, Versorgung und damit für das Funktionieren des Staates. Die Branche für kritische Kommunikation ist daher nicht nur ein technologisches Ökosystem – sie ist ein strategisch relevantes Ökosystem. Sie stärkt die Handlungsfähigkeit unseres Landes und steht für ein sicheres und resilientes Europa.

Digitalisierung

Zu den wichtigsten branchenrelevanten technologischen Entwicklungen der vergangenen Jahre zählt vor allem die Digitalisierung. Mit ihrem Voranschreiten gewinnen Softwareanwendungen rapide an Bedeutung und Daten an Wert. Dies schafft neue Möglichkeiten für Unternehmen aller Branchen und auch Behörden. Gleichzeitig erhöht sich hiermit die Notwendigkeit sicherer und hochverfügbarer Kommunikationslösungen. So ist z. B. ein 5G-Campusnetz Grundvoraussetzung für viele neue digitale Prozesse und Anwendungen zur Steigerung der Effizienz, Flexibilität und Sicherheit eines Unternehmens und wird damit zu einer geschäftskritischen Komponente. Es muss für die sichere Digitalisierung der Wirtschaft daher hochverfügbar sein.

Drei technologische Megatrends

Im heutigen Technologieumfeld gibt es drei Megatrends: Breitband, Cloud und künstliche Intelligenz. Diese Technologietrends werden zukünftig auch im Umfeld der professionellen mobilen Kommunikation zum Einsatz kommen. Sie bieten nicht nur neue Möglichkeiten für die Anwender, sondern auch neue Angriffsmöglichkeiten. Diese gilt es mit geeigneten Mitteln abzuwehren. Obwohl Sprache noch für viele Jahre der dominierende Dienst für die kritische Kommunikation bleibt, werden Datenanwendungen zunehmen – und sie werden in rasantem Tempo auch kritisch werden. Künstliche Intelligenz wird Abläufe beschleunigen, Entscheidungen aufgrund der genauen Analyse großer Datenmengen schnell und treffend vorbereiten und zudem auch helfen, den steigenden Fachkräftemangel zu kompensieren.

Multitechnologiekonvergenz in der kritischen Kommunikation

Unter Multitechnologiekonvergenz versteht man im Kontext kritischer Kommunikation die nahtlose Zusammenführung und das koordinierte Zusammenspiel mehrerer Kommunikationstechnologien zu einer einheitlichen, hochverfügbaren und resilienten Kommunikationsumgebung – insbesondere für sicherheits- und missionskritische Anwendungen. Multitechnologiekonvergenz beschreibt den Betrieb mehrerer Funk-, IP- und Netzwerktechnologien in einer gemeinsamen Architektur, sodass Anwender sie transparent und situationsabhängig nutzen können. Statt isolierter Systeme („Technologiesilos“) entsteht ein integriertes Kommunikationsökosystem.

In der kritischen sicheren Kommunikation bedeutet Multitechnologiekonvergenz,

mehrere bewährte und neue Kommunikationstechnologien intelligent zu verbinden, um jederzeit sichere, verfügbare und anwendungsoptimierte Kommunikation für lebenswichtige Einsätze zu gewährleisten. Die Vorteile der Multitechnologiekonvergenz (insbesondere in der kritischen Kommunikation) lassen sich aus operativer, technischer und strategischer Sicht klar darstellen. Kurz gesagt: Sie erhöht Leistungsfähigkeit, Resilienz und Zukunftssicherheit von Kommunikationslösungen.

Hochverfügbare Kommunikation für KRITIS, Industrie und Wirtschaft

KRITIS, Industrie und viele weitere Wirtschaftssektoren benötigen eine hochverfügbare Kommunikation sowie tragfähige Cybersecurity-Lösungen. Sichere und zuverlässige Kommunikation ist – auch im Rahmen der Digitalisierung – für alle Branchen und Wirtschafszweige unverzichtbar. In Zeiten zunehmender Cyberangriffe und realer physischer Bedrohungen gilt es, sich mehr denn je Gedanken über die Sicherheit und den Schutz von Kommunikationsnetzen zu machen. Unternehmen benötigen wirksame Cybersecurity-Mechanismen, um sich vor Angriffen zu schützen. Die Resilienz von Unternehmen und KRITIS muss erhöht werden.

Wie Trends die Verbandsarbeit verändern

Der PMeV arbeitet für ein sicheres, resilientes und vernetztes Europa durch Förderung sicherer Kommunikationslösungen. Darüber hinaus begleiten wir die professionellen Anwender bei neuen Technologietrends und Entwicklungen und den damit verbunden Möglichkeiten und Herausforderungen. Die politischen, wirtschaftlichen und technologischen Veränderungen erfordern eine hohe Flexibilität der PMeV-Arbeit: Neue Themen werden sukzessive und je nach Bedarf vom Verband und seinen Mitgliedern flexibel aufgegriffen. So steht 2026 eine weiter gehende thematische Ausweitung an. Es werden neue Arbeitskreise zu folgenden Themen gegründet: Anwenderdialog, Breitbandendgeräte, 5G-Campusnetze, Internet of Things (IoT), Künstliche Intelligenz (KI), Satellitenkommunikation und Zivil-Militärische Zusammenarbeit (ZMZ). Bereits im Jahr 2024 gründete der Verband Arbeitskreise zu den Themen Cybersicherheit, BOS-Messengerlösungen, sowie Krisen- und Notfallkommunikation – um nur einige zu nennen.

Parallel zu den neuen Themen setzt der PMeV seine Verbandsarbeit bei den bereits etablierten klassischen Themen mit fortschreitenden innovativen Konzepten, Strategien und Standardisierungen fort. Neben neuen technischen und regulatorischen Themen wird sich die Verbandsarbeit weiterhin verstärkt auf die Sensibilisierung der Politik, der Gesellschaft und der Anwender im Hinblick auf die Anforderungen an sichere hochverfügbare Kommunikationslösungen und deren Unverzichtbarkeit für die Sicherheit und Versorgung unserer Gesellschaft konzentrieren. GIT

Bundesverband Professioneller Mobilfunk e. V. (PMeV)
www.pmev.de

KRITIS

Wie man Sicherheit auf die Schiene bringt

Ein Gespräch mit Dr. Patrick Hennies, Security-Chef bei der Deutschen Bahn

Der Deutsche Bahn_Konzern steht vor einer umfassenden Sicherheitstransformation, die Resilienz, Digitalisierung und Kooperation in den Mittelpunkt stellt. Dr. Patrick Hennies, Chief Security Officer Deutsche Bahn, schildert im Gespräch mit GIT SICHERHEIT, wie die DB sich gegen multiple_Bedrohungen stärkt – von langfristigen Drohneneinsätzen über KI_gestützte Video_Analyse bis hin zu Body_Cams für das Zugpersonal. Im Kontext des neuen Kritis_Dachgesetzes betont Hennies die enge Partnerschaft mit Bundes_ und Sicherheitsbehörden sowie die Notwendigkeit einheitlicher Sicherheitsstandards im europäischen Schienennetz.

GIT SICHERHEIT: Herr Dr. Hennies, bei der Deutschen Bahn ist vieles im Umbruch – wir werden gleich davon reden. Könnten Sie zum Einstieg bitte einmal sich selbst, Ihren professionellen Background und Ihre eigene Vision für die Konzernsicherheit skizzieren?

Patrick Hennies: Inzwischen blicke ich auf fast zwei Jahre bei der Deutschen Bahn zurück. Eine Zeit, in der ich eine neue Welt kennenlernen durfte. In meinem bisherigen Berufsleben habe ich vielfältige Erfahrungen gesammelt – in Europa, in Asien, weltweit und in ganz unterschiedlichen Kulturen. Von Tag zu Tag wird mir aber deutlicher, warum so viele von der Bahn als eigene Welt sprechen. Im Securitybereich arbeiten wir mit modernster Technik und KI, und doch bleibt zugleich vieles analog. Ein Beispiel dafür ist die gigantische Infrastruktur, deren Zugänge nicht wie ein Werksgelände verschlossen werden können. Wir produzieren 365 Tage im Jahr, 24/7

unter ständiger Aufsicht der der Politik und unseres Eigentümers und immer live vor einem Millionen-Publikum.

...im Prinzip eine kaum überschaubare Aufgabe?

Patrick Hennies: Wo gesellschaftliche und persönliche Konflikte aufeinandertreffen, können wir als Unternehmen nur begrenzt entgegenwirken. Da können auch Technologie und KI immer nur Teile einer größeren Lösung sein. Selbst, wenn uns viele als riesigen Konzern der öffentlichen Hand sehen: wir sind eine Aktiengesellschaft, keine Behörde. Zusammen mit kommunalen Partnern sind wir als Unternehmen in höchstem Maße und zumeist ganz lokal und analog gefordert. Gerade im sozialen Bereich geraten wir darum viel zu oft an die Grenzen unserer Möglichkeiten und brauchen die Unterstützung der Kommunen. Ohne Kooperationen und Netzwerke bekommen wir das soziale Problem in Deutschland und die Auswirkungen in und um unsere 5.700 Bahnhöfe nicht in den Griff.

> Technologie und KI können immer nur Teile einer größeren Lösung sein.

© Deutsche Bahn AG, Max Lautenschläger

Dr. Patrick Hennies, Leiter Konzernsicherheit und Chief Security Officer (CSO) des DB-Konzerns

Die Deutsche Bahn dürfte im Bereich Verkehr und Logistik eine der größten kritischen Infrastrukturen des Landes und auch Europas sein. Sie steckt in einem gewaltigen Sanierungs- und Restrukturierungsprogramm – und natürlich inmitten des weltpolitischen Geschehens. Fangen wir doch mal mit der Sicherheitslage an und wie sie sich auf die Deutsche Bahn auswirkt. Was hat sich geändert im Vergleich mit der Lage vor fünf oder gar zehn Jahren?

Patrick Hennies: Im Zentrum steht heute das Thema Resilienz – und das ist ein gewaltiger Kraftakt. Im Fokus steht die Stärkung unserer Prozesse und der Infrastruktur gegen Einflüsse von außen: virtuelle oder physische Angriffe, großräumige Unwetterfolgen, Ausfall von Energieversorgung oder Pandemien. Was wir in diesem Bereich aufbauen, geht nahtlos über in das, was die Militärexperten mit Verteidigungsfähigkeit umschreiben. Die Bahn hat eine Schlüsselrolle in der zivilen und militärischen Verteidigung unseres Landes und Europas. Das reicht von Militärtransporten über die Sicherstellung von Transport- und Beförderungsleistungen unter extremen Bedingungen bis hin zu Projekten, in denen wir gemeinsam mit der Bundeswehr übergreifende Konzepte zum Schutz der Bevölkerung oder sensible Verkehre im Krisenfall planen.

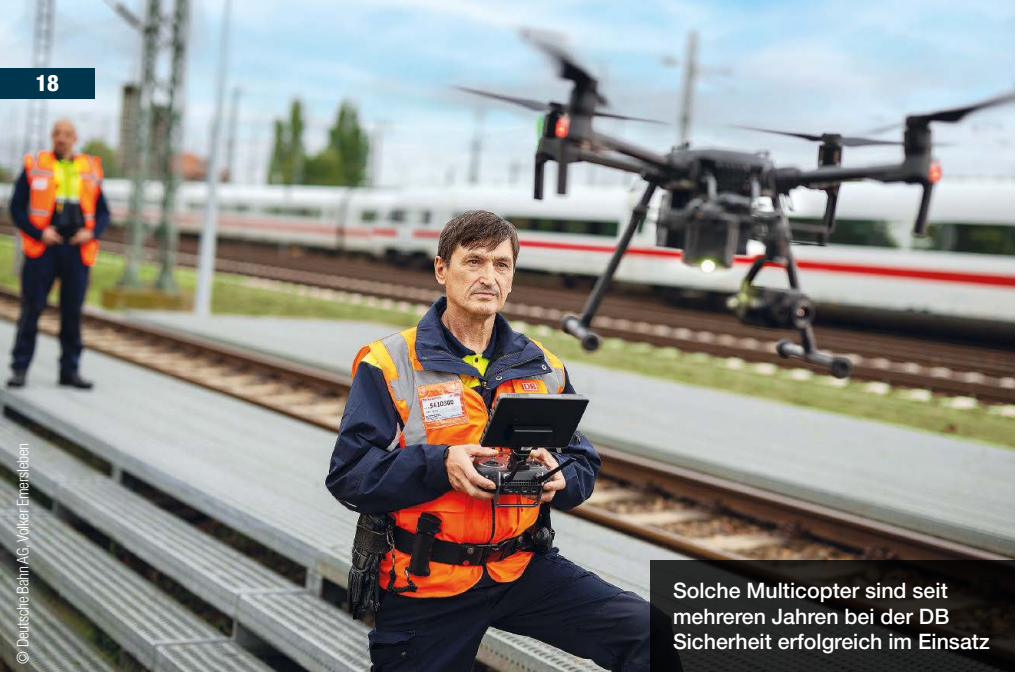
© Deutsche Bahn AG, Dominic Dupont

Bundespolizei und DB Sicherheit im Berliner Ostbahnhof

Parallel dazu gibt es ja das gerade beschlossene Kritis-Dachgesetz?

Patrick Hennies: Viele unserer Aktivitäten decken sich bereits mit künftigen Anforderungen des Kritis-Dachgesetzes, das hohe Anforderungen an die Betreiber kritischer Infrastrukturen stellt. Die reichen vom technischen und personellen Schutz der Eisenbahninfrastruktur über die ständige Weiterentwicklung der IT-Netzwerke und deren Sicherheit, bis hin zur flächendeckenden und konsequenten Nutzung zeitgemäßer Sicherungstechnologien in der Objektsicherheit. Genaugenommen definiert das Kritis-Dachgesetz etwas, das nahe am Optimum der unternehmerischen Sicherheitsvorsorge liegt. Daher ist klar, dass wir die Ziele des Gesetzgebers auch aus eigenem Interesse verfolgen. Allerdings handelt es sich dabei um eine Pionierleistung: bisher hat niemand so ein Konzept für eine flächendeckende Infrastruktur wie das deutsche Eisenbahnnetz realisiert.

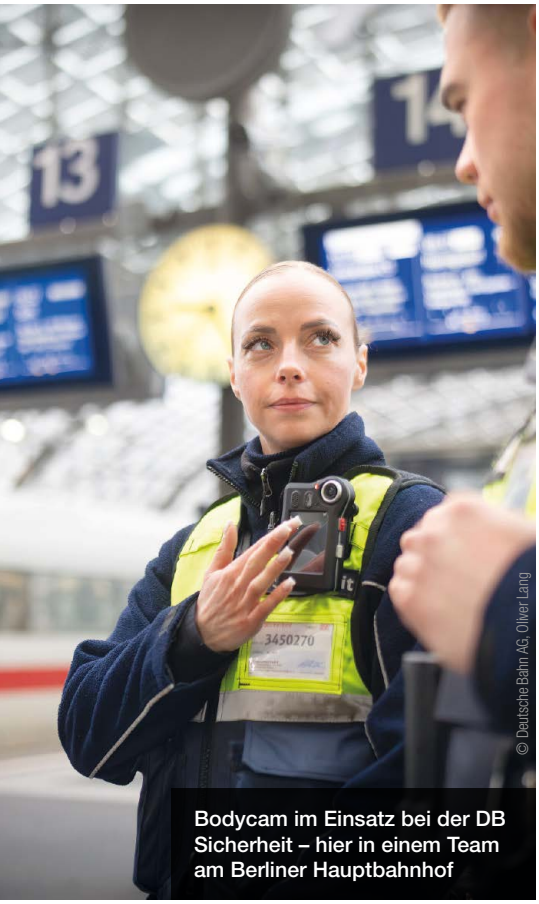
Welche Folgen und Maßnahmen ergeben sich daraus insbesondere für die Konzernsicherheit? Geben Sie uns ein paar Beispiele?



Solche Multicopter sind seit mehreren Jahren bei der DB Sicherheit erfolgreich im Einsatz

Patrick Hennies: Wir haben mehr im Blick als die Aktivitäten in Deutschland. Unsere Einkäufer, die zumeist europaweit tätig sind, oder unsere Experten, die unsere Projekte in anderen Ländern betreuen, sind ständig unterwegs. Dabei steht die Gewährleistung der Reisesicherheit und der Schutz von Lieferketten immer im Fokus. Wir bleiben im ständigen Austausch mit den Sicherheitsbehörden, allen voran der Bundespolizei. Aber auch das Bundesinnenministerium, der Verfassungsschutz oder der Bundesnachrichtendienst sind wichtige Dialogpartner. Das ist entscheidend für unsere Aktivitäten im In- und Ausland, umgekehrt können wir aus unserem weltweiten Netzwerk Informationen zurückbringen.

Ein anderes Beispiel: wir möchten zur Überwachung der 34.000 Kilometer umfassenden Gleisanlagen verstärkt Langstreckendrohnen einsetzen. Die müssen vom Flug bis zur Datenspeicherung und -übertragung sicher sein. Also verbietet sich die Nutzung von Produkten oder Komponenten aus bestimmten Weltregionen. Das ist ein Kostenfaktor und verzögert den Einsatz neuer Technologien.



Bodycam im Einsatz bei der DB Sicherheit – hier in einem Team am Berliner Hauptbahnhof

Herr Dr. Hennies, lassen Sie uns einen näheren Blick auf die Veränderungen werfen, die durch neue Technologien entstehen – Stichworte wären hier etwa Videotechnik und KI, Sensorik und Drohnen...

Patrick Hennies: Eines unserer Topthemen ist die künftige Nutzung von Langstrecken-Drohnen. Wir haben unter anderen bei der DB Sicherheit seit mehreren Jahren erfolgreich Multicopter im Einsatz, die Technologiesprünge der letzten Jahre bieten jedoch völlig neue Einsatzmöglichkeiten von Drohnen. Bisher braucht jede Drohne einen Drohnenpiloten, der das Gerät unmittelbar und auf Sicht steuert. Künftige Drohnen können automatisiert Bahnstrecken abfliegen und aus einem Operation Center überwacht werden. Sie sollen lange vor Eintreffen von Einsatzkräften Situationen vor Ort erfassen und klären. So kann wesentlich schneller entschieden werden, ob und welche Maßnahmen erforderlich sind. Je nachdem, ob etwa Metalldiebe unterwegs sind, Bäume ein Gleis blockieren oder sich Personen im Gleisbereich aufhalten, können wir von Anfang an die „richtige" Intervention auslösen oder den Bahnbetrieb schneller wieder aufnehmen. Allerdings zeigt die Erfahrung auch, dass nicht alles, was technisch möglich ist, direkt einsetzbar ist. Erst wenn die Industrie eine Lösung serienreif anbietet und alle erforderlichen Zulassungen vorliegen, kann sie bei uns zum Einsatz kommen. Also ganz klar: lieber etwas später, aber dafür sicher.

Sie investieren stark in Kameratechnik für Bahnhöfe, die Gleisüberwachung und anderes?

Patrick Hennies: Gemeinsam mit dem Bund haben wir gerade ein umfassendes Ausbauprogramm für Videotechnik abgeschlossen. 11.000 Kameras an den 1.000 am stärksten frequentierten Bahnhöfen liefern jetzt durchweg hochauflösende Bilder. Von den Aufzeichnungen profitiert vor allem die Bundespolizei bei der Ermittlung zu Straftaten, von denen übrigens nur ein Teil etwas mit der Bahn oder ihren Kunden und Mitarbeitenden zu tun hat. Wir werden oft gefragt, warum nicht alle Bahnhöfe Videokameras haben. Die Antwort ist ganz einfach, der rechtliche Rahmen gibt das nicht her. Nur wenn die Bundespolizei eine entsprechende Gefährdungseinschätzung abgibt, wird der Bahnhof mit Videotechnik ausgerüstet. Das ergibt sich aus Faktoren wie Besucherzahlen oder Straftaten.

Wie sieht es mit Videotechnik bei anderen Anlagen aus, also abgesehen von Bahnhöfen?

Patrick Hennies: Der Schutz vor unberechtigtem Betreten von Anlagen ist hier als weiterer Anwendungszweck von Videotechnik zu nennen. Mithilfe von KI wollen wir künftig als Securityorganisation automatisiert erkennen, wenn Personen sich aus dem öffentlichen Bereich in Bahnanlagen begeben – sei es in einen Tunnel oder auch in Rangierbahnhöfe. In Bahnhöfen wollen wir mit KI zuverlässig informiert werden, wenn Personen stürzen oder sich an ungeeigneten Stellen niederlassen. Ob medizinischer Notfall, Schlägerei oder Nickerchen. Das alles haben wir mit wissenschaftlicher Unterstützung im Sicherheitsbahnhof Berlin Südkreuz – unserem Security-Labor – im Blick und werden es einsetzen, sobald es zuverlässig funktioniert und erforderliche Genehmigungen vorliegen. Zur Klarstellung: Die DB wird dabei nicht mit Gesichtserkennung arbeiten. Es geht darum, Gefahrensituationen zu erkennen, nicht Personen zu identifizieren.

Ein Problem, von dem zunehmend berichtet wird, besteht aus Gewalt gegen Bahnpersonal. Wie ist die Lage genau?

Bitte umblättern ▶

Ihr Gebäude kann mehr –

mit smarten Lösungen von Bosch Building Technologies

Über 100 Jahre technisches Know-how gepaart mit Leidenschaft, um Menschen und ihre Umgebung zu schützen. Als führender Systemintegrator bieten wir Lösungen für Gebäudesicherheit, Brandschutz, Gebäudeautomation und Energieeffizienz.
Von der Beratung bis zum Service – immer an Ihrer Seite.
Performance built on Partnership.

Technik fürs Leben

BOSCH

© Deutsche Bahn AG, Max Lautenschläger

DB Sicherheit: Prüfdienst im Zug

Patrick Hennies: Jeder Angriff auf einen Kollegen oder eine Kollegin ist einer zu viel. Es gibt keine Rechtfertigung für Übergriffe jedweder Art, Gewalt hat in Zügen, Bussen und Bahnhöfen nichts zu suchen. Die Sicherheit unserer Mitarbeitenden in allen Geschäftsfeldern ist seit jeher ein Top-Thema: es ist omnipräsent, verändert sich ständig und muss jeden Tag neu gedacht werden. Wir passen unsere Sicherheitskonzepte in enger Kooperation mit den Securitymanagements der Geschäftsfelder kontinuierlich an, haben Hilferuf-Apps eingeführt, Videotechnik ausgebaut und konsequent in Deeskalations- und Verhaltenstrainings für Mitarbeitende investiert. Wir müssen aber leider feststellen, dass wir die gesellschaftliche Entwicklung der zunehmenden Respektlosigkeit, der Verrohung und Gewaltbereitschaft nicht aufhalten können.

Die allermeisten Situationen, die zu Gewalt führen, entstehen aus einem vorherigen Fehlverhalten des Angreifenden. Das reicht vom Fahren ohne Fahrschein bis zum Fahrgast, der wütend ist, weil der Zug Verspätung hat oder er zu spät merkt, in den falschen Zug gestiegen zu sein. In vielen Situationen reichen professionelles Auftreten und die trainierte Deeskalationsstrategie nicht.

Der Tod eines unserer Zugbegleiter ist der traurige Beweis dafür, dass es bei allem Bemühen keine absolute Sicherheit geben kann. Umso mehr ist unsere Pflicht als Arbeitgeber, stets bestmöglich die Sicherheit unserer Mitarbeitenden zu gewährleisten. Das nehme ich als Sicherheitschef der DB sehr ernst.

Sie haben nach diesem tödlichen Angriff einen Sicherheitsgipfel angesetzt. Welche Themen haben Sie dort gesetzt und was dürfen die Mitarbeiter der DB erwarten?

Patrick Hennies: Der Sicherheitsgipfel am 13. Februar wurde persönlich von unserer Vorstandsvorsitzenden Evelyn Palla einberufen und baut auf unseren bisherigen Aktivitäten auf. Neu ist, dass wir mit Bundes- und Landespolitik, Verbänden, Gewerkschaften und Interessenvertretern auf Basis eines gemeinsamen Verständnisses einen Aktionsplan erarbeitet haben. Für niemanden war das Thema neu. Jetzt haben wir einen breiten Konsens, der es uns ermöglicht, schneller Maßnahmen für die DB-Kollegen und auch allen anderen Mitarbeitenden der Branche auf den Weg zu bringen.

Mit der Bundespolizei und den DB-Geschäftsfeldern sowie den weiteren Beteiligten konnten wir eine Reihe von Maßnahmen identifizieren, die wirkungsvoll und schnell umsetzbar sind. Wir brauchen Geschwindigkeit bei der Ausstattung unserer Mitarbeitenden und müssen an die Ursachen zunehmender Gewalt ran. Wichtig war, keine langfristigen Masterpläne zu schreiben, sondern vor allem Themen anzugehen, die wir in diesem Jahr realisieren können. Die kontinuierliche Zusammenarbeit mit der Bundespolizei hat geholfen, schnell einen Rahmen für ein gemeinsames Vorgehen zu setzen.

Mit welchen Schutzmaßnahmen – Bodycams, Videotechnik etc. – machen Sie gute Erfahrungen?

Patrick Hennies: Sehr gute Erfolge erzielen wir mit Bodycams. Seit 2016 tragen unsere Sicherheitskräfte die Geräte, seit 2024 wird unter anderen das Zugpersonal von DB Regio nach und nach ausgerüstet. Die Zugbegleiter machen dieselbe Erfahrung wie die Sicherheitskräfte: Wer eine Bodycam trägt, wird quasi nicht angegriffen, da mögliche Täter mit Konsequenzen rechnen können. Neben der beweissicheren Dokumentation einer eskalierten Situation schätzen die Nutzer der Bodycams deswegen vor allem die präventive abschreckende Wirkung, bevor es überhaupt zu Gewalt kommt. Daher ist es schade, dass die Anforderungen des Gesetzgebers sehr hoch sind – trotzdem werden wir bis zum Jahresende alle Mitarbeitenden im Kundenkontakt mit den Geräten ausrüsten. Das ist ein Ergebnis des Sicherheitsgipfels. GIT

© Deutsche Bahn AG, Oliver Lang

Der Sicherheitsgipfel in Berlin am 13.02.2026 wurde nach dem tödlichen Angriff auf einen Zugbegleiter angesetzt. V. l.n.r.: Mitarbeiter DB Sicherheit mit Bodycam Evelyn Palla, Vorstandsvorsitzender Deutsche Bahn AG Patrick Schnieder, Bundesverkehrsminister Christian Bernreiter, Vorsitzender der Verkehrsministerkonferenz

Deutsche Bahn
www.deutschebahn.com

NRW Sicherheitstag

24. Juni 2026

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

Zwischen Geopolitik und Unternehmensrealität – Wirtschaftsschutz als Erfolgsfaktor

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

DLR
Schutz terrestrischer Infrastrukturen

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

ASW West

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

© BHE

Innovationsfreude und technischer Fortschritt

Trendbericht von Axel Schmidt, Vorstandsvorsitzender des Bundesverbandes Sicherheitstechnik (BHE)

Die Sicherheitsbranche zeichnet sich seit jeher durch Innovationsfreude und technische Fortschritte aus. Das haben auch die vergangenen Jahre wieder gezeigt, die nicht nur auf den BHE, sondern auf die gesamte Branche nachhaltige Auswirkungen hatten. Manche Entwicklungen, die zuvor eher langsam und schrittweise vorangingen, wurden durch äußere Rahmenbedingungen deutlich beschleunigt – allen voran durch die Corona-Pandemie. Sie machte digitale Kommunikations- und Arbeitsformen nicht nur notwendig, sondern verankerte sie dauerhaft im Verbandsalltag.

Die Digitalisierung hat grundlegend verändert, wie wir zusammenarbeiten, Wissen vermitteln und Leistungen anbieten. Digitale Meetings ermöglichen heute schnellere Abstimmungen und erleichtern die Einbindung von Experten aus dem gesamten Bundesgebiet. Gleichzeitig hat der BHE sein Online-Schulungsangebot massiv ausgebaut: Webinare und neu etablierte Formate wie die digitalen BHE-Thementage erweitern die Möglichkeiten für Unternehmen, ihre Mitarbeiter flexibel und bedarfsgerecht zu qualifizieren. Das Ergebnis: Prozesse verlaufen effizienter, Informationen fließen schneller und fachliche Inhalte können zielgerichteter aufbereitet werden.

© Hikvision

Seit Jahren nutzen wir die GIT SICHERHEIT als starke Plattform für unsere Präsenz und als Kompass für Branchen-Trends.

Thorsten Wallerius, Team Leader Key Account Management, Hikvision Deutschland GmbH

35 JAHRE GIT SICHERHEIT

Sichtbarkeit sicherheitstechnischer Themen

Auch unsere eigenen Kommunikationskanäle haben sich weiterentwickelt. Mit dem Start und konsequenten Ausbau unserer Social-Media-Aktivitäten sprechen wir Mitglieder, Partner und Interessierte direkter an, schaffen neue Zugänge zu Fachinformationen und stärken die Sichtbarkeit sicherheitstechnischer Themen.

Parallel dazu ist der BHE selbst gewachsen: Steigende Mitgliederzahlen sowie neue Themen und Aufgabenfelder sind ein Zeichen dafür, wie dynamisch sich das Umfeld der Sicherheitstechnik entwickelt. Um dieser Breite gerecht zu werden, haben wir das Team in der BHE-Geschäftsstelle ausgebaut und unsere internen Strukturen geschliffen. Mit dem Wechsel in der Geschäftsführung des BHE und seiner Tochtergesellschaften wurden Weichen für die kommenden Jahre neu gestellt.

Von KI bis Cybersicherheit

Gleichzeitig verändert sich die Sicherheitstechnik selbst in rasantem Tempo. Ein zentrales Zukunftsthema ist die Künstliche Intelligenz. KI wird in der Videotechnik, in Zutrittslösungen und in Alarmierungssystemen zunehmend eingesetzt – aber genauso auch in der Unterstützung von Technikern oder in administrativen Geschäftsprozessen. Damit entstehen neue Chancen aber auch neue Anforderungen gleichermaßen. Die Qualität und Verlässlichkeit von Informationen rückt stärker in den Fokus. Insbesondere, wenn KI bei der Wissensvermittlung oder Entscheidungsfindung eingesetzt wird, kommt Verbänden wie dem BHE eine wichtige Rolle zu: Orientierung bieten, Standards mitgestalten, belastbares Fachwissen bereitstellen und die Branche bei verantwortungsvollen Anwendungen unterstützen.

Das Thema Cyber-Sicherheit gewinnt ebenfalls weiter an Bedeutung. Regulatorische Vorgaben wie die NIS2-Richtlinie oder das Kritis-Dachgesetz werden die Branche nachhaltig beschäftigen. Cyber-Sicherheit ist zum integralen Bestandteil sicherheitstechnischer Lösungen geworden. Für Errichter, Planer und Hersteller entstehen neue Anforderungen, aber auch Marktchancen. Der Bedarf an nachweislich sicherer Technik sowie an qualifizierten Fachunternehmen steigt. Neue Prüf- und Zertifizierungsverfahren werden daher eine zentrale Rolle spielen, um Sicherheitstechnik verlässlich bewerten zu können. Im Interesse seiner Mitglieder wird sich der BHE hier wie bisher intensiv in den entsprechenden Normungsgremien einbringen.

Unternehmensnachfolge und Konstanz

Neben all diesen technischen und regulatorischen Entwicklungen bleibt ein weiteres Thema prägend: die Unternehmensnachfolge. Viele Betriebe stehen vor einem Generationswechsel, der durch den Fachkräftemangel zusätzlich erschwert wird. Das stellt die Branche vor strukturelle Herausforderungen, bietet aber gleichzeitig jungen Fachkräften attraktive Perspektiven in einem höchst interessanten Markt.

Trotz aller Veränderungen bleibt eines konstant: Sicherheitstechnik ist ein Zukunftsfeld – komplex, anspruchsvoll, gesellschaftlich relevant – und der BHE ist die zentrale Anlaufstelle für sicherheitstechnische Fragen. Nach über 50 Jahren Verbandsarbeit verstehen wir den Wandel nicht als Ausnahme, sondern als Normalzustand. Als Experten-Netzwerk und Wissensplattform wird der BHE auch künftig die Bedürfnisse der Branche im Blick haben, Entwicklungen einordnen und den Dialog zwischen Herstellern, Errichtern, Planern und Anwendern fördern. Denn eines ist klar: Die Branche verändert sich – und wir gestalten diesen Wandel aktiv mit. GIT

BHE Bundesverband Sicherheitstechnik e.V.
www.bhe.de

© BVSW

Stabilität, Vertrauen und Zukunftsfähigkeit

Ein Trendbericht von Caroline Eder, Geschäftsführerin des BVSW

Die Welt der Sicherheit hat sich in den vergangenen Jahren rasant und tiefgreifend verändert – dynamischer, komplexer und anspruchsvoller als je zuvor. Als BVSW stehen wir dabei nicht am Rand, sondern mitten im Geschehen und gestalten diesen Wandel aktiv mit. Seit 15 Jahren begleite ich diese Entwicklungen im Verband und habe hautnah erlebt, wie sich Anforderungen, Risiken und Erwartungen an unsere Branche kontinuierlich weiterentwickelt haben.

Die Bedrohungslage ist komplexer geworden. Klassische Risiken bestehen fort, werden jedoch zunehmend überlagert durch hybride Szenarien, in denen physische und digitale Angriffe ineinandergreifen. Themen wie Cyberkriminalität, Sabotage, geopolitische Spannungen und gesellschaftliche Polarisierung wirken sich unmittelbar auf die Sicherheitslage von Unternehmen und Institutionen aus. Sicherheit ist heute kein isolierter Aufgabenbereich mehr – sie ist integraler Bestandteil unternehmerischer Resilienz.

Neue Möglichkeiten – neue Herausforderungen

Gleichzeitig erleben wir einen massiven technologischen Umbruch. Künstliche Intelligenz, vernetzte Systeme und datenbasierte Analysen eröffnen neue Möglichkeiten, stellen uns aber auch vor neue Herausforderungen. Die Sicherheitswirtschaft entwickelt sich zunehmend zu einer technologiegetriebenen Branche. Das verändert nicht nur Prozesse und Werkzeuge, sondern auch die Anforderungen an die Menschen, die in ihr arbeiten.

Denn der Faktor Mensch bleibt entscheidend – und genau hier zeigt sich eine der größten Herausforderungen unserer Zeit: der Mangel an qualifizierten Fachkräften. Die Anforderungen steigen stetig, während geeignete Bewerberinnen und Bewerber schwerer zu finden sind. Das zwingt uns, neue Wege zu gehen: in der Aus- und Weiterbildung, in der Positionierung der Branche und in der Frage, wie wir Qualität nachhaltig sichern.

Für uns als BVSW bedeutet das: Wir müssen Orientierung geben, Standards setzen und Innovation fördern. Wir verstehen uns als Plattform für Austausch, als Impulsgeber für zukunftsfähige Konzepte und als Stimme der Branche gegenüber Politik und Öffentlichkeit.

Ganzheitliche Sicherheitsarchitekturen

Der Blick nach vorne zeigt klar: Die Sicherheitswirtschaft steht vor einem Paradigmenwechsel. Es geht nicht mehr allein um Schutz im klassischen Sinne, sondern um ganzheitliche Sicherheitsarchitekturen. Die Verzahnung von physischer Sicherheit, IT-Security und organisatorischen Maßnahmen wird zur Selbstverständlichkeit. Technologie und Mensch werden dabei nicht gegeneinander ausgespielt, sondern sinnvoll miteinander verbunden.

Die Rolle unserer Mitgliedsunternehmen wird sich weiterentwickeln – hin zu spezialisierten Dienstleistern und strategischen Partnern, die ihre Kunden nicht nur schützen, sondern umfassend beraten und begleiten. Unsere Aufgabe wird es sein, diesen Wandel aktiv zu gestalten: mit klaren Qualitätsmaßstäben, mit praxisnahen Qualifizierungsangeboten und mit einem starken Netzwerk, das Wissen bündelt und weiterträgt.

Sicherheit ist und bleibt eine zentrale Voraussetzung für wirtschaftliche Stabilität und gesellschaftliches Vertrauen. Gerade in einer Zeit zunehmender Unsicherheiten kommt unserer Branche eine besondere Verantwortung zu. Diese Verantwortung nehmen wir an – entschlossen, vorausschauend und gemeinsam mit unseren Mitgliedern im BVSW. GIT

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

Unsere Fachmessen für Sicherheit

AFAG WIR MACHEN MESSEN

SICHERHEITS EXPO

Fachmessen für innovative Sicherheitslösungen
Trade fairs for innovative security solutions

- **Zutrittskontrolle** *Access Control*
- **Videoüberwachung** *Video Surveillance*
- **Brandschutz** *Fire Protection*
- **Perimeter Protection**
- **IT-Security**

SICHERHEITS EXPO München

MOC München

1. + 2. Juli 2026
1 + 2 July 2026

Jetzt Tickets sichern!
Secure your tickets now!

SICHERHEITS EXPO Alpe Adria

Messe Klagenfurt

14. + 15. Okt 2026
14 + 15 Oct 2026

Save the Date!

SICHERHEITS EXPO Berlin

Station Berlin

22. + 23. Sept 2027
22 + 23 Sept 2027

Save the Date!

www.sicherheitsexpo.de

KRIFA

Fachkongress + Ausstellung
Sicherheit und Krisenvorsorge

15. + 16. Juli 2026
MCC Halle Münsterland

Die KRIFA ist das neue Event

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

www.krifa.de

Fachlicher Träger

BSKI Bundesverband für den Schutz Kritischer Infrastrukturen e. V.

Veranstalter

AFAG WIR MACHEN MESSEN

Hauptsitz von Boehringer Ingelheim

GEFAHRENMANAGEMENT

Integriertes Gefahrenmanagement

Boehringer Ingelheim: Offene Plattform für globale Pharmastandorte

Boehringer Ingelheim zählt zu den weltweit führenden forschenden Pharmaunternehmen. Rund 55.000 Mitarbeiter arbeiten international an der Entwicklung innovativer Therapien für Mensch und Tier. Die weltweit verteilten Forschungs-, Produktions- und Verwaltungsstandorte stellen hohe Anforderungen an Sicherheitsorganisation, Alarmmanagement und Leitstellenbetrieb. Das Unternehmen setzt auf die offene Gefahrenmanagementplattform Winguard von Advancis.

Im industriellen Umfeld der Pharmaforschung müssen sicherheitstechnische Systeme zuverlässig und standortübergreifend überwacht werden. Dazu gehören insbesondere Brandmelde-, Einbruchmelde-, Zutrittskontroll- und Videosysteme sowie weitere technische Anlagen. Ziel ist eine konsistente Lageübersicht in der Leitstelle sowie eine schnelle und strukturierte Bearbeitung von Ereignissen.

Ausgangssituation: heterogene Systemlandschaft

Vor der Einführung einer zentralen Plattform arbeiteten viele sicherheitstechnische Systeme an den deutschen Standorten Ingelheim am Rhein und Biberach an der Riß weitgehend getrennt voneinander. Unterschiedliche Herstellerlösungen, proprietäre Schnittstellen und separate Bedienoberflächen erschwerten eine einheitliche Lagebewertung in der Leitstelle.

Im Rahmen des Projekts „Leitstelle Deutschland“ wurde daher eine übergeordnete Integrationsplattform gesucht, die unterschiedliche Gewerke in einer gemeinsamen Systemumgebung zusammenführen kann. Wie Michael Klier aus dem Bereich IT O&L Security Operations erläutert, war es dem Unternehmen dabei besonders wichtig, alle sicherheitstechnischen Gewerke in einem System zusammenzuführen. Gleichzeitig sollte das Gefahrenmanagementsystem ausreichend flexibel sein, um auch international eingesetzt werden zu können und verschiedene Betriebsmodelle zu unterstützen.

Integrationsplattform

Die Wahl fiel auf Winguard, eine offene Gefahrenmanagementplattform von Advancis Software & Services. Die Software dient als Integrations- und Leitstellenplattform, über die unterschiedliche sicherheitstechnische Subsysteme angebunden und zentral visualisiert werden können. Ereignisse aus Brandmelde-, Einbruchmelde- oder anderen technischen Anlagen werden im System konsolidiert und in grafischen Lageplänen dargestellt. Gleichzeitig lassen sich Alarmmeldungen automatisiert an angeschlossene Einsatzleitsysteme weitergeben. Dadurch erhalten Leitstellenmitarbeiter eine konsolidierte Sicht auf sicherheitsrelevante Ereignisse und können Maßnahmen strukturiert einleiten. Neben den funktionalen Anforderungen spielte auch die Zusammenarbeit mit dem Hersteller eine Rolle. Advancis überzeuge laut Klier insbesondere durch kurze Reaktionszeiten und eine kompetente Unterstützung, die sich gerade bei kritischen Ereignissen bewähre.

Für die Leitstellen bildet das integrierte Gefahrenmanagementsystem einen zentralen Baustein im täglichen Betrieb. Durch die Zusammenführung aller sicherheitsrelevanten Informationen in einer Plattform lassen sich Ereignisse schneller bewerten und geeignete Maßnahmen ohne Verzögerung einleiten. Dadurch werde nicht nur die operative Qualität verbessert, sondern auch ein hohes Sicherheitsniveau für die Standorte gewährleistet, erläutert Jonas Michel, Head of Operations Center Germany.

Digitale Unterstützung für Betriebsprozesse

Neben der Ereignisverarbeitung unterstützt das System auch organisatorische Abläufe im Sicherheitsbetrieb. Bei Boehringer Ingelheim wird Winguard beispielsweise für die Verwaltung sogenannter Schaltaufträge genutzt. Diese kommen zum Einsatz, wenn Meldergruppen im Zuge von Wartungs- oder Bauarbeiten temporär deaktiviert werden müssen.

Die entsprechenden Prozesse lassen sich im System planen, freigeben und dokumentieren. Verantwortlichkeiten, Zeitfenster und Statusinformationen werden automatisch protokolliert. Dadurch wird die Nachvollziehbarkeit erhöht und der administrative Aufwand reduziert.

Flexible Architektur für internationale Strukturen

Heute wird Winguard an mehreren Standorten weltweit eingesetzt. Die Systemarchitektur erlaubt unterschiedliche Betriebsmodelle – von lokalen Installationen einzelner Werke bis hin zu zentralen Leitstellen oder regionalen Security Operation Centers, die mehrere Standorte überwachen. Diese Flexibilität war laut Klier ein wesentlicher Faktor bei der Systementscheidung. Gleichzeitig hebt er hervor, dass Advancis bereit sei, flexibel auf individuelle Anforderungen zu reagieren und gemeinsam neue Lösungsansätze zu entwickeln. Gerade diese partnerschaftliche Zusammenarbeit mache den Anbieter zu einem wichtigen Bestandteil des Sicherheitsmanagements.

Die Implementierung der Plattform zeigt, dass Gefahrenmanagementsysteme heute weit über die reine Alarmverarbeitung hinausgehen. Offene Integrationsplattformen ermöglichen eine zentrale Lageübersicht, unterstützen operative Prozesse und schaffen die Grundlage für standortübergreifende Sicherheitsstrategien.

Chemische Entwicklung in Biberach an der Riß

Für international tätige Unternehmen wie Boehringer Ingelheim wird damit deutlich: Die Integration technischer Systeme und organisatorischer Abläufe ist ein entscheidender Baustein für ein effizientes und zukunftsfähiges Sicherheitsmanagement. GIT

Advancis Software & Services GmbH
www.advancis.net

Sicherheit ganzheitlich denken

Ein Trendbericht von Prof. Dr. Clemens Gause, Geschäftsführer des Verbands für Sicherheitstechnik

Wie hat sich die Sicherheitswelt in den jüngsten Jahren verändert? Welche Entwicklungen waren die einschneidendsten – und wo geht die Reise hin?

Geopolitische Lage

Die letzten Krisen – von der längst vergessenen Pandemie, über den russischen Angriffskrieg bis hin zu den neuesten Energieengpässen durch den Iran-Krieg– verdeutlichen immer wieder aufs Neue: Sicherheit muss zunehmend ganzheitlich gedacht werden. Und Schutzmaßnahmen in Einzelbereichen wie etwa der Cybersicherheit allein reichen nicht aus. Lange Zeit konzentrierte sich die Gesetzgebung in Deutschland vor allem auf den digitalen Bereich. Genau hier setzt das neue KRITIS-Dachgesetz an – es soll die Lücke zwischen digitaler und physischer Sicherheit schließen.

Unsere moderne und immer stärker vernetzte Gesellschaft hängt von funktionierenden Infrastrukturen ab. Nehmen wir z. B. die Sektoren Strom, Wasser, Transport, Telekommunikation und die Gesundheitsversorgung. Sie bilden das Rückgrat unseres täglichen Lebens. Der Schutz dieser kritischen Infrastrukturen (KRITIS) ist daher eine der zentralen Sicherheitsaufgaben unserer Zeit. Mit dem frisch verkündeten KRITIS-Dachgesetz wird erstmals ein einheitlicher Rechtsrahmen für den physischen Schutz und die Resilienz dieser Anlagen geschaffen. Da der physische Schutz die Grundlage unserer Verbandstätigkeiten darstellt hat diese Entwicklung natürlich erheblichen Einfluss auf unsere Arbeit und unsere Expertise ist dieser Tage gefragter denn je.

Drohnen

Drohnenerkennung sowie -abwehr gewinnen rasant an Bedeutung, da unbemannte Fluggeräte längst vom Freizeitgerät zum sicherheitsrelevanten Risiko geworden sind. Moderne Systeme setzen auf eine Kombination aus Radar, Funkfrequenzanalyse, optischen und akustischen Sensoren sowie zunehmend auf KI-gestützte Mustererkennung. Dadurch lassen sich selbst kleine, leise und schwer detektierbare Drohnen in komplexen Umgebungen identifizieren.

Die Herausforderungen wachsen jedoch mit der Vielfalt der Drohnentypen: unterschiedliche Flugprofile, geringe Radarquerschnitte und die Nutzung autonomer Flugmodi erschweren eine zuverlässige Klassifizierung. Urbanes Umfeld verstärkt das Problem durch Störsignale, Reflexionen und hohe Hintergrundaktivität, was Fehlalarme begünstigt. Abwehrmaßnahmen wie Störsender, Netzdrohnen oder kinetische Systeme sind technisch anspruchsvoll und müssen präzise eingesetzt werden, um Kollateralschäden zu vermeiden.

Drohnenerkennung und -abwehr: unbemannte Fluggeräte gehören schon längst zum sicherheitsrelevanten Risiko

Rechtlich bleibt die Lage dabei anspruchsvoll. Eingriffe in den Luftraum, das Stören von Funkverbindungen oder das Neutralisieren eines Flugobjekts unterliegen strengen gesetzlichen Vorgaben. Betreiber kritischer Infrastrukturen fordern daher klarere, praxisnahe Rahmenbedingungen, die Sicherheit gewährleisten, ohne regulatorische Grenzen zu überschreiten. Fest steht: Mit zunehmender Drohnennutzung steigt der Druck, Erkennung und Abwehr technologisch wie rechtlich auf ein neues Niveau zu heben.

Bereits seit fast zehn Jahren beteiligt sich der VfS an unterschiedlichen nationalen sowie internationalen Forschungsprojekten, die sich allesamt mit der Sicherheit rund um den unbemannten Flugverkehr unter Einsatz von KI auseinandersetzen.

Künstliche Intelligenz

Apropos Künstliche Intelligenz: KI wird zum Gamechanger der physischen Sicherheit, weil sie sicherheitsrelevante Datenströme nicht nur erfasst, sondern in Echtzeit analysiert und kontextualisiert. KI-Modelle verarbeiten Videofeeds, Sensorwerte und Telemetriedaten parallel, erkennen Anomalien anhand trainierter Muster und adaptiver Schwellenwerte und klassifizieren Ereignisse innerhalb von Millisekunden. Durch kontinuierliches Training mit Edge- und Cloud-Ressourcen verbessert sich die Präzision fortlaufend. Jede zusätzliche Kamera, jeder IoT-Sensor erweitert das Datenmodell und erhöht die Fähigkeit, Risiken frühzeitig zu prognostizieren, statt sie nur zu protokollieren. Angesichts wachsender Bedrohungsszenarien wird KI damit zu einem zentralen Sicherheitslayer, der klassische Systeme funktional überlagert und zumindest teilautomatisiert. Aber auch KI hat seine Fähigkeitsgrenzen im Einsatz. Wir als Verband verstehen es als unsere Aufgabe die Möglichkeiten aber auch die Grenzen aufzuzeigen, um den Nutzen von KI für ein hohes Sicherheitsniveau zu maximieren aber auch Schaden durch den unsachgemäßen Einsatz von KI zu verhindern.

35 JAHRE GIT SICHERHEIT

VISION

Zunehmend hybride Bedrohungen machen die sicherheitsrelevanten Schwächen siloartiger Strukturen in Wirtschaftsunternehmen sichtbar; eine wirksame Antwort liegt in der Konvergenz von physischer Sicherheit und Cybersicherheit zu einer ganzheitlichen Sicherheitsarchitektur im Sinne eines All-Hazards-Ansatzes.

Florian Haacke, ASW-BW Vorstandsmitglied

Integrierte Sicherheit

In einer hochgradig vernetzten Wirtschaft können Störungen einer Produktion oder Dienstleistungserbringung erhebliche Schäden verursachen. Bedrohungen wie Kriminalität, Terror, Sabotage oder Naturereignisse erfordern daher zunehmend veränderte Sicherheitskonzepte. Einzelmaßnahmen reichen nicht mehr aus; wirksam wird Sicherheit erst, wenn Technik, Organisation und Mensch nahtlos und professionell zusammenwirken. Genau das beschreibt die integrierte Sicherheit. Sie umfasst den gesamten Prozess von der Planung über die Umsetzung bis zum Betrieb und bezieht alle technischen und organisatorischen Elemente ein – von Perimeterschutz, Zutrittskontrolle, Einbruchmeldetechnik und Videoüberwachung bis hin zu Bewachung, Empfangsdiensten und Risikomanagement. Durch dieses abgestimmte Zusammenspiel entsteht ein Sicherheitsniveau, das sowohl robust als auch wirtschaftlich ist. Dabei sind vom Fachplaner über den Sicherheitsdienstleister, Systemlieferanten, Errichter und Betreiber alle Prozessbeteiligten einzubeziehen.

Auf der Basis des Verständnisses für integrierten Sicherheit und im Rahmen der hybriden Gefährdungslage ist die Absicherung von Objekten komplexer denn je, und führt zwangsläufig zu einem substanziellen Anstieg des Aufklärungsbedarf, den wir als Verband für Sicherheitstechnik versuchen zu decken.

Digitaler Zwilling in der Perimetersicherung

Wagen wir einen kleinen Ausblick in die nicht allzu ferne Zukunft: In einer bewegten Welt gibt es viele Themen, die auch die Perimetersicherung maßgeblich beeinflussen. Nehmen wir nur einige Beispiele wie das KRITIS-Umsetzungsgesetz, Cloud, BIM (Building Information Modelling), 3D, KI, Biometrie, NIS-2, um nur einige zu nennen. All dies erfordert erweiterte Maßnahmen bzw. bringt die Perimetersicherung in eine neue Dimension.

In einem aktuellen Forschungsprojekt „KRITIS 3D“ wird eine innovative, automatisierte Prozesskette zur hochpräzisen und vollständigen 3D-Erfassung, Analyse und Dokumentation der Perimetersicherung kritischer Infrastrukturen und von Hochsicherheitseinrichtungen entwickelt. Die Kombination modernster hochaufgelöster 3D-Vermessung, Panoramaaufnahmen und KI-gestützter Objekt- und Mängelerkennung werden eine objektive, transparente und vollautomatisierte und schnelle Sicherheitsbeurteilung ermöglichen. Hierfür werden die Prozesse der Erfassung über die Verarbeitung bis hin zur Visualisierung auf die für die Sicherheitsbeurteilung relevanten Informationen maßgeschneidert. Die modulare, innovative Plattform verbindet Hardware, Software und KI zu einer nachhaltigen Lösung, die zukünftigen gesetzlichen Anforderungen gerecht und den Markt für digitale Sicherheitsanalysen transformieren wird. Dem „Digitalen Zwilling in der Perimetersicherung“ GIT

Verband für Sicherheitstechnik e. V.
www.vfs-hh.de

© Bilder: VfS

© Werkhalle, Rüsselsheim

Sicherheitstage 2026

Praxiswissen für sensible Bereiche – zwei Termine, ein starkes Partnernetzwerk

Physische Sicherheit, Perimeterschutz, Zutrittskontrolle und intelligente Videoüberwachung stehen im Mittelpunkt der Sicherheitstage 2026 – einer Fachveranstaltung von Hirsch, die am 9. Juni in der Werkhalle Rüsselsheim und am 11. Juni im Radisson Blu Hamburg stattfindet. Errichter, Integratoren und Sicherheitsverantwortliche erwartet ein praxisnaher Mix aus Fachvorträgen und direktem Austausch mit führenden Lösungsanbietern.

Das Programm der „Sicherheitstage 2026“ von Hirsch richtet sich an Fachplaner, Errichter, Integratoren und Sicherheitsverantwortliche. Es gibt zwei Vortragsblöcke, ergänzt durch ausgedehnte Zeiten für vertiefte Gespräche. Im ersten Block (9:30 bis 10:30 Uhr) sprechen Experten von Hirsch, Accellence Technologies und Vivotek über integrierte Sicherheitslösungen für sensible Bereiche. Nach einer Gesprächspause am Stand folgt ab 11:30 Uhr der zweite Block mit Beiträgen von Hirsch und Quanergy zum Thema Perimeterschutz und Slat über Lösungen für die kontinuierliche Videoüberwachung. Bei allen Vorträgen steht der Praxisbezug im Vordergrund und es werden konkrete Projektlösungen besprochen.

Die Partner und ihre Themen: Hirsch – Perimeterschutz & Zutrittskontrolle

Hirsch präsentiert an beiden Veranstaltungstagen sein Gesamtportfolio für physische Sicherheit. Im Bereich Perimeterschutz zeigt Hirsch u.a. zaunmontierte Erschütterungskabel, Infrarotbarrieren, Dual-Technologie-Sensoren, Mikrowellen-Barrieren und unterirdische Kabel.

Highlight ist zunächst „Lumor“, ein faseroptischer DAS-Analysator (Distributed Acoustic Sensing), der Eindringversuche in Echtzeit erkennt, geolokalisiert und klassifiziert – auf Distanzen von bis zu 100 km. Das System eignet sich insbesondere für kritische Infrastrukturen wie Energie, Logistik oder Bahnanlagen.

Im Bereich Zutrittskontrolle steht „Microsesame“ im Fokus: Die Software ermöglicht Multi-Site-, Multi-Technologie- und Multi-Identitäts-Management und unterstützt über 250 Protokolle. Damit lassen sich heterogene Systeme – Video, Biometrie, IT, IoT – in einer einheitlichen Architektur zusammenführen.

Accellence Technologies – Videomanagementsystem

Accellence Technologies aus Hannover präsentiert mit „Vimacc“ eine skalierbare, plattformunabhängige Videomanagementsoftware für anspruchsvolle Sicherheitsanwendungen. Im Fokus des Roadshow-Auftritts stehen vor allem die Tiefenintegration von Infrarotsäulen, mit der Betreiber im Perimeterschutz zur zusätzlichen Absicherung hinter dem physischen einen virtuellen Zaun ziehen können sowie aktuelle Entwicklungen rund um künstliche Intelligenz.

Dabei greift das Unternehmen unter anderem auch Themen auf, die über den klassischen Perimeterschutz hinaus an Bedeutung gewinnen, etwa die Verbindung von Videosicherheit, KI und neuen Anwendungen im Umfeld unbemannter Flugsysteme (Drohnen).

Vivotek – IP-Videoüberwachung

Vivotek präsentiert sein vollständiges Portfolio für IP-Videoüberwachung: Dome-, Bullet-, PTZ-, Fisheye- und Wärmebildkameras für Innen- und Außeneinsatz, ergänzt durch NVR, Switches und PoE-Lösungen. Ein Alleinstellungsmerkmal sind die tief integrierte Cybersecurity-Funktionen.

Alle Informationen

Termine

09. Juni 2026
Werkhalle Rüsselsheim

11. Juni 2026
Radisson BLU Hamburg

Das Programm der „Sicherheitstage 2026“

09:30 – 09:50
Hirsch: Zukunftssichere Zutrittskontrolllösungen für eine praxisnahe Umsetzung der NIS2-Richtlinie

09:50 – 10:10
Accellence Technologies: Videosicherheit trifft Datenschutz

10:10 – 10:30
Vivotek: Intelligente Videoüberwachung in der Praxis

10:30 – 11:30
Gespräche an den Ständen

11:30 – 11:50
Hirsch: Wirkungsvoller Perimeterschutz in sicherheitssensiblen Umgebungen

11:50 – 12:10
Slat: 24/7-Videoüberwachung über das vorhandene Beleuchtungsnetz

12:10 – 12:30
Quanergy: LiDAR als neue Dimension der Detektion und Klassifizierung

12:30 – 13:30 Mittagessen
13:30 – 15:00 Gespräche an den Ständen

Weitere Informationen zur Anmeldung und Programm finden Sie hier: www.hirschsecure.com/germany/de/sicherheitstage-2026

© Hirsch Group

Die Sicherheitstage 2026 von Hirsch finden am 9. Juni in der Werkhalle Rüsselsheim und am 11. Juni im Radisson Blu Hamburg statt

Die Smart-Stream-Technologie des Unternehmens senkt den Speicher- und Bandbreitenbedarf um bis zu 80 %. Auf Softwareseite stehen „Vast“ für lokales Multi-Kamera-Management und „Vortex“ als Cloud-Plattform mit KI-Analyse, AES-256-Verschlüsselung, Multi-Faktor-Authentifizierung und bis zu 365 Tagen Cloud-Speicher – skalierbar ohne eigene Serverinfrastruktur.

Quanergy – LiDAR als neue Dimension der Detektion

Quanergy beleuchtet LiDAR als neue Dimension der Sicherheitsdetektion. Im Vergleich zu Kameras, PIR-Sensoren und Radar liefert LiDAR präzise 3D-Daten, arbeitet licht- und wetterunabhängig und reduziert Fehlalarme erheblich. Das System ist intrinsisch DSGVO-konform, da keine identifizierbaren Bilder entstehen – ein starkes Argument für Anwendungen in kritischer Infrastruktur, Logistik und Smart Spaces.

Slat – Sicherheit ohne dauerhaften Stromanschluss

Slat zeigt, wie sich vorhandene Infrastruktur – etwa das Netz der Straßenbeleuchtung – für eine lückenlose Rund-um-die-Uhr-Videoüberwachung ohne aufwendige Tiefbauarbeiten nutzen lässt. Selbst an Standorten mit nur zeitweiser Stromversorgung ermöglichen intelligente Pufferlösungen autarke, kosteneffiziente Systeme.

Relevant für städtische Überwachung, Perimeterschutz und die Detektion illegaler Müllentsorgung – Slat bringt Sicherheit an Standorte, die bisher als technisch unversorgbar galten.

Hirsch Group
www.hirschsecure.com

Sicherheit als strategischer Erfolgsfaktor

Ein Trendbericht von André F. Kunz, ASW-BW Geschäftsführer

In den vergangenen Jahren hat sich die Welt der Sicherheit für die ASW-BW und deren Mitgliedsunternehmen grundlegend verändert. Sicherheitsfragen betreffen längst nicht mehr ausschließlich physische Schutzmaßnahmen wie Objektschutz, Alarmanlagen oder Wachpersonal. Die fortschreitende Digitalisierung und zunehmende Vernetzung der Wirtschaft haben neue Bedrohungen hervorgebracht, die Unternehmen umfassend betreffen.

Cyberangriffe, Wirtschaftsspionage, hybride Risiken und Störungen in globalen Lieferketten prägen die Sicherheitslandschaft heute mehr denn je. Unternehmen stehen vor der Herausforderung, ihre Sicherheit ganzheitlich zu denken, Risiken frühzeitig zu erkennen und flexibel auf dynamische Bedrohungslagen zu reagieren. Sicherheit ist damit zu einem zentralen Bestandteil moderner Unternehmensstrategie geworden, der technologische, organisatorische und strategische Maßnahmen gleichermaßen erfordert.

Cyber-Bedrohung im Vordergrund

Besonders einschneidend waren in den letzten Jahren mehrere Entwicklungen. Die Digitalisierung hat Cyber-Bedrohungen in den Vordergrund gerückt. Unternehmen müssen nicht nur ihre IT-Systeme schützen, sondern auch sensible Daten, geistiges Eigentum, interne Kommunikationskanäle und zunehmend auch Cloud-Infrastrukturen absichern. Informationssicherheit und Datenschutz sind zu Kernaufgaben geworden, die heute integraler Bestandteil jeder Sicherheitsarchitektur sein müssen.

Gleichzeitig hat sich das Verständnis von Sicherheit deutlich erweitert: Physischer Schutz, Notfallvorsorge, Krisenmanagement, strategische Risikoanalysen und Compliance bilden heute eine untrennbare Einheit. Sicherheit ist nicht mehr nur eine operative Aufgabe, sondern eine strategische Verantwortung, die alle Ebenen eines Unternehmens betrifft.

Eine weitere prägende Veränderung ist die verstärkte Vernetzung zwischen Unternehmen, Sicherheitsbehörden und Verbänden. Der Austausch von Informationen über aktuelle Bedrohungen, Best Practices und Handlungsempfehlungen ist essenziell, um zeitnah auf neue Entwicklungen reagieren zu können. Die ASW-BW übernimmt hierbei die Rolle einer zentralen Plattform, die Wissen bündelt, den Dialog fördert und Unternehmen praxisnah unterstützt. Durch diese Vernetzung können Unternehmen schneller auf Bedrohungen reagieren, sich über innovative Sicherheitslösungen informieren und voneinander lernen. Gerade in Zeiten geopolitischer Unsicherheiten, wirtschaftlicher Turbulenzen oder globaler Krisen zeigt sich, wie wertvoll ein starkes Netzwerk ist.

Integriert, digital, vorausschauend

Blickt man in die Zukunft, lässt sich eine klare Richtung erkennen: Sicherheitsstrategien werden zunehmend integriert, digital und vorausschauend sein. Cyber- und Informationssicherheit werden als unverzichtbare Kernbestandteile jeder Sicherheitsarchitektur etabliert. Die Abwehr von Angriffen allein reicht nicht mehr aus; Unternehmen müssen Risiken proaktiv erkennen, analysieren und ihnen vorbeugen. Künstliche Intelligenz und Automatisierung werden dabei eine Schlüsselrolle spielen. KI-gestützte Systeme können Bedrohungen frühzeitig identifizieren, Muster in Daten erkennen, Anomalien aufspüren und konkrete Handlungsempfehlungen liefern.

Zugleich gewinnt ein ganzheitliches Risiko- und Krisenmanagement an Bedeutung. Sicherheit wird nicht isoliert betrachtet, sondern als strategische Aufgabe verstanden, die alle Unternehmensbereiche betrifft. Know-how-Schutz, Überwachung von Lieferketten, Business Continuity Management und Corporate Security sind künftig noch stärker miteinander verzahnt. Unternehmen müssen resilient sein – das heißt, nicht nur reaktiv auf Störungen zu reagieren, sondern proaktiv Strategien zu entwickeln, um Angriffe, Ausfälle oder Krisen abzufedern.

Darüber hinaus wird die Zusammenarbeit zwischen Staat und Wirtschaft weiter intensiviert. Angesichts globaler geopolitischer Unsicherheiten, komplexer Sicherheitslagen und neuer Bedrohungsszenarien ist der Austausch zwischen Behörden, Sicherheitsverbänden und Unternehmen unerlässlich. In diesem Zusammenhang

35 JAHRE GIT SICHERHEIT

Die GIT SICHERHEIT ist für mich wichtig, weil sie Innovationen eine Bühne gibt und Entwicklungen auf den Punkt bringt – und so seit Jahren verlässlich Orientierung für unsere Branche schafft.

Thomas Quante, CEO Bosch Building Technologies

fungiert die ASW-BW als zentraler Knotenpunkt, der Fachwissen, praxisnahe Lösungen und Vernetzung bündelt. Sie unterstützt Unternehmen dabei, Sicherheit nicht nur als Pflicht, sondern als strategische Chance zu begreifen.

Kultureller Wandel

Neben technologischen und organisatorischen Veränderungen zeigt sich auch ein kultureller Wandel: Sicherheit wird zunehmend als Teil der Unternehmensidentität verstanden. Mitarbeiterinnen und Mitarbeiter werden stärker in Sicherheitsprozesse einbezogen, Awareness-Programme und Schulungen gewinnen an Bedeutung, und Sicherheitsbewusstsein wird auf allen Ebenen gefördert. Ein umfassender Sicherheitsansatz berücksichtigt somit nicht nur Technik und Prozesse, sondern auch die Menschen, die ein Unternehmen ausmachen.

Zusammengefasst zeigt sich: Die Welt der Sicherheit ist komplexer, vernetzter und technologiegetriebener geworden. Physische Schutzmaßnahmen allein genügen nicht mehr. Sicherheitsstrategien müssen digital, integriert und vorausschauend sein, um den dynamischen Bedrohungen unserer Zeit gerecht zu werden. Die ASW-BW nimmt in diesem Wandel eine Schlüsselrolle ein, indem sie Unternehmen befähigt, aktuelle Herausforderungen zu meistern, Risiken frühzeitig zu erkennen und proaktiv auf die Sicherheit der Zukunft vorbereitet zu sein. Sicherheit wird so zu einem strategischen Erfolgsfaktor, der Unternehmen widerstandsfähig, flexibel und zukunftsfähig macht – ein Anspruch, der heute und in den kommenden Jahren immer relevanter wird.

Mit ihrem breiten Spektrum an Fachwissen, praxisnahen Lösungen und der Vernetzung von Wirtschaft und Behörden gestaltet die ASW-BW aktiv die Sicherheitslandschaft mit. Sie zeigt, dass Sicherheit nicht statisch ist, sondern ein dynamischer Prozess, der Innovation, Kooperation und kontinuierliche Anpassung erfordert. Die Zukunft der Sicherheit wird von Intelligenz, Vernetzung und Resilienz geprägt sein – und die ASW BW wird auch weiterhin eine treibende Kraft sein, um Unternehmen auf diesem Weg zu begleiten. GIT

ASW Baden-Württemberg
www.asw-bw.com

© VSW

Sicherheit neu denken

Warum Wirtschaftsschutz zur Schlüsselfrage geworden ist – ein Trendbericht von Peter H. Bachus, Vizepräsident & Vorstand der Vereinigung für die Sicherheit in der Wirtschaft e. V. (VSW)

Das Jahr 2025 markierte eine Zäsur, nicht nur für die Sicherheitsarchitektur Deutschlands, sondern insbesondere für die Rolle der Wirtschaft darin. Aus Sicht des VSW-Bundesverbands hat sich die Welt in den vergangenen Jahren fundamental verändert: Unternehmen sind heute nicht mehr nur Beobachter, sondern längst Akteure in einem komplexen sicherheitspolitischen Gefüge und zunehmend auch Zielscheibe strategischer Angriffe.

Geopolitische Spannungen, hybride Bedrohungen, staatlich gesteuerte Cyberangriffe, Sabotage kritischer Infrastrukturen und gezielte Desinformationskampagnen haben eine neue Qualität erreicht. Hinzu kommen wirtschaftliche Risiken durch fragile Lieferketten, zunehmende Abhängigkeiten und eine wachsende Verwundbarkeit digitaler Systeme. Die Trennlinie zwischen innerer und äußerer Sicherheit verschwimmt zunehmend. Die Konsequenz: Wertschöpfung, Versorgungssicherheit und gesellschaftliche Stabilität stehen gleichermaßen unter Druck. Wirtschaftsschutz ist damit keine isolierte Aufgabe einzelner Unternehmen mehr, sondern ein zentraler Bestandteil nationaler Sicherheitsvorsorge.

Diese Entwicklung war in ihrer Dynamik und Wucht die einschneidendste der vergangenen Jahre. Sie hat offengelegt, dass bestehende Strukturen und Zuständigkeiten vielfach nicht mehr ausreichen. Fehlende rechtliche Klarheit beim Informationsaustausch, fragmentierte Verantwortlichkeiten und unzureichend institutionalisierte Kooperationen zwischen Staat und Wirtschaft bremsen effektive Prävention und erhöhen reale Schadensrisiken. Verzögerungen, Unsicherheiten und Abstimmungsdefizite werden in einer beschleunigten Bedrohungslage selbst zum Sicherheitsrisiko.

Stabile Entwicklung

Der VSW-Bundesverband hat auf diese veränderte Lage konsequent reagiert. 2025 stand im Zeichen des gezielten Ausbaus belastbarer Partnerschaften mit Sicherheitsbehörden und politischen Entscheidungsträgern. Neue Austauschformate, engere Abstimmungsprozesse und eine deutlich intensivierte Zusammenarbeit haben nicht nur den Informationsfluss verbessert, sondern auch das Vertrauen in den Verband nachhaltig gestärkt. Der VSW wird zunehmend als verlässlicher Partner wahrgenommen, der sicherheitspolitische Anforderungen der Wirtschaft bündelt und lösungsorientiert in politische Prozesse einbringt.

Parallel dazu spiegelt sich die gewachsene Relevanz des Wirtschaftsschutzes auch in der positiven Entwicklung unserer Organisation wider. Die stabile wirtschaftliche Entwicklung des Verbands sowie eine steigende Zahl an Fördermitgliedern sind ein klares Signal für die zunehmende Anerkennung unserer Arbeit und die wachsende Sensibilität für sicherheitspolitische Risiken in der Wirtschaft.

Ein sichtbares Zeichen strategischer Weiterentwicklung war 2025 zudem die Umfirmierung des Bundesverbands und der meisten Landesverbände. Dieser Schritt steht für mehr Geschlossenheit, klare Wiedererkennbarkeit und den Anspruch, bundesweit mit einer starken, einheitlichen Stimme aufzutreten. In einer zunehmend komplexen Sicherheitslandschaft sind klare Strukturen und eindeutige Ansprechpartner ein entscheidender Erfolgsfaktor.

Gleichzeitig bleibt der politische Handlungsbedarf erheblich. Wirtschaftsschutz ist eine gesamtstaatliche Aufgabe – doch die dafür notwendigen rechtlichen und strukturellen Rahmenbedingungen sind vielerorts noch unzureichend. Insbesondere beim Informationsaustausch zwischen Unternehmen und Sicherheitsbehörden bestehen weiterhin Unsicherheiten, die präventives Handeln erschweren. Der VSW-Bundesverband positioniert sich daher bewusst als zentrale Schnittstelle zwischen Wirtschaft, Sicherheitsbehörden und Politik, mit dem Ziel, bestehende Lücken zu schließen und tragfähige Strukturen zu etablieren.

Blick nach vorn

2026 wird im Zeichen der Konsolidierung und des gezielten Ausbaus zentraler Handlungsfelder stehen. Dazu gehört vor allem die Schaffung rechtssicherer Grundlagen für den Informationsaustausch – eine Voraussetzung, damit Prävention nicht an Haftungsfragen oder regulatorischen Unsicherheiten scheitert. Ebenso entscheidend ist die strukturelle Stärkung von Public-Private-Partnerships. Kooperationen zwischen Staat und Wirtschaft dürfen kein projektbezogenes Nebenprodukt bleiben, sondern müssen dauerhaft verankert, finanziert und strategisch gesteuert werden.

Darüber hinaus rücken Prävention und Resilienz weiter in den Fokus. Die Widerstandsfähigkeit von Unternehmen, insbesondere im Mittelstand, wird zunehmend zur sicherheitspolitischen Schlüsselressource. Business Continuity Management, strategische Risikovorsorge und Sicherheitskompetenz sind heute zentrale Voraussetzungen für unternehmerische Handlungsfähigkeit. Der VSW wird hier gezielt Impulse setzen und seine Rolle als Plattform zur Bündelung sicherheitsrelevanter Expertise aus Wirtschaft, Wissenschaft und Praxis weiter ausbauen.

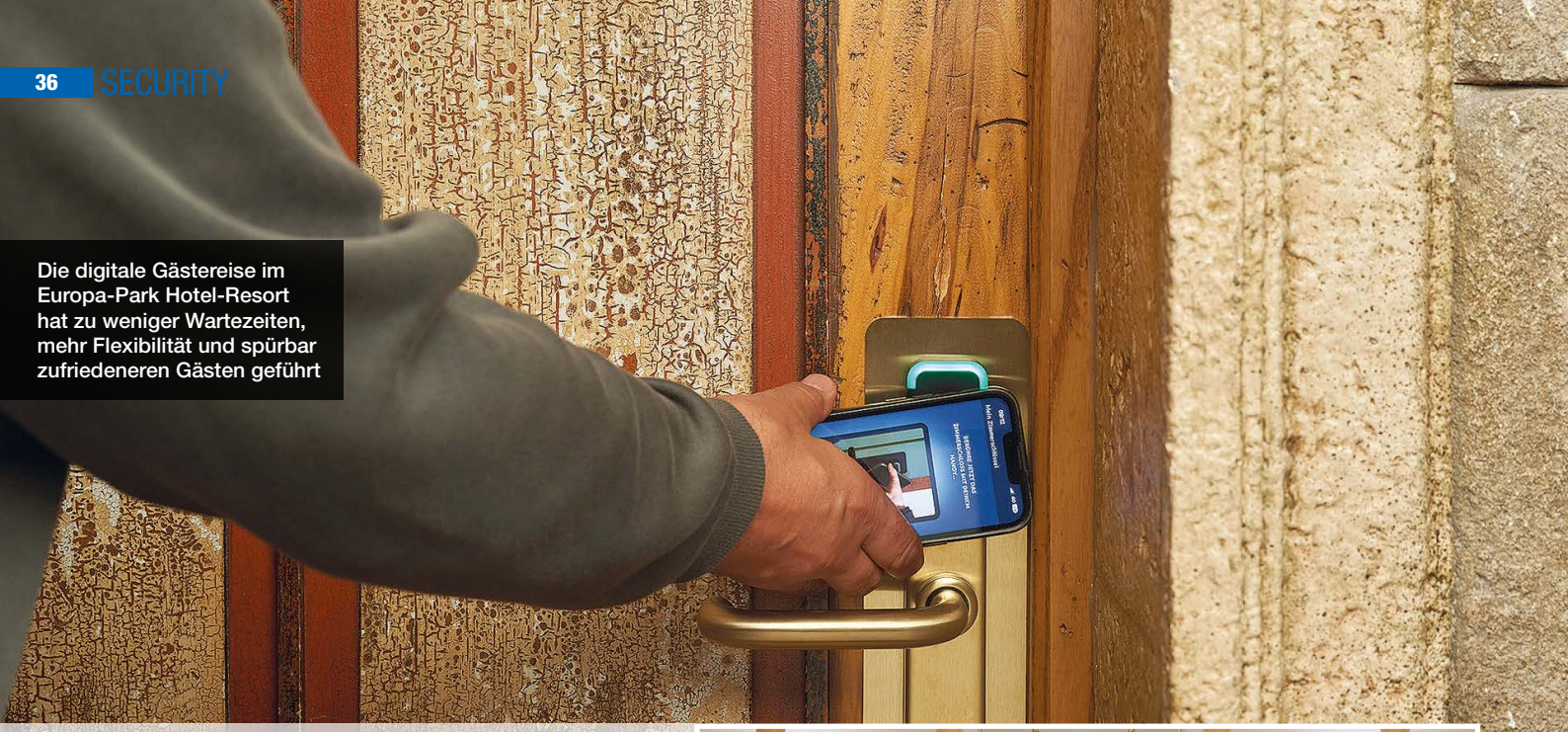
Auch die Entwicklung gemeinsamer Lagebilder, Frühwarnsysteme und abgestimmter Reaktionsmechanismen wird an Bedeutung gewinnen. Gerade im Cyberraum und beim Schutz kritischer Lieferketten braucht es ein eng verzahntes Zusammenspiel aller relevanten Akteure. Sicherheit wird damit zunehmend zur Gemeinschaftsleistung.

Strategisches Ziel

Bis 2029 wollen wir den VSW-Bundesverband als führende Plattform für Wirtschaftsschutz in Deutschland etablieren – als zentralen Ansprechpartner der Politik, als Impulsgeber für eine moderne Sicherheits- und Resilienzpolitik und als koordinierende Instanz für den strukturierten Austausch zwischen Wirtschaft und Sicherheitsbehörden. Denn eines ist offensichtlich: Wirtschaftsschutz ist längst Standortpolitik. Ohne wirksamen Schutz der wirtschaftlichen Basis sind weder Sicherheit noch Wohlstand langfristig zu gewährleisten. Resilienz entscheidet über Wettbewerbsfähigkeit, Innovationskraft und Souveränität.

Die kommenden Jahre werden darüber entscheiden, wie gut Deutschland und Europa auf die Herausforderungen einer neuen sicherheitspolitischen Realität vorbereitet sind. Der VSW-Bundesverband wird diesen Prozess aktiv mitgestalten – gemeinsam mit seinen Partnern in Wirtschaft, Politik und Behörden. GIT

Verband für Sicherheit in der Wirtschaft e. V., VSW-Bundesverband
www.vsw-bundesverband.de

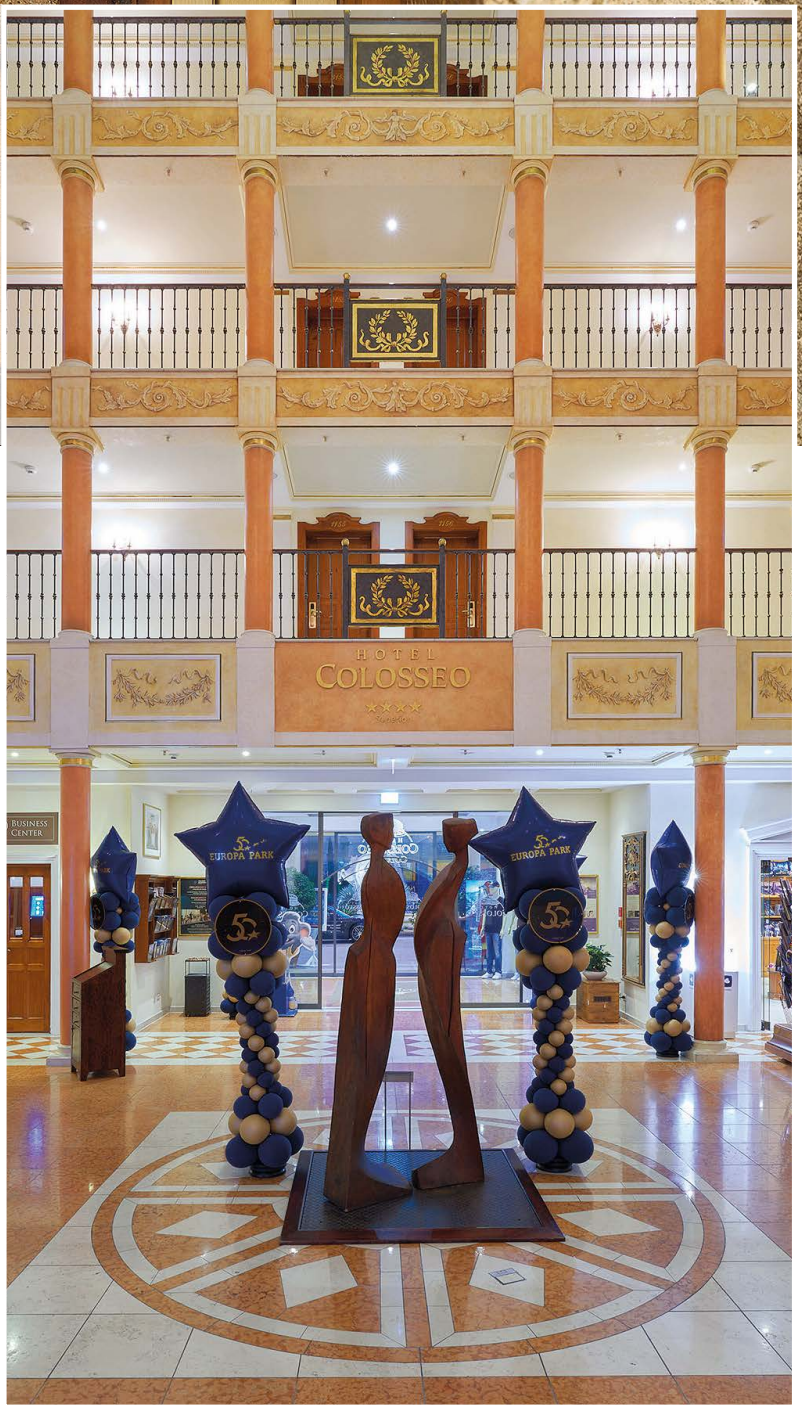


Die digitale Gästereise im Europa-Park Hotel-Resort hat zu weniger Wartezeiten, mehr Flexibilität und spürbar zufriedeneren Gästen geführt

ZUTRITT

App in den Urlaub

Europa-Park Hotel-Resort digitalisiert Zutritt und Gästereise



© Bilder: Salto

Das Europa-Park Hotel-Resort hat sein digitales Serviceangebot weiter ausgebaut und eine umfassende Zutrittslösung von Salto eingeführt, die vollständig in die bestehende Europa-Park „Hotels App“ von Hotelsuite integriert ist. Die Lösung deckt die gesamte Gästereise von der Buchung bis zum Check-out ab und sorgt für mehr Komfort, Effizienz und Flexibilität für Gäste und Personal.

Mit der neuen Zutrittslösung wurde ein zentrales Ziel erreicht: Sämtliche Interaktionen der Gäste sollten digital, intuitiv und ohne Medienbruch funktionieren. Gleichzeitig galt es, die Prozesse im Hintergrund zu automatisieren, die Verwaltung effizienter zu gestalten und den Wartungsaufwand zu senken. Die „Hotels App“ von Hotelsuite spielt dabei eine Schlüsselrolle. Sie ermöglicht nicht nur den digitalen Zugang zu den Zimmern, sondern vereint ebenso Buchung, Ticketing, Tischreservierungen, das Hotel-Friends-Treueprogramm, Wellness Services und vieles mehr. Über Schnittstellen bindet sie ebenso die Eintrittskarten für den Europa-Park und die Wasserwelt Rulantica ein, was zu einer

spürbaren Zeitersparnis und reduzierten Arbeitsbelastung an der Rezeption führt.

Neben der digitalen Integration hatte das Projekt hohe gestalterische und bauliche Anforderungen zu erfüllen. Die Hardware der Zutrittslösung musste sich harmonisch in die thematisch gestalteten Hotels einfügen. Zudem waren umfangreiche Brandschutzvorgaben einzuhalten, die eine Vielzahl unterschiedlicher Türtypen und acht verschiedene Hersteller betrafen. Die enge Abstimmung zwischen allen Beteiligten – dem Europa-Park Hotel-Resort, dem Salto Fachpartner Koch Freiburg und der Open New Media als Anbieter der App-Lösung – war dabei entscheidend für das Gelingen des Projekts. Das sorgte für reibungslose Abläufe und dafür, dass die technischen Komponenten, die App-Integration und das Nutzererlebnis optimal zusammenspielen.

Seit der Inbetriebnahme zeigt die Lösung hervorragende Ergebnisse, wie die Beteiligten berichten: Die Gäste nehmen die mobilen Schlüssel sehr gut an – bereits mehr als die Hälfte nutzt sie aktiv. Defekte Ausweiskarten gehören der Vergangenheit an. Außerdem haben sich die Warteschlangen beim Check-in und Check-out deutlich reduziert. Das Personal profitiert zugleich von automatisierten Abläufen. So bleibt mehr Zeit für die Betreuung der Gäste, während Routineaufgaben im Hintergrund effizienter organisiert sind. GIT

Salto Systems GmbH
www.saltosystems.de

Seit 35 Jahren steht GIT SICHERHEIT für eine hochwertige und verlässliche Berichterstattung in der Sicherheitsbranche. Die klare Einordnung von Trends, Normen und Lösungen bietet eine wichtige Orientierung im Arbeitsalltag. Zugleich ist der persönliche Kontakt über all die Jahre hinweg ein prägendes Element geblieben. Für die Zukunft wünschen wir allen, die zum Gelingen von GIT SICHERHEIT beitragen, weiterhin viel Erfolg.

Christian Kühn und Marius Schanz,
Geschäftsführer bei Schlentzek & Kühn

35 JAHRE GIT SICHERHEIT

Team mit Technik beim Testen

SERIE: TESTGELÄNDE IM TEST – TEIL 2

Drohnen im Visier

Praxisnahe Drohnendetektion: Radar, Video, Audio und KI im realen Testeinsatz bei Walaris

Keine Showrooms, keine PowerPoint-Bühnen – sondern Umgebungen, in denen Sicherheitstechnik zeigen muss, was sie wirklich kann. In Teil 2 der Serie „Testgelände im Test“ war GIT SICHERHEIT gemeinsam mit dem Sachverständigen Markus Piendl auf dem Testgelände der Walaris GmbH unterwegs. Im Fokus: praxisorientierte Prüfungen unterschiedlicher Sensoren zur Drohnendetektion, KI-gestützte Videoanalyse sowie das hauseigene Command-and-Control-System (C2).

Dipl.-Phys. Johannes Hölzl, Geschäftsführer der Walaris GmbH

Das Thema Drohnenschutz gewinnt angesichts wachsender Bedrohungslagen in urbanen Räumen und bei kritischen Infrastrukturen deutlich an Bedeutung. Auf dem Testgelände von Walaris untersucht Markus Piendl für GIT SICHERHEIT Radar-, Audio-, Remote-ID- und Videosensorik – jeweils im Zusammenspiel mit KI-basierter Auswertung und dem zentralen C2-System. Gleichzeitig wurden mit dem Hersteller konkrete Weiterentwicklungsmöglichkeiten für Betreiber kritischer Infrastrukturen diskutiert.

Das „Drei-in-Eins-Testgelände“ – und wie es dazu kam

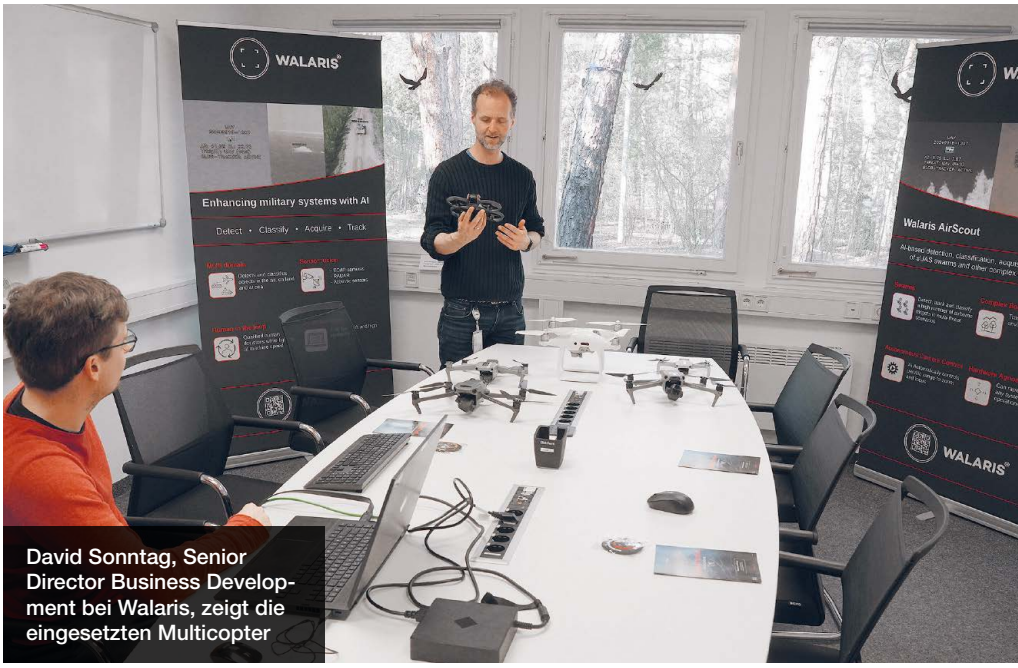
Walaris ist ein auf KI-gestützte Lageerkennung spezialisiertes Unternehmen für Drohnen- und Perimeterschutz. Das globale Headquarter befindet sich in Atlanta (USA), die deutsche Gesellschaft inklusive Entwicklung ist in Nürnberg ansässig. Seit der Gründung im Jahr 2017 hat sich Walaris von einem Anbieter optik- und KI-basierter Drohnenerkennung zu einem breit aufgestellten Spezialisten für autonome Lagebilder weiterentwickelt.

Zu den Kunden zählen Militär, Behörden sowie Betreiber kritischer Infrastrukturen. Rund 40 Mitarbeitende arbeiten an

der Softwareplattform AirScout Verify, die Sensordaten in Echtzeit verarbeitet, Bedrohungen erkennt, klassifiziert und verfolgt. Ergänzt wird dies durch ein eigenentwickeltes C2-System, in dem zahlreiche Sensoren über Schnittstellen intelligent in einer Multisensor-Oberfläche zusammengeführt werden.

Das firmeneigene Testgelände – dessen genaue Lage nicht öffentlich genannt werden darf – ist umfassend gesichert: Zäune, Kameras, Perimeter-Sensorik und Sicherheitspersonal sorgen für kontrollierten Zugang. Der besondere Mehrwert liegt jedoch in der Struktur des Geländes selbst: Ein Waldstück mit Lichtung, ein Gebäude sowie die Möglichkeit zur Installation von Systemen auf Langdistanz ermöglichen drei realistische Anwendungsszenarien an einem Ort.

Die Entscheidung für ein eigenes Testgelände ist historisch gewachsen. Erste Tests fanden in einfachen Holzbaracken statt – nur wenige Meter von einer Freifläche entfernt. Mit steigenden Projektanforderungen, insbesondere aus dem militärischen und behördlichen Umfeld, wurde der Platz knapp. Heute nutzt das Technikteam das Gelände exklusiv, während Verwaltung sowie große Teile der Software- und KI-Entwicklung in Nürnberg angesiedelt sind.



David Sonntag, Senior Director Business Development bei Walaris, zeigt die eingesetzten Multicopter

Der Besuch von Markus Piendl im März 2026 resultierte aus mehreren konkreten Anfragen von Bedarfsträgern. Gesucht wurde jeweils eine leistungsfähige, zuverlässige und bezahlbare Drohnendetektion auf Basis von Radar, Video, Audio, Remote-ID und ADS-B – ergänzt durch KI-Analyse und ein in Europa entwickeltes C2-System.

Bitte umblättern ▶

„Gelungene Generalprobe für anstehende Termine“

GIT SICHERHEIT: Herr Sonntag, welche Rolle spielt das Testgelände für Ihre Arbeit?

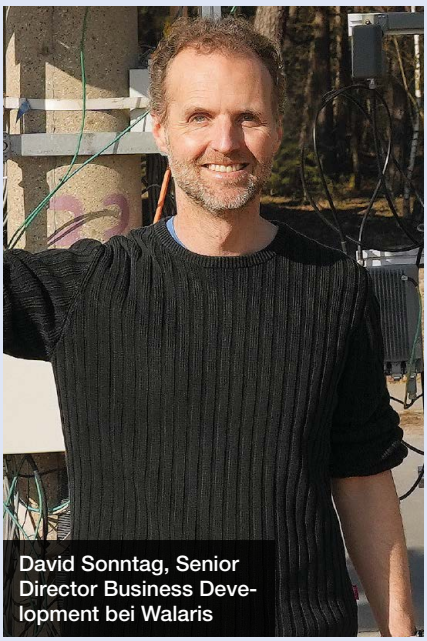
David Sonntag: Unser Testgelände liefert uns wertvolle Hinweise, wie sich Sensoren im realen Einsatz verhalten. Gemeinsam mit Markus Piendl haben wir ein sehr klares Verständnis für Stärken und Grenzen der einzelnen Komponenten entwickelt. Deshalb setzen wir konsequent auf einen Multisensor-Ansatz.

Warum ist das so? Gibt es nicht den einen Sensor für alles?

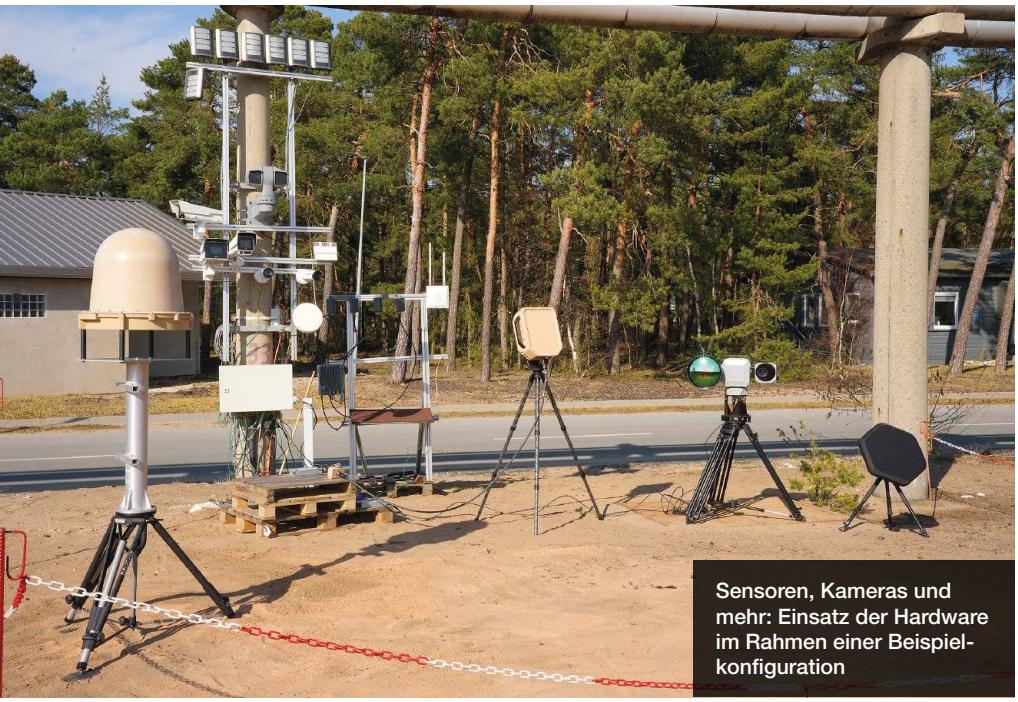
David Sonntag: Nein. Kein Sensor kann für sich allein alle Drohnen erkennen. RF-Sensoren stoßen bei autonom fliegenden Drohnen an Grenzen, Akustiksensoren sind reichweitenbeschränkt und Kameras benötigen freie Sicht. Entscheidend ist, die Stärken von Radar, Video, Audio, RF und Remote ID standortabhängig zu kombinieren. Erst danach folgt – je nach rechtlichem Rahmen – die Abwehr. Sollte das Budget des Endkunden sehr beschränkt sein, kann eine Basislösung mit Remote-ID und Kameras eine erste Option sein, die zu einem späteren Zeitpunkt bei einer erhöhten Gefährdungslage erweitert wird. Die berühmte ‚eierlegende Wollmilchsau‘, also ein Alleskönner-Sensor, hat sich bis heute bei uns noch nicht vorgestellt.

Wie profitieren Sie von unabhängigen Tests, wie wir ihn heute und in dieser Form durchführen?

David Sonntag: Wir erwarten zeitnah den Besuch verschiedener Kunden auf unserem Testgelände, um unser neu entwickeltes C2 zu demonstrieren, das im Laufe des Jahres 2026 zur Verfügung stehen wird. Auf diese Begehungen sind wir nach den gemeinsam durchgeführten Tests jetzt bestens vorbereitet. Das war unsere C2-Generalprobe, bei der wir sehr viel gelernt haben. Die Vorschläge von Markus Piendl befinden sich in der technischen Bewertung – einige davon bereits in der Umsetzung. Ein voller Erfolg also für alle Beteiligten. Ich rate anderen Anbietern in der Sicherheitstechnik, ebenfalls in ein Testgelände,


David Sonntag, Senior Director Business Development bei Walaris

egal ob klein oder groß, Zeit und Nerven zu investieren. Viele Streitkräfte verfahren nach dem Prinzip: Schweiß in der Ausbildung spart Blut im Einsatz. Im übertragenen Sinn trifft das genauso auf Testgelände zu. Hard- und Software, die über einen längeren Zeitraum ausführlich von Profis getestet, bewertet, eventuell auch überarbeitet wird, besteht auch im Ernstfall.



Sensoren, Kameras und mehr: Einsatz der Hardware im Rahmen einer Beispielkonfiguration

Sensorik und Systemintegration im Fokus

Dann geht es an die Tests. Dafür bereitet das Walaris-Team eine Beispielkonfiguration vor. Zum Einsatz kommen unter anderem 3D-Radarsensoren für kurze sowie mittlere bis lange Reichweiten, verschiedene Kamerasysteme von Axis und OpenWorks, ein Akustiksensor von Squarehead, ein Remote-ID-Sensor von Dronetag sowie ADS-B zur Erfassung kooperativer Luftfahrzeuge.

RF-basierte Sensoren werden bewusst nicht eingesetzt, da diese in vielen Projekten bereits vorhanden sind und ihre Meldungen über Schnittstellen in das Walaris-System integriert werden können. Softwareseitig verarbeitet die KI-gestützte Videoanalyse AirScout Verify die Videostreams direkt am Edge, während das C2-System alle Sensordaten in einer gemeinsamen Lageansicht zusammenführt.

Als Recheneinheit dient ein robuster Edge-Server mit Nvidia Jetson AGX Orin. Für Nachttests kommt leistungsfähige Beleuchtungshardware zum Einsatz.

Übersicht:

- 3D Radarsensoren Echoguard (kurze Reichweite) und EchoShield (mittlere bis lange Reichweite)
- Q6225 sowie weitere Axis-Kameramodelle
- VisionFlex IR900XHD und HD360 EO Kamera von OpenWorks
- Discovair G2 von Squarehead
- dronetag Scout von dronetag
- ADS-B (Automatic Dependent Surveillance – Broadcast)

Ablauf der Prüfungen und Kriterien

Die Vorbereitung der Testflüge erfolgen im Schulungsraum. David Sonntag, Senior Director Business Development bei Walaris, erläutert die eingesetzten Multicopter und die jeweiligen Testziele. Diese reichen von

„Testgelände – neu gedacht“

GIT SICHERHEIT: Herr Piendl, welchen Nutzen hatte Ihr Besuch bei Walaris?

Markus Piendl: Besonders ist die Kombination aus Wald, Gebäude und Langdistanztests an einem Ort. Besucher können ihre eigenen Szenarien realistisch nachstellen.

Was zeichnet das Testgelände aus?

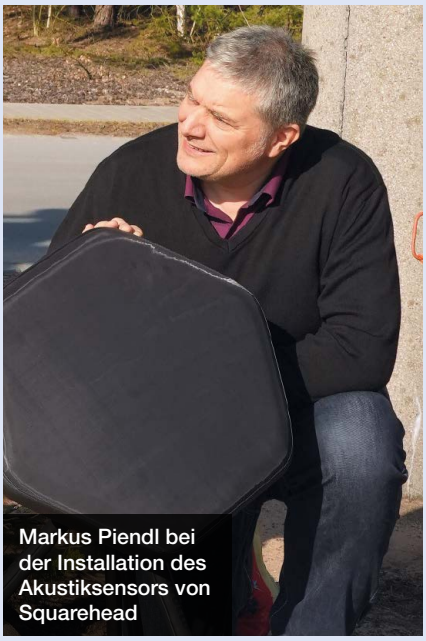
Markus Piendl: Das Technikteam ist vor Ort, Sensoren lassen sich schnell installieren und einmessen. Tag- und Nachttests, Nah- und Fernflüge – alles ist möglich.

Welche Empfehlungen geben Sie Errichtern und Betreibern aufgrund der Erfahrungen bei Walaris?

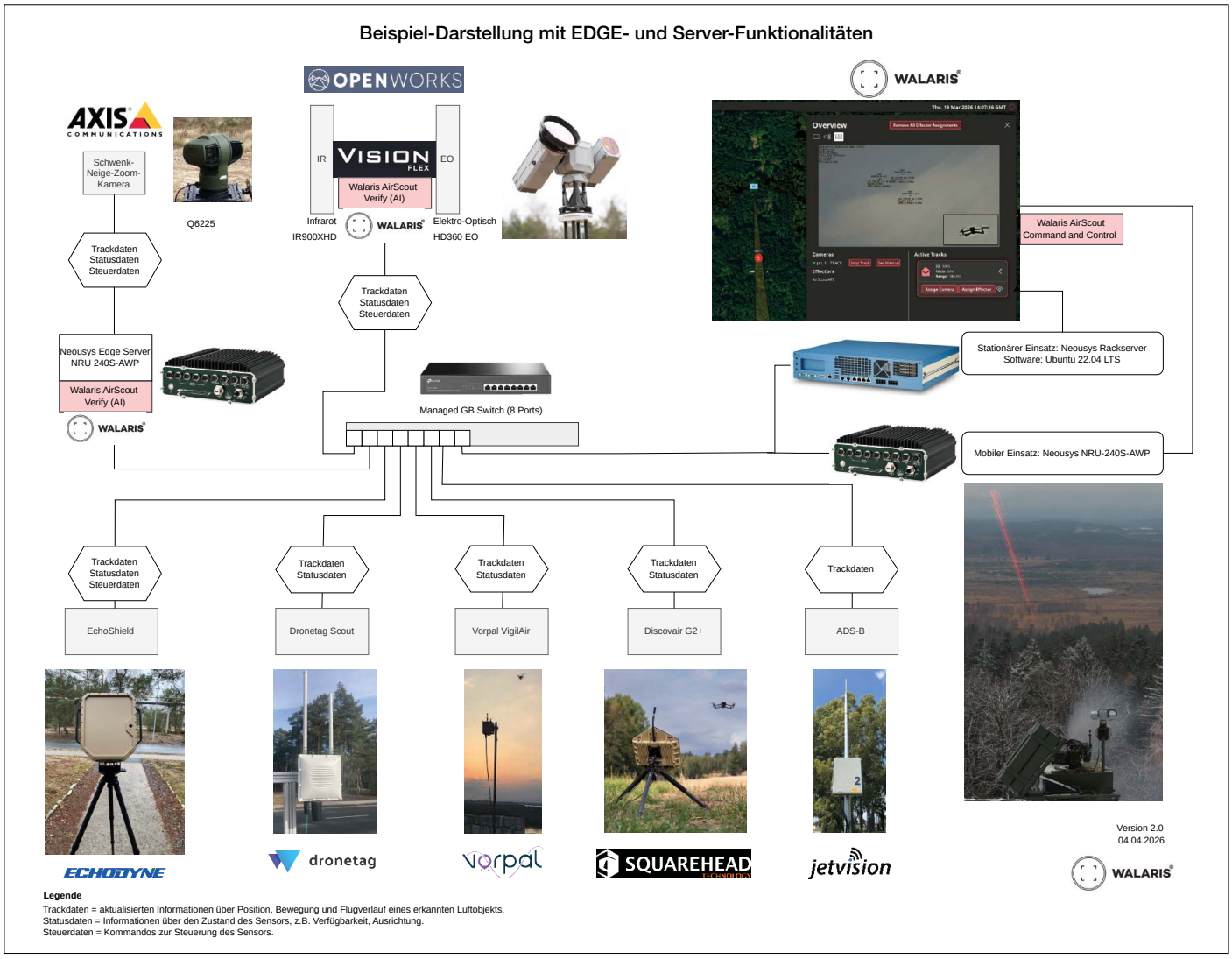
Markus Piendl: Der modular auswählbare Ansatz von Walaris ist besonders. Es besteht die Möglichkeit, unterschiedliche Sensoren für sich allein, aber auch im Zusammenwirken mit anderen Sensoren ausführlich zu testen. Nehmen wir als Beispiel den direkten Vergleich zwischen DJI Aeroscope und Dronetag Scout, der aktuell viele Behörden interessiert. Die Reichweite der beiden Echodyne-Hardwarekomponenten zu sehen, war beeindruckend. Viele Endkunden interessiert die Detektion via Radar und die Verifikation und Analyse via Video: das ist bei Walaris sowohl auf Basis von Axis als auch OpenWorks im praktischen Einsatz im Rahmen einer Verifikation als auch mit KI gestützten Algorithmen durch Walaris AirScout Verify erlebbar. Eine weitere Besonderheit war der Einsatz des robusten Jetvision ADS-B Empfängers, mit der kooperative Luftfahrzeuge passiv, rechtlich unkritisch und mit geringer Integrationshürde in Echtzeit erfasst und Positionsdaten direkt angezeigt wurden. Das ist bei der Unterscheidung Drohne, Hubschrauber und/oder Flugzeug ein großer Vorteil.

Was macht gute Drohnen-Detektion aus?

Markus Piendl: Früh, zuverlässig, präzise, falschalarmarm, integrierbar und betreibbar. Ein System muss auch nachts, bei schlechtem Wetter und in komplexen Umgebungen funktionieren – ohne den Operator zu überfordern. Genau das ließ sich hier hervorragend nachstellen und prüfen. Danke, dass ich für die Leserinnen und Leser der GIT SICHERHEIT vor Ort sein durfte.



Markus Piendl bei der Installation des Akustiksensors von Squarehead



Detektionsentfernungen über Track-Aufbau und -Stabilität bis hin zur Integration der Sensoren in das C2-System.

Die standardisierten Flugprofile umfassen Direkt- und Queranflüge, Ab- und Kreisflüge, Hovern, Steig- und Sinkflüge sowie den Einsatz von Schwärmen. Der hohe Realitätsbezug war und ist für beide Seiten entscheidend.

David Sonntag: „Wir haben in der Vergangenheit mit Markus Piendl in mehreren kritischen Einsatzlagen sehr erfolgreich zusammengearbeitet. Mir gefiel an allen unseren gemeinsamen Tests der starke Realitätsbezug und die Tatsache, dass wir die Anforderungen an unser C2 Schritt für Schritt erhöht haben."

Ergebnisse: belastbare Daten und konkrete Weiterentwicklungen

Markus Piendl als kritisch bewertender Sachverständiger schließlich ist zufrieden: Alle Drohnenflüge wurden erfolgreich detektiert. Die Testergebnisse konnten live verfolgt und unmittelbar ausgewertet werden.

Johannes Hölzl fasst zusammen: „Die Ideen zur Weiterentwicklung von Markus Piendl betrafen unter anderem die graphische Aufbereitung der Sensordaten. Wichtig ist uns, dass der der Operator schnell zwischen ADS-B Informationen (zivile und militärische Luftfahrzeuge), guten Drohnen, die etwa im Rahmen einer Veranstaltung eingesetzt werden, und böse Drohnen unterscheiden kann. Ferner empfahl uns Piendl, die verwendete Datenbank gegen Manipulation im Kontext digitaler Forensik zu schützen. Wir haben aufgrund der Anforderungen aus aktuellen Projekten mit Herrn Piendl überlegt, welche Lösungen es zum Beispiel für Klein- und Großstädte im Rahmen einer Mietvariante geben könnten. Wir teilen die Meinung, dass sich aktuell sowohl Unternehmen aber auch Behörden aus Ressourcengründen zu Interessens- und Arbeitsgemeinschaften zusammentun, um das Thema Drohnenschutz organisatorisch und finanziell zu bearbeiten. Piendls Empfehlung war, dass wir kurz- bzw. mittelfristig eine cloudbasierte Lösung in unser Portfolio aufnehmen. Gut gefallen haben uns auch Piendls Ideen zu einer strukturierten Auswertung der Datenbank in Form standardisierter Berichte vor, während und nach einem Einsatz. Gemeinsam überarbeitet haben wir auch die Darstellung der System-Architektur-Übersicht mit Edge/Server-Funktionalitäten sowie Bandbreiten für die einzelnen Sensoren." (Grafik oben)

Die Verbesserungsvorschläge von Piendl betrafen u.a. die Darstellung der verschiedenen Sensordaten sowie der Luftlage, also ziviler und militärischer Flugverkehr, gute und böse Drohnen. Besonderes Augenmerk galt der verwendeten Datenbank, der Struktur, Auswertbarkeit sowie dem Schutz im Hinblick auf Manipulation.

Darüber hinaus wurden Mietmodelle für Städte und Kommunen diskutiert, ebenso perspektivischer Ausbau um Cloud-Lösungen. Auch standardisierte Berichte vor, während und nach Einsätzen sowie eine überarbeitete Darstellung der Systemarchitektur fließen in die Weiterentwicklung ein. Fazit: Wichtige Erkenntnisse gewonnen, umfangreiche Tests erfolgreich bestanden, Weiterentwicklung angestoßen. GIT

Walaris GmbH
www.walaris.com

© Bilder: Walaris

PRAXIS & PROJEKTE

Best of Perimeter

Perimetersicherheit im Realbetrieb: Experten berichten über ihre besten Projekte, spektakuläre Herausforderungen – und zeigen, worauf es heute und morgen wirklich ankommt

4 FRAGEN

9 x 4 Fragen und Antworten: Zum 35-jährigen Geburtstag der GIT SICHERHEIT haben ausgewiesene Spezialisten aus den Bereichen Perimeter-, Video- und Drohnensicherheit drei zentrale Fragen zu besonders anspruchsvollen Projekten, prägenden Herausforderungen und zukünftigen Entwicklungen beantwortet. Die Antworten geben einen offenen Einblick in reale Schutzkonzepte, technische Grenzen, erfolgreiche Ansätze – und in das, was moderne Perimetersicherheit heute leisten muss.

1 Welches Ihrer Projekte im Bereich der Perimetersicherheit steht für Sie beispielhaft für die Anforderungen und Möglichkeiten moderner Sicherheitslösungen?

Gerhard Harand (Wehrhan TPS): Wir haben vor kurzem ein Projekt für einen Gas-Infrastruktur-Betreiber in einer Großstadt erfolgreich umgesetzt. Besonders war, dass mehrere Detektionstechnologien kombiniert wurden. Der Endkunde war bereits vor der Beauftragung gemeinsam mit Markus Piendl auf unserem Testgelände und konnte unter anderem die Radar-Detektion selbst ausprobieren. Dieses Vorgehen brachte einen hohen Erkenntnisgewinn für alle Beteiligten und schuf Vertrauen. Der Endkunde verfügte bereits über viel Erfahrung im Perimeterbereich und kannte Themen wie Detektionswahrscheinlichkeit, Fehlalarme und technologische Grenzen sehr genau.

Testbericht über das Wehrhan-TPS Testgelände

Frank Pokropp (Freihoff): Vor wenigen Monaten haben wir die Absicherung mehrerer großer unterirdischer Gasspeicher umgesetzt. Bei solchen Anlagen ist die Besonderheit, dass das eigentliche Speichervolumen unter Tage liegt, die kritischen Angriffspunkte aber überwiegend oberirdisch an den Betriebsanlagen entstehen. Die Anforderungen waren insbesondere bei IT-Themen wie IT-Sicherheit, sichere Datenkommunikation und die Integration in eine bestehende Leitstellenstruktur hoch. Der Betreiber legte großen Wert auf Verfügbarkeit und Stabilität. Entscheidend war, ein durchgängiges Sicherheitskonzept zu entwickeln, das nicht nur die klassische Perimetersicherheit abbildet, sondern auch die bestehende IT-Infrastruktur berücksichtigt. Die Abstimmungen mit den IT-Verantwortlichen waren nicht immer einfach und haben Zeit gekostet – im Rückblick aber genau der Punkt, der den Unterschied gemacht hat.

Peter Zehetner (i-Alarmsysteme/Schloss+Riegel): Ein besonderes Projekt für uns war die Absicherung eines großen, international tätigen Automobillogistikers. Die erste Besonderheit ist die Art des Schutzguts: Es geht häufig nicht um ein einzelnes Hochwertobjekt, sondern um sehr viele Fahrzeuge gleichzeitig – in diesem Fall auf mehreren großen Freiflächen, in Reihen, mit hoher Umschlaggeschwindigkeit. Dadurch ist das Risiko weniger der Einzelangriff, sondern eher Diebstahl, unbefugte Entnahme, Teilentwendung, Manipulation, Vandalismus oder das unbemerkte Ausschleusen einzelner Fahrzeuge oder Fahrzeugteile. Fehlen Fahrzeuge oder sind Fahrzeugteile beschädigt, kann unser Endkunde nicht liefern und wird vertragsbrüchig – das galt es in jedem Fall zu verhindern. Die Behörde und die Experten Markus Piendl und Hannes Dopler legten besonderen Wert auf eine erstklassige Videoanalyse.

Stefan Blohm (Raytec): In den vergangenen Jahren haben wir eine Reihe von Raytec Vario2-Scheinwerfer für die Grenzabsicherung in Polen, Lettland, Finnland und Estland geliefert. Unsere Beleuchtungskörper sind von entscheidender Bedeutung für eine klare und verlässliche Bildgebung bei Nacht. Zudem tragen sie wesentlich zur wirksamen Unterstützung des Perimeterschutzes bei. Die Sicherung von Grenzen erfordert eine multifunktionale Beleuchtung, die nicht nur die Ausleuchtung, sondern auch die Detektion, Beobachtung, Identifikation, Abschreckung und Einsatzunterstützung gewährleistet – oft in großen, abgelegenen und witterungsbelasteten Bereichen. Häufig müssen wir uns mit Mitbewerbern auseinandersetzen, die in ihren Datenblättern mit falschen Angaben zu Lichtleistungen und Reichweiten werben.

Gutes Licht am Perimeter: warum das für Projekte entscheidend ist

Rainer Gräfendorf (Honeywell): Ein Projekt, das mir bis heute in Erinnerung geblieben ist betraf die Absicherung eines großenn Solarparks in Ostdeutschland die wir gemeinsam mit unserem Partner Styx effektiv durchgeführt haben. Vier professionelle Diebstähle


© Dallmeier/Benjamin Knobloch

Christian Linthaler, Dallmeier


© Freihoff

Frank Pokropp, Freihoff


© Optex

Johannes Faber, Optex


© Raytec

Stefan Blohm, Raytec


© Peter Zehetner

Peter Zehetner, i-Alarmsysteme/Schloss+Riegel


© Walaris

David Sonntag, Walaris


© Concepts 4 Security

Andreas Keller, Keller Sicherheitstechnik


© Wehrhan TPS

Gerhard Harand, Wehrhan TPS


© Honeywell

Rainer Gräfendorf, Honeywell


© SMP

Markus Piendl, SMP

sowie zwei Brände mit einer Schadenshöhe im sechsstelligen Bereich im vermeintlich sicheren Deutschland machten, wieder einmal, deutlich, dass Sicherheit messbar funktionieren und Angriffen der Gegenseite standhalten muss. Heutige Perimeter-Sicherheitslösungen bestehen nicht aus einem einzelnen Produkt, sondern aus einer Risikobewertung, herstellerneutraler Planung, Leitstellenanbindung, IT-Aspekten, Testbarkeit und Betriebsrealität. In diesem Projekt waren wir als Hersteller ebenso wie der Sicherheits-Errichter gefordert: es durfte nichts schiefgehen – und wir waren erfolgreich.

Draußen bei den Wildschweinen: Praxisbericht-Bericht Perimeterschutz im Solarpark

Andreas Keller (Keller Sicherheitstechnik, Concepts 4 Security): Gerne berichte ich von der Absicherung zweier Photovoltaik Großprojekte. Ein anspruchsvolles Projekt mit 10 Megawatt befand sich in der Region Venetien, ein anderes mit Projekt mit 80 MW in Ostdeutschland. In beiden Projekten hatte die Ergo-Versicherung Mindestanforderungen für die Perimeter-Sicherheit definiert. Der Verfasser dieser herstellerneutralen Mindestanforderungen war Markus Piendl. Mit ihm konnten wir in den vergangenen Jahren viele Projekte erfolgreich bearbeiten. Als Sicherheits-Errichter war ich dankbar dafür, dass es Mindestanforderungen gab. Damit war klar, was ich für die ehemaligen militärischen Liegenschaften, auf denen nun Strom erzeugt wurde, anbieten und installieren musste.

Christian Linthaler (Dallmeier): Vor fünf Jahren standen wir vertrieblich mit einem Anbieter im Kontakt, der für Hoch- und Höchstspannungsnetze zuständig ist. Das Unternehmen hatte diverse Standorte identifiziert, die es professionell vor unberechtigtem Zutritt zu schützen galt. Dabei bestand von Anfang an die klare Vorgabe, ausschließlich NDAA-konforme Lösungen einzusetzen. Das kam uns als Hersteller von hochwertiger Video-Soft- und -Hardware ‚made in Germany' entgegen. Sämtliche eingesetzten Komponenten bedurften einer finalen Freigabe durch die IT-Abteilung. Eine Besonderheit war die eigene Leitstelle des Endkunden, deren Mitarbeiter ein großes, nachvollziehbares Interesse daran hatten, nur qualifizierte Alarme abzuarbeiten.

Johannes Faber (Optex): In den vergangenen Monaten hat mich ein großer Industriekunde auf Trab gehalten, der seinen Produktionsstandort absichern wollte. Der Beschaffungsprozess zog sich über mehrere Jahre, da der Standort im Lauf der Zeit mehrfach aus- und umgebaut wurde. Für einen Produktionsstandort hat eine Perimeter-Absicherung zentrale Bedeutung, weil sie die erste Schutz- und Frühwarnlinie gegen unbefugtes Eindringen, Diebstahl, Sabotage und Störungen des Betriebs bildet. Der Perimeter war für diesen Endkunden der Schlüssel für Abschreckung, Erkennung, Verzögerung und Reaktion. Besonders an diesem Projekt war, dass die Detektionsflächen räumlich sehr beschränkt waren und der Endkunde an dem Einsatz einer guten Drohne interessiert war, um Infrastrukturkosten zu minimieren.

David Sonntag (Walaris): Vor einigen Wochen haben wir eine der größten Sportveranstaltungen in Europa im Rahmen einer professionellen Drohnen-Detektion und Drohnen-Abwehr zuverlässig in einer Großstadt abgesichert. Vor Ort kam ein Multisensoransatz zum Einsatz. Selbstbau- und kommerzielle Drohnen wurden durch Sensoren auf Basis von Radar, Radiofrequenz, Video, Remote-ID und ADS-B detektiert und in unserem Command and Control System fusioniert. Ferner stellte ein Telekommunikationsanbieter eine Drohnendetektion auf Basis von 4G/5G im Rahmen einer nachträglichen Auswertung von Funkzellen zur Verfügung. Eine Abfangdrohne stand in ständiger Bereitschaft, die im Fall der Fälle von der Behörde bei Ausschluss der Gefahr für Dritte zum Einsatz gekommen wäre.

Bitte umblättern ▶

Luftaufnahme Projekt Keller Sicherheitstechnik, Concepts 4 Security

2 Welche Herausforderungen haben dieses Projekt besonders geprägt – und welche Lösungen haben sich in der Praxis bewährt?

Gerhard Harand: Die Liegenschaft des Endkunden war verschachtelt. Es gab keinen linearen Zaunverlauf. Zudem gab es sogenannte Ex-Zonen, also Bereiche mit Explosionsgefahr. Dort kann sich eine explosionsfähige Atmosphäre bilden, also ein Gemisch aus brennbaren Gasen, Dämpfen, Nebeln oder Stäuben mit Luft, das durch eine Zündquelle entzündet werden kann. Die angesprochene Stadtlage war besonders. Wir haben vor Ort mit Zaun-, Boden- und Radarsensorik sowie PTZ-Kameras installiert und ein sogenanntes Double-Knock-Verfahren angewandt. Ein Vollalarm wird erst dann ausgelöst, wenn zwei voneinander unabhängige Detektionen stattfinden. Das Ziel, Fehlalarme deutlich zu reduzieren, wurde durch die Kombination verschiedener Technologien sofort erreicht.

Frank Pokropp: In unserem Projekt kamen ein Alarmzaun, Videoüberwachung, Zutrittskontrolle sowie ein Gefahrenmanagement zum Einsatz. Das Gefahrenmanagementsystem hat in die Aufgabe, alle sicherheitsrelevanten Meldungen und Systeme in einer zentralen Bedien- und Auswerteplattform zusammenzuführen. Es ist damit das Leit- und Entscheidungssystem über dem eigentlichen Perimeterschutz. Statt einzelne Sensoren getrennt zu betrachten, bündelt das System alle Informationen in einem gemeinsamen Lagebild. Den Endkunden konnten wir durch eine ausführliche technische Dokumentation überzeugen; das ist im Umfeld eines KRITIS-Projekts außerordentlich wichtig und wird in vielen Sicherheitsprojekten, egal ob klein oder groß, häufig vernachlässigt.

Peter Zehetner: Die Liegenschaft des Endkunden war unübersichtlich. Es gibt keinen durchgängigen Zaun-Verlauf, sondern viele Ecken und Kanten. Da es noch zu keinem Diebstahl gekommen war, gab uns der Endkunde nur ein knappes Budget. Wir sind nach dem Ausschluss-Prinzip vorgegangen: der Einsatz von Mikrowellen, Infrarotlichtschranken, Radar, Lidar, Boden und Zaunsensorik war nicht möglich – es verblieb nur eine professionelle Videoanalyse mit hochwertigen Thermalkameras, die auf eine Leitstelle aufzuschalten waren. Zugute kam uns, dass wir als Hausherr die Tests der GIT SICHERHEIT zu den Themen Videoanalyse & Perimeter veranstaltet hatten: wir wussten, dass die Kombination Dahua-Kameras und Honeywell-Analyse funktionieren würden.

Peter Zehetner im Interview: i-Alarmsysteme als Sicherheits-Errichter für den GIT System Test Video Analytics

Stefan Blohm: Wir mussten die Kunden davon überzeugen, wer letztendlich die bessere Lösung hat. Dazu haben wir das Mitbewerberprodukt gekauft und ausführliche Messungen durchgeführt. Diese Messungen zeigten, dass wir über die höhere Lichtleistung bei gleicher Wattzahl verfügen. Mit unseren verschiedenen IR-Varianten sind Reichweiten von bis zu 500 Metern möglich. Durch wechselbare Linsen und der Hot-Spot-Reduction-Technologie können wir sicherstellen, dass das Licht besser zum Sichtfeld der Kamera passt und gleichmäßiger ausgeleuchtet wird. Das ist für lange Zaunlinien, Grenzbereiche und Zufahrten entscheidend. Eine höhere Reichweite bedeutet weniger Infrastruktur im Feld: einige Hundert Kameras, Masten, Verkabelung sowie hoher Installationsaufwand konnten eingespart werden.

Peter Zehetner im Interview: i-Alarmsysteme als Sicherheits-Errichter für den GIT System Test Video Analytics

Rainer Gräfendorf: Wir mussten mit einem sehr professionellen Täterverhalten, nämlich Kriechen, Rollen und vorsichtiges Bewegen entlang des Perimeters rechnen. Die richtige Technologieauswahl war anspruchsvoll. Da die Beteiligten nach dem Ausschlussprinzip vorgingen, kamen unsere Passiv-Infrarot-Detektoren und unsere Videoanalyse zum Einsatz. Die Bauherrin wollte vor der Kaufentscheidung alles selbst testen. Der Generalunternehmer hatte Sorgen, dass bei Grabarbeiten vorhandene Kabel beschädigt würden. Besonders Wildschwein-Rotten ließen die Alarmquote zeitweise deutlich ansteigen. Bewährt haben sich hier Empfehlungen zur Schwarzwild-Abwehr sowie die punktuelle Ertüchtigung des beschädigten Zauns, um auch dieses Problem in den Griff zu bekommen.

Perimeterschutz: Hinter den Kulissen eines Video-Drehs über Perimeterschutz und Sachverständigenarbeit

Andreas Keller: In beiden Projekten waren wir von Anfang an involviert und konnten bereits in der Planung Anforderungen zu Mast-Positionen, Infrastruktur, Monitoring, Aufschaltung auf Leitstelle und Klimatisierung mit den Verantwortlichen diskutieren. Eine Besonderheit stellte in Italien die Netz-Ersatz-Anlage dar, die wir installierten. Zum Einsatz kamen eine digitale Zaunsensorik bzw. ein intelligenter Meldedraht am Zaun, Passiv-Infrarotmelder und eine Video-Verifikation mit PTZ-Kameras, die dynamisch angesteuert wurden. Beide Konzepte, die sich je Standort voneinander in Details unterscheiden, sind tipptopp aufgegangen. Die unerwünschten und Falschalarme halten sich in Grenzen und beide Betreiber sind bis heute sehr zufrieden. Das ist das Wichtigste für uns, denn auch in unserem Geschäft zählt Mundpropaganda mehr als Hochglanzbroschüren.

Christian Linthaler: Die Anbindung an das Security Operation Center als zentrale Hauptleitstelle mit Verbindung zu allen Umspannwerken musste im Rahmen der Kommunikation aller Systemkomponenten verschlüsselt erfolgen. Bei der Abnahme durch die Experten Markus Piendl und Hannes Dopler versuchten sich beide durch den Alarmzaun zu schneiden und unsere Videoanalyse zu überlisten. Wir haben erfolgreich bestanden. Eine zentrale Herausforderung bestand darin,

unsere KI-Systeme so zu trainieren, dass spezielle Anforderungen insbesondere zu unkonventionellen Täterverhalten und zu cleveren Manipulationsversuchen zuverlässig erfüllt werden. Das haben wir mit den beiden Sachverständigen gemeinsam im Vorfeld optimiert. Sehr hilfreich dabei war auch der GIT SICHERHEIT Videoanalyse Test."

GIT System Test Video Analytics – Testergebnisse Teil 1

Johannes Faber: Zusammen mit dem Planer und Systemintegrator wurden verschiedene Technologien miteinander technisch und kommerziell verglichen. Dabei konnte die Kombination unseres Laserscanner RedScan Pro 2D in Verbindung mit Wärmebildkameras sowie Videoanalyse als Teil des Gesamtsystems überzeugen. Der RedScan Pro 2D ist ein präziser Laserscanner für die Perimeter-Sicherheit, der eine unsichtbare Schutzfläche erzeugt und Eindringlinge beim Durchqueren dieser Fläche erkennt. Zugutekam uns der in der GIT SICHERHEIT durchgeführte Test des Sensors durch die Sachverständigen Piendl und Dopler. Die Veröffentlichung der sehr guten Resultate hat das Projekt beflügelt."

GIT System Test Video Analytics & Perimeter – Testergebnisse Teil 2

David Sonntag: „Die Anfrage für die Absicherung traf sehr kurzfristig bei uns ein. Wir mussten die Verfügbarkeit der angefragten Sensoren und die Montage-Orte klären. Bestandssensoren des Kunden mussten über eine Protokoll-Schnittstelle integriert werden. Gute Drohnen, die von verschiedenen Dienstleistern im Rahmen von Fernsehproduktionen rund um das Spielgeschehen gestartet wurden, musste präzise von bösen Drohnen unterschieden werden. Die vor Ort zuständige Behörde musste überzeugt werden. Von dem Know-how der Beamten war ich begeistert. Alles in allem ein sehr anspruchsvolles Projekt, in dem wir uns als Teamplayer verstanden haben und einen echten Mehrwert für alle Beteiligten sicherstellen konnten.

3 Welche Lehren aus diesem Projekt sind richtungsweisend für die Zukunft der Perimetersicherheit?

Gerhard Harand: Wir haben für uns gelernt, dass es entscheidend ist, wann wir in Projekte einsteigen können. Ein Beispiel: bei einem neuen Standort ist es viel leichter, eine Boden-Sensorik zu planen und zu verbauen. Mir sind Installationen mit Boden-Sensorik bekannt, die seit 40 Jahren problemlos laufen. Bei IP-Kameras, Videomanagement-Systemen, Recordern, Edge-Analytics-Geräten oder Cloud-Video-Diensten kann dies in der Praxis bedeuten: Ist ein System nicht mehr patchbar, weist bekannte Schwachstellen auf, erlaubt keine sichere Administration, stammt aus einer kritischen oder risikobehafteten Lieferkette oder lässt sich insgesamt nicht mehr angemessen absichern, kann ein Austausch technisch wie auch rechtlich naheliegend – oder sogar zwingend erforderlich – sein, um die Anforderungen der NIS2-Richtlinie zu erfüllen.

Frank Pokropp: In diesem Projekt hat es sich einmal mehr bezahlt gemacht, dass wir mit dem Endkunden ausführlich das Sicherheitskonzept besprochen und bewertet haben. Gemeinsam haben wir überlegt, wie Täter vorgehen würden, welches Einbruchmaterial sie gegebenenfalls mit sich führen, wo sie versuchen könnten, einzudringen – und wie sich die Intervention gestalten muss. Wir waren quasi in einer Moderatorenrolle. IT-Themen haben heute eine sehr hohe Relevanz in der Perimetersicherheit, weil moderne Perimeter-Systeme kaum noch rein mechanisch oder isoliert arbeiten. Kameras, Radar, Zutrittskontrolle, Sensorik, VMS, Leitstellenanbindung, Cloud-Dienste und mobile Clients sind in der Regel vernetzte IT-Systeme und damit zugleich Sicherheits- und Angriffsfläche. Der Schutz vor Selbstbau- und kommerziellen Drohnen wird immer wichtiger.

Telekom: Großangelegte Tests des „Magenta Drohnenschutzschildes"

Peter Zehetner: Die erfolgreiche Absicherung eines Perimeter-Projekts mit Videoanalyse beginnt mit einer klaren Zieldefinition, also was genau erkannt werden soll. Entscheidend ist außerdem eine saubere Analyse der Umgebung, etwa hinsichtlich Gelände, Vegetation, Licht und möglicher Störquellen. Ebenso wichtig sind passend ausgewählte Kameras, geeignete Montagepositionen und die richtige Optik. Ein zentraler Erfolgsfaktor ist die Reduzierung von Fehlalarmen bei gleichzeitig hoher Erkennungswahrscheinlichkeit. Erforderlich sind eine sorgfältige Kalibrierung und Inbetriebnahme durch Profis. Ebenso wichtig sind klare Prozesse zur Alarmverifikation und Reaktion in der Leitstelle. Die regelmäßige Wartung, Tests und Nachjustierungen sichern die dauerhafte Wirksamkeit der Systeme.

Bitte umblättern ▶

Optex Redscan Pro: Sicherheit auf Dach eines Data-Centers

Stefan Blohm: Für uns als Hersteller ist es wichtig, dass wir uns noch konsequenter gegen Kameras mit integriertem Infrarot positionieren. Integrierte Infrarot-Beleuchtung ist fast immer schwächer als ein separater Infrarot-Scheinwerfer: Ein großer Nachteil sind Reflexionen und Überstrahlungen. Eingebautes Infrarot kann an Wänden, Decken, Fenstern, Masten oder hellen, glänzenden Flächen zurück in das Objektiv reflektieren und die Bildqualität deutlich verschlechtern. Gerade bei Dome-Kameras können außerdem Schmutz, Staub, Wasser, Schnee oder Eis auf der Kuppel starke Reflexionen verursachen. Hinzu kommt, dass integriertes Infrarot häufig Insekten und Spinnen anzieht. Diese können direkt vor der Kamera oder auf der Kuppel sitzen, was zu Fehlalarmen bei Videoanalysesystemen führen kann.

Rainer Gräfendorf: Die Zukunft der Perimeter-Sicherheit liegt in frühzeitiger Detektion am Perimeter plus technischer Verifikation und nicht in blindem Vertrauen auf reine Mechanik. Perimetersicherheit muss risikobasiert und angriffsgerecht geplant werden. Die umfangreiche, herstellerneutrale Ausschreibung von Piendl und Dopler sowie saubere Anforderungsdefinitionen zu den Themen Redundanz, Blitzschutz, VPN, IT-Härtung, technischer Dokumentation sowie Kennzahlen zu PD, VD, NAR, FAR und MTBF* werden immer wichtiger. Zukunftsfähige Projekte verbinden physische Sicherheit, Systemtechnik, IT und Betriebsqualität in einem sauberen Anforderungskatalog, der für alle Beteiligten verständlich sein muss. Und: Drohnen zur Verifikation werden immer wichtiger.

* Probability of Detection, Vulnerabiltiy to Defeat, Nuisance Alarm Rate, False Alarm Rate und Meantime Between Failure

Perimeterschutz: Hinter den Kulissen eines Video-Drehs über Perimeterschutz und Sachverständigenarbeit

Andreas Keller: Nicht alle Entwicklungen in der Industrie zum Thema Perimeter-Sicherheit sind erfreulich. Ein Hersteller, der jahrelang die Branche im Bereich Passiv-Infrarotmelder und Videoanalyse dominierte, nahm an Innovationskraft ab, nachdem dieser an einen Großkonzern verkauft wurde. Hersteller müssen sich konsequent mit den Anforderungen von uns Sicherheits-Errichtern weiterentwickeln und idealerweise über ein eigenes Testgelände verfügen, das ich mit meinen Kunden besuchen kann. Jedes Projekt ist individuell in der Planung und im Betrieb. Nur wer örtliche Gegebenheiten, Anforderungen der Behörden und Versicherungen berücksichtigt, hat Erfolg. Was bei Projekt A funktioniert, muss nicht automatisch bei Projekt B funktionieren.

Christian Linthaler: Zur Umsetzung des Projekts wurde ein Panomera-Kamerasystem mit einem speziell trainierten Perimeter-Netz eingesetzt. Die Aufzeichnungen und Analysen erfolgen über die Dallmeier-Software. Zusätzlich wurde das System in das übergeordnete PSIM Winguard von Advancis integriert, um eine zentrale Überwachung und Steuerung zu ermöglichen. Ein entscheidendes Element der Lösung ist die Doppel-Validierung von Alarmen: durch die Kombination des Alarmzaunsystems mit der Panomera-Kameratechnologie können Falschalarme reduziert und echte Sicherheitsvorfälle zuverlässig erkannt werden. Wir sind froh und dankbar darüber, dass der Endkunde die Relevanz deutscher Hersteller für sich erkannt hat.

Johannes Faber: Die Integration in ein übergeordnetes Videomanagementsystem (VMS) war wichtig, weil dadurch Ereignisse nicht isoliert, sondern im Zusammenhang mit Bild, Ort und Alarmprozess bearbeitet werden konnten. Ein Sensor meldet dann nicht nur „Etwas ist passiert“, sondern das VMS verknüpft die Meldung direkt mit der passenden Kamera, der Karte, dem Alarmfenster und den Reaktionsschritten. Eine gute Drohne im Rahmen der Verifikation von Alarmen einzusetzen, um so Kameramasten einzusparen ist ein neuer, zukunftsweisender Ansatz, den wir in den kommenden Monaten und Jahren noch häufiger sehen werden. Diese Technik ist zuverlässiger und günstiger geworden – benötigt aber weiterhin ein zuverlässiges Alarmkriterium am Perimeter.

David Sonntag: Ich sehe Parallelen zu den klassischen Ansätzen der geschätzten Kollegen, die über ihre Perimeter-Projekte berichtet haben. Auch beim Drohnenschutz gibt es nicht den einen Sensor, der alle Probleme löst. Erfolgreich ist ein wirksames Konzept nur, sofern der Endkunde – in diesem Projekt das Stadion und der Sportveranstalter – verstehen, was Sensoren in der Lage sind zu leisten und warum ein Sensor-Mix erforderlich ist. Das hat Markus Piendl vor Ort genau erklärt. Entscheidend war ferner, dass wir die Sensor-Fusion der eingesetzten Sensoren auf unserem Testgelände in Nürnberg im Vorfeld immer wieder geübt haben – und dass unser technisches Team während der Veranstaltung vor Ort war. Sicher ist sicher.

GIT Testgelände im Test – Testergebnisse Teil 2

4 Was wünschen Sie sich von der GIT SICHERHEIT für die Zukunft?

Gerhard Harand: Als klassische Fachzeitschrift und als digitales Branchenportal genießt die GIT SICHERHEIT hohes Ansehen. Für mich persönlich dürfen es gerne noch mehr Berichte aus der Praxis sein. Die konkrete Darstellung von gewerkübergreifenden Ansätzen interessiert mich sehr. Danke an die GIT für den Mut, mit ihren beiden Perimeter- und Videoanalyse-Tests Neuland zu betreten: das waren für mich die stärksten Berichte der letzten Jahre, da diese einen konkreten Mehrwert in Projekten boten. Diese Serie sollte unbedingt fortgeführt werden.

GIT System Test Video Analytics – Testergebnisse Teil 1

GIT System Test Video Analytics & Perimeter – Testergebnisse Teil 2

Frank Pokropp: Ich wünsche mir noch mehr konkrete Projektberichte aus dem KRITIS-Umfeld. Einen moderierten, ehrlichen Austausch zwischen Herstellern und Errichtern im Hinblick auf die Umsetzung des KRITIS-Dachgesetzes als Artikel kann ich mir sehr gut vorstellen. Die Sicht von Betreibern sollte stärker gehört werden. Alle Systemintegratoren haben ähnliche Herausforderungen in der Planung und im Betrieb von Perimeter-Lösungen. Klartext im Hinblick auf die Herausforderungen in

Projekten zu sprechen ist wichtig. Darüber lohnt es sich zu berichten, um Erfahrungswerte auszutauschen.

Peter Zehetner: Die GIT SICHERHEIT berichtet seit Jahren nicht nur über Produkte, sondern auch über Anwendungen, Markttrends und regulatorische Entwicklungen. Das ist ein großer Mehrwert für uns und unsere Kunden. Das Team hinter den Kulissen leistet sehr gute Arbeit und schafft es meisterlich, viele Informationen strukturiert aufzuarbeiten. Mein Team und ich denken gerne an die gemeinsamen Tests zurück, auf die wir noch heute im In- und Ausland angesprochen werden. Dieses Lob teilen wir sehr gerne mit dem Geburtstagskind GIT SICHERHEIT.

Stefan Blohm: Ich möchte anregen, dass mehr über Normen berichtet wird. Als Beispiel darf ich die EN-Norm 62676 nennen, die internationale Anforderungen an Videoüberwachungsanlagen (VSS) für Sicherheitsanwendungen definiert. Wenn Normen mit guten Beispielen veranschaulicht werden, kann der Sinn einem breiten Publikum besser vermittelt und mehr Akzeptanz sichergestellt werden. Danke für die trotz journalistischer Neutralität immer faire und partnerschaftliche Zusammenarbeit mit dem Team der GIT SICHERHEIT.

Rainer Gräfendorf: Die GIT SICHERHEIT schafft es hervorragend, die verschiedenen Felder Management, Security, IT-/Cyber-Security, Brandschutz und Safety abzudecken. Ich möchte an dieser Stelle das Team der GIT SICHERHEIT ausdrücklich loben: Wir pflegen einen unkomplizierten, vertrauensvollen und partnerschaftlichen Umgang miteinander – dafür danken meine Kolleginnen, Kollegen und ich sehr. Mein Wunsch an das Geburtstagskind sind noch mehr praxisnahe Tests und Anwenderberichte, gerne auch weiterhin so objektiv gestaltet wie heute.

Andreas Keller: Für mich ist die Betrachtung technologischer Entwicklungen in den Bereichen Perimeter-, Gebäude-, Video-, Brand- und Drohnensicherheit besonders wichtig. Praxisnahe Berichte von Unternehmen, die wie wir als Sicherheits-Errichter tätig sind, helfen uns sehr. Artikel zu Tests, idealerweise im direkten Vergleich, sind hilfreich, da uns als Errichter oft Ressourcen fehlen, eigenständig umfangreiche Tests nachstellen zu können. Zum nächsten runden Geburtstag der GIT SICHERHEIT wünsche ich mir ein großes Symposium zum Thema Perimeter-Sicherheit 2030.

Christian Linthaler: Die GIT SICHERHEIT ist für uns eines der besten und renommiertesten Magazine, da die Schnittstelle zwischen Technik, Anwendung und Markt sehr gut abgebildet wird. Mein Wunsch ist, in der GIT SICHERHEIT den Endkundenfokus weiter zu schärfen. Viele Berichte beschäftigten sich mit Herstellern und Sicherheits-Errichtern. Das ist gut und wichtig. Letztendlich jedoch bezahlt uns alle ein Endkunde. Viele Endkunden treiben Fragen etwa nach dem Projektierungsaufwand, Integration in Bestandssysteme, Schulungs- und Betriebskosten, Abhängigkeiten um. Ich würde mich freuen, diese Themen noch stärker in Fachartikel aus Sicht der Endkunden zu thematisieren.

Johannes Faber: Ich verfolge die Print- und E-Paper-Ausgaben, laufende Online-Beiträge, Newsletter sowie thematische Specials der GIT SICHERHEIT mit großem Interesse. Insbesondere die Hersteller-, Integratoren- und Anwenderprojekte gefallen mir gut. Ich hoffe auf eine Neuauflage der Videoanalyse & Perimeter Tests in 2026, da vielen meiner Kunden Vergleichsmaßstäbe, Referenzwerte und Marktstandards sehr wichtig sind. Schwerpunktausgaben und Inforeihen zu Sensoren der unterschiedlichen Detektionsverfahren inklusive Hinweise zu Stärken und Einschränkungen, etwa im Hinblick auf Sabotageversuche, wären super.

David Sonntag: Unsere Kunden befinden sich sowohl im militärischen Umfeld als auch in zivilen Behörden und in der Privatwirtschaft. Viele Anforderungen ähneln sich. Wir tun gut daran, möglichst viel voneinander zu lernen und keine Insellösungen aufzubauen. Als ehemaliger Offizier der Bundeswehr erhoffe ich mir, dass die GIT SICHERHEIT noch stärker den Ansatz der zivil-militärischen Zusammenarbeit darstellt. Artikel, in denen dargelegt wird, wie zum Beispiel die Streitkräfte mit zivilen Firmen zusammenarbeiten, wo es Gemeinsamkeiten in Vorgehensweisen und Strategien gibt, faszinieren mich und bereichern den Austausch untereinander. Voneinander zu lernen ist äußerst wichtig. GIT

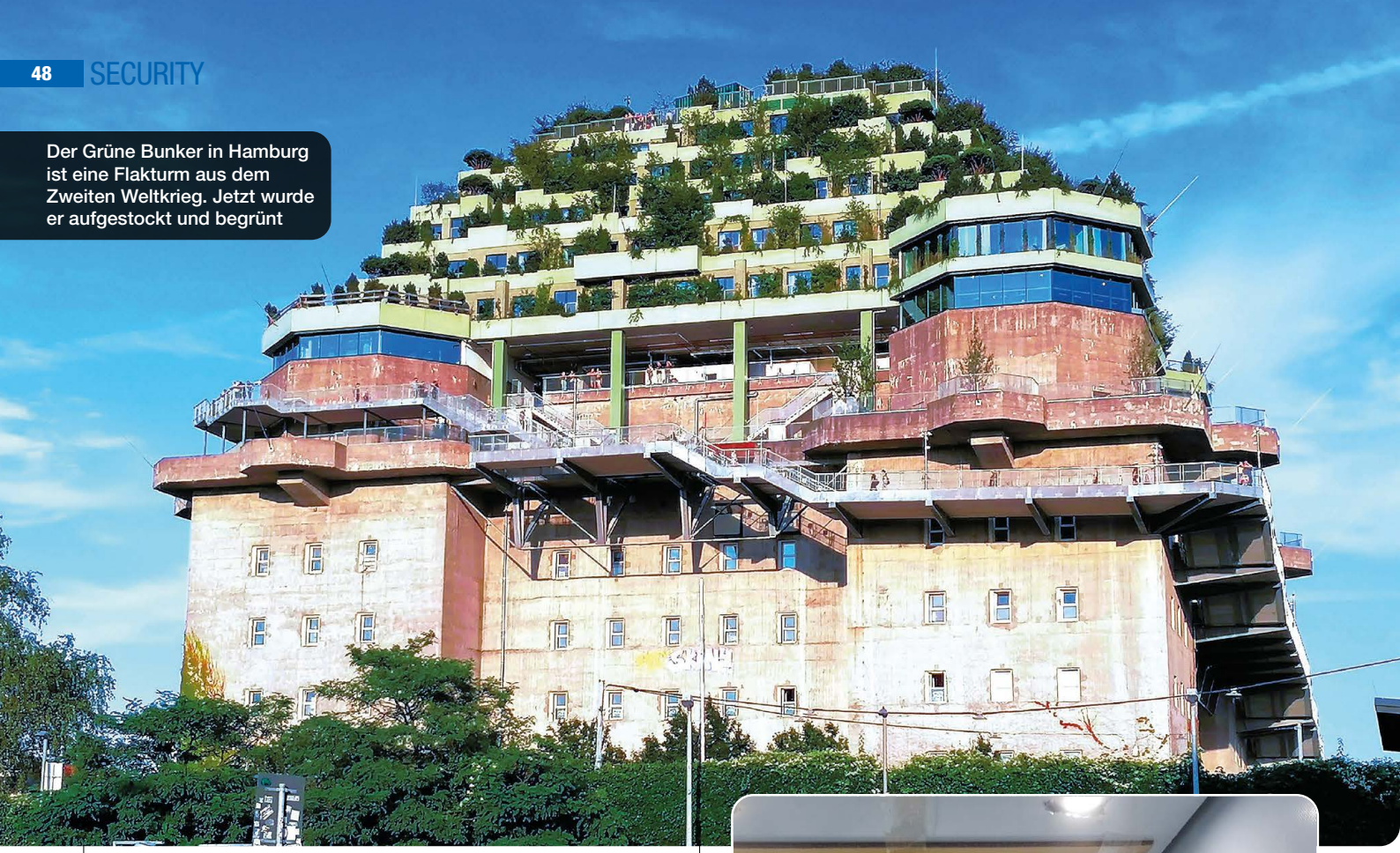
Unser Dank für die spannenden Berichte aus der Praxis, die Offenheit und die Glückwünsche zum Jubiläum gilt: Gerhard Harand (TPS Wehrhan), Frank Pokropp (Freihoff Sicherheitsservice), Peter Zehetner (iAlarmsysteme / Schloss & Riegel), Stefan Blohm (Raytec), Rainer Gräfendorf (Honeywell), Andreas Keller (Keller Sicherheitstechnik, Concepts 4 Security), Christian Linthaler (Dallmeier), Johannes Faber (Optex) und David Sonntag (Walaris) – sowie Markus Piendl für die Recherchen.

VISION

Innerhalb der nächsten Jahre muss es uns gelingen, im Bereich Sicherheit den Wirtschaftsschutz verbindlich zu verankern, den Informationsaustausch zwischen allen Playern rechtssicher zu gestalten und die Resilienz der Wirtschaft nachhaltig zu stärken.

Johannes Strümpfel, Präsident des Verbands für Sicherheit in der Wirtschaft, Bundesverband e.V. – VSW-Bundesverband

35 JAHRE GIT SICHERHEIT



Der Grüne Bunker in Hamburg ist eine Flakturm aus dem Zweiten Weltkrieg. Jetzt wurde er aufgestockt und begrünt

VIDEOSICHERHEIT

Hängende Gärten

Sicherheitstechnik im Grünen Bunker in Hamburg

Hamburg hat eine neue Attraktion – den grünen Bunker. Auf den ehemaligen Flak-Bunker wurden sechs Ebenen aufgestockt – mit Hotel, Veranstaltungshalle, Büroräumen, Gastronomie und Geschäften sowie einem Stadtgarten auf dem Dach. Dorthin führt ein „Bergpfad“, wo sich dem Besucher ein Rundblick über Hamburg eröffnet. Die Planungsarbeiten zur Sicherheitstechnik übernahm das Planungsbüro Nolle in Berlin. Dessen Leiter, Mario Nolle, plante und koordinierte alle Arbeiten. Die Firma B.I.N.S.S. in Berlin führte die Arbeiten zur Errichtung der sicherheitstechnischen Anlagen aus. Als Projektleiter dort war Dennis Klinghardt verantwortlich. GIT SICHERHEIT sprach mit den beiden Experten über die Planung und Errichtung der sicherheitstechnischen Anlagen beim Grünen Bunker.

Dennis Klinghardt von B.I.N.S.S. (links) und Mario Nolle vom Planungsbüro Nolle, beide in Berlin

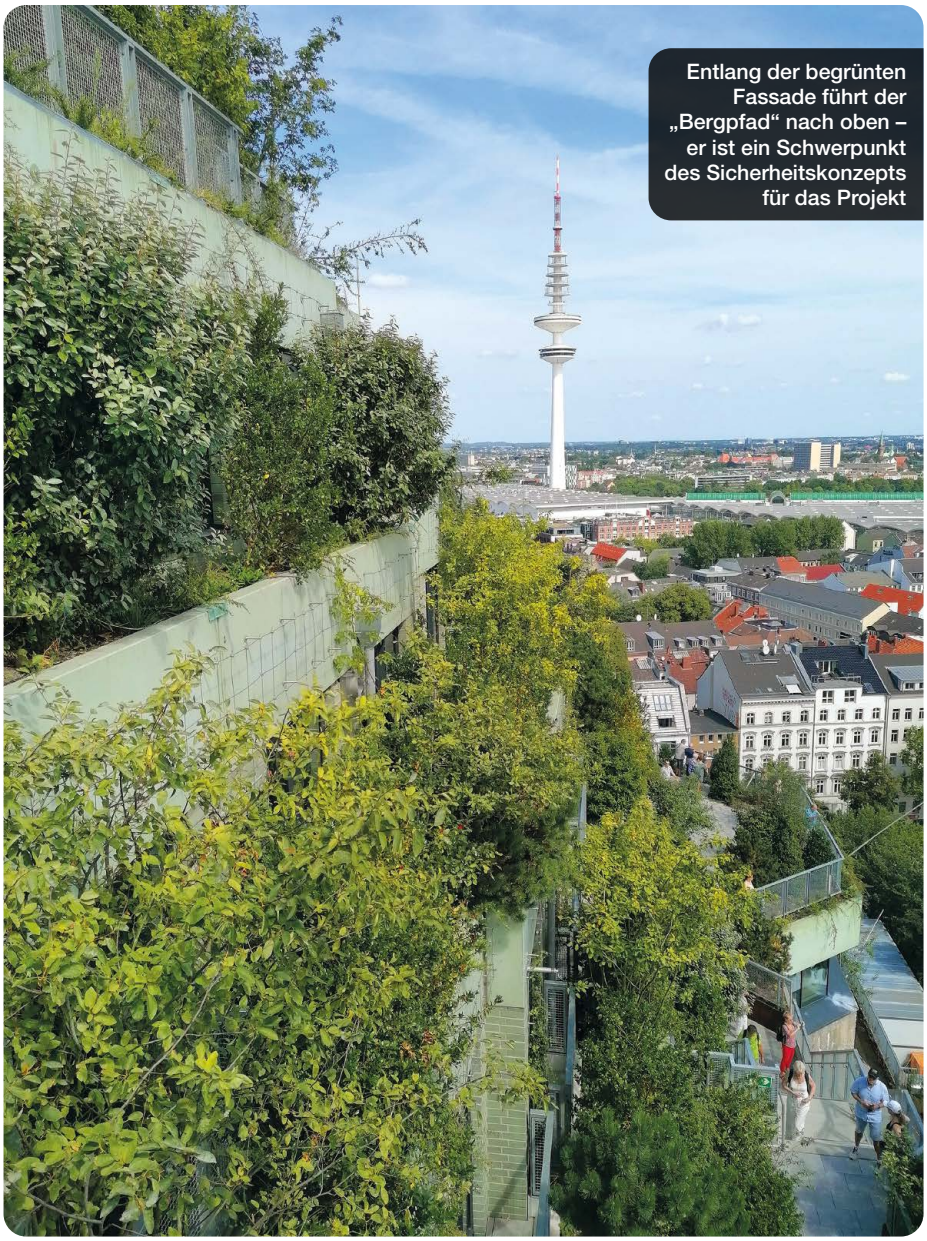
GIT SICHERHEIT: Herr Nolle, so eine Planungsaufgabe wie für den Grünen Bunker in Hamburg bekommt man nicht alle Tage. Wie sind Sie das Projekt angegangen?

Mario Nolle: Die Sicherheitstechnik, insbesondere die Systeme zur Personenzählung und Videoüberwachung, ist für ein solches Bauwerk in der Tat sehr anspruchsvoll. Es kommen hier mehrere Anforderungen zusammen, die üblicherweise nicht Gegenstand solcher Planungsarbeiten sind. Um eine klare Aufgabenstellung abzustimmen, wurde ein Lastenheft erstellt, das alle sicherheitsrelevanten Vorgaben und Aufgaben beinhaltete. Für das Verständnis aller am Bau Beteiligten ist so ein Lastenheft außerordentlich wichtig. Es liefert allen die gleiche Ausgangsbasis und Grundlage für die Bewertung der abzurechnenden Leistungen.

Welche speziellen Bedingungen mussten berücksichtigt werden?

Mario Nolle: Der Bergpfad ist im Gefahrenfall gemeinsam mit dem Treppenhaus auf der Ostseite Fluchtweg von oben nach unten. Das ist ein Schwerpunkt der Sicherheitsmaßnahmen. Da in den Bauauflagen festgelegt ist, wie viele Personen sich gleichzeitig maximal auf dem Bergpfad, den Aufbauten und dem Stadtgarten aufhalten dürfen, ist es erforderlich, sowohl Besucher als auch das vor Ort tätige Personal zu zählen. Dies geschieht mit einer videobasierten Zähltechnik im Bereich der Drehkreuze zu Beginn des Bergpfades, über den Bergpfad verteilt, auf dem Stadtgarten, jeweils den Zugängen zum Hotel sowie im Bereich der Zu- und Abgänge für die Aufzüge.

Bei Überschreitung der zulässigen Personenanzahl wird der Zugang automatisch gesperrt. Die Zählstellen auf dem Bergpfad sollen im Fall einer Verdichtung des Personenstromes nach oben oder unten informieren. Über Lautsprecherdurchsagen kann in diesem Fall darauf hingewiesen werden, dass der Fluchtweg freizuhalten ist. Zur Information einlassbegehrender Besucher stehen entsprechende Monitore zur Verfügung. Gleichzeitig ist im Fluchtfall zu gewährleisten, dass die für den Fluchtweg vorgesehenen Tore im Drehkreuzbereich geöffnet werden.



Entlang der begrünten Fassade führt der „Bergpfad“ nach oben – er ist ein Schwerpunkt des Sicherheitskonzepts für das Projekt

Welche Besonderheiten waren für die Videoüberwachungstechnik insgesamt zu berücksichtigen?

Mario Nolle: Das Gebäude ist kein Hochsicherheitsbereich. Anfangs hatte der Bauherr Bedenken bezüglich des Umfangs der Videoüberwachung. Auch aus architektonischer Sicht ergaben sich Einwände. Eine Einigung wurde jedoch erreicht und alle Anforderungen sind in das Pflichtenheft eingeflossen. Die Videoüberwachungstechnik konzentriert sich neben den Anforderungen, die sich aus dem Hotelbetrieb, der Gastronomie und den Verkaufseinrichtungen ergeben, auf die Außenanlagen mit Schwerpunkt Bergpfad und Stadtgarten. Hier ging es im Detail um das Maß der Präsenz der Videoüberwachung für die Besucher, um bauliche Gegebenheiten und die Form der Kameras. Gemäß Datenschutzgrundverordnung werden alle Besucher über das Vorhandensein der Videoüberwachung informiert.

Zur Zeit der Planung für die Videoüberwachungsanlage gab es nur wenig detaillierte Vorstellungen von der Begrünung des Bunkers. Bezüglich der Kamerastandorte ist es natürlich von großer Bedeutung, ob nach der Bepflanzung noch die erforderliche freie Sicht der Kameras gewährleistet ist. Im Laufe der Bauarbeiten war es nötig, Kamerastandorte und Begrünung in „Koexistenz“ zu bringen. Es konnte zum Beispiel passieren, dass plötzlich ein großer Apfelbaum vor der Kamera eingepflanzt wurde. Ein Kompromiss musste mit allen Beteiligten gefunden werden. Auch künftig ist das regelmäßige Beschneiden der Pflanzen in Kameranähe unabdingbar.

Welche Kameratypen sind eingesetzt?

Mario Nolle: Als Fixkameras werden überwiegend Bulletkameras mit Varioobjektiven unterschiedlicher Brennweitenbereiche genutzt, was das genaue Einstellen auf den jeweiligen Beobachtungsbereich ermöglicht. An vor Witterungseinflüssen geschützten Orten wie unterhalb der Aufzugsübergänge in das Gebäude sind Fixdomekameras in Deckenmontage eingesetzt.

Bitte umblättern ▶

Bei Überschreitung der zulässigen Personenanzahl wird der Zugang automatisch gesperrt

Um eine allzu starke Anhäufung von Kameras an den Gebäudeecken zu vermeiden, haben wir dort Multiheadkameras mit drei separaten Kameras eingesetzt, die jede für sich ausgerichtet werden kann. Auch Speed-Domekameras wurden erwogen. Wegen deren beweglichen Kameras und Motor-Zoomobjektiven können Details von Ereignisorten abgebildet werden, was mit Fixkameras nicht möglich ist. Ein wesentlicher Nachteil dieses Kameratyps ist jedoch, dass diese in der Ausgangsposition nur einen der drei gewünschten Überwachungsbereiche überblicken können. Selbst bei automatischen „Rundgängen" der Kamera, bleiben die jeweils abgewandten Bereiche für eine definierte Zeit unbeobachtet. Zur manuellen Bedienung der Speed-Domekamera braucht man auch

Um eine allzu starke Anhäufung von Kameras an den Gebäudeecken zu vermeiden, werden dort Multiheadkameras eingesetzt

Personal. Letztendlich entschied man sich also für die Multiheadkameras.

Was geschieht mit den Videobildern?

Mario Nolle: Sie werden von einem Videomanagementsystem verwaltet. Sie können als Livebilder auf Monitore aufgeschaltet und im System gespeichert werden. Damit wird es möglich, Bilder von Ereignissen auch im Nachhinein auszuwerten. Die gespeicherten Bilder sind nur in einem gemäß Datenschutz zulässigen Zeitraum verfügbar und werden danach gelöscht. Zur Dokumentation von Ereignisbildern können diese auf externe Speichermedien ausgelagert werden. So ist gesichert, dass diese für Beweise und Untersuchungen von Polizei und Gerichten verfügbar sind. Selbstredend ist der Zugriff sowohl auf Livebilder als auch gespeicherte Bilder nur autorisiertem Personal vorbehalten.

Das Videoüberwachungssystem kann weitestgehend autark arbeiten. Bei Erkennen sicherheitsrelevanter Ereignisse kann zielgerichtet nach den dazugehörigen Bildern gesucht werden. Die Suche wird durch zahlreich zu wählende Suchparameter unterstützt. Bei einer ereignisgesteuerten Aufzeichnung von Bildern stehen diese separat für jedes Ereignis zu Verfügung.

Herr Klinghardt, auch für Sie als Projektleiter war die Aufgabe sicher eine Herausforderung?

Dennis Klinghardt: Die Firma B.I.N.N.S. hat schon zahlreiche äußerst komplexe sicherheitstechnische Anlagen mit hohen Sicherheitsanforderungen errichtet. Insofern war die Aufgabe nicht vollständig neu für uns. Wegen des einzigartigen Charakters des Baus sowie des allgemeinen Interesses an ihm war es eine Herausforderung für alle Beteiligten. Da auch während der Corona-Zeit gebaut werden musste, gab es nicht nur technische Herausforderungen sondern auch logistische. Aus heutiger Sicht können wir jedoch konstatieren, dass wir unseren Aufgaben gerecht geworden sind.

Können Sie einige dieser spezifischen Aufgaben näher erläutern?

Dennis Klinghardt: Der Bergpfad, der Schwerpunkt der Videoüberwachung ist, wurde als eine der letzten Baumaßnahmen errichtet. Damit verzögerte sich natürlich auch die Montage der Kameras. Um Zeit und Klarheit zu gewinnen, haben wir an den potentiellen Kamerastandorten Testbilder erstellt und diese in einem provisorischen Kameraregister dokumentiert. Dadurch wurde Sicherheit gewonnen, dass die ausgewählten Standorte genutzt werden können. Das war wichtig, da die Kabel für das Netzwerk und die Anbindung der Kameras lange vor deren Montage verlegt werden mussten. Der gewählte Weg hat sich als richtig erwiesen, da nur wenige der Kabel nachträglich noch einmal rangiert wurden.

Das Netzwerk wurde als Loop auf Basis von Singlemode-LWL gestaltet. Das ermöglicht, die Bilder zusätzlicher Kameras oder solche mit künftig höherer Auflösung ohne

VISION

Innerhalb der nächsten zehn Jahre werden wir mit integrierten Sicherheitssystemen in der Lage sein, nicht nur die wachsenden Bedrohungen abzuwehren, sondern auch unseren Kunden das (Geschäfts)leben leichter zu machen.

Michael Schreiber,
General Manager Hirsch Secure GmbH

35 JAHRE GIT SICHERHEIT

Änderungen an diesem zu übertragen. Alle Kameras sind mittels PoE mit entsprechenden Switches verbunden. Die Anforderungen an maximale Kabellängen sind nicht trivial, wenn der endgültige Kamerastandort weiter entfernt ist als der geplante. Letztendlich konnten die Positionen der Switches auf unterster Ebene so gewählt werden, dass alle maximalen Kabellängen eingehalten werden konnten.

Neben der Sicherheit des Alt- und Neubaus entstanden auch Forderungen des Hotels, der Gastronomie und Verkaufseinrichtungen hinsichtlich des Einsatzes von Videoüberwachungstechnik. Da hier viele Interessen unter einen Hut gebracht werden mussten, war die Aufgabe recht komplex. So gibt es Kameras, deren Bilder sowohl für die Mieter als auch für die allgemeine Sicherheit des Objektes wichtig sind. Entsprechende Unterbereiche im Videomanagementsystem wurden eingerichtet und die Zugriffsberechtigungen für die jeweiligen Bilder abgestimmt.

Herr Klinghardt, es ist anzunehmen, dass während der Nutzung weitere Anforderungen an die Videoüberwachung entstehen. Ist die Anlage darauf vorbereitet?

Dennis Klinghardt: Auch umfangreichere Erweiterungen sind möglich. In einem Vorbereich der Gastronomie gab es jüngst z.B. ein sicherheitsrelevantes Ereignis. Die dort befindliche Kamera hat die Treppe des Bergpfades im Fokus und den Eingang zum Restaurant nur am Rand im Blick. Die Möglichkeit, eine Kamera mit erweitertem Blickwinkel einzusetzen, wurde verworfen, sieht diese die jeweiligen Bereiche nur mit geringerer Auflösung. Zusätzliche Kameras erfordern neue Verbindungkabel, was im Nachhinein mit hohem Aufwand verbunden wäre. Wir haben uns entschieden, anstelle der Bulletkameras eine Multiheadkamera zu nutzen. Damit konnten die jeweiligen sicherheitsrelevanten Bereiche voll erfasst werden. Ich gehe davon aus, dass auch künftige Anforderungen, die sich aus dem täglichen Betrieb und neuen Bedingungen für die Nutzung des Objektes mit dem vorhandenen Videoüberwachungs-system umsetzen lassen.

Herr Nolle, Herr Klinghardt würden Sie eine solche Aufgabe wie die am Grünen Bunker in Hamburg noch einmal übernehmen?

Dennis Klinghardt: Trotz aller Schwierigkeiten, die es in der Bauphase gab, sehr gern. Wir haben nicht nur ein Sicherheitssystem errichtet, das den Anforderungen in der ersten Phase der Nutzung des Bunkers gerecht geworden ist, sondern auch sehr viel wertvolle Erfahrungen für künftige Aufgaben gewonnen. GIT

PBN Planungsbüro Nolle
nolle@planungsbüro-nolle.de

B.I.N.S.S. Datennetze und Gefahrenmeldesysteme GmbH
dklinghardt@binss.de

Die GIT SICHERHEIT ist wichtig für uns, weil sie nicht nur für den Monitor-Sicherheitsmarkt stets inspirierend, professionell und einen Schritt voraus informiert!

Team AG Neovo D/A/CH:
Udo Moritz, Reinhard Schweizer, Thore Peters, Frank Voss, Ralf A. Thomas, Niklas Beste (v.l.n.r.)

35 JAHRE GIT SICHERHEIT

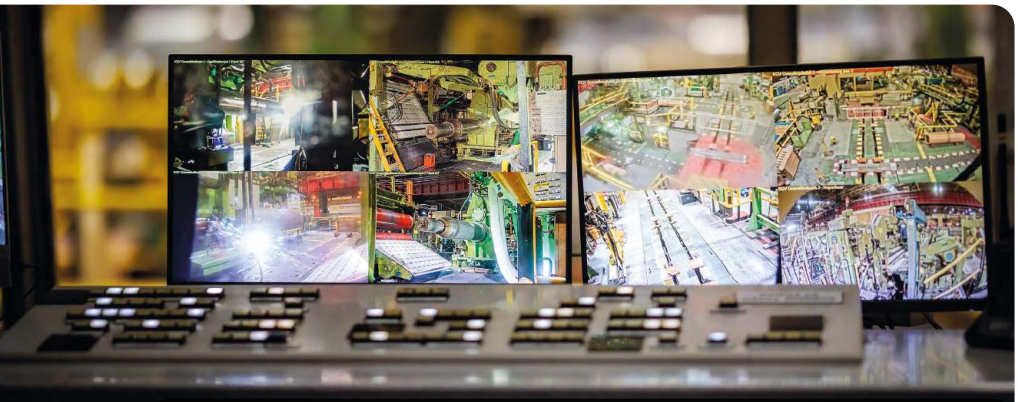
Arcelor Mittal setzt auf Netzwerkkameras von Axis Communications in Kombination mit eigens entwickelten KI-Anwendungen

VIDEOTECHNIK

Smarte Stahlherstellung

Netzwerkkameras und KI-Analysen bei Arcelor Mittal in Belgien

Das Marktumfeld der europäischen Stahlindustrie ist herausfordernd. Rückläufige Produktionsmengen, veränderte Nachfrage und hohe Energiepreise erhöhen den Druck auf die Werke, ihre bestehenden Anlagen möglichst effizient und stabil zu betreiben. Digitale Technologien wie KI-basierte Netzwerkkameras gewinnen weiter an Bedeutung – die unterstützen u. a. dabei, Produktionsunterbrechungen zu vermeiden und sicherheitskritische Prozesse effizienter abzusichern. Wie dies in der Praxis gelingt, zeigt ein Blick auf die Stahlwerke von ArcelorMittal in Belgien. Dort werden u. a. smarte Netzwerkkameras von Axis Communications eingesetzt.



Die modularen Kamerasysteme von Axis Communications erkennen Abweichungen im Produktionsablauf in Echtzeit und informieren die Bedienenden automatisch

Die Arcelor Mittal-Gruppe zählt mit rund 222.000 Mitarbeitern weltweit und 400 Standorten allein in Europa zu den global führenden Stahl- und Bergbauunternehmen und beliefert Kunden in mehr als 60 Ländern. In Belgien betreibt das Unternehmen sieben verschiedene Produktionsbereiche – vom Stahlwerk über das Warm- und Kaltwalzwerk – und setzt dort auf Netzwerkkameras von Axis Communications in Kombination mit eigens entwickelten KI-Anwendungen. Die Systeme überwachen Produktionsprozesse in Echtzeit, sichern die Qualität und erhöhen die Sicherheit in Hochrisikobereichen.

Aktuell sind mehr als 2.700 Netzwerkkameras von Axis Communications dort im Einsatz, mit dem Ziel, Ausfallzeiten zu reduzieren, Abläufe zu standardisieren und Mitarbeiter zu entlasten. So mussten an Produktionslinien zuvor häufig zehn bis 20 Live-Feeds gleichzeitig überwacht werden, um Prozessabläufe, Materialflüsse und Qualitätsparameter im Blick zu behalten. In bestimmten Situationen war es zudem erforderlich, dass Mitarbeiter sich von den Monitoren entfernen und den betreffenden Anlagenbereich direkt vor Ort überprüfen, was regelmäßig sowohl Unterbrechungen im Produktionsablauf als auch zusätzlichen Aufwand bedeutete.

KI-gestützte Videoanalyse für mehr Effizienz

Um die Betriebseffizienz zu steigern, entwickelte Arcelor Mittal Belgien eine Reihe

VISION

Innerhalb der nächsten zehn Jahre werden wir mit unseren Systemen/Leistungen in der Lage sein, komplexe Videonetzwerke durch den gezielten Einsatz von Software und Künstlicher Intelligenz noch intelligenter, effizienter und sicherer zu machen.

Rudolf Rohr, Geschäftsführer
Barox Kommunikation GmbH

35 JAHRE GIT SICHERHEIT

spezialisierter KI-Anwendungen, die direkt auf den Axis-Netzwerkkameras ausgeführt werden. Die Kameras liefern selbst unter extremen Bedingungen – etwa bei den oftmals herausfordernden Licht- und Temperaturverhältnissen an den Produktionslinien in der Stahlproduktion – eine stabile und hochauflösende Bildqualität.

Die offenen VAPIX-Schnittstellen der Axis-Plattform ermöglichen es zudem, KI-gestützte Videoanalysen flexibel und in Echtzeit auf unterschiedlichen Kameramodellen und in mehreren Produktionsbereichen durchzuführen. Neue Analysefunktionen können so ohne zusätzliche Infrastruktur ergänzt oder angepasst werden, was die Skalierbarkeit der Lösung signifikant steigert.

Die modularen Kamerasysteme erkennen Abweichungen im Produktionsablauf in Echtzeit und informieren automatisch – beispielsweise, wenn ein Objekt vor dem Transport nicht korrekt ausgerichtet wurde. Auf diese Weise wird die Fehleranfälligkeit von kritischen Prozessschritten reduziert und die generelle Anlagenstabilität erhöht.

Sicherheit in Hochrisikoprozessen

Ein besonders sicherheitskritischer Bereich ist der Transport von geschmolzenem Stahl, der per Kran in großen Pfannen mit einem Fassungsvermögen von bis zu 300 Tonnen bewegt wird. Bevor eine solche Pfanne angehoben werden darf, überprüft eine KI-gestützte Anwendung automatisch, ob die Kranhaken korrekt positioniert und vollständig verriegelt sind.

Erkennt das System eine Abweichung, wird der Hebevorgang sofort blockiert und ein Alarm ausgelöst. Die Anwendung ist dabei direkt in die Steuerung des Krans integriert und gibt den Vorgang erst wieder frei, wenn die sichere Befestigung der Pfanne eindeutig bestätigt wurde – entweder durch die KI-Anwendung oder durch eine manuelle Überprüfung. So werden Fehlbedienungen verhindert und die Prozesssicherheit deutlich erhöht.

Automatische Qualitätsprüfung und Gefahrenprävention

Auch bei der Qualitätssicherung spielen die KI-gestützten Axis-Kameras eine zentrale Rolle, um Prüfprozesse effizienter und weniger fehleranfällig zu gestalten. Vor dem Versand kontrollieren sie bei jeder Stahlcharge automatisiert die korrekte Kennzeichnung sowie die Qualität der Schweißnähte – beispielsweise, ob während der Fertigung Risse, Verunreinigungen oder Porosität entstanden sind. Gleichzeitig wird so sichergestellt, dass die Materialgüte dem jeweiligen Kundenauftrag entspricht.

Darüber hinaus nutzt Arcelor Mittal in sicherheitsrelevanten Bereichen eine KI-gestützte Objekterkennung, um unbefugtes Betreten von Gefahrenzonen zuverlässig zu erkennen. Sobald jemand einen gesperrten Bereich betritt, lösen die Systeme automatisch akustische und visuelle Warnsignale aus. Funktionen zur Wahrung der Privatsphäre wie dynamische Maskierung von Personen gewährleisten dabei die Einhaltung gesetzlicher Vorgaben zum Datenschutz.

Das Beispiel zeigt, wie sich die Stahlproduktion durch den gezielten Einsatz von Netzwerkkameras und KI-gestützten Videoanalysen effizienter, zuverlässiger und sicherer gestalten lässt. Die offene Plattform von Axis ermöglicht es, die entwickelten Anwendungen künftig flexibel auf weitere Produktionsbereiche oder Standorte zu übertragen – ohne umfangreiche zusätzliche Infrastruktur. GIT

Axis Communications
www.axis.com

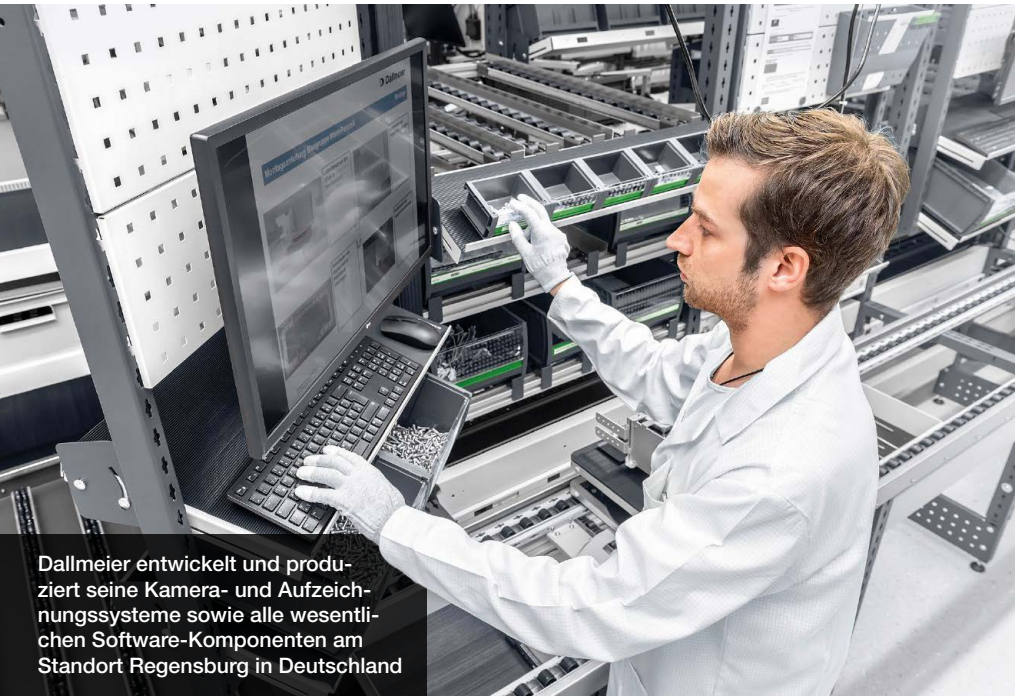
© Bilder: Axis Communications

KI made in Germany

Ein Trendbericht von Georg Martin, Chief Communications Officer bei Dallmeier electronic

In den vergangenen Jahren hat sich das Umfeld, in dem wir als Hersteller von Videotechnologie für Sicherheitsanwendungen arbeiten, deutlich dynamischer entwickelt. Gleichzeitig beobachten wir eine stark wachsende Nachfrage nach intelligenten Sicherheitslösungen. Kritische Infrastrukturen, Städte, Flughäfen, Industrieanlagen oder Logistikzentren stehen heute vor völlig neuen Herausforderungen – von komplexeren Bedrohungslagen bis hin zu steigenden Anforderungen an Effizienz und Transparenz. Videotechnologie wird deshalb zunehmend nicht nur als klassisches Sicherheitssystem verstanden, sondern als strategisches Instrument zur Unterstützung von Prozessen, zur Situationsanalyse und zur Entscheidungsfindung.

Parallel dazu hat sich das Bewusstsein für Themen wie Cybersecurity, Datensouveränität und technologische Unabhängigkeit deutlich geschärft. Viele Betreiber hinterfragen heute sehr viel stärker, wo Technologien entwickelt werden, wie sicher sie sind und ob sie langfristig zuverlässig betrieben werden können. Für uns als Hersteller, der seit jeher konsequent auf „Made in Germany“ setzt und Entwicklung sowie Produktion am Standort Deutschland bündelt, ist diese Entwicklung natürlich eine Bestätigung unserer strategischen Ausrichtung.



Dallmeier entwickelt und produziert seine Kamera- und Aufzeichnungssysteme sowie alle wesentlichen Software-Komponenten am Standort Regensburg in Deutschland

Ein weiterer wichtiger Punkt ist die Geschwindigkeit technologischer Innovation. Fortschritte in Bereichen wie KI-gestützter Videoanalyse verändern die Möglichkeiten moderner Videotechnologie fundamental. Systeme werden leistungsfähiger, skalierbarer und intelligenter. Für uns bedeutet das vor allem eines: kontinuierliche Weiterentwicklung. Wer in diesem Markt erfolgreich sein will, muss Innovation als dauerhaften Prozess verstehen.

Die einschneidendste Entwicklung

Eine der prägendsten Entwicklungen der letzten Jahre ist der enorme Fortschritt in der Videoanalyse – insbesondere durch den Einsatz von Künstlicher Intelligenz. Moderne Systeme sind heute in der Lage, große Datenmengen in Echtzeit auszuwerten und relevante Ereignisse automatisiert zu erfassen.

Künstliche Intelligenz ist für uns dabei kein Trend, sondern ein zentraler Baustein unserer Entwicklungen. Um Qualität und Transparenz sicherzustellen, gehen wir bewusst unseren eigenen Weg: Wir trainieren unsere neuronalen Netze auf unserem firmeneigenen, speziell dafür ausgestatteten Testgelände – und das unter realen Einsatzbedingungen. Entscheidend ist dabei die Kontrolle über die Trainingsdaten.

Effiziente Prozesse dank KI „trained by Dallmeier“

Bei vielen am Markt verfügbaren Systemen ist unklar, auf welcher Datenbasis sie trainiert wurden – mit entsprechenden Risiken, etwa durch Verzerrungen oder nicht nachvollziehbare Ergebnisse. Wir dagegen erstellen unsere Trainingsdaten selbst, exakt abgestimmt auf die Anforderungen unserer Kunden. Dadurch erreichen wir eine besonders hohe Präzision bei Funktionen wie Objektklassifizierung und Objekterkennung – bei gleichzeitig deutlich reduzierten Falschalarmen. Gleichzeitig schaffen wir damit eine wesentliche Grundlage für Vertrauen: Unsere Systeme sind nachvollziehbar, transparent und praxisnah trainiert. Kurz gesagt: Wir setzen auf „AI made in Germany“.

Mindestens ebenso wichtig ist der zunehmende Fokus auf Cybersecurity. Videotechnologie ist heute vollständig in IT-Infrastrukturen integriert. Damit gelten auch dieselben Anforderungen an Sicherheit, Integrität und Schutz vor Cyberattacken. Für Hersteller bedeutet das, Sicherheitsaspekte von Beginn an in Architektur und Entwicklung zu integrieren.

Auch geopolitische Entwicklungen und die Erfahrungen aus globalen Lieferkettenkrisen haben den Markt nachhaltig verändert. Viele Betreiber kritischer Infrastrukturen achten heute stärker auf vertrauenswürdige Lieferketten und langfristige technologische Partnerschaften. In diesem Zusammenhang gewinnt europäische Technologiekompetenz zunehmend an Bedeutung.

Wo geht die Reise hin?

Insgesamt entwickelt sich Videotechnologie immer mehr zu einer zentralen Informationsquelle. Sie liefert nicht nur sicherheitsrelevante Erkenntnisse, sondern unterstützt auch operative Prozesse und strategische Entscheidungen. Genau darin sehen wir die Zukunft: in intelligent vernetzten Systemen, die weit über klassische Security hinaus Mehrwert schaffen.

Ein entscheidender Trend ist dabei die zunehmende Integration unterschiedlicher Systeme. Videotechnologie wird immer stärker mit angrenzenden Sicherheitssystemen wie Zutrittskontrolle sowie mit zusätzlichen Datenquellen und Managementplattformen vernetzt. Ziel ist ein ganzheitliches Lagebild, das es Betreibern ermöglicht, Situationen schneller und fundierter zu bewerten.

Gleichzeitig rückt das Thema Wirtschaftlichkeit stärker in den Fokus. Betreiber erwarten Lösungen, die nicht nur leistungsfähig, sondern auch langfristig effizient sind. Hier spielen moderne Kameratechnologien eine wichtige Rolle: Durch den Einsatz von Multifocal-Sensortechnologie lassen sich große Bereiche mit deutlich weniger Kameras abdecken. Das reduziert nicht nur den Installationsaufwand, sondern senkt auch nachhaltig die Total Cost of Ownership – von der Infrastruktur über die Verkabelung bis hin zum Betrieb.

Parallel dazu steigen die Anforderungen an Skalierbarkeit. Systeme müssen so ausgelegt sein, dass sie mit den Anforderungen wachsen können – sei es durch zusätzliche Standorte, höhere Auflösungen oder neue Analysefunktionen. Offene Plattformen und flexible Architekturen sind hier der Schlüssel, um Investitionssicherheit zu gewährleisten.

Ein weiterer entscheidender Faktor ist Vertrauen. Betreiber erwarten transparente Technologien, nachvollziehbare Systeme und Hersteller, die langfristig Verantwortung übernehmen. Aspekte wie Datensouveränität, Cybersecurity und verlässliche Partnerschaften werden künftig noch stärker in den Mittelpunkt rücken. Unser Anspruch als Hersteller ist es, diese Entwicklungen mit innovativen, zuverlässigen und verantwortungsvoll entwickelten Lösungen aktiv mitzugestalten. GIT

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

KOMPLETTSYSTEME

Ein Jahr der Skalierung

Erneuertes Produktportfolio für professionelle Sicherheitsanwendungen

Ajax Systems hat das Jahr mit einer umfassend erneuerten Produktgeneration begonnen und präsentiert ein Portfolio, das auf professionelle Sicherheitsanwendungen in unterschiedlichsten Projektgrößen ausgerichtet ist. Im Gespräch mit GIT SICHERHEIT erläutert Aljona Göttert, Cluster Director DACH bei Ajax Systems, die zentralen Neuerungen, darunter den Superior Mega Hub für großflächige Installationen, ein drahtloses Einbruchschutzsystem mit EN Grad 3 Zertifizierung sowie ein erweitertes Videoüberwachungsangebot mit KI gestützten Funktionen. Das Jahr 2026 steht bei Ajax im Zeichen technologischer Weiterentwicklung, wachsender Systemvielfalt und einer intensiveren Zusammenarbeit mit Fachpartnern.

GIT SICHERHEIT: Frau Göttert, noch im vergangenen Jahr haben Sie hier in der GIT SICHERHEIT eine umfassende Erneuerung Ihres Portfolios der Öffentlichkeit vorgestellt – mit nicht weniger als 55 neuen Produkten. Sie haben dafür das Motto „Dare to be first" gewählt. Was steckt hinter dieser Botschaft und an wen richtet sie sich?

Aljona Göttert: Das Ajax-Team war das erste, das ein Sicherheitssystem entwickelt hat, bei dem der Mensch im Mittelpunkt steht – einfach zu bedienen, leicht verständlich und angenehm in der Nutzung. Wir waren die Ersten, die Geräte entworfen haben, die Anwender mit Stolz installieren. Wir waren die Ersten, die ein integriertes Ökosystem geschaffen haben, das unabhängig von Größe oder Komplexität nahtlos funktioniert.

Die neuen Produkte, die auf dem Ajax Special Event „Dare to be first" vorgestellt wurden, richten sich an Sicherheitsexperten, Installateure, Distributoren und Elektriker. Was bislang kabelgebundenen Systemen vorbehalten war, gelingt nun erstmals drahtlos: Ajax Systems bringt als erster Hersteller weltweit ein Funk-Sicherheitssystem mit EN-Grad-3-Zertifizierung auf den Markt. Damit verschiebt das Unternehmen die Grenzen etablierter Sicherheitsstandards und eröffnet neue Möglichkeiten für den professionellen Einsatz funkbasierter Technologien. Unser Team arbeitet kontinuierlich daran, Sicherheitslösungen zu entwickeln, die auf jede Projektart zugeschnitten sind.

Was macht das neue Portfolio aus, an welchen Kundenkreis richtet es sich – und was ist im Kern das Neue?

Aljona Göttert: Der Superior Mega Hub wurde als Antwort auf die wachsende Größe von Projekten entwickelt. Er unterstützt bis zu 999 kabelgebundene oder drahtlose Geräte in beliebiger Kombination sowie eine unbegrenzte Anzahl von Sirenen. Darüber hinaus unterstützt er 100 Gruppen, 100 Automatisierungsszenarien und 1.000 Nutzer. Einkaufszentren, Businessparks, Fabriken, Logistikstandorte und große Lagerhallen – all diese Objekte lassen sich mit nur einer Zentrale absichern. Die weitreichenden Fibra- und Superior-Jeweller-Technologien gewährleisten eine stabile Kommunikation, unabhängig von der Projektgröße.

Der Hub wird als Platine bereitgestellt und kommt mit dem neuen Case E, das vollständig kompatibel ist und sämtliche für den zuverlässigen Schutz erforderlichen Elemente bereits integriert: Ethernet, WLAN, zwei SIM-Karten-Steckplätze (2G/

Aljona Göttert, Cluster Director DACH bei Ajax Systems

LTE), Funkmodule und einem integrierten Netzteil. Nicht nur der integrierte Sabotageschutz, sondern auch die EN-Grad-3-Zertifizierung machen das System zu einer idealen Lösung für hochsicherheitsrelevante Anwendungen und besonders anspruchsvolle Objekte.

Kommen wir zum drahtlosen Grade 3-Einbruchschutzsystem. Wie sieht das genau aus?

Aljona Göttert: Es umfasst alles, was für den Schutz von Hochrisikoobjekten jeder Größe erforderlich ist: Bewegungs- und Öffnungsmelder, Außen Leser, Sirenen, Paniktaster, Funk-Repeater, Integrationsmodule sowie eine Zentrale – den Superior Hub G3 Jeweller. Der Hub unterstützt bis zu 250 Geräte und bleibt dank Ethernet, WLAN und zwei 2G/LTE-SIM-Karten jederzeit verbunden, mit automatischem Umschalten bei Ausfällen.

Die Geräte verfügen über vorinstallierte Hochleistungsbatterien mit einer Lebensdauer von bis zu sieben Jahren. Sie liefern eine präzise Detektionsleistung und sind durch erweiterten Sabotageschutz gesichert. Die Montage erfolgt innerhalb weniger Minuten, während die Konfiguration und Verwaltung unkompliziert über die Ajax Apps – sowohl vor Ort als auch aus der Ferne – möglich ist.

Die drahtlosen nach EN-Grad-3-Zertifizierung Geräte von Ajax kommunizieren über Superior Jeweller, eine Funktechnologie der neuen Generation. Sie setzt neue Maßstäbe in Reichweite, Stabilität und Desgin. Das neue Protokoll ermöglicht eine Reichweite von bis zu 3.500 Metern im freien Feld. Die verbesserte Verschlüsselung wird durch fortschrittliche Anti-Jamming-Funktionen ergänzt, die 17 verschiedene Frequenzen über vier europäische Bänder nutzen.

Generell steht Ajax aber weiterhin sowohl für drahtlose, verkabelte und hybride Lösungen...?

Aljona Göttert: Ja, Ajax Produkte ermöglichen die Umsetzung hybrider Projekte, bei denen drahtlose und kabelgebundene Lösungen kombiniert werden. Dies richtet sich nach den Anforderungen und Spezifikationen des jeweiligen Objekts. Wir bieten Installateuren maximale Flexibilität. Unsere Superior-Linie umfasst drahtlose Jeweller- sowie kabelgebundene Fibra-Geräte für den Einbruchschutz bei besonders anspruchsvollen Projekten.

Kommen wir zum großen Thema Videoüberwachung, die Sie als Baseline- sowie als Superior-Variante anbieten. Was zeichnet diese Produktlinien aus – und für welche Projekte sind sie jeweils gedacht?

Aljona Göttert: Das Ajax-Videoüberwachungsportfolio wächst rasant und folgt derselben Logik wie der Einbruchschutz von Ajax. Die Baseline-Produktlinie bietet alle wesentlichen Funktionen für eine effektive Videoüberwachung. Die Superior-Produktlinie hingegen steht für robustere Hardware, leistungsstärkere Funktionen, erweiterte KI und noch mehr Möglichkeiten, kompromisslose Sicherheit für jede Art von Objekt zu realisieren.

Vor allem bei der Superior-Reihe spielt die Künstliche Intelligenz eine wichtige Rolle. In welcher Weise spielt sie hier ihre Möglichkeiten aus?

Aljona Göttert: Die Superior-Videoüberwachung spart dank ihrer verbesserten Onboard-KI Zeit und Speicherplatz. Mit einer viermal mehr leistungsfähigeren Hardware erkennt die Kamera Personen, Haustiere und Fahrzeuge deutlich präziser als eine Baseline-Kamera. Zudem kann das Gerät Aufzeichnungen und Benachrichtigungen ausschließlich dann auslösen, wenn Bewegungen oder ausgewählte Objekttypen erkannt werden. Flexible KI-Einstellungen helfen Anwendern, sich auf das Wesentliche zu konzentrieren und Speicherressourcen zu sparen.

Die Superior-NVRs verfügen über eine proprietäre Onboard-KI und bringen intelligente Ajax-Videoüberwachung selbst in veraltete Setups. Die Rekorder ermöglichen es auch einfachen Kameras, Personen, Haustiere und Fahrzeuge zu erkennen – mit derselben Genauigkeit wie native Ajax-Kameras. Angeschlossene Drittanbieter-Kameras lassen sich über die Superior-NVRs nahtlos in das System integrieren. Sie können Bewegungen erkennen, sofort

Bitte umblättern ▶

Der Superior Mega Hub unterstützt bis zu 999 kabelgebundene oder drahtlose Geräte sowie eine unbegrenzte Anzahl von Sirenen

Benachrichtigungen versenden, Sirenen auslösen und definierte Automatisierungsszenarien aktivieren. All dies lässt sich mit nur einem Ajax Superior NVR realisieren – ganz ohne kostspielige Austauschmaßnahmen bei den Kameras.

Welche Vorzüge hat das neue Programm aus dem Blickwinkel des Errichters und Systemintegrators? Wie sieht Ihr Vertriebs- und Supportmodell aus?

Aljona Göttert: Der Status als autorisierter Ajax-Partner eröffnet nicht nur den Verkauf und die Installation von Ajax Produkten, sondern auch den Zugang zu zahlreichen Werkzeugen für das Unternehmenswachstum. Partner erhalten sofort einsetzbare Marketingmaterialien, nützliche Web-Tools sowie Zugang zu Online- und Offline-Kanälen zur Steigerung der eigenen Bekanntheit. Wir bieten rund um die Uhr Support und Beratung.

Zur zentralen Organisation dient das Partner Portal, über das Installateure Zugang zu exklusiven Partner-Events, Webinaren und Kursen der Ajax Academy erhalten. Es ist eine wichtige Informationsquelle für Branchentrends, da wir unsere Partner kontinuierlich über neue Produkte und deren Funktionen informieren.

Sie bieten mit Ihrer Ajax-Academy entsprechende Weiterbildungen und Zertifizierungsmöglichkeiten an?

Aljona Göttert: Ja, mit der Ajax Academy ermöglichen wir es Installateuren, ihre Fähigkeiten im Umgang mit Ajax Lösungen nach einem weltweit einheitlichen Bildungsstandard zu vertiefen. Die Ajax Academy bietet Kurse, die sowohl theoretische als auch praktische Aspekte der Arbeit mit Ajax Geräten abdecken. Jeder Kurs wird mit einem eigenen Zertifikat abgeschlossen, das Kunden überprüfen können. Für die Installation von Superior-Produkten ist die Akkreditierung als Partner obligatorisch. Erst nach erfolgreicher Zertifizierung dürfen diese Produkte installiert werden.

Was haben Sie bei Ajax dieses Jahr noch alles vor...?

Aljona Göttert: 2026 steht für uns bei Ajax ganz klar im Zeichen der neuen Produktgeneration – sie wird einen großen Teil unserer Aktivitäten prägen. Gleichzeitig ist das Jahr für uns deutlich breiter aufgestellt: Neben den Produktlaunches investieren wir stark in den Ausbau unseres Ökosystems, insbesondere in Zertifizierungen, Trainings und die Unterstützung unserer Partner im professionellen Projektgeschäft. Ein weiterer Schwerpunkt liegt auf der Stärkung unserer lokalen Präsenz in den Märkten – mit mehr Nähe zu Kunden, intensiverem Austausch und gezielten Formaten wie Roadshows Messen und Fachveranstaltungen. Kurz gesagt: 2026 ist für Ajax ein Jahr der Skalierung – technologisch, organisatorisch und in der Zusammenarbeit mit dem Markt. GIT

Ajax Systems
www.ajax.systems

VISION

In den nächsten zehn Jahren wird der Brandschutz in Deutschland durch vollständig vernetzte, vorausschauende Systeme geprägt sein, die Risiken früh erkennen, Compliance automatisieren und so datenbasierte Entscheidungen ermöglichen.

Klaus Hirzel, Business Leader Europe Central Region (DACH), Honeywell Fire Products

35 JAHRE GIT SICHERHEIT

WILEY

35 Jahre

GIT SICHERHEIT

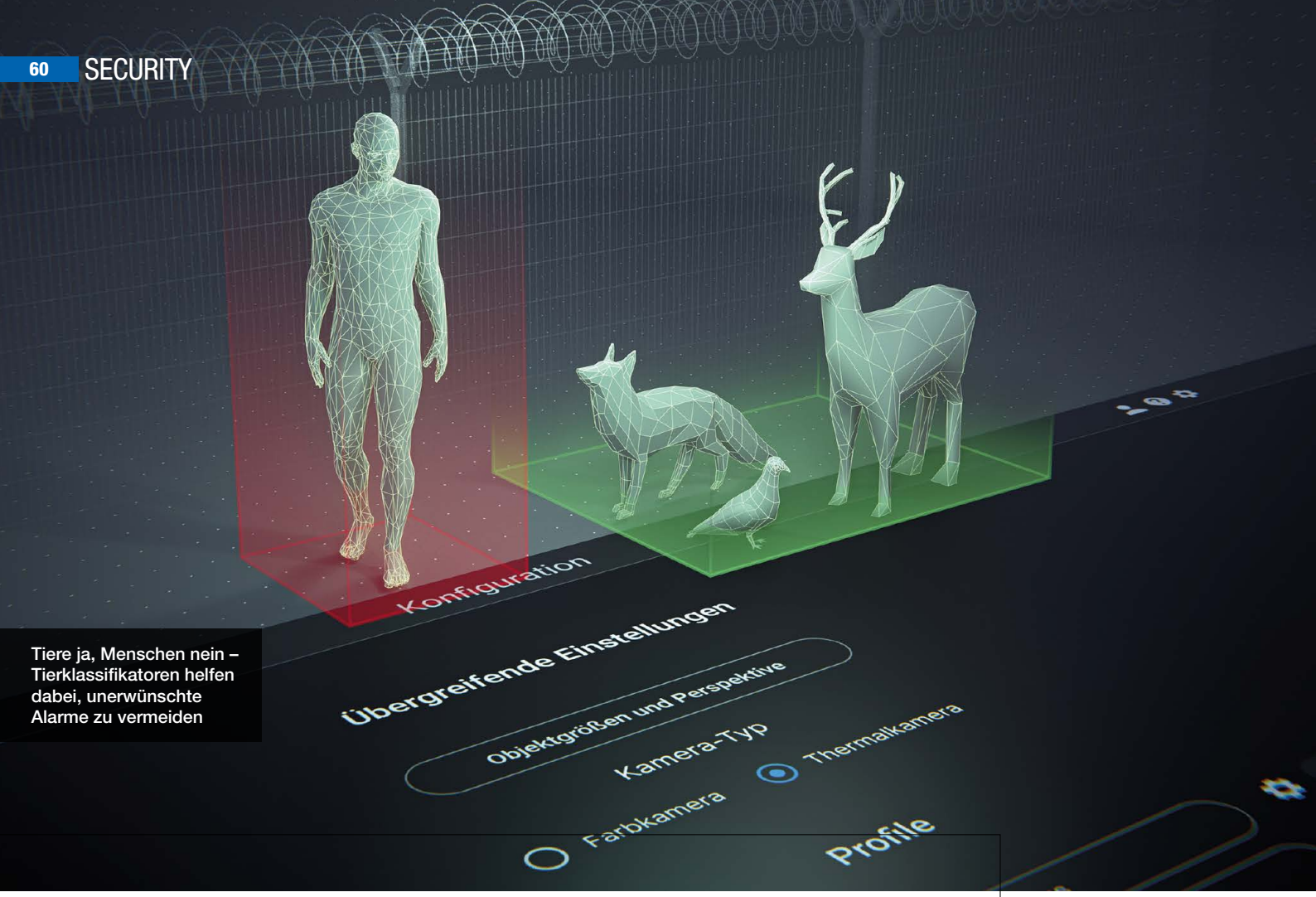
Die Jubiläumsausgabe

Seit 35 Jahren begleitet GIT SICHERHEIT den Sicherheitsmarkt – kritisch, unabhängig und immer nah an den relevanten Fragen der Zeit. Dieses Jubiläum ist für uns mehr als ein Rückblick: Es ist Anlass, Entwicklungen einzuordnen, Stimmen zu Wort kommen zu lassen und den Blick nach vorn zu richten.

Auf unserer Jubiläums-Landing-Page finden Sie exklusive Interviews mit Entscheiderinnen und Entscheidern, fundierte Trendberichte, pointierte Analysen und besondere Specials, die zeigen, wie sich Sicherheitstechnologien, Strategien und Märkte verändert haben – und was heute wirklich zählt.

Entdecken Sie 35 Jahre SICHERHEIT im Kontext.

Jetzt online auf:
git-sicherheit.de/de/
35-Jahre-GIT-SICHERHEIT



Tiere ja, Menschen nein – Tierklassifikatoren helfen dabei, unerwünschte Alarme zu vermeiden

VIDEOTECHNIK

Zwei Lidschläge extra

Neue Generation: Videoanalyse für Industrie und KRITIS

Mit der Version 17 des IPS Video Manager präsentiert die Technologiemarke IPS von Securiton Deutschland eine neue Generation intelligenter Videosicherheit. Besonders für Betreiber kritischer Infrastrukturen und Industrieunternehmen mit großen oder ländlich gelegenen Außenanlagen bringen neue Features eine spürbare Entlastung bei der lückenlosen Absicherung großer Perimeter.

© generiert mit Adobe Firefly

Weniger unerwünschte Alarme, sehr hohe Detektionsqualität, eine robuste und zugleich auditfähige Systemarchitektur: Der IPS Videomanager von Securiton kombiniert modernste IT-Security-Mechanismen, erweiterte Videoanalysefunktionen für IPS Next Gen Video Analytics und einen leistungsstarken IPS Next Gen Client, der die Einsatzsteuerung und Ereignisrecherche mit der Videomanagementplattform deutlich beschleunigt.

Anlagen und Perimeter sicherheitskritischer Einrichtungen müssen rund um die Uhr zuverlässig überwacht werden. Unnötige Alarme binden Personal und verursachen Kosten. Sie entstehen etwa durch Wärmeschlieren, kurzzeitige Bildirritationen oder Tiere, wie Rehe, Vögel oder Spinnen. Die neue Softwareversion verifiziert Alarme mit erweiterten Klassifikatoren und sortiert kurzzeitige Störungen aus.

Frühwarnsysteme wie der IPS Videomanager von Securiton sorgen für lückenlose Perimetersicherung und entlasten das Sicherheitspersonal

Die IPS Next Gen Video Analytics sind zudem um Mechanismen für den Einsatz von Thermalkameras erweitert worden. Weniger unnötige Alarme beruhigen insgesamt den Systembetrieb und steigern die Produktivität einer Leitstelle. Derart effiziente Workflows und skalierbare Sicherheitsplattformen, die sich intuitiv bedienen lassen, sind eine große Hilfe für Sicherheitsteams mit meist begrenzten Ressourcen. Überflüssige Außeneinsätze und ihre Kosten werden vermieden.

Eliminierung von Kurzzeit-Artefakten

Securiton hat auch die Alarmverifizierungsfunktion zur Eliminierung möglicher Kurzzeit-Artefakte optimiert: Für die Dauer von etwa zwei Lidschlägen, also 250 Millisekunden, wird kein Alarm ausgelöst. Diese Verzögerung macht die Feststellung einer realen Gefahr noch zuverlässiger. Es sind sogar zonenspezifische Einstellungen möglich, die sich visuell in der Videoanalyse-Konfiguration darstellen lassen und das Verfahren dadurch für den Anwender vereinfachen.

Anforderungen an die Compliance sind in Hochsicherheitsanwendungen besonders streng. Mit der Version 17 führt Securiton eine einheitliche, serverseitige Berechtigungsprüfung ein. Alle Client-Aktionen werden zentral geprüft, nicht autorisierte Befehle konsequent blockiert und vollständig dokumentiert – für mehr Revisionssicherheit, minimale Bedienrisiken und die Einhaltung grundlegender Sicherheitsprinzipien. Ein Berechtigungsmanagement, die Dokumentation und die Nachvollziehbarkeit von Handlungen sind essenziell für KRITIS- und Zertifizierungsanforderungen.

Keine zeitraubende Suche

Der IPS Video Manager Next Gen Client bietet eine vollständig überarbeitete Ereignisrecherche mit Filtermöglichkeiten nach Zeit, Alarmtyp oder Kategorie. Die Meldungen können als fortlaufende Liste oder strukturiert dargestellt werden. Diese Funktionen beschleunigen die forensische Analyse erheblich. Der Next Gen Client unterstützt nun auch Dualkopf-Kameras (Farb- und Thermalkameras auf einem Stativ) mit separater Zoomsteuerung je Kamera. Axis-Bediengeräte wie Joystick und Keypad sind vollständig integriert und erlauben eine präzise, haptische Steuerung.

Ob Umspann-, Wasserwerk oder Produktionsanlage – der Schutz sicherheitskritischer Grundstücke in ländlicher Umgebung oder großflächigen Außenbereichen erfordert eine leistungsstarke Softwarelösung mit Echtzeit-Alarmverifizierung und fortschrittlichen forensischen Analysen. Die Version 17 des IPS Video Manager liefert in allen Szenarien Verbesserungen: weniger unerwünschte Alarme, klarere Fokusalarme, schnellere Analysen und eine robuste, auditfähige Sicherheitsarchitektur. GIT

Securiton Deutschland
www.securiton.de

VIDEOSYSTEME

Strategisches Werkzeug

KI-Videoüberwachung in der Logistik stärkt Sicherheit und Effizienz

Von der Verbesserung der Versandzeiten und der Effizienz der Lieferkette bis hin zur Kostensenkung: Logistikunternehmen stehen vor vielen herausfordernden Aufgaben. Es geht um die Bewältigung globaler Komplexität und die Reduzierung von Verlusten. Kriminelle haben es vor allem auf Waren mit hohem Wiederverkaufswert abgesehen, wie Elektronik, Pharmazeutika und lebenswichtige Güter. Hanwha Vision setzt zur Absicherung auf KI-gestützte Videoüberwachungslösungen.

Etwa 8,2 Milliarden Euro jährlich. So hoch sind die Verluste, die von Logistikunternehmen in Europa verzeichnet werden. Lagerhäuser werden am häufigsten ins Visier genommen – sie machen 41 % der gemeldeten Vorfälle in Großbritannien und Europa aus. Betrug und Vandalismus sind weitere Sorgen für Logistikleiter, die zu Ausfallzeiten von Geräten oder Fahrzeugen, Versandverzögerungen und unzufriedenen Kunden führen.

Stärkung der Sicherheit vor Ort

Traditionelle Sicherheitsmaßnahmen reichen unter solchen Umständen nicht mehr aus. KI-gestützte Videoüberwachung bietet eine dynamischere Lösung, die kontinuierlich nach ungewöhnlichen Aktivitäten sucht, Echtzeitwarnungen für Ereignisse ausgibt, die überprüft werden müssen, und Betreiber auf potenzielle Eindringlinge, Diebstahl, Vandalismus oder andere verdächtige Verhaltensweisen hinweist.

Moderne Videosysteme bieten mehrere Schutzschichten, die alles abdecken, von Ladebereichen und Haupteingängen bis hin zu Verarbeitungszentren und Parkplätzen. Die Konsolidierung aller Kamera-, Sensor-, Planungs-, Alarmüberwachungs- und Zugangskontrollinformationen an einer zentralen Stelle stellt sicher, dass die Betreiber vollständig darüber informiert sind, wer vor Ort ist, ob er dazu berechtigt ist, den Status und den Standort von Lagerbeständen und Fahrzeugen, mögliche Eindringlinge und mehr.

Mehrwert durch betriebliche Erkenntnisse

KI-gestützte Videos gehen über die bloße Verbesserung der Sicherheit hinaus und erhöhen zusätzlich die betriebliche Effizienz. Durch die Integration von KI-Videoanalysen mit Warehouse-Management-Systemen (WMS) können Logistikunternehmen tiefere Einblicke in ihre Arbeitsabläufe gewinnen und ihre Prozesse feinabstimmen, um potenzielle Verluste zu reduzieren, die Planung zu verbessern und den Warenfluss zu optimieren.

KI kann Engpässe, untergenutzte Räume, potenzielle Geräteausfälle (oder den Bedarf an Maschinenwartung), fehlplatzierte Pakete und langsame Prozesse, die zu Verzögerungen führen können, identifizieren.

Als Teil seiner Funktion zur Warteschlangenverwaltung und Sicherheit kann Hanwha Visions neue KI-gesteuerte Logistiklösung die Aktivitäten in Ladebuchten genau überwachen, verfolgen, ob die richtigen Fahrzeuge dort geparkt sind, wo sie sein sollten, ob sie die richtigen Pakete erhalten und, ebenso wichtig, wie lange sie benötigen, um volle Ladezeiten zu erreichen.

Automatisierung für mehr Effizienz

KI-gestützte Videosysteme können einige Aufgaben automatisieren, um den Betreibern mehr Zeit für strategische Aktivitäten auf höherer Ebene zu geben. Es wird geschätzt, dass der Einsatz von Automatisierung und KI durch Logistikunternehmen bis zu 20 % der Betriebskosten einsparen könnte. Fahrzeuge auf der Whitelist können beispielsweise automatisch identifiziert und über verbundene Barrieren auf das Gelände gelassen werden, und wichtige Nachrichten zum Tragen von PSA oder zur Nutzung einer bestimmten Route können über integrierte digitale Beschilderung übermittelt werden.

Die Dual-Lens Barcode Reader Camera von Hanwha Vision verwendet KI zur Erkennung von Barcode-Etiketten auf Hochgeschwindigkeits-Förderbändern, was es den Betreibern erleichtert, Etiketten effizient zu finden und Sendungen mit Barcode-Informationen und -Historie in Echtzeit zu verfolgen. Da Filmmaterial und Barcode-Informationen in einem einzigen

35 JAHRE GIT SICHERHEIT

VISION

Innerhalb der nächsten zehn Jahre werden wir im Bereich Sicherheit in der Lage sein, durch KI-gestützte Früherkennung und integrierte Krisenmanagementsysteme hybride Bedrohungen proaktiv abzuwehren und die Resilienz von Unternehmen entscheidend zu stärken.

Jürgen Wittmann, Vice President Corporate Security bei der Robert Bosch GmbH und Präsident der ASW-BW

Gerät erfasst werden, können die Betreiber Standort, Zeit und Filmdetails von Paketen und Ereignissen überprüfen, ohne die Systeme wechseln zu müssen, was die Effizienz des Teams weiter verbessert.

Letztendlich erhöhen der Einsatz von KI und Automatisierung in der Lager- und Bestandsverwaltung die Rückverfolgbarkeit, reduzieren den Versandaufwand und die Rücksendungen und verbessern die Kundenzufriedenheit.

Datengetriebene Entscheidungen ermöglichen

Im Laufe der Zeit können die von Videosystemen gesammelten Daten die zukünftige Strategie beeinflussen und den Führungskräften helfen, die Haupttreiber hinter Verzögerungen zu identifizieren. Die Konsolidierung von Informationen und Echtzeitanalysen unterstützt Führungskräfte bei der Analyse der großen Datenmengen, die aus allen Teilen der Lieferkette eingehen.

Für Logistikleiter bedeutet dies weniger betriebliche Blindspots und weniger Zeitverlust durch Streitigkeiten, Ausfallzeiten oder vermeidbare Risiken. Automatisierte Berichterstattung und klare Aufzeichnungen helfen Unternehmen auch, die Einhaltung von Vorschriften leichter nachzuweisen, wodurch die Haftung bei Unfällen oder Ansprüchen reduziert wird. Da die Regulierungsbehörden die Standards verschärfen und die Kunden Transparenz fordern, summieren sich diese Vorteile schnell.

Der Logistiksektor entwickelt sich rasant weiter und die für ihn entwickelten Überwachungslösungen halten mit dieser Entwicklung Schritt. KI-gestützte Videolösungen liefern heute viel mehr als nur Sicherheit, sie werden zu wichtigen strategischen Werkzeugen, die Effizienz, Compliance und langfristiges Wachstum verbessern. GIT

Hanwha Vision
www.hanwhavision.eu

© Barox

TRENDBERICHT

Global gefestigt

Ein Trendbericht von Barox-Geschäftsführer Rudolf Rohr

In den vergangenen Jahren hat sich unser Unternehmen dynamisch entwickelt und seine internationale Ausrichtung konsequent ausgebaut. Barox ist dadurch zunehmend zu einem international tätigen Unternehmen geworden, unter anderem durch die Festigung unserer Marktposition im Vereinigten Königreich und die kürzliche Gründung unserer Tochtergesellschaft in den USA.

Die technologischen Veränderungen in der Branche haben auch unser Unternehmen stark beeinflusst. Die Grenzen zwischen Operational Technology (OT) und Information Technology (IT) verschwimmen zunehmend. Diese Entwicklung eröffnet für uns neue Chancen, bringt aber auch zusätzliche Anforderungen an Sicherheit, Integration und Know-how mit sich.

Eine der einschneidendsten Entwicklungen für unser Unternehmen war der kürzlich erfolgte Markteintritt in die USA mit der Gründung der Barox Communication Corp. Mit diesem Schritt haben wir nicht nur unsere internationale Präsenz deutlich ausgebaut, sondern auch eine wichtige strategische Grundlage geschaffen. Der Eintritt in den US-Markt eröffnet uns langfristig neue Wachstumschancen, stärkt unsere globale Wettbewerbsfähigkeit und ermöglicht es uns, gezielt weitere Märkte zu erschließen. Damit haben wir eine belastbare Basis gelegt, um unsere Expansion in den kommenden Jahren nachhaltig voranzutreiben.

Wo geht die Reise hin?

Die Zukunft der Sicherheit wird zunehmend durch die enge Verzahnung von IT- und OT-Systemen geprägt sein. Netzwerke werden komplexer, gleichzeitig steigen die Anforderungen an Transparenz, Verfügbarkeit und Cybersecurity. In diesem Umfeld gewinnen intelligente, softwarebasierte Lösungen immer mehr an Bedeutung.

Künstliche Intelligenz wird dabei eine zentrale Rolle spielen, insbesondere bei der Analyse großer Datenmengen, der frühzeitigen Erkennung von Anomalien und der Automatisierung von Prozessen. Ziel ist es, Systeme nicht nur sicherer, sondern auch effizienter und einfacher beherrschbar zu machen.

Für uns bedeutet das, unsere Kompetenzen in den Bereichen Software, Netzwerkmanagement und intelligente Assistenzsysteme konsequent weiter auszubauen. Gleichzeitig bleibt der Mensch ein entscheidender Faktor: Nur durch das Zusammenspiel von innovativer Technologie und fundiertem Know-how lassen sich nachhaltige und zuverlässige Sicherheitslösungen realisieren.

Im Bereich Software treiben wir diese Entwicklung konkret mit unserem Network Management System (NMS) aktiv voran. Das NMS wird im Hintergrund kontinuierlich weiterentwickelt und im September an der Security Essen erstmals einem breiten Fachpublikum präsentiert. GIT

Barox Kommunikation GmbH
www.barox.ch

© Advancis

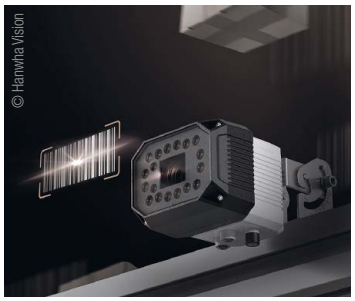
VISION

Innerhalb der nächsten zehn Jahre werden wir mit unseren offenen Softwareplattformen in der Lage sein, Sicherheits- und Gebäudetechnik weltweit intelligenter zu vernetzen und damit neue Maßstäbe für Transparenz, Effizienz und Resilienz in komplexen Infrastrukturen zu setzen.

Andre Meiswinkel,
COO Advancis Software & Services GmbH

35 JAHRE GIT SICHERHEIT

Modulare Barcode-Leser-Kamera



Hanwha Vision hat eine Barcode-Leser-(BCR)-Kamera für die Logistikbranche eingeführt. Mit einem modularen Design für flexible Konfiguration, verbesserter Barcode-Erkennungsleistung und nahtloser Systemintegration erhöht diese Lösung die Effizienz für den Logistiksektor.

Die Kamera bietet eine modulare Struktur, die es den Benutzern ermöglicht, das Objektiv, das LED-Modul und die Frontabdeckung an die spezifischen Anforderungen des Standorts anzupassen. Mit vielfältigen Objektivoptionen von 6 mm bis 25 mm und LED-Modulen mit sowohl breiten als auch schmalen Abstrahlwinkeln gewährleistet die Kamera optimale Betrachtungswinkel und Helligkeit in verschiedenen Installationseinstellungen. Diese Flexibilität ermöglicht es den Kunden, nur die Komponenten auszuwählen, die sie benötigen, und hilft dabei, komplexe Installationsherausforderungen zu bewältigen und gleichzeitig die Rentabilität zu maximieren. Die 3 MP monochrome (schwarz und weiß) Kamera ist für die Barcode-Erkennung optimiert und liefert verbesserte Bildklarheit bei gleichzeitiger Minimierung der Datenverarbeitungsanforderungen. **https://hanwhavision.eu**

VISION

Innerhalb der nächsten zehn Jahre werden wir im Bereich Sicherheit in der Lage sein, Bedrohungen frühzeitig durch KI-gestützte Analysen zu erkennen, Risiken präziser vorherzusagen und durch vernetzte Systeme schneller, koordinierter und transparenter zu reagieren.

André F. Kunz,
ASW-BW Geschäftsführer

35 JAHRE GIT SICHERHEIT

Telenot: Schutz sensibler Gebäude

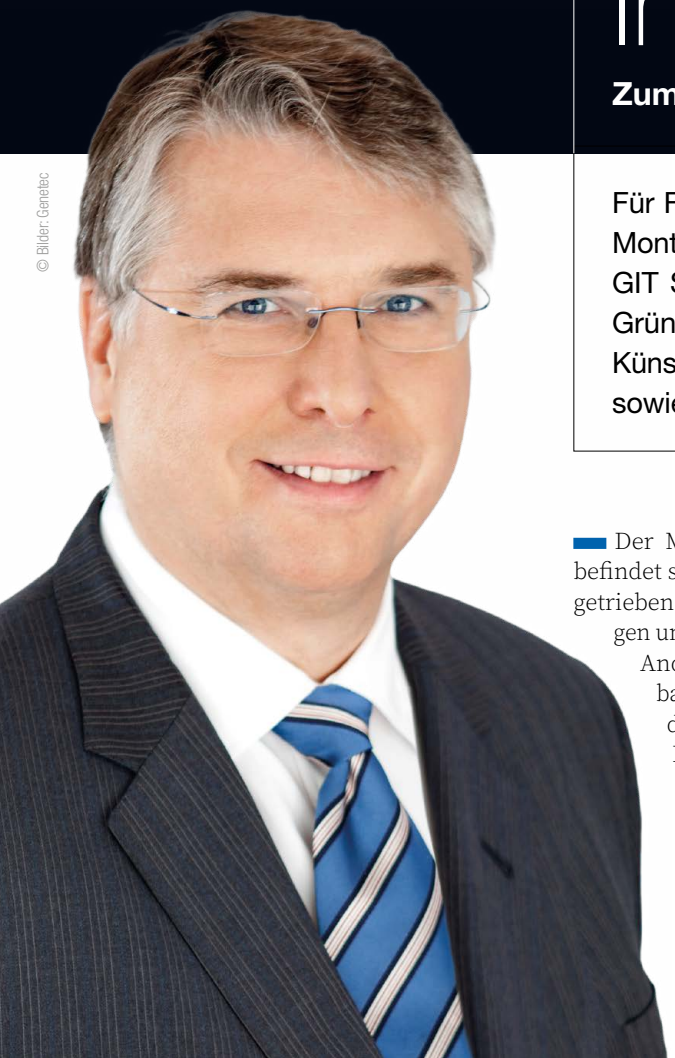
Die Software CompasZ 5500 dient der Verwaltung des Zutrittskontrollsystems Hilock 5000 TK von Telenot. Nun hat die Software die anspruchsvolle sicherheitstechnische Prüfung Atruvia AG bestanden, Digitalisierungspartner der Volks- und Raiffeisenbanken. Diese Geldinstitute haben damit die Freigabe zum Einsatz des Zutrittskontrollsystems für ihre Standorte. Anfang Januar 2023 hat die Zutrittsverwaltungssoftware CompasZ 5500 (ab Version 3.1.0.0.) von Telenot nach umfassenden Tests durch die Atruvia AG die Unbedenklichkeitsbestätigung bekommen. Die Verwaltungssoftware hat bei dieser Prüfung das von der Atruvia geforderte Sicherheitsniveau deutlich überschritten. Die Software ist Teil des flexiblen und einfach skalierbaren Zutrittskontrollsystems Hilock 5000 ZK. Das Zusammenspiel der Verwaltungssoftware mit dem Auswertesteuergerät Hilock 5500 ermöglicht es Nutzern, wirtschaftliche Zutrittslösungen für jede Objektgröße und -art zu realisieren. **www.telenot.com**

Leitstelle in der Mont Royal Shopping Mall in Montréal, die mit Videotechnik von Genetec ausgestattet wurde

VIDEO

Künstlicher Impressionismus

Zum praktischen Einsatz von KI bei Genetec



© Bilder: Genetec

Für Februar dieses Jahres hatte Genetec an seinem Hauptsitz in Montreal ein zweitägiges Programm organisiert. Matthias Erler von GIT SICHERHEIT nutzte die Gelegenheit, mit CEO Pierre Racz, Gründer und Präsident von Genetec, über sein Verständnis von Künstlicher Intelligenz, deren Anwendung in der Sicherheitstechnik sowie über die neuesten Projekte des Unternehmens zu sprechen.

Der Markt für physische Sicherheit befindet sich in einem rasanten Wandel – getrieben von geopolitischen Entwicklungen und technologischen Fortschritten. Andrew Elvish, Vice President Global Marketing bei Genetec, gab auf dem Global Press Summit, der im Februar am Genetec-Hauptsitz in Montréal stattfand, einen Überblick über den aktuellen Stand und die wahrscheinliche Zukunft des Marktes aus Sicht des Unternehmens. Im Interview mit GIT SICHERHEIT erläuterte CEO Pierre Racz insbesondere seine Sicht auf die Rolle der künstlichen Intelligenz in der Sicherheitsbranche.

GIT SICHERHEIT: Herr Racz, was ist derzeit der wichtigste Einfluss, den künstliche Intelligenz auf Ihre Produkte und Ihr Unternehmen ausübt?

Pierre Racz: Zunächst muss man verstehen, dass sich der Begriff „KI“ im Laufe der Zeit stark verändert hat. Ich arbeite seit den 1980er-Jahren in diesem Bereich, als KI noch Logikprogrammierung bedeutete –

Lisp, Prolog und Ähnliches. Später kamen neuronale Netze und Support Vector Machines hinzu. Technologien, die damals als KI galten, verwendetn wir schon seit 2003 in unseren Produkten. Mit dem Aufkommen tiefer neuronaler Netze um 2010 sind wir auf diese umgestiegen, und seit 2012 sind sie ein zentraler Bestandteil unserer Systeme. Seit einiger Zeit experimentieren wir auch mit großen Sprachmodellen.

Als Ingenieur ist für mich entscheidend, die Stärken und Schwächen der Werkzeuge zu kennen. Es ist wie beim Brückenbau: Wenn man schwere Lasten erwartet, verwendet man nicht Holz-, sondern Stahlträger. Das gilt auch für den Einsatz von KI: Man muss wissen, wo sie gut funktioniert – und wo nicht. Deshalb gestalten wir unsere Systeme so, dass Fehler möglichst geringe Auswirkungen haben. Praktisch bedeutet das: KI bleibt bei uns bei der finalen Entscheidungsfindung außen vor. Menschen liefern Urteilsvermögen und Kreativität – Maschinen übernehmen die schweren Arbeiten.

Wie kann man sich das konkret vorstellen?

Pierre Racz: KI ist besonders gut in dem, was man eine unscharfe, annäherungsweise Suche nennen könnte. Sie erkennt Muster und Ähnlichkeiten in großen Datenmengen, ist aber erstaunlich schlecht im Erfassen feiner Details. Das liegt daran, dass sie probabilistisch, also mit Wahrscheinlichkeiten arbeitet. Sie weiß nichts – sie schätzt. Was viele als „Halluzinationen“ bezeichnen, sind statistisch naheliegende, aber trotzdem falsche Ergebnisse.

Sie haben in Ihrem Vortrag den Begriff „Impressionismus“ dafür verwendet…

Pierre Racz: Ja, das ist ein hilfreicher Vergleich. Vor der Fotografie versuchten Maler – vor allem solche des Realismus –, die Realität so exakt wie möglich abzubilden. Mit der Fotografie wurde das überflüssig, und darauf reagierte die Kunst. Die Impressionisten malten abstrakter, „pixeliger“, also eher mit großen Pinselstrichen, die erst aus der Entfernung ein Bild ergeben. Es werden keine Details wiedergegeben, sondern ein Eindruck vermittelt. KI funktioniert ähnlich: Sie erzeugt einen Eindruck der auf Trainingsdaten basiert und projiziert die Frage darauf. Das Ergebnis ist im Grunde eine Schätzung – manchmal erstaunlich gut, aber eben eine Schätzung.

Was erwarten Ihre Kunden heute vom Beitrag Künstlicher Intelligenz?

Pierre Racz: Viele Kunden sind inzwischen skeptisch. Auf Messen preisen Anbieter KI begeistert an, aber Kunden sagen oft: „Geben Sie mir kein Verkaufsgetöse, geben Sie mir etwas Nützliches.“ Sie haben keine Zeit, ständig neue Technologien zu bewerten. Und es wächst das Bewusstsein, dass „KI-gestützt“ nicht automatisch wertvoll bedeutet. Im Gegenteil: Es kann ein Warnsignal sein. Manche verwenden „KI“ sogar als Synonym für schlecht gemachte Arbeit. Einige scherzen, KI sei wie ein fauler Praktikant mit schlechter Arbeitsmoral.

Also ist KI eher ein Werkzeug als eine Lösung?

Pierre Racz: Genau. Sie ist wie ein Taschenrechner: Er macht Sie nicht klüger oder dümmer – nur schneller, wenn Sie wissen, wie man ihn richtig nutzt. Zudem erkennen immer mehr Menschen KI-generierte Inhalte. Hat man die Muster einmal verstanden, sieht man sie überall – Wiederholungen, typische Formulierungen usw. Und grundsätzlich: KI innoviert nicht – sie imitiert. Sie kombiniert Bestehendes neu.

Showroom im Hauptsitz von Genetec in Montréal

Wie wird KI die Sicherheitsbranche in den nächsten fünf bis zehn Jahren verändern?

Pierre Racz: Kurzfristig erwarte ich Probleme. Wir werden „schlampiger Sicherheit“ begegnen – Systemen, die im Labor gut funktionieren, aber in der Realität versagen. Das erzeugt eine falsche Sicherheit, die Angreifer ausnutzen werden. Ich rechne mit einigen ernsthaften Vorfällen. Es gibt sogar einen Begriff dafür: „AI slop“ – also minderwertige, schlecht implementierte KI.

Passiert das bereits?

Pierre Racz: Ja, aber noch ohne große, öffentlich bekannt gewordene Katastrophen. Aber es ist eben wie bei jeder neuen Technologie: Es braucht Zeit, um sie richtig einzusetzen. Als Elektrizität neu war, nutzte man sie für die absurdesten Dinge. Es dauert Jahrzehnte, bis sich sinnvolle Anwendungen durchsetzen.

Sie erwähnten auch, dass Menschen KI leicht vermenschlichen.

Pierre Racz: Ja, das ist ein großes Problem. Menschen projizieren automatisch Intelligenz auf solche Systeme. Das war schon bei frühen Chatbots wie „Eliza“ so. Heute sind die Systeme komplexer, aber die grundlegende Einschränkung bleibt: Sie verstehen nicht wirklich. Und sie haben Schwierigkeiten mit Mehrdeutigkeiten, die Menschen intuitiv erfassen.

Was sind für Sie bei Genetec die wichtigsten Vorhaben in den kommenden Jahren?

Pierre Racz: Unser Fokus liegt darauf, Kunden zu mehr betrieblicher Effizienz zu verhelfen. Viele stehen unter Budget- oder Regulierungsdruck und wollen wissen, wie Technologie ihnen dabei helfen kann, ihre Aufgaben trotzdem zu erfüllen. Interessanterweise sind etwa 50 % unserer Produktfunktionen direkt aus dem Feedback unserer Kunden entstanden. Die anderen 50 % sind Ideen, die wir selbst entwickeln – nicht alle davon sind nützlich. Unser Ansatz ist exploratives Problemlösen: eng mit Kunden arbeiten, Ideen testen, iterieren – ohne ihre Ressourcen zu verschwenden.

Gibt es aktuelle Entwicklungen, die Sie nennen können?

Pierre Racz: Ein wichtiger Schwerpunkt ist unser hybrider Ansatz – die Brücke zwischen Cloud und On-Premise. Organisationen haben sehr unterschiedliche Anforderungen: Manche wollen alles in der Cloud, andere möglichst wenig, viele brauchen eine Mischung. Wir haben unsere Systeme so entwickelt, dass sie diese Flexibilität mit einer einzigen Codebasis unterstützen. So können wir uns an verschiedene Umgebungen anpassen, ohne Kunden in starre Architekturen zu zwingen. GIT

Genetec
www.genetec.com

© LivEye

„Sicherheitstechnik, die man nicht kontrolliert, ist ein Widerspruch in sich“

Ein Trendbericht von Carsten Simons, CEO von LivEye

Wer glaubt, Sicherheit sei ein Produkt, das man kauft und vergisst, hat das Problem noch nicht verstanden. Ein geschütztes Bild, das niemand sieht, nutzt niemandem. Ein Alarm, auf den niemand reagiert, ist lediglich Lärm. Und eine Lieferkette, die reißt, wenn es ernst wird – ist keine Grundlage für irgendetwas. Genau da stehen wir gerade. Die Branche hat jahrzehntelang Abhängigkeiten aufgebaut, die heute jeder spürt – bei Chips, bei Firmware, bei Hersteller-Support aus Regionen, denen niemand mehr bedenkenlos vertraut. Das war bequem. Jetzt ist es ein Risiko. Bei LivEye haben wir das früh so gesehen – und Konsequenzen gezogen.

Die einschneidendste Entwicklung der letzten Jahre war für uns keine technische. Es war eine Erkenntnis: Fast die gesamte Sicherheitstechnik, die in Deutschland eingebaut wird, kommt von außen. Hergestellt in Regionen, die heute geopolitisch unter Druck stehen, mit Lieferketten, die niemand wirklich überblickt. Das war immer so. Aber seit Chips fehlen, seit Firmware-Updates auf einmal zur Sicherheitsfrage wurden, seit Hersteller-Support plötzlich nicht mehr selbstverständlich war – seitdem ist es jedem klar: Sicherheitstechnik, die man nicht kontrolliert, ist ein Widerspruch in sich.

Made in Germany

Deshalb hat LivEye bereits 2022 begonnen, konsequent auf „Made in Germany“ zu setzen – gegen den Trend, weil es in der Startphase teurer ist und Zeit benötigt. Aber wir wollten Sicherheitsinfrastruktur bauen, die wir selbst beherrschen: kontrollierbare Komponenten, auditierbare Prozesse, verlässliche Verfügbarkeit. Heute bestätigt die geopolitische Realität genau diesen Schritt. Gerade bei Kunden aus KRITIS, Energie, Bau und öffentlicher Hand ist die Frage „Wer kann das im Zweifel morgen noch betreiben?“ wichtiger als jede Feature-Liste.

Aus dieser Strategie ist NSTR.security entstanden – eine eigenständige Marke, entwickelt und produziert in Deutschland, als direkte Antwort auf das, was dem Markt fehlte: KI-gestützte Videosicherheitslösungen, die nicht komplex in der Einführung sind, sondern schnell, skalierbar und operativ beherrschbar. NSTR.security steht für eigene Hardware, eigene Software und eine eigene Leitstelle – alles unter einem Dach, alles in Deutschland.

Vom Aufzeichnen zum Handeln

Die zweite einschneidende Veränderung: Videoüberwachung hat sich vom Aufzeichnen zum Handeln entwickelt. Ein Bild ist wertlos, wenn niemand rechtzeitig reagiert. Deshalb rückt der Betrieb in den Mittelpunkt – 24/7-Leitstelle, klare Eskalationswege, definierte Reaktionszeiten, dokumentierte Maßnahmen. Bei LivEye und NSTR.security ist das kein Add-on, sondern der Kern des Modells: Operatoren sprechen Täter live an, noch während sie auf dem Gelände sind – parallel wird Polizei oder Wachschutz benachrichtigt.

Aus diesen Erkenntnissen haben wir das Modell konsequent weiterentwickelt. LivEye hat das bewährte Videotower-Konzept strategisch ausgebaut und zu einem Plug-and-Play-CCTV-Ansatz umgebaut – inklusive semi-fester Installation, online-gestützter Planung und aktivem Leitstellen-Betrieb. NSTR.security ist dabei der nächste logische Schritt: Sicherheitstechnik, die online planbar ist, schnell steht und sich skalieren lässt – ohne Projektkomplexität, ohne monatelange Vorlaufzeiten. Die Einstiegshürde sinkt drastisch. Betreiber ohne eigene Spezialabteilung können professionell aufstellen – ab dem ersten Standort.

Belastbares Konzept

Disruptiv wird es dort, wo Komplexität verschwindet. NSTR.security macht genau das: Der Kunde wählt Areal, Risikoprofil und Schutzziel – und erhält ein belastbares Konzept. Kein Papierprozess, sondern ein digitaler Ablauf, der sich wiederholen und ausrollen lässt. Kombiniert mit KI-gestützter Detektion und der LivEye-Leitstelle, die nicht nur entgegennimmt, sondern aktiv interveniert.

Wo geht die Reise hin? Die entscheidende Frage der nächsten Jahre lautet: Wann versteht ein System wirklich, was es sieht? Nicht nur Bewegung erkennen – Szenen einordnen. Was passiert hier? Ist das normal oder ein Vorfall? Vision-Language-Modelle machen genau das möglich: Sie beschreiben keine Bilder, sie beschreiben Situationen – in Sprache, die Menschen sofort verstehen. Fehlalarme sinken, echte Vorfälle werden sofort erkannt, Leitstellen-Teams entscheiden schneller. Bei LivEye und NSTR.security ist das kein Zukunftsszenario – es ist die Richtung, in die wir aktiv entwickeln.

Physische und IT-Sicherheit verschmelzen

Gleichzeitig verschmelzen physische Sicherheit und IT-Sicherheit weiter. Kameras, Gateways und Leitstellen sind heute Netzwerkteilnehmer – und damit Angriffsfläche. Wer Videotechnik wie NSTR.security baut und betreibt, muss Härtung, Zugriffskontrolle, Updatefähigkeit und saubere Protokollierung beherrschen. Datenschutz ist dabei keine Bremse – er ist die Eintrittskarte. DSGVO-Konformität ist bei LivEye und NSTR.security kein bloßes Versprechen, sondern Teil der Architektur.

Mein Blick nach vorn ist klar: Deutschland kann in der Sicherheitstechnik wieder Hersteller sein – nicht nur Integrator. LivEye und NSTR.security zeigen, dass das geht. Wer jetzt aufbaut, mit kontrollierbarer Technik, verlässlichen Prozessen und dem Anspruch, wirklich zu handeln statt nur aufzuzeichnen, der wird in zehn Jahren nicht mehr erklären müssen, warum das richtig war. GIT

LivEye
www.liveye.com

Michael Schreiber, Vice PresidentSales EMEA & APAC bei Hirsch Secure

Heiko Viehweger, Vertriebsleiter DACH bei Hirsch Secure

Tiefgreifender Umbruch

Ein Blick in die Zukunft der Sicherheit

Hirsch Secure – die neue DACH-Einheit der internationalen Hirsch-Gruppe – steht mitten im Zentrum eines tiefgreifenden Branchenumbruchs. Das sagen Michael Schreiber, Vice President Sales EMEA & APAC, und Heiko Viehweger, Vertriebsleiter DACH. Sie geben Auskunft darüber, was sich verändert hat – und wagen einen Blick in die Zukunft.

Aus Einzelunternehmen in den Bereichen Perimeterschutz, Zutrittskontrolle, Identitätsauthentifizierung und Videoanalyse entstand unter dem Dach der Firma Hirsch im Juni 2025 eine schlagkräftige neue Einheit. „Wir bündeln jetzt in der Hirsch Secure unsere Kompetenz für Hochsicherheits-Technologien in der DACH-Region“, erklärt Michael Schreiber. Heiko Viehweger ergänzt: „Wir waren bisher so etwas wie ein Hidden Champion der Branche“ – ein Umstand, der sich mit der neuen Marke und Struktur gezielt ändern soll.

Das KRITIS-Dachgesetz und vergleichbare europäische Regelwerke hätten den Handlungsdruck auf Betreiber kritischer Infrastrukturen erheblich erhöht. Wer Kraftwerke, Rechenzentren, Verkehrsinfrastrukturen oder Behörden betreibe, komme am Thema Perimeter- und Zutrittssicherheit nicht mehr vorbei. Dabei sei Sicherheit kein solitäres Thema mehr. Kunden verlangten die nahtlose Vernetzung von Perimeterschutz, Videoanalyse, Zutrittskontrolle und Cybersicherheit in einer einheitlichen Plattform.

Weniger Falschalarme, Sensorfusion, Cybersicherheit

Hirsch setzt auf Hardware in höchster Qualität und auf Software und Algorithmen, die Eindringlinge in jeder Umgebung erkennen und Falschalarme eliminieren. Erst dieser Fortschritt ermöglicht eine wirtschaftlich tragfähige Automatisierung ganzer Alarmketten.

Ein wichtiger Trend aus Sicht des Unternehmens ist die Sensorfusion. Kein einzelner Sensor sei allwissend. Die Erkenntnis, dass erst die intelligente Kombination verschiedener Detektionsmethoden – Zaundetektionssysteme, Infrarotlichtschranken, LiDAR, Radar, Mikrowellen- und PIR-Sensoren sowie Videoanalyse – ein wirklich robustes System ergibt, habe die Produktentwicklung und Projektplanung tiefgreifend verändert. Die eigene Produktbreite sei dabei ein entscheidender Wettbewerbsvorteil.

Die zunehmende Vernetzung physischer Sicherheitssysteme über IP-Netzwerke habe eine neue Angriffsfläche geschaffen. Hirsch Secure investiert deshalb gezielt in Cybersicherheit und wählt Hardwarepartner nach deren Cybersicherheitsstandards aus.

In einem Markt voller ähnlicher Versprechen gewinnen objektive Benchmarks an Bedeutung. Beim GIT System Test Perimeter Protection erzielte die Infrarotlichtschranke Maxiris Topbewertungen; bei einem Benchmark eines großen deutschen Integrators gehörte unsere Videoanalyse zu den Spitzenreitern. Langzeittests an Militärstandorten in Skandinavien und an hochsensiblen Standorten in der Schweiz runden das Bild ab.

Wo geht die Reise hin?

Klare Entscheidungen trotz komplexer Lage

Sicherheit ist heute komplexer denn je: fragmentierte Systeme, steigende Compliance-Anforderungen und veraltete Infrastruktur. Nur mit Erfahrung und optimal eingestellten Produkten lassen sich sicherheitskritische Lösungen umsetzen, ein Ansatz, der sich insbesondere bei KRI-

TIS-Betreibern, Flughäfen und anderen hochsicheren Bereichen durchsetzen wird.

■ **Vollautomatische Alarmketten**

Die Reduktion von Falschalarmen durch Sensorfusion und KI-Analytik schafft die Grundlage für vollständig automatisierte Alarmketten – von der Detektion über die visuelle Verifikation bis zur Steuerung von Interventionskräften. Reaktionszeiten werden drastisch sinken, der Bedarf an dauerhaft präsentem Sicherheitspersonal sich wandeln.

■ **Zero Trust auch im physischen Raum**

Das aus der IT bekannte Prinzip „kein Zugang ohne Verifikation“ greift auch in der physischen Welt. Biometrische Systeme, Hochsichere Authentifizierung und automatisch angepasste Zutrittsrechte – wie sie Hirsch Secure mit BSI- und ANSSI-zertifizierten Lösungen bereits anbietet – werden zum Standard.

■ **Offene Plattformen statt proprietärer Silos**

Die Zukunft gehört herstellerübergreifenden Sicherheitsplattformen. Kunden wollen bestehende Investitionen schützen und Systeme verschiedener Hersteller über eine einheitliche Oberfläche verwalten. Unsere Managementsysteme und die angebotenen SDKs für Drittintegration zeigen die strategische Richtung.

■ **Der One-Stop-Shop als Marktmodell**

Die wachsende Komplexität der Systeme und der regulatorische Druck sprechen für Anbieter, die das komplette Spektrum – von der Außengrenze bis zum Arbeitsplatz – aus einer Hand liefern können. „Wir sehen uns dabei als One-Stop-Shop“, bringt es Viehweger auf den Punkt. Und: „Nur gemeinsam lassen sich die wachsenden wirtschaftlichen und technologischen Anforderungen von Seiten der Kunden und durch den Gesetzgeber meistern.“ GIT

Hirsch Secure GmbH
www.hirschsecure.de

Im Namen von Klüh Security gratuliere ich der GIT SICHERHEIT herzlich zum 35-jährigen Jubiläum. Das Magazin begleitet die Branche seit vielen Jahren mit fachlicher Tiefe und Praxisnähe. Auch künftig wird es mit Sicherheit wichtige Impulse setzen.

Sven Horstmann,
Geschäftsführer
Klüh Security

35 JAHRE GIT SICHERHEIT

Vom Schlüsselbund zur digitalen Identität

Ein Trendbericht von Axel Schmidt, Geschäftsführer Salto Systems

Zutrittskontrolle hat sich vom Einzelsystem zur Grundlage moderner Gebäude- und Sicherheitsarchitekturen entwickelt. Virtuelle Vernetzung, Funkvernetzung und digitale Schlüssel ermöglichen heute eine Breite an Anwendungen, die früher nicht wirtschaftlich abbildbar war. Salto steht dabei für einen Weg, der Innovation an Sicherheit, Flexibilität, Effizienz und übergreifenden Systemfunktionen misst.

Als man vor gut zwei Jahrzehnten über Zutrittskontrolle sprach, ging es meist um Schlüssel und um wenige, verkabelte OnlineLeser an Außentüren. Salto ist in dieser Zeit mit dem Anspruch angetreten, mechanische Schlüssel in der Breite abzulösen und Zutritt als digitale Funktion für praktisch jede Tür zugänglich zu machen. Heute ist der Maßstab ein anderer, weil Zutritt nicht mehr nur Türöffnung bedeutet, sondern Teil von Betriebsabläufen, Sicherheitsarchitekturen und digitaler Steuerbarkeit geworden ist.

Geändertes Nutzerverhalten

Bei der Entwicklung dorthin haben sich geänderte Anforderungen und neue Technologien gegenseitig vorangetrieben. 2002 hat Salto mit dem Salto Virtual Network (SVN) einen Ansatz in den Markt gebracht, der virtuelle Vernetzung und verschlüsselte bidirektionale Datenübertragung in eine praxistaugliche, kabellose Architektur übersetzt hat. Damit wurde es möglich, deutlich mehr Zutrittspunkte wirtschaftlich zu digitalisieren und den Betrieb flexibler zu gestalten, ohne jede Tür aufwendig zu verkabeln.

Salto sieht in der nahtlosen Verzahnung von Identitätsmanagement und Zutrittskontrolle einen der wichtigsten Markttrends

2008 folgte mit Salto Wireless der nächste Schritt, weil Funkvernetzung wirtschaftlich und technisch praktikabel wurde. Heute steht dafür Salto Bluenet als kabellose EchtzeitFunkvernetzung, die gezielt an den Zutrittspunkten eingesetzt wird, an denen OnlineFunktionen und schnelle Reaktion benötigt werden. Seit 2015 kommt Mobile Access als logische Erweiterung hinzu, weil digitale Schlüssel Prozesse vereinfachen und Zutritt noch näher an den von Smartphones geprägten Alltag der Nutzer bringen. Diese Entwicklungen münden in einer enormen Flexibilität, weil Betreiber heute Sicherheitsniveau, Funktionsumfang und Betriebseffizienz je Zutrittspunkt maßgeschneidert ausbalancieren können.

Bedeutung von digitalen Identitäten wächst

Je digitaler Zutritt wird, desto stärker rückt die Identität in den Mittelpunkt. Entscheidend sind heute Rechte- und Rollenmodelle, die auch bei wechselnden Teams, Fremdpersonal und standortübergreifenden Strukturen stabil bleiben und zugleich im Audit belastbar sind. Genau hier setzt Identitätsmanagement an, weil es den gesamten Lebenszyklus von Identitäten

35 JAHRE GIT SICHERHEIT

Die GIT SICHERHEIT ist für mich wichtig, weil sie Technik von Wirkung trennt – und zeigt, was im Betrieb wirklich funktioniert. Die LivEye GmbH gemeinsam mit ihrer Tochtergesellschaft NSTR Security gratulieren der GIT SICHERHEIT herzlich zum 35-jährigen Jubiläum. Wir wünschen Ihr auch in Zukunft weiterhin viel Erfolg, Innovationskraft und ihre starke Position als Impulsgeber der Sicherheitswirtschaft.

Carsten Simons, CEO von LivEye

und Berechtigungen strukturiert, von der Anlage über Änderungen bis zum Entzug.

Salto treibt diese Entwicklung mit Salto IDM voran und verzahnt das Identitätsmanagement nahtlos mit seinen Zutrittsplattformen. Das Resultat sind konsistente und administrativ beherrschbare digitale Identitäten, die nicht nur für die Zutrittskontrolle, sondern zugleich für weitere Managementplattformen nutzbar sind und so eine übergreifende Daten- und Berechtigungsstruktur für Anwender gewährleisten.

Digitale und physische Sicherheit wachsen zusammen

Mit der zunehmenden Vernetzung wächst zugleich die Anforderung, Zutritt im Zusammenspiel von digitaler und physischer Sicherheit zu betrachten. Rahmenwerke wie NIS2 verschieben Verantwortung und Erwartungshaltung hin zu Risikomanagement, Meldefähigkeit und Governance, wodurch Sicherheitsarchitekturen ganzheitlicher geplant werden müssen. Damit rückt auch die physische Umgebung von ITSystemen stärker in den Fokus, weil Resilienz im Alltag und im Störfall nicht an Zuständigkeitsgrenzen haltmacht. Die Zutrittssysteme von Salto erfüllen diese hohen Anforderungen, weil sie schon immer als Sicherheitslösungen ausgelegt waren und nach dem Prinzip „Security by Design“ konzipiert wurden und werden.

Plattformlogik ersetzt Einzellösungen

Am Ende entscheidet bei der Zutrittskontrolle nicht nur die FeatureListe, sondern ebenso die Beherrschbarkeit und Sicherheit im Betrieb. Integrationen werden zum Standard, weil Gebäudeautomation, Sicherheitsgewerke und Unternehmensprozesse Daten austauschen müssen, um Abläufe zu automatisieren und Vorfälle sauber zu bearbeiten. Salto prägt diese Entwicklung, weil virtuelle Vernetzung, Funkvernetzung, Mobile Access und Identitätsmanagement nicht als Einzellösungen nebeneinanderstehen, sondern als Plattformlogik gedacht werden, die Anwendern Planungssicherheit und Effizienz im Betrieb gibt. GIT

Salto Systems
www.saltosystems.com

© Bilder: Salto Systems

CSO IM GESPRÄCH

„Richtlinien schrecken keinen Angreifer ab“

Telekom: Risikobasiert und wirkungsorientiert gegen Cyberkriminalität

Thomas Tschersich ist Globaler Chief Security Officer (CSO) der Deutschen Telekom und CEO der Telekom Security. Neben der Cybersicherheit verantwortet er die Cybersicherheit sowie die operativen Sicherheitsthemen des Konzerns. Daneben ist er u. a. Vorsitzender des Vorstands bei „Deutschland sicher im Netz“ und Mitglied im Cybersicherheitsrat. Im Gespräch mit GIT SICHERHEIT spricht Thomas Tschersich über aktuelle Herausforderungen seiner Arbeit und darüber, wie 2.500 Experten täglich 76 Millionen Angriffe erfolgreich abwehren. Wir befragten Dr. Tschersich außerdem zu „OnNet“, einem Dienst, der Sicherheit automatisch ins Netz integriert – sowie zu den Gefahren KI-gestützter Gegner, die Schwachstellen in Sekunden ausnutzen.

GIT SICHERHEIT: Herr Tschersich, das Thema Cybersecurity ist für die Deutsche Telekom naturgemäß ein zentrales Thema. Lassen Sie uns mit dem Organisatorischen anfangen. Wie ist die Cybersecurity innerhalb der Deutschen Telekom aufgestellt und organisiert?

Thomas Tschersich: Historisch kommen wir – wie viele Unternehmen – aus einer stark verteilten Struktur, was die Aufgabenteilung betrifft. Das Thema IT-Sicherheit lag bei der IT, davon getrennt die Netzwerksicherheit, die Unternehmenssicherheit oblag der Konzernsicherheit, etc. Das führt zu einem strukturellen Problem: Als Sicherheitsverantwortlicher sind Sie oft unter dem CIO aufgehängt, der in der Regel eine Kostensenkungsagenda verfolgt. In der Cybersecurity müssen Sie aber häufig investieren, also eher Kosten steigern. Das ist ein klassischer Zielkonflikt.

Wir haben deshalb schon vor rund 15 Jahren entschieden, diesen Konflikt aufzulösen und Sicherheit auf Augenhöhe mit CIO und CTO zu bringen. Ich bin als Global CSO direkt auf derselben Ebene angesiedelt. Wir berichten an denselben Vorstand. Das bedeutet: Ich kann nicht alles durchsetzen, was ich möchte – aber umgekehrt können CIO und CTO auch nichts gegen die Sicherheit durchsetzen. Es gibt einen Zwang zur Einigung, aber kein Abhängigkeitsverhältnis.

Zusätzlich haben wir die Verantwortung gebündelt: Cybersecurity sowie physische und personelle Sicherheit gehören zusammen. Denn Bedrohungen sind nicht nur digital. Ein Rechenzentrum, um ein einfaches Beispiel zu nennen, kann man auch physisch angreifen – etwa über die Kühlung.

Das wird in letzter Zeit ja immer stärker betont …

Thomas Tschersich: Ja. Man braucht einen ganzheitlichen Blick. Viele Unternehmen betreiben Sicherheit stark dokumentationsgetrieben. Es gibt Policies und Richtlinien. Aber kein Angreifer lässt sich von einer Richtlinie abschrecken. Wir verfolgen deshalb einen risikobasierten und wirkungsorientierten Ansatz. Das größte Risiko bekommt die meisten Ressourcen. Und wir setzen nur Maßnahmen um, die messbar die Sicherheit verbessern. Dokumentation ist notwendig, aber nicht ausreichend. Anstatt zum Beispiel jemanden zu fragen, ob ein System sicher konfiguriert ist, lassen wir das System selbst den Zustand melden. Wir wollen die Realität messen, nicht Selbstauskünfte.

Wie groß ist eigentlich Ihr Bereich innerhalb der Telekom?

Thomas Tschersich: Im Headquarter habe ich ein kleines Team von etwa 20 Personen. Insgesamt umfasst die Telekom Security rund 2.500 Mitarbeiter. Etwa 500 arbeiten für die interne Sicherheit des Konzerns, rund 2.000 für externe Kunden. Diese Trennung ist nicht strikt. Wir nutzen bewusst Synergien: Was wir im Konzern lernen, geben wir an Kunden weiter – und umgekehrt. Wir haben rund 700 Kunden im Bereich aktiver Cyberabwehr. Wenn bei einem etwas passiert, können wir daraus sofort lernen und die Schutzmechanismen für alle anpassen.

Welcher Art sind die externen Kunden, die Sie ansprechen?

Thomas Tschersich: Das reicht von großen Fluggesellschaften, Energieversorgern, Banken und anderen kritischen Infrastrukturen bis hin zu kleinen Mittelständlern. Zu unseren Kunden zählen zum Beispiel auch sehr erfolgreiche Mittelständler im Automotive-Sektor, Weltmarktführer auf

verschiedensten Gebieten, etc. Auch im Privatkundenbereich sind wir tätig, wobei es dort vor allem um den Schutz vor Schadsoftware-Schutz geht.

Lassen Sie uns etwas näher auf Ihr Security Operation Center und das spezialisierte Computer Emergency Response Team (CERT) werfen...

Thomas Tschersich: Das Security Operations Center ist unsere erste Verteidigungslinie. Dort überwachen wir Logdaten und Systeme, um Angriffe zu erkennen. Wir sprechen von mehreren Hundert Terabyte Daten pro Tag, die gegen etwa 2,5 Millionen Angriffsindikatoren – sogenannte Indicators of Compromise (IOCs) – geprüft werden. Das ist ohne Automatisierung nicht mehr machbar. Deshalb setzen wir stark auf maschinelles Lernen und Automatisierung. Etwa 80 Prozent der Tätigkeiten laufen automatisiert, nur 20 Prozent erfordern menschliches Eingreifen.

Wird ein Angriff bestätigt, dann übernimmt das Computer Emergency Response Team. Das ist gewissermaßen die Feuerwehr. Zunächst wird der Angriff eingegrenzt – etwa indem man verhindert, dass sich ein Angreifer im Netzwerk weiter ausbreitet. Danach wird er entfernt. Zusätzlich verarbeitet das Team täglich eine große Zahl von Schwachstellenmeldungen von Herstellern. Diese werden bewertet und an die zuständigen Stellen weitergegeben, damit entsprechende Maßnahmen ergriffen werden.

Es ist die Rede von zehntausenden Angriffen pro Minute auf Telekom-Systeme. Wie kommen Sie da noch hinterher?

Thomas Tschersich: Wir betreiben weltweit sogenannte Honeypots. Das sind Systeme, die bewusst wie verwundbare echte Systeme aussehen. Angreifer stoßen darauf und versuchen, diese zu kompromittieren. In Wirklichkeit handelt es sich um Sensoren. Dank ihrer können wir beobachten, welche Methoden und Werkzeuge eingesetzt werden. Ein Großteil dieser Angriffe läuft automatisiert ab. Wir haben weltweit über 2.000 solcher Sensoren im Einsatz, auch durch Kooperationen mit Forschungseinrichtungen. Dadurch erhalten wir ein sehr gutes Bild der aktuellen Bedrohungslage.

Wir bilden die Vorgänge auf einer eigenen Website öffentlich verfügbar ab – dort kann man zum Beispiel gerade sehen, dass es in den letzten 60 Sekunden 51.005 Angriffe gegen diese Sensoren gab – innerhalb der letzten Stunde 3,3 Millionen. In den letzten 24 Stunden 76 Millionen. Das sind unvorstellbar hohe Zahlen.

Das können ja nicht alles ernst zu nehmende Angriffsversuche sein...?

Thomas Tschersich: Nein, aber es sind Vorbereitungshandlungen. Das können Sie sich so vorstellen: Wenn Sie jemanden sehen, der durch ein Hochhaus geht und an jeder Türklinke guckt, ob die Tür vielleicht offensteht und nicht abgeschlossen ist, ist das erst mal noch kein wirklicher Einbruch. Der Einbruch fängt erst dann an, wenn er eine offene Tür findet und dann auch durchgeht.

KI-gestützte Angriffe dürften das Spiel auf ein neues Level heben?

Thomas Tschersich: Zunächst einmal sehen wir aktuell eine massive Bewegung von organisierter Kriminalität in Richtung staatliche Akteure. Früher kam nach einem DDoS-Angriff eine E-Mail mit Lösegeldforderung. Jetzt passiert das Ganze ohne diese Lösegeldkomponente. Es kommt einfach nur noch der Angriff.

Die zweite Veränderung ist die KI-Geschwindigkeit. Wenn Microsoft ein Update für eine kritische Schwachstelle veröffentlicht, dauert es nur Minuten, bis jemand anfängt, das Internet abzusuchen nach genau dieser Schwachstelle. Früher hat das Monate gedauert. Mittlerweile sind das Minuten. Es gibt Angriffswerkzeuge, die Sie im Darknet nutzen können, die KI-getrieben sind. Sie müssen kein Angreifer-Know-how mehr haben, das macht das Werkzeug alles selber. Wir kennen Angriffe, bei denen es nur 70 Sekunden gedauert hat vom ersten Versuch bis zum erfolgreichen Eindringen ins System.

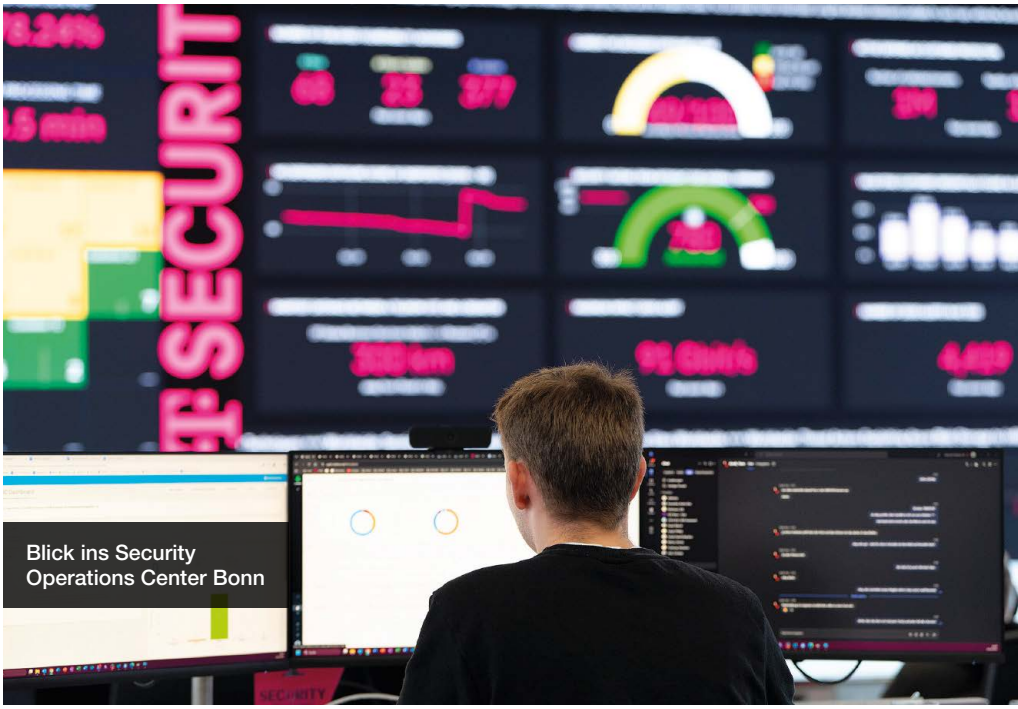
Herr Tschersich, die Geschäftsbereiche der Telekom sind ja sehr vielfältig. Und überall spielen Sicherheitsanforderungen eine Rolle – von Produktentwicklung, Netzbetrieb bis Kundenservice, sogar Magenta-TV. Wie lässt sich das Sicherheitsdenken in dieser komplexen Welt effektiv verankern?

Thomas Tschersich: Wir betrachten drei Ebenen: technische Systeme, physische Objekte und Geschäftsprozesse. Technische Systeme müssen jederzeit im Zustand bekannt sein. Bei physischen Objekten geht es um Sabotage- oder Brandrisiken, bei Geschäftsprozessen um deren Verfügbarkeit. Dazu kommt indirekt der Faktor Mensch.

Organisatorisch haben wir klare Zuständigkeiten – fachlich und geografisch. Für jede Einheit gibt es Verantwortliche. Wichtig ist der Ansatz „Security by Design". Sicherheit wird von Anfang an mitgedacht. Wenn neue Technologien entstehen, sind wir von Beginn an dabei und gestalten mit. Zusätzlich gibt es vor Inbetriebnahme eine Sicherheitsabnahme. Wir priorisieren nach Risiko: Hohe Risiken erfordern individuelle Prüfungen, bei Standardfällen greifen wir auf bewährte Blaupausen zurück.

Der entscheidende Punkt ist dabei: Wir lernen kontinuierlich. Jeder Angriff – egal ob im eigenen Konzern oder bei Kunden – verbessert unser Verständnis und unsere Schutzmechanismen. Dieses Lernen in Echtzeit ist ein zentraler Bestandteil unserer Sicherheitsstrategie.

Bitte umblättern ▶



Blick ins Security Operations Center Bonn

Die weiter zunehmende Vernetzung von Mobilfunk, Cloud, IoT und Festnetz sind sicher zusätzlich herausfordernd für Ihre Sicherheitsarchitektur...

Thomas Tschersich: Je mehr Geräte vernetzt sind, desto mehr sind potenziell angreifbar. Wir müssen das Maß an Sicherheitsmaßnahmen auf dieses Wachstum anpassen. Wenn Sie uns in unserem Cyber Defence Center besuchen, so treffen sie dort auf lauter smarte Mitarbeiter. Statt Angriffe jedes Mal individuell zu bearbeiten, tun sie das genau einmal und automatisieren diese Schritte dann anschließend. Nicht aus Faulheit, sondern im Hinblick auf Effizienz und die wachsende Zahl an Angriffen.

Mit „Security OnNet" bieten Sie Schutz direkt aus dem Netz heraus. Das ist ja besonders für kleinere Unternehmen interessant?

Thomas Tschersich: Wenn Sie heute Sicherheit machen, ist es oft damit verbunden, dass Sie dem Kunden sagen: „Du musst auf deinem Endgerät etwas installieren, konfigurieren, regelmäßig aktualisieren." Da sind ganz viele Menschen abgehängt, weil sie nicht die Fachexpertise haben. Wir haben uns deshalb die Frage vorgelegt, warum kommt die Sicherheit nicht schon ganz automatisch aus dem Netz, ohne dass man etwas tun muss? Das bietet natürlich kein 100-Prozent-Sicherheitsniveau, aber man kommt schon sehr weit. Die Idee ist, die ersten 80 Prozent schon mal zu lösen für den Kunden, ohne dass er irgendetwas tun muss. Es kommt einfach als Teil des Mobilfunktarifes im Geschäftskundenumfeld mit. Der Kunde kann es ein- oder ausschalten – ohne, dass eine Detailkonfiguration nötig ist.

Sie berichten von der Abwehr von hunderttausenden Angriffen und der Blockierung von über einer Million betrügerischer Websites. Hier ist vermutlich kein Ende abzusehen...?

Thomas Tschersich: Immer dann, wenn wir irgendetwas blockieren, geht der Angreifer wieder einen Schritt weiter. Häufig funktioniert das so: Sie bekommen eine SMS – ein Paket für Sie, DHL, DPD. Da ist ein Link drauf. Wenn Sie draufklicken, sollen Sie sich eine App installieren – und wenn das geschehen ist, übernimmt der Angreifer Kontrolle über Ihr Gerät. Wir können diesen Zustellversuch zwar technisch erkennen und verhindern – wir dürfen das aber nicht, weil das Telekommunikationsgeheimnis dagegenspricht. Aber: Wenn Sie auf diesen Link klicken, baut Ihr Handy einen Zugang zu einer Internetseite auf. Wenn wir die als bekannt schädlich kennen, dürfen wir sie sperren und das machen wir auch.

Sie haben gerade schon einen regulatorischen Aspekt angesprochen. Wie sehen Sie eigentlich insgesamt die normative Lage zu diesem Themenkomplex?

Thomas Tschersich: Wenn Sie kritischer Infrastrukturbetreiber sind, müssen Sie heute – je nach Fall – alleine in Deutschland bei einem Vorfall an fünf Behörden melden: BaFin, Datenschutzbeauftragten, Bundesnetzagentur, BSI und BBK. Fünf Behörden, fünf komplett unterschiedliche Meldewege, fünf komplett unterschiedliche Formblätter, aber 95 Prozent deckungsgleicher Inhalt. Aus Sicht des Betreibers bedeutet das: Ich beschäftige wertvolle Mitarbeiter, die eigentlich mein Problem lösen sollten, erst mal damit, dass sie irgendwelche Meldungen abgeben. Das löst aber noch kein Problem. Erst wenn ich fertig bin mit dem Meldungen-Abgeben, kann ich anfangen, das Problem zu lösen. Das ist ein gefährlicher Pfad, auf dem wir unterwegs sind. Solange wir noch melden, um uns rechtlich abzusichern, hat der Angreifer freie Bahn. Wir sehen natürlich das legitime Interesse der Behörden. Aber so, wie die Prozesse gestaltet sind, tragen sie nicht zu mehr Sicherheit bei.

Ist es überhaupt möglich, der Bedrohungslage hinterherzukommen?

Thomas Tschersich: Es gibt keine Befreiungsschläge in diesem Bereich – aber man kann schon etwas tun. Sie müssen jedes System rund die Uhr zu jeder beliebigen Zeit gegen alle denkbaren Angriffe sichern. Der Angreifer ist im Vorteil, denn er kann sich das Ziel aussuchen. Er bestimmt den Angriff und den Zeitpunkt. Sie haben nie Waffengleichheit. Aber man kann dranbleiben. GIT

Deutsche Telekom AG
www.telekom.de

VISION

Innerhalb der nächsten zehn Jahre werden wir im Bereich Sicherheit in der Lage sein, einen nahezu autonomen Betrieb sowie eine umfassende Vernetzung aller sicherheitsrelevanten Systeme zu realisieren, um komplexe Lagen schneller und besser zu bewerten und wirksamer zu beherrschen.

Dipl.-Ing Jörg Marks, 1. Vorsitzender des Verbands für Sicherheitstechnik e.V., VfS

35 JAHRE GIT SICHERHEIT

35 JAHRE GIT SICHERHEIT

VISION

Innerhalb der nächsten zehn Jahre werden wir in der Lage sein, die Herausforderungen der Branche weiterhin zu meistern und zukunftsfähige Entscheidungen zu treffen – mit unternehmerischem Mut, einem starken Team und starken Partnern.

Günther Rossdeutscher, Geschäftsführender Gesellschafter, Asecos GmbH

Barox und Gallagher Security erweitern Netzwerkdiagnose

Die Barox Kommunikation AG gibt eine neue Integration mit der Site-Management-Plattform Command Centre von Gallagher Security bekannt. Die Lösung ermöglicht eine umfassende Überwachung und Diagnose von Zutrittskontrollsystemen, Sicherheitsnetzwerken und der zugrunde liegenden Netzwerkinfrastruktur. Command Centre wird weltweit in Behördenumgebungen sowie in kritischen Infrastrukturen eingesetzt und bietet Funktionen wie intelligente Zutrittskontrolle, Standortmanagement, Reporting und Echtzeit-Alarmmanagement. Durch die neue Integration können Anwender Barox-Netzwerkswitches und angeschlossene Geräte direkt über die Plattform überwachen und steuern. Dies erhöht Transparenz, Ausfallsicherheit und Effizienz im Betrieb von Sicherheitsnetzwerken. Die Integration greift tief in die Layer-3-Managed-Switch-Technologie von Barox ein und ermöglicht umfangreiche Netzwerkmanagementfunktionen direkt in Command Centre.

www.barox.de

TeleTrusT-Stellungnahme zum BMI-Referentenentwurf zur Cyberresilienz-Verordnung

Der Bundesverband IT-Sicherheit (TeleTrusT) nimmt Stellung zum BMI-Referentenentwurf für ein Durchführungsgesetz zur EU-Cyberresilienz-Verordnung. Der Referentenentwurf greift die durch den CRA erforderlichen nationalen Regelungen zwar im Grundsatz auf, bleibt in seiner derzeitigen Fassung jedoch in zentralen Punkten hinter den praktischen und rechtlichen Anforderungen zurück.

Die vorgesehene Aufgabenbündelung beim BSI ist nur dann tragfähig, wenn dessen personelle, technische und organisatorische Ausstattung verlässlich und dauerhaft abgesichert wird. Daran fehlt es bislang, so der Verband.

Besonders kritisch sind die zu weit gefasste Ausnahmeregelung für die Notifizierung von Konformitätsbewertungsstellen ohne Akkreditierung, die unzureichend konkretisierten Unterstützungsleistungen für Wirtschaftsakteure sowie die unklare Ausgestaltung des Reallabors für Cyberresilienz. In allen drei Bereichen besteht die Gefahr, dass der Entwurf formale Strukturen schafft, ohne deren praktische Wirksamkeit belastbar sicherzustellen.

TeleTrusT hält daher eine deutliche Nachschärfung des Entwurfs für erforderlich. Notwendig sind insbesondere eine verlässliche Finanzierung und Ausstattung des BSI und der DAkkS, enge und klare Voraussetzungen für Ausnahmen von der akkreditierungsbasierten Notifizierung, ein substanziell ausgebautes und praxisnahes Unterstützungskonzept für Unternehmen sowie transparente und nachvollziehbare Regelungen zum Reallabor.

www.teletrust.de

STUDIE

Cybersicherheit mit Dividende

Studie zum Nutzen besserer Integration von Sicherheitsmaßnahmen

Eine weltweite Umfrage von IBM, IBV (Institute for Business Value) und Palo Alto Networks zeigt, dass „75 % der befragten Organisationen, die einen konsolidierten Sicherheitsansatz verfolgen, der Meinung sind, dass eine bessere Integration von Sicherheit, Hybrid-Cloud, KI und anderen Technologieplattformen entscheidend ist“.

Für die Studie „Capturing the cybersecurity dividend“ wurden von Juli bis September 2024 insgesamt 1.000 Führungskräfte aus 21 Branchen und 18 Ländern befragt. Sie ergab, dass die befragten Organisationen mit Herausforderungen hinsichtlich der Komplexität der Sicherheit konfrontiert sind, da sie durchschnittlich 83 verschiedene Sicherheitslösungen von 29 Anbietern unter einen Hut bringen müssen. Sieben von zehn befragten Unternehmen mit einem hohen Grad an Sicherheitsplattformen berichten, dass ihre Investitionen in die Cybersicherheit zu Geschäftsergebnissen wie Betriebseffizienz und Umsatzsteigerung beigetragen haben.

Mehr als die Hälfte (52 %) der befragten Führungskräfte gab an, dass die Fragmentierung der Sicherheitslösungen ihre Fähigkeit zum Umgang mit Cyberbedrohungen einschränkt. Allerdings stimmen 75 % der Organisationen, die sich für eine Sicherheitsplattform entschieden haben, der Aussage zu, dass eine bessere Integration von Sicherheit, Hybrid Cloud, KI und anderen Technologieplattformen von entscheidender Bedeutung ist. Die Analyse, so die Studienherausgeber, legt nahe, dass der Trend, weitere Lösungen zur Bekämpfung sich entwickelnder Sicherheitsbedrohungen hinzuzufügen, zur Ineffizienz beiträgt. Dies wirke sich sowohl auf die Leistung als auch auf das Endergebnis aus. Die Umstellung auf einen plattformbasierten Sicherheitsansatz könne Unternehmen dabei helfen, Reaktionszeiten und Kosten zu reduzieren, ohne die Sicherheitseffizienz zu beeinträchtigen.

Beängstigende Komplexität

Eine zunehmende digitale Vernetzung vergrößere die Angriffsfläche und könne neue Schwachstellen in der Cybersicherheit schaffen. Cyberangriffe würden immer ausgefeilter und die Abwehr dagegen werde immer schwieriger. Gleichzeitig nutzten sowohl Verteidiger als auch Angreifer künstliche Intelligenz, was zu einem Wettlauf bei den Cybersicherheitsfähigkeiten führe.

Hier finden Sie die vollständige Studie:

„Capturing the cybersecurity dividend:
How security platforms generate business value
(Die Cybersicherheitsdividende nutzen:
Wie Sicherheitsplattformen geschäftlichen
Mehrwert generieren)“

Herzlichen Glückwunsch zum 35-jährigen Jubiläum!
Die Zusammenarbeit mit Ihnen ist für uns seit vielen Jahren eine feste Konstante. Jede und jeder Einzelne in Ihrem Team überzeugt nicht nur durch hohe fachliche Kompetenz, sondern vor allem durch ein herzliches Miteinander, Offenheit und großes Engagement. So ist dann auch jede Ausgabe der GIT Sicherheit informativ, inspirierend und immer am Puls der Zeit. Vielen Dank für Ihre Arbeit und alles Gute für die kommenden Jahre!

Claudia Lindner und Susanne Plank von PCS Systemtechnik mit Miryam Reubold von GIT SICHERHEIT (Mitte)

35 JAHRE GIT SICHERHEIT

Angesichts einer sich ständig weiterentwickelnden Bedrohungslandschaft gehen die befragten Führungskräfte davon aus, dass die Fragmentierung und Komplexität der Sicherheit ihre Unternehmen durchschnittlich 5 % ihres Jahresumsatzes kostet. Für ein Unternehmen mit einem Jahresumsatz von 20 Milliarden USD seien das insgesamt Kosten von 1 Milliarde USD. Zähle man die Kosten von Sicherheitsvorfällen, Produktivitätsverlusten, fehlgeschlagenen digitalen Transformationen, ins Stocken geratenen KI-Initiativen, verlorenem Kundenvertrauen und Reputationsschäden zusammen, komme man auf eine hohe Summe.

„Organisationen stehen weiterhin vor der Herausforderung, ihre Sicherheitsvorkehrungen zu aktualisieren, um neuen Bedrohungen zu begegnen, während sie gleichzeitig dazu gedrängt werden, die Komplexität zu reduzieren und die Kosten zu senken", sagt Mark Hughes, Global Managing Partner für Cybersecurity Services bei IBM. „Führungskräfte im Bereich Sicherheit müssen Innovationen ermöglichen, Assets schützen und aus ihren Investitionen in die Cybersicherheit einen Mehrwert schöpfen, um ihre Organisationen zum Erfolg zu führen und ihre Geschäftsziele zu fördern."

„Wir haben die positiven Auswirkungen eines plattformbasierten Sicherheitsansatzes und die Vorteile gesehen, die er Organisationen bietet. In der heutigen KI-gesteuerten Welt sind starke Partnerschaften wichtiger denn je", sagte Karim Temsamani, President, Next Generation Security, Palo Alto Networks.

Geschäftsverbesserung durch Plattformisierung

Untersuchungen zeigen, so die Studienherausgeber, dass in der heutigen Welt für wirksame Sicherheit eine Plattformisierung erforderlich ist. Durch die Konsolidierung mehrerer Tools auf einer einheitlichen Plattform werde nicht nur die Sicherheitslage verbessert, sondern Organisationen könnten auch einen fast viermal besseren Return-on-Investment (ROI) aus ihren Investitionen in die Cybersicherheit erzielen, was zu Umsatzsteigerung und Betriebseffizienz führe.

Wenn es um KI geht, könne ein Plattformansatz einem Unternehmen auch dabei helfen, Daten besser zu erfassen und zu analysieren, um umsetzbare Erkenntnisse zu gewinnen. 90 % der befragten Führungskräfte gehen davon aus, dass sie in den nächsten zwei Jahren mithilfe von KI skalieren, optimieren oder Innovationen einführen werden. Daher kann die Integration von KI in ihre Plattformen eine entscheidende Rolle bei der Verbesserung ihrer Sicherheitsvorkehrungen spielen. Beispiele hierfür sind die Beschleunigung der Einführung agentenbasierter KI für mehr Sicherheit und die Nutzung der Plattformisierung für kürzere Investitionszyklen; oder die Nutzung der Plattformisierung zur Schaffung der gemeinsamen Governance, die für die Bereitstellung der KI-Fähigkeiten erforderlich ist, die die Zukunft prägen.

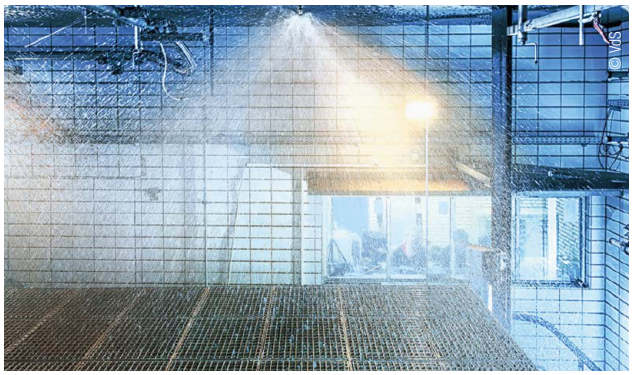
Durch die Einführung eines Plattformansatzes können Unternehmen Technologien aufeinander abstimmen, Innovationen vorantreiben und Sicherheit als zentrale Geschäftsanforderung priorisieren. GIT

IBM
www.ibm.com

Palo Alto Networks
www.paloaltonetworks.com

VdS-Innovationsanerkennung für Löschanlagen-Testsystem

Automatische Löschanlagen sind komplexe Systeme, die nur dann zuverlässig funktionieren, wenn sie regelmäßig gewartet und überwacht werden. Für durchgängiges Monitoring hat Minimax ein direkt in bestehende Sprinkleranlagen integrierbares Testsystem aus Controller vor Ort, Gateway und Cloud entwickelt. Die Verlässlichkeit dieser Erfindung wurde jetzt mit der VdS-Anerkennung nachgewiesen. „Wir freuen uns sehr, dass die Wirksamkeit und Zuverlässigkeit unseres ‚Automatic Inspection and Testing System' nun durch VdS eindeutig belegt ist", betont Jan Witte, Director Product Compliance der Minimax Viking Products Group GmbH. „AITS überwacht, prüft und dokumentiert präzise die sicherheitsrelevanten Funktionen der Technik. Selbst die geforderten wöchentlichen Alarmproben, Pumpenstarts oder Dichtigkeitsprüfungen erledigen unsere Anlagen ab sofort selbst." **www.vds.de**



Instandhaltung erleichtern, Störungen frühzeitig erkennen, Wartungsaufwand reduzieren und Fachpersonal entlasten: AITS von Minimax hat seine Leistungsstärke in umfassenden VdS-Innovationsprüfungen belegt

Vorbeugender Brandschutz auf der Interschutz

Der wirksamste Schutz gegen Brände ist, sie gar nicht erst entstehen zu lassen. Vorbeugender Brandschutz hilft, das Risiko so gering wie möglich zu halten. In einem eigenen Ausstellungsschwerpunkt zeigen Aussteller dazu auf der Interschutz 2026 in Hannover ihre Technologien und innovativen Konzepte. Angesichts allgemein wachsender Anforderungen an das Thema Brandschutz – in Deutschland, Europa und auch weltweit – ist auch die Bandbreite an Produkten und Dienstleistungen der ausstellenden Unternehmen auf der Interschutz gewachsen. Der vorbeugende Brandschutz muss sich ständig anpassen – an moderne Bauweisen, an neue Vorschriften, an größere und hoch komplexe Gebäude und an eine dichtere Bebauung, besonders in Metropolen.

In den Hallen 12 und 13 stellen auch die Anbieter von Löschtechnik und Löschmitteln aus, genauso wie Aussteller aus dem Bereich Bauwesen und technischer Brand- und Gebäudeschutz. **www.messe.de**

GIT SICHERHEIT

INNENTITEL – BRANDSCHUTZ

BRANDMELDEANLAGEN

Who Guards the Guardian

Wie Feuerwehrgerätehäuser technisch wirksam abgesichert werden können

Feuerwehrgerätehäuser sind zentrale Elemente der Gefahrenabwehr und Teil der kritischen Infrastruktur, jedoch häufig unzureichend geschützt. Moderne Einsatzfahrzeuge, IT- und Funktechnik sowie Ladeinfrastruktur erhöhen das Brandrisiko deutlich. Elektrotechnische Defekte und Akkubrände zählen zu den häufigsten Ursachen. Wird ein Ereignis erst spät erkannt, breiten sich Brände aufgrund offener Hallenstrukturen und hoher Brandlasten oft sehr schnell aus – mit gravierenden Folgen für Gebäude, Fahrzeuge und Einsatzbereitschaft.

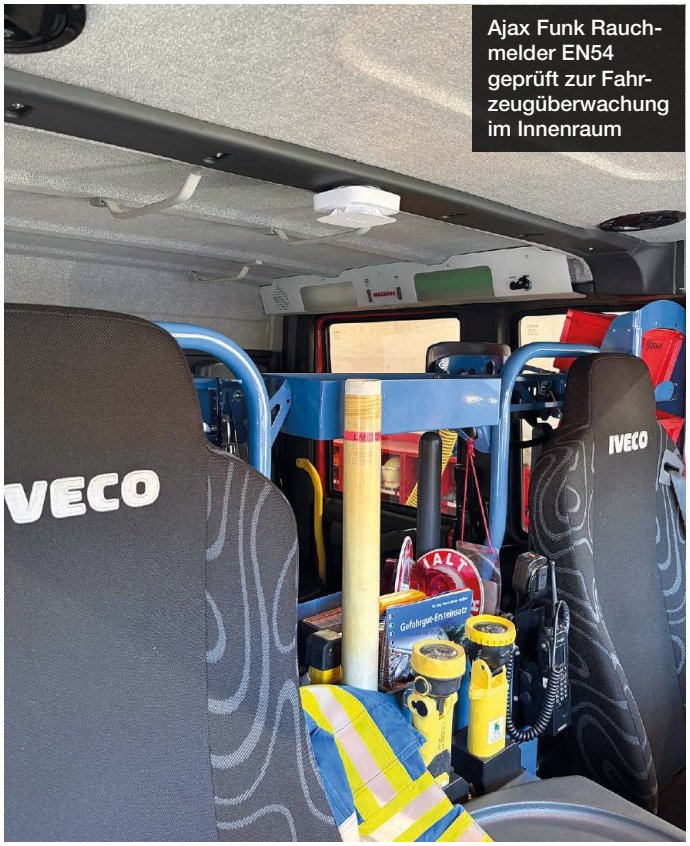
Baurechtlich gelten Feuerwehrgerätehäuser in vielen Bundesländern als ungeregelte Sonderbauten. Verbindliche Vorgaben zur automatischen Brandfrüherkennung fehlen häufig oder liegen im Ermessen der Kommunen. In der Praxis führt dies dazu, dass entweder gar keine automatischen Meldesysteme installiert werden oder auf Lösungen zurückgegriffen wird, die ursprünglich für den Wohnbereich konzipiert sind. Fachverbände wie der BHE weisen jedoch ausdrücklich darauf hin, dass Rauchwarnmelder aus dem Smart Home Umfeld den Anforderungen an Verfügbarkeit, Überwachung und Störsicherheit in sicherheitskritischen Umgebungen nicht gerecht werden. Empfohlen werden stattdessen normenkonforme Systeme nach EN 54, wie sie auch in professionellen Brandmelde und Brandwarnanlagen eingesetzt werden.

Steigende Risiken durch Technik und Ladeprozesse

Die technische Ausstattung moderner Feuerwehrhäuser hat sich in den vergangenen Jahren stark verändert. Akkubetriebene Werkzeuge, persönliche Schutzausrüstung mit Ladeeinheiten sowie elektrisch unterstützte Fahrzeuge befinden sich vielfach im Dauerladebetrieb – in den Fahrzeugen ebenso wie in den Hallen. Einsatzberichte zeigen, dass Brände häufig im oder am Fahrzeug entstehen. Wird ein solcher Brand nicht frühzeitig erkannt, bleibt oft kaum Zeit für Gegenmaßnahmen. Der wirtschaftliche Schaden übersteigt dabei regelmäßig die Kosten präventiver Schutzmaßnahmen um ein Vielfaches.

Frühzeitige Detektion und Alarmverifikation

Vor diesem Hintergrund gewinnen Schutzkonzepte an Bedeutung, die eine frühe Branderkennung mit einer zuverlässigen Alarmierung verbinden und zugleich Fehlalarme minimieren. Moderne Gefahrenmeldekonzepte kombinieren unterschiedliche Sensoriken – etwa Rauch , Temperatur



Ajax Funk Rauchmelder EN54 geprüft zur Fahrzeugüberwachung im Innenraum

Ajax Funk Rauchmelder mit integrierter Sirene und EN54 Zulassung zur Überwachung der Fahrzeughall

oder Multisensorik – und lassen sich durch Video oder Thermalsensoren ergänzen. Entscheidend ist dabei die Möglichkeit der Alarmverifikation: Verantwortliche erhalten im Ereignisfall nicht nur eine Meldung, sondern können die Lage unmittelbar bewerten und gezielt reagieren, etwa durch das Abschalten von Ladesystemen oder die sofortige Alarmierung der Einsatzkräfte.

Fällt ein Feuerwehrstandort infolge eines Brandes aus, müssen benachbarte Wehren einspringen – oft über lange Zeiträume. Der Wiederaufbau von Gebäuden und die Ersatzbeschaffung von Fahrzeugen sind kosten und zeitintensiv. Gleichzeitig leiden Ausbildung, Wartung und Einsatzvorbereitung. Fachgremien und Landesfeuerwehrverbände fordern daher, den Eigenschutz systematischer zu betrachten: durch individuelle Gefährdungsanalysen, normenkonforme Technik und klar definierte Alarm und Zuständigkeitsstrukturen.

Lösungsansätze aus der Praxis: EPS als Systemintegrator

Wirksam werden technische Schutzmaßnahmen nur dann, wenn sie an die baulichen, organisatorischen und betrieblichen Rahmenbedingungen des jeweiligen Feuerwehrhauses angepasst sind. Hier setzt EPS Vertiebs GmbH als Systemanbieter und deren Kunden und Integratoren an. Der Ansatz besteht nicht in der Bereitstellung einzelner Komponenten, sondern in der Integration unterschiedlicher Funktionen zu einem abgestimmten Gesamtkonzept. Ausgangspunkt ist stets eine Gefährdungsanalyse, aus der sich ableiten lässt, welche Sensorik, Alarmierungswege und organisatorischen Abläufe erforderlich sind.

Als technologische Basis kommen bei EPS die neu entwickelte, EN54 zugelassene Funk Brandwarnanlagen von Ajax zum Einsatz. Dieses System ist sowohl als EN54 konforme Brandwarnanlage und gleichzeitig auch als EN 50131- Grad 2 Gefahrenmel-

Die Funk Brandwarnanlage Ajax EN-54 Fire HUB ist die Zentrale Steuereinheit für die Überwachung von Feuerwehrgerätehäuser

desysteme zugelassen. Diese ermöglichen es, Rauch und Temperatursensoren, Bewegungsmelder, Wassermelder, Türkontakte und Videoüberwachung in einem gesamtheitlichen System zu vereinen. Charakteristisch ist die permanente Überwachung aller Komponenten: Energiezustände, Funkverbindungen und Funktionsfähigkeit werden kontinuierlich kontrolliert, Störungen oder Manipulationen frühzeitig gemeldet.

Aus der Praxis zeigt sich, dass sich für Feuerwehrgerätehäuser insbesondere solche Ajax Komponenten eignen, die eine frühzeitige Detektion ermöglichen, dauerhaft überwacht werden und sich flexibel an unterschiedliche Gebäudestrukturen anpassen lassen. EPS setzt dabei auf eine Kombination aus Brandmeldetechnik, Einbruchmeldetechnik und Videoüberwachung, die je nach Gefährdungslage modular zusammengestellt wird.

Im Zentrum stehen funkbasierte Rauchmelder wie der Ajax EN 54 FireProtect, die Rauch und Temperaturveränderungen erfassen und kontinuierlich ihren eigenen Betriebszustand überwachen. Durch die permanente Statusmeldung lassen sich Ausfälle, Verschmutzungen oder Energieprobleme frühzeitig erkennen – ein wesentlicher Unterschied zu einfachen Rauchwarnmeldern nach der Norm EN14604. Zur Absicherung der Feuerwehrgerätehäuser gegen Einbruch und Vandalismus kommen ergänzend Sensoren zur Überwachung von Räumen, Türen, Rolltoren und Zugängen zum Einsatz, etwa DoorProtect Plus oder Bewegungsmelder mit Fotoverifikation MotionProtect.

Herzstück des Systems ist die Ajax Zentrale (Hub), über die alle Komponenten zusammengeführt werden. Sie übernimmt die permanente Überwachung der Funkverbindungen, die Auswertung der Sensordaten sowie die Alarmweiterleitung an definierte Personengruppen. Alarmierungen können parallel über mehrere Kanäle erfolgen, etwa per NSL Aufschaltung, App, Push Nachricht oder akustische Signalgeber wie Ajax Sirenen. Es besteht auch die Möglichkeit das Ajax Sicherheitssystem an Alarmierungssystem der Feuerwehren direkt zu übertragen.

Mehrwert für Feuerwehren

Ein wesentlicher Vorteil des Ajax Sicherheitskonzeptes für Feuerwehren und Feuerwehrgerätehäuser liegt in der Modularität auf Funkbasis und der vollumfänglichen Normenkonformität nach der EN Norm für Brandmeldeanlagen (EN 54) und der EN Norm für Einbruchmeldetechnik (EN 50131 – Grad 2). Schutzkonzepte lassen sich schrittweise aufbauen und an veränderte Anforderungen anpassen – etwa bei neuen Fahrzeugen, zusätzlicher Ladeinfrastruktur oder baulichen Erweiterungen. Für Bestandsgebäude bedeutet dies, dass der Eigenschutz ohne tiefgreifende Eingriffe realisiert und bei Bedarf erweitert werden kann. GIT

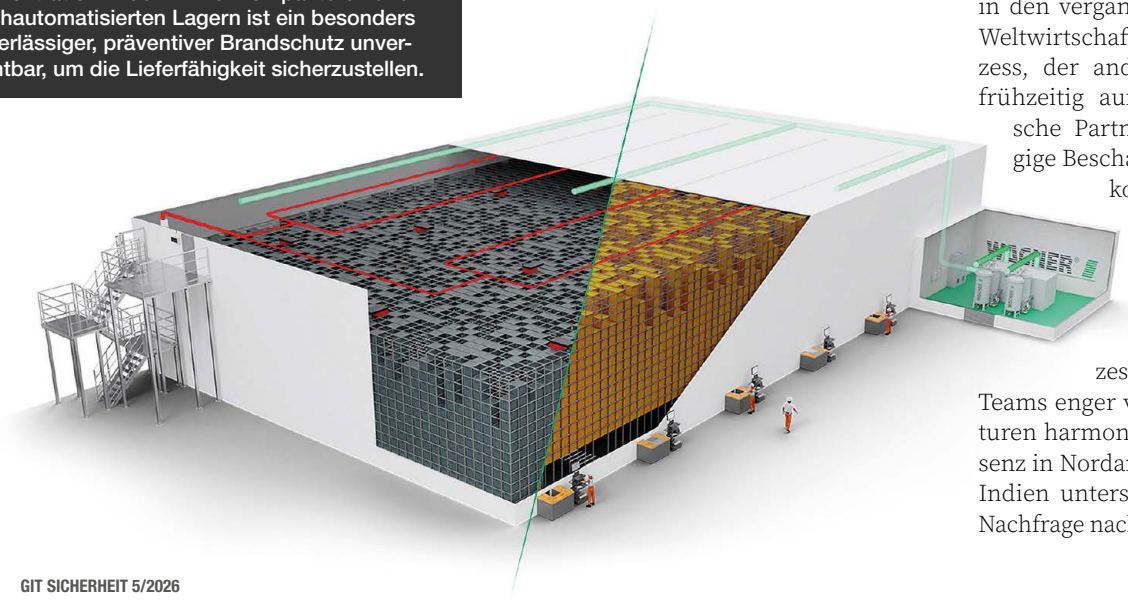
EPS Vertriebs GmbH
www.eps-vertrieb.de

Ein dynamischer Markt

Trendbericht von Steffen Springer, Geschäftsführer der Wagner Group

Die Sicherheitsanforderungen steigen in vielen Branchen seit Jahren deutlich an. Dies prägt technologische Entwicklungen ebenso wie Investitionsentscheidungen. Besonders in der Logistik verschärfen automatisierte Prozesse sowie eine immer kompaktere Lagerung mit einhergehender Wertekonzentrationen das Brandrisiko. Betreiber benötigen daher Lösungen, die Brände frühestmöglich erkennen und idealerweise präventiv vermeiden, da ein Brand in hochautomatisierten Strukturen oft zum Vollbrand und der vollständigen Zerstörung von Ausrüstung und Lagergut führt – mit entsprechenden Folgen für Betrieb und Umwelt.

Auch im Rechenzentrumsumfeld wächst der Druck: Die Hochverfügbarkeit von Daten ist geschäftskritisch und erfordert zuverlässige, integrierte Brandschutzsysteme, während die Zahl der zentralen und dezentralen Rechenzentren weltweit rasant zunimmt. Parallel dazu ist der Schutz kultureller Einrichtungen stärker in den Fokus gerückt, nachdem mehrere Vorfälle die Verletzlichkeit von Museen und Archiven mit ihren einzigartigen Beständen aufgezeigt haben. Weitere Impulse kommen zunehmend aus dem Verteidigungssektor, da die geopolitische Lage einen steigenden Bedarf an robusten, ausfallsicheren Schutzlösungen für derartige Logistikzentren erzeugt. Dieses Anwendungsfeld rückt zunehmend in den Fokus.



Für die moderne Intralogistik mit hoher Wertekonzentration in den immer kompakteren und hochautomatisierten Lagern ist ein besonders zuverlässiger, präventiver Brandschutz unverzichtbar, um die Lieferfähigkeit sicherzustellen.

Optimierung und Lieferketten

Vor diesem Gesamtbild gewinnen technologiespezifische Weiterentwicklungen an Bedeutung. Wagner hat seine Systeme gezielt hinsichtlich Sensitivität, Ausfallsicherheit und Anwendungsflexibilität optimiert. Damit kann das Unternehmen gezielt auf unterschiedliche Branchenanforderungen reagieren und selbst komplexe Anwendungen zuverlässig absichern.

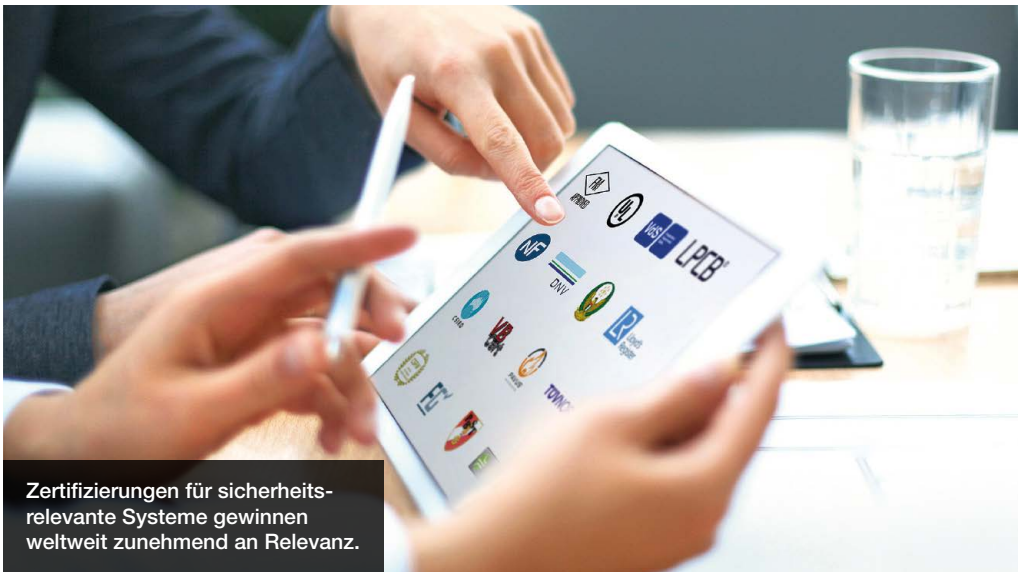
Gleichzeitig haben volatile Lieferketten in den vergangenen Jahren die gesamte Weltwirtschaft herausgefordert. Ein Prozess, der andauert. Unternehmen, die frühzeitig auf Diversifikation, strategische Partnerschaften und unabhängige Beschaffungswege gesetzt haben, konnten negative Auswirkungen minimieren und Lieferfähigkeit sichern. Um diesen Marktveränderungen gerecht zu werden, hat Wagner u. a. digitale Prozesse optimiert, internationale Teams enger vernetzt und globale Strukturen harmonisiert. Der Ausbau der Präsenz in Nordamerika, der Golfregion und Indien unterstützt zudem die steigende Nachfrage nach modernen, ganzheitlichen

Brandschutzlösungen in dynamisch wachsenden Märkten.

Technische Entwicklung

Besonders prägend waren technologische Veränderungen. Automatisierte Lager, steigende Energiedichten und boomende Anwendungen neuer Technologien wie Lithium-Ionen-Batterien kombiniert mit Schutzbedürfnissen bezüglich der Erhaltung der Lieferfähigkeit, der Betriebsbereitschaft und von Resilienz, bringen konventionelle Brandschutzlösung unter Umständen an den Rand der Leistungsfähigkeit. Wagner hat daher gezielt in Weiterentwicklungen investiert – etwa in sensitivere, besonders schnell ansprechende Branddetektion, KI-gestützte Datenanalysen für ein professionelles Systemmonitoring sowie digitale Services für eine vorausschauende Wartung.

Auch der steigende Bedarf an nachhaltigen Lösungen wirkt sich auf Markt und Branche aus. Energieeffizienz ist bei Wagner von jeher ein zentraler Aspekt; modulare Ansätze verhindern den Einsatz überdimensionierter Systeme. Das gilt gleichermaßen für kompakte Brandschutzlösungen im Schienenverkehr wie für Sauerstoffreduzierungssysteme zur Brandvermeidung. Seit 2025 ergänzt OxyReduct FLine das Portfolio: Das System verbindet wirtschaftlichen und nachhaltigen Brandschutz mit CO_2neutraler, autarker Energieerzeugung auf Basis innovativer Brennstoffzellentechnik. In Kombination mit weiteren OxyReductSystemen entsteht ein flexibel skalierbares, hybrides Schutzkonzept, das auch große Bereiche in Lager- und Logistikumgebungen zuverlässig schützt.



Zertifizierungen für sicherheitsrelevante Systeme gewinnen weltweit zunehmend an Relevanz.

Rolle der Versicherungen

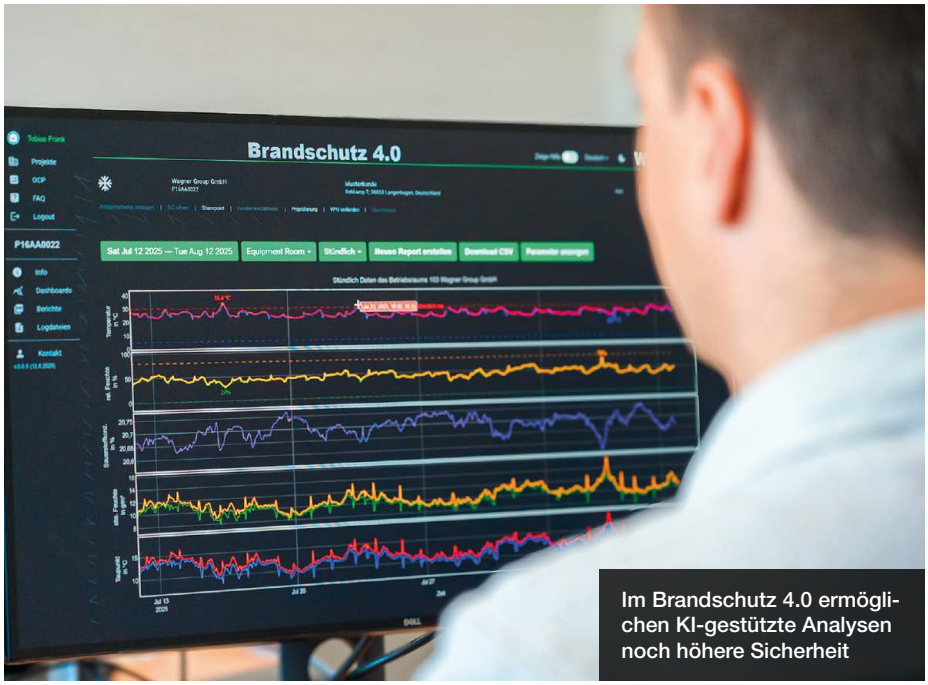
Die stärkere Berücksichtigung von Resilienz in der Risikobewertung rückt die Rolle von Versicherungen in den Fokus. Vor diesem Hintergrund war für Wagner die FMZulassung für das Sauerstoffreduzierungssystem Oxyreduct ein wichtiger Meilenstein. Die Zertifizierung gilt international als verlässlicher Gradmesser für die Sicherheit und Zuverlässigkeit von Systemen und stärkt so die Position von Wagner und erweitert die internationalen Einsatzmöglichkeiten von Oxyreduct, insbesondere in Hochregal- und Tiefkühllagern sowie in Rechenzentren.

Diese Meilensteine der Entwicklung wurden vorausschauend als Reaktion auf veränderte Marktbedingungen angestoßen. Strukturell hat das Unternehmen mit der Wachstumsstrategie Wagner 2026 wichtige Veränderungen eingeleitet: stärkere geografische Diversifikation, Ausbau internationaler Tochtergesellschaften, neue Serviceangebote, optimierte Prozesse und eine gestärkte Unternehmenskultur durch globale Zusammenarbeit. Neue Standorte in Indien und den Vereinigten Arabischen Emiraten sowie internationale Akquisitionen wie jüngst in Frankreich stärken die weltweite Marktpräsenz nachhaltig.

Wo geht die Reise hin

Die Zukunft des Brandschutzes wird noch stärker präventiv, digitalisiert und vernetzt sein. Während klassische Systeme vor allem reagieren, ermöglichen innovative Technologien proaktive Sicherheitslösungen: KI-gestützte Analysen werden Muster in der Brandentstehung besser erkennen, Sensorik wird noch sensitiver und cloudbasierte Plattformen werden eine zentrale Überwachung und vorausschauende Wartung ermöglichen. Wagner investiert hierfür gezielt in „Brandschutz 4.0“ und schafft datenbasierte Serviceangebote, die Anlagenzustände permanent bewerten und die Betriebssicherheit weiter erhöhen.

Parallel bleibt die internationale Expansion ein wesentlicher Wachstumstreiber. Die globalen Megatrends – Urbanisierung, Automatisierung, Digitalisierung und Nachhaltigkeit – sorgen in vielen Regionen für wachsende Märkte im vorbeugenden Brandschutz. Die Stärkung der internationalen Präsenz ermöglicht es Wagner, stets nah an seinen strategischen Zielmärkten zu agieren und für global operierende Kunden ein zuverlässiger Partner zu sein. GIT



Im Brandschutz 4.0 ermöglichen KI-gestützte Analysen noch höhere Sicherheit

Wagner Group GmbH
www.wagnergroup.com


© Sonja - stock.adobe.com

FEUERWEHR

Taktgeber Technik

Parlamentarischer Abend des VDMA Feuerwehrtechnik

Innovative Feuerwehrtechnik ist gefragt wie selten zuvor. Während die Anforderungen in der Brandabwehr, im Katastrophen- und Zivilschutz stetig wachsen, erhöht sich die Taktzahl in allen Einsatzbereichen – denn Geopolitik und Klimawandel erweitern das Handlungsfeld der Feuerwehren spürbar. Zum ersten „Parlamentarischen Abend der Feuerwehrtechnik“.

„Angesichts neuer Schadenslagen nehmen Einsatzfrequenz und Einsatzintensität schon heute deutlich zu. Dafür braucht es leistungsfähige Technik, die sich am Anwender orientiert.

Die heimische Feuerwehrtechnikindustrie liefert sie: passgenau und zuverlässig. Daher müssen wir die Brandbekämpfung und den Zivilschutz in Deutschland auf eine neue Stufe heben“, sagt Dr. Tobias Ehrhard, Geschäftsführer des Branchenverbandes VDMA Feuerwehrtechnik, anlässlich des ersten Parlamentarischen Abends der Feuerwehrtechnik begrüßte Ehrhard in Berlin zahlreiche Vertreter aus Politik, Industrie und Verbänden.

Veränderte Einsatzlagen

Neben klassischer Brandbekämpfung spielt der Bevölkerungsschutz aufgrund von Extremwetterereignissen und äußeren Bedrohungsszenarien eine immer wichtigere Rolle. Die Feuerwehren müssen sich verstärkt auf neue Szenarien einstellen, wozu auch die resiliente Abwehr chemischer, biologischer und nuklearer Gefahren im Rahmen des Zivilschutzes gehört. „Die Feuerwehren benötigen die bestmögliche Ausstattung, um Krisenlagen optimal managen zu können. Unsere Industrie hat hier eine dreifache Aufgabe: als Enabler für innovative Brandabwehr und Katastrophenschutz, als Partner der Feuerwehren und als Brückenbauer für den Zivilschutz“, erläutert Michael Kristeller, stellvertretender Vorsitzender des VDMA Feuerwehrtechnik.

© Karin Neuhauser

Auf dem ersten Parlamentarischen Abend der Feuerwehrtechnik des VDMA: v. l.n.r.: Martin Gerster, Klaus Wickboldt, Michael Kristeller, Heinz Kreuter, Karl-Heinz Banse und Dirk Aschenbrenner

Digitalisierung beschleunigt Entscheidungen

Technologisch hat die Feuerwehrtechnikbranche viel zu bieten. Vernetzte Fahrzeugflotten, Löschroboter und teilautonome Systeme halten verstärkt Einzug in die Produktportfolios der Industrie. Aber auch ohne hochwertige persönliche Schutzausrüstung sind erfolgreiche Einsätze undenkbar. „Umso wichtiger ist es, die Arbeit der Feuerwehrleute so sicher wie möglich zu gestalten. Datenhelme, die Bilder von Wärmebildkameras, Gebäudepläne oder Vitaldaten in das Sichtfeld des Feuerwehrmannes projizieren, leisten dazu einen wichtigen Beitrag“, sagt Kristeller.

Für die Einsatzleitung vor Ort gewinnen darüber hinaus Künstliche Intelligenz und digitale Lagebilder rasant an Bedeutung. Tritt eine Großschadenslage ein, so lassen sich Entscheidungen spürbar beschleunigen und besser validieren. „Datenanalysen in Echtzeit sind dafür ein mächtiges Tool“, erläutert Kristeller.

Jetzt effektiv vorsorgen

Wer von gesellschaftlicher Resilienz spricht, muss aus Branchensicht den Investitionsstau der Feuerwehren zügig angehen. Man müsse Innovation forcieren, denn eine Investition in die Einsatzkräfte sei immer auch eine Investition in unser Gemeinwesen, so Michael Kristeller.

Wo die Branche mittlerweile steht, macht er mit Nachdruck deutlich: „Unsere Industrie hat heute weit mehr zu bieten als abwehrenden Brandschutz. So gehören längst Spezialfahrzeuge zum Portfolio, die für den Katastrophenfall sowie den Strahlen- und Chemieschutz optimiert sind.“ Eine moderne technische Ausstattung der Feuerwehren müsse „vor allem auf Robustheit und Gebrauchstauglichkeit ausgelegt sein“.

Martin Gerster, Bundestagsabgeordneter der SPD und ehrenamtlicher Präsident der THW-Bundesvereinigung, schließt sich dieser Argumentation an. „Wir haben auf Bundesebene die finanziellen und strukturellen Voraussetzungen dafür geschaffen, dass der Bevölkerungsschutz zukunftsfähig aufgestellt wird. Denn klar ist: Sicherheit geht vor“, betont der Haushaltspolitiker und Zivilschutzexperte.

Zusammenspiel von Bund, Ländern und Kommunen

Damit das gelingt, müssen auch die Kommunen, in deren Trägerschaft die Feuerwehren stehen, mitgenommen werden. „Die Herausforderungen steigen, gleichzeitig erwarten Kommunen Orientierung und Unterstützung. Entscheidend ist insofern ein funktionales Zusammenspiel zwischen Bund, Ländern und Kommunen“, sagt Klaus Wickboldt, Referatsleiter Brandschutz im Niedersächsischen Innenministerium.

Auf die Komplexität und Vielfalt heutiger Einsätze und künftiger Szenarien macht der Deutsche Feuerwehrverband aufmerksam. „Ohne moderne Technik und verlässliche Ausstattung geraten selbst hervorragend ausgebildete Einsatzkräfte an ihre Grenzen“, warnt Verbandspräsident Karl-Heinz Banse.

Wie wichtig es in dieser Frage ist, dass Regularien und Normen mit dem technischen Fortschritt mithalten, erläutert Dirk Aschenbrenner, Präsident der Vereinigung zur Förderung des Deutschen Brandschutzes: „Risiken verändern sich weit schneller als Regularien. Wenn wir den Katastrophenschutz zukunftsfest machen wollen, müssen wir Innovation, Normung und Gesetzgebung besser und vor allem zügiger miteinander synchronisieren. Entscheidend ist, dass wir deutlich schneller werden, insbesondere in der Digitalisierung“, sagt der Brandschutzprofi.

Großes Potential zum Bürokratieabbau

Der Anspruch, effektiv Vorsorge zu leisten, eint alle Beteiligten. „Unser Auftrag ist es, die Feuerwehren in jeder Dimension, in jedem Handlungsfeld zu ertüchtigen. Das geht aber nur gemeinsam mit Kommunen, Politik und Industrie. Dabei müssen wir auch an Prozesse im Vergabe- und Ausschreibungsrecht ran, das viel zu kompliziert geworden ist. Hier gibt es ein großes Potential zur Vereinfachung und Entbürokratisierung – mit nennenswertem Nutzen für den Mittelstand“, resümiert Kristeller. GIT

VDMA
www.vdma.eu

Von Compliance zu intelligenter, vernetzter Sicherheit

Brandschutz im Wandel: Ein Trendbericht von Klaus Hirzel, Business Leader Europe Central Region (DACH) bei Honeywell Fire Products

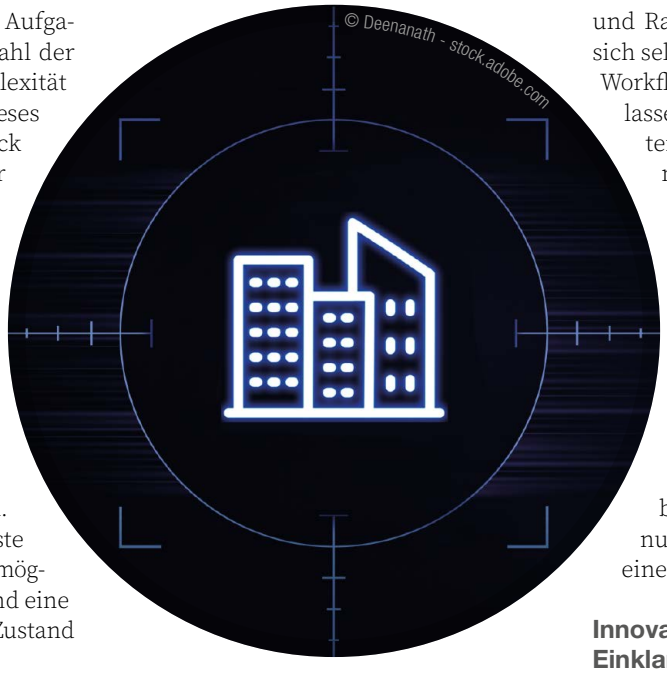
In den vergangenen Jahren hat sich die Brandschutz- und Gefahrenmeldetechnik in Deutschland und Europa deutlich verändert. Was lange als weitgehend eigenständiges Fachgebiet galt, entwickelt sich zunehmend zu einem integralen Bestandteil vernetzter, intelligenter Gebäudeökosysteme. Treiber dieser Entwicklung sind unter anderem bestehende, teils veraltete Infrastrukturen, steigende Gebäudekomplexität, höhere Anforderungen an Resilienz, ein anhaltender Fachkräftemangel sowie die rasante Weiterentwicklung von Konnektivität und Rechenleistung.

Eine zentrale Veränderung ist die wachsende Kluft zwischen der Nachfrage nach qualifizierten Fachkräften und deren Verfügbarkeit. Die Installation, Inspektion und Wartung von Brandschutzanlagen sind nach wie vor hochspezialisierte Aufgaben. Gleichzeitig schrumpft die Zahl der Facharbeiter, während die Komplexität der Systeme weiter zunimmt. Dieses Ungleichgewicht erhöht den Druck auf Betreiber und Serviceanbieter und verstärkt den Bedarf an effizienteren, intelligenteren Lösungen.

Digitalisierung als Treiber

Vor diesem Hintergrund entwickelt sich die Digitalisierung zur prägenden Kraft der Branche. Vernetzung, Automatisierung und datengestützte Erkenntnisse verändern den Brandschutz – weg von rein reaktiven Ansätzen hin zu vorausschauenden Strategien. Anstatt sich ausschließlich auf feste Wartungsintervalle zu verlassen, ermöglichen moderne Systeme zunehmend eine kontinuierliche Transparenz über Zustand und Leistungsfähigkeit.

Technologien wie automatisierte Selbsttests, Ferndiagnosen und cloudbasierte Überwachung erlauben es Betreibern, potenzielle Probleme frühzeitig zu erkennen, Wartungsprozesse gezielt zu optimieren und die Dokumentation für Compliance-Anforderungen zu verbessern. Dies erhöht nicht nur die Sicherheit, sondern reduziert auch Betriebsunterbrechungen und die Abhängigkeit von Vor-Ort-Einsätzen. Vorausschauende Wartung und KI-gestützte Analysen helfen dabei, Ausfälle oder Fehlfunktionen frühzeitig zu identifizieren, bevor sie ein Risiko darstellen.



Honeywell trägt dieser Entwicklung mit der Honeywell Self-Test-Serie Rechnung, bei der Melder eigenständig reale Wärme- und Rauchbedingungen simulieren und sich selbst prüfen – ergänzt durch digitale Workflows und Fernverifikation. Dadurch lassen sich Prüfungen häufiger, konsistenter und mit deutlich geringerem manuellem Aufwand durchführen.

Parallel dazu schaffen Plattformen wie Honeywell Connected Life Safety Services (CLSS) ein neues Maß an Transparenz, indem sie Echtzeit-Einblicke in Systemzustände, Wartungsaktivitäten und Compliance-Daten liefern. Für Systemintegratoren, Dienstleister und Facility Manager entsteht so eine belastbare Datenbasis für effizientere Wartungsplanung, höhere Erstlösungsquoten und eine verbesserte Auditfähigkeit.

Innovation und Regulierung in Einklang bringen

Technologische Innovation muss stets im Kontext bestehender regulatorischer Rahmenbedingungen betrachtet werden. Normen wie DIN 14675 und die Richtlinien des VdS spielen eine zentrale Rolle für

35 JAHRE GIT SICHERHEIT

Die GIT SICHERHEIT ist für mich wichtig, weil sie unsere Expertise sichtbar macht und uns gezielt mit den relevanten Entscheidern der Branche vernetzt.

Günther Rossdeutscher, Geschäftsführender Gesellschafter, Asecos GmbH

Sicherheit, Zuverlässigkeit und Vertrauen in Deutschland. Die Herausforderung besteht darin, diese Regelwerke mit neuen technologischen Möglichkeiten zu verknüpfen.

Viele Vorschriften basieren weiterhin auf präsenzgebundenen Prozessen wie manuellen Inspektionen und festen Wartungsintervallen. Diese Ansätze haben sich bewährt, bilden jedoch nicht immer das Potenzial vernetzter und automatisierter Systeme ab. Das führt zu einem Spannungsfeld zwischen Innovation und Regulierung, das die weitere Entwicklung der Branche maßgeblich prägen wird. Um die Vorteile der Digitalisierung voll auszuschöpfen, braucht es perspektivisch stärker ergebnisorientierte Sicherheitsstandards. Automatisierte Selbsttests, Remote-Inspektionen und digitale Berichterstattung sollten dort anerkannt werden, wo sie nachweislich ein gleichwertiges oder höheres Sicherheitsniveau gewährleisten.

Gleichzeitig bringt die zunehmende Vernetzung neue Verantwortlichkeiten mit sich. Cybersicherheit, Datenintegrität und Prüfbarkeit werden zu entscheidenden Faktoren für das Vertrauen in digitale Systeme. Entsprechend müssen sich auch regulatorische Rahmenbedingungen weiterentwickeln, um Innovation zu ermöglichen und gleichzeitig verlässlich abzusichern.

Zukünftig werden Brandschutzsysteme noch stärker in übergeordnete Gebäudeökosysteme integriert sein. Sie werden enger mit Gebäudeleittechnik, Energiesystemen, Belegungsdaten und integrierten Alarmmanagementlösungen zusammenarbeiten, um ein ganzheitliches Bild von Sicherheit und Betrieb zu liefern.

Lösungen wie Winmag zeigen, wie sich verschiedene Sicherheitsbereiche – von Brandmeldetechnik über Einbruchmeldung und Videoüberwachung bis hin zur Zutrittskontrolle – auf einer gemeinsamen Plattform bündeln lassen. Diese Integration ermöglicht schnellere und fundiertere Entscheidungen, insbesondere in komplexen oder kritischen Umgebungen.

Gleichzeitig entstehen neue Risiken. Der zunehmende Einsatz von Lithium-Ionen-Batterien in Energiespeichern, Mobilität und Industrie bringt zusätzliche Sicherheitsherausforderungen mit sich, die spezialisierte Detektionstechnologien erfordern. Mit Lösungen wie Li-ion Tamer unterstützt Honeywell die frühzeitige Erkennung von Batterie-Ausgasungen und trägt dazu bei, kritische Vorfälle zu vermeiden.

Integrierte, datenbasierte Sicherheitsökosysteme

Der Blick nach vorn ist klar: Der Brandschutz in Deutschland und Europa wird vernetzter, datengesteuerter und vorausschauender. Entscheidend für den Erfolg ist jedoch nicht allein der technologische Fortschritt. Es braucht eine enge Zusammenarbeit zwischen Industrie, Regulierungsbehörden und Betreibern, um sicherzustellen, dass Innovationen zu konkreten Verbesserungen bei Sicherheit, Widerstandsfähigkeit und Effizienz führen.

Im Kern bleibt Brandschutz der Schutz von Menschen und Sachwerten. Zukünftig geht es darüber hinaus darum, Sicherheitsverantwortliche mit besseren Werkzeugen, verlässlichen Daten und intelligenteren Systemen zu unterstützen. So können wir nicht nur sicherere Gebäude, sondern auch widerstandsfähigere Infrastrukturen und Gesellschaften schaffen. GIT

Honeywell
www.honeywell.com/de/de

© Bilder: Honeywell

© Gloria

Brandschutz im Wandel

Marion Heidrich, Operations Director Gloria, über Trends, Technologie und Zukunft der Branche

Die Brandschutzbranche ist in Bewegung. Was lange Zeit als etabliertes, überwiegend regulatorisch getriebenes Feld galt, wird heute von gleich mehreren Faktoren gleichzeitig umgetrieben – zum einen sind es die strengere Umweltgesetzgebung sowie die zunehmende Digitalisierung. Doch auch neue Brandrisiken durch moderne Energieträger sind ein entscheidender Punkt in der Entwicklung der Branche. Für einen Hersteller wie Gloria ist dieser Wandel keine Bedrohung, sondern vertrautes Terrain. Das Unternehmen aus Wadersloh hat es sich zur strategischen Aufgabe gemacht, technologische Entwicklungen nicht nur zu verfolgen, sondern aktiv umzusetzen.

© Alex_Po - stock.adobe.com

Das wohl drängendste regulatorische Ereignis der jüngsten Zeit ist die EU-Verordnung 2025/1988, die im Oktober 2025 in Kraft getreten ist und PFAS in Feuerlöschschäumen schrittweise verbietet. Die Konsequenzen für die Branche sind erheblich und betreffen Hersteller wie Betreiber gleichermaßen. Ab Oktober 2026 ist das Inverkehrbringen PFAS-haltiger Löschschäume in tragbaren Feuerlöschern untersagt, die tatsächliche Nutzung bereits vorhandener Geräte bleibt jedoch bis Ende 2030 gestattet. Die Übergangsfrist klingt großzügig – doch der Handlungsdruck ist bereits heute real. Da herkömmliche PFAS-haltige Schaumfeuerlöscher und Ersatzfüllungen bereits ab Oktober 2026 nicht mehr angeboten werden dürfen, bleibt für den ein Austausch des Löschmittels in bestehenden Geräten nicht mehr viel Zeit.

Der Transformationsprozess umfasst dabei nicht nur die Neuentwicklung der Geräte selbst, sondern auch den Austausch von Altgeräten und deren fachgerechte Entsorgung. Zudem ist die regulatorische Reise

noch nicht abgeschlossen, die Richtung aber eindeutig. Daher hat Gloria bereits seit Ende 2024 auf die ausschließliche Produktion und den Vertrieb PFAS-freier Feuerlöscher umgestellt.

Parallel dazu stellt der Vormarsch der Lithium-Ionen-Technologie die Branche vor neue Aufgaben. So haben Elektromobilität und moderne Energieversorgungssysteme dazu geführt, dass entsprechende Brände heute eine ganz eigene Gefährdungskategorie darstellen. Normative Regelungen für geeignete Löschmittel befinden sich noch in der Entwicklung, erste Lösungsansätze sind jedoch bereits am Markt verfügbar. Neue Technologien bedürfen zeitnah auch neuer Schutzkonzepte – dabei ist es wichtig, dass die Industrie nicht auf den Gesetzgeber wartet, sondern eigeninitiativ vorangeht.

Brandschutzausbildung der Zukunft

Der Wandel der Branche zeigt sich jedoch nicht nur in der Produktchemie. Die Digitalisierung hat selbstverständlich auch im Brandschutz Einzug erhalten, und Gloria steht dabei für den innovativen Umgang mit dieser Entwicklung. Mit dem VR Fire Trainer wurde ein Schulungsinstrument entwickelt, welches das klassische Feuerlöschtraining von Grund auf neu denkt. Mithilfe von Virtual-Reality-Brille, Controller und einer Feuerlöscher-Attrappe tauchen Teilnehmende vollständig in simulierte Brandszenarien ein. Sie erleben Flammen und Rauchentwicklung in realistischer Umgebung, müssen in Echtzeit Entscheidungen treffen und können dabei Fehler machen, ohne dass reale Konsequenzen drohen.

Das System ist kompakt, flexibel einsetzbar und kommt ohne Löschmittelverbrauch aus. Es entstehen weder Entsorgungskosten noch Emissionen – ein Argument, das in Zeiten wachsenden Umweltbewusstseins zunehmend an Gewicht gewinnt. Schon heute berichten zahlreiche Brandschutzbeauftragte und Sicherheitsverantwortliche von messbaren Verbesserungen in Motivation und Lernerfolg. In naher Zukunft wird das System um einen Augmented-Reality-Modus erweitert. Anders als bei der vollständigen virtuellen Immersion überlagert AR die reale Umgebung mit simulierten Brandszenarien, sodass Mitarbeitende buchstäblich an ihrem eigenen Arbeitsplatz den Ernstfall üben können. Die psychologische Wirkung dieser Verbindung aus realem Kontext und virtuellem Szenario ist erheblich und macht das Training noch einprägsamer.

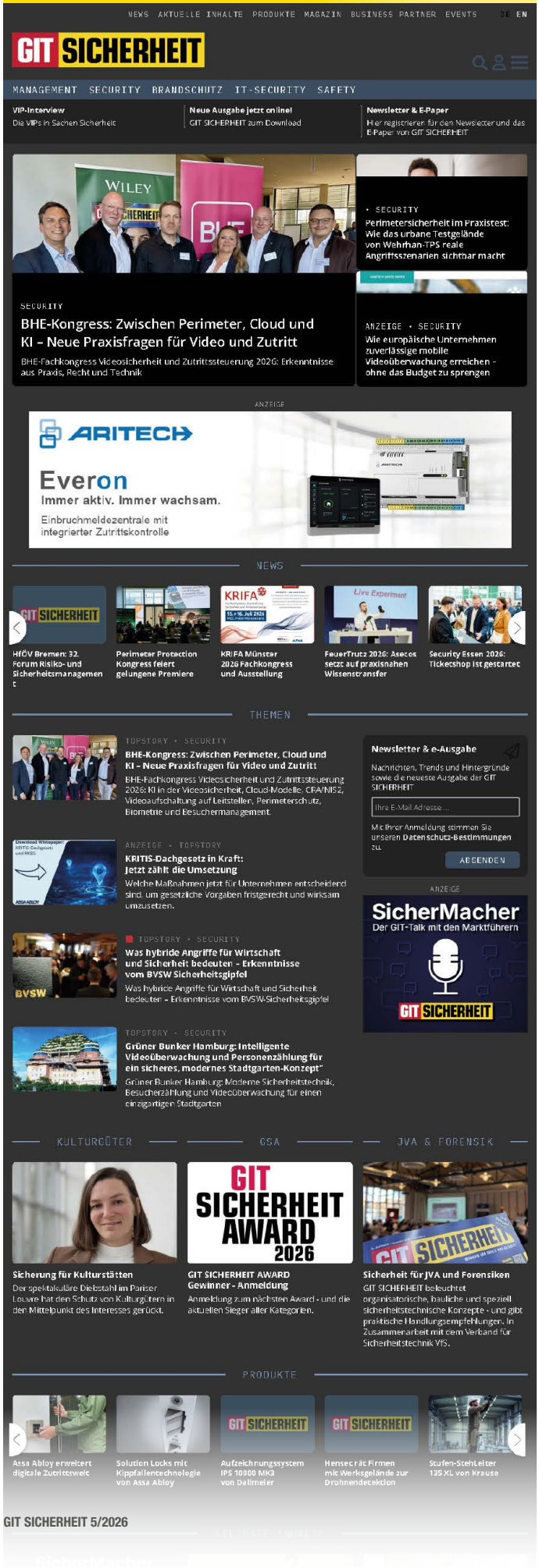
Einsatz von KI

Der Einsatz von KI und modernen Technologien aus den Bereichen Extended Reality mittels VR und AR wird den Brandschutz auf die nächste Ebene bringen und somit deutlich digitaler werden lassen. Für Gloria bedeutet das keinen Bruch mit der eigenen Philosophie, sondern deren konsequente Weiterentwicklung. Digitalisierung ist kein Selbstzweck, sondern steht immer im Dienst eines konkreten Nutzens – mehr Sicherheit für Menschen und Sachwerte.

„Brandschutz ist keine statische Disziplin. Er ist eine der dynamischsten Sicherheitstechnologien unserer Zeit – getrieben von regulatorischem Druck, ökologischer Verantwortung und dem schlichten Anspruch, dass im Ernstfall jeder Handgriff sitzt. Die Zukunft des Brandschutzes wird digitaler, nachhaltiger und näher am Menschen sein als je zuvor. GIT

Gloria GmbH
www.gloria.de

Diesen Monat auf GIT-SICHERHEIT.de



IMPRESSUM

Herausgeber
Wiley-VCH GmbH

Geschäftsführer
Dr. Guido F. Herrmann

Senior Director, Publishing and Content Services
Dr. Katja Habermüller

Publishing Director
Dipl.-Betriebswirt Steffen Ebert

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

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

Anzeigenleitung
Miryam Reubold
+49 6201 606 127

Sales Director
Jörg Wüllner
+49 6201 606 748

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

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

Dr. Timo Gimbel
+49 6201 606 049

Tina Renner
+49 6201 606 021

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

Herstellung
Jörg Stenger
+49 6201 606 742

Claudia Vogel (Anzeigen)
+49 6201 606 758

Satz + Layout
Andreas Kettenbach

Lithografie
Elke Palzer

Sonderdrucke
Miryam Reubold
+49 6201 606 172

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

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

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

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

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

Abonnement 2026
10 Ausgaben (inkl. Sonderausgaben)
122,30 €, zzgl. MwSt.
Einzelheft 17 € zzgl. Porto + MwSt.

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

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

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

Druck
westermann DRUCK | pva

Printed in Germany, ISSN 2751-4536

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

WILEY

Garant

WORKWEAR, SO DYNAMISCH WIE DU.

Du hast höchste Ansprüche an deine Arbeit? Wir haben das richtige Werkzeug, das perfekt zu dir passt: mehr als 55.000 zertifizierte System-Werkzeuge in höchster Qualität für alle Anwendungen rund um deinen Arbeitsplatz. Entdecke dein Werkzeug:

www.garant-tools.com

Industrial Tooling and Equipment by Hoffmann Group

TITELTHEMA

Pflicht zur Umsetzung nachweisbarer Security-Maßnahmen

Wie industrielle Netzwerke widerstandsfähiger gegen Cyber-Angriffe und Co. gestaltet werden

Die steigende Digitalisierung industrieller Prozesse erhöht neben der Effizienz und Flexibilität auch die Angriffsfläche moderner Produktionsanlagen. Cyber-Bedrohungen treffen heute nicht mehr nur IT-Systeme, sondern immer häufiger die operative Technologie (OT). Um diese ausreichend zu schützen, gibt es zunehmend Normen und gesetzliche Vorgaben.

Zu den zentralen Regelwerken zählt die internationale Normenreihe IEC 62443, die Anforderungen an Komponenten, Systeme und Prozesse der industriellen Automatisierung definiert. Ergänzt wird sie durch europäische Gesetzgebungen wie die NIS-2-Richtlinie und den Cyber Resilience Act (CRA), die Betreiber und Hersteller verpflichten, nachweisbare Sicherheitsmaßnahmen umzusetzen. NIS-2 weitet die Verantwortung über Systeme der kritischen Infrastrukturen hinaus auf große Teile der industriellen Wertschöpfung aus. Der CRA adressiert hingegen die Cyber-Sicherheit von Produkten mit digitalen Elementen über deren gesamten Lebenszyklus. Gemeinsam verfolgen diese Vorgaben das Ziel, industrielle Netzwerke widerstandsfähiger und anhaltend verfügbar zu machen.

Sicher entwickelte Geräte mit umfassenden Security-Funktionen

Industrielle Netzwerke bestehen aus unterschiedlichen Komponenten, die jeweils eigene sicherheitsrelevante Rollen übernehmen. Hersteller wie Phoenix Contact bieten für diese Gerätekategorien Lösungen an, die in sicheren Entwicklungsprozessen entstehen und mit umfassenden Sicherheitsfunktionen ausgestattet sind.

Einsatz von Managed Switches und Security-Routern im Schaltschrank

Managed Switches bilden das Rückgrat der Kommunikation. Sie sorgen für die Segmentierung, Priorisierung und Stabilität des Datenverkehrs. Security-Router mit Firewall-Funktionalität schützen die Übergänge zwischen Zonen respektive Netzwerksegmenten und kontrollieren, wer worauf zugreifen darf. Drahtlose Infrastrukturen – von industriellen WLAN Access Points bis zu Mobilfunk-Routern – ermöglichen flexible Anwendungen und Remote-Zugriffe. Sie eröffnen aber gleichzeitig zusätzliche Angriffsvektoren über Funktechnologien im öffentlichen Raum. Viele dieser Geräte arbeiten über lange Lebenszyklen in heterogenen Anlagenstrukturen. Fehlkonfigurationen, unzureichend gesicherte Schnittstellen oder nicht eingespielte Firmware-Updates können mit der Zeit kritische Schwachstellen offenlegen und so zu einem großen Sicherheitsrisiko werden.

Vielfältige Anforderungen an die Netzwerkkomponenten

Wie können zertifizierte Netzwerkkomponenten die Cyber-Sicherheit industrieller Netzwerke tatsächlich erhöhen? Aus Sicht der IEC 62443 müssen Komponenten dazu beitragen, die von der Norm definierten Security-Level in einer Anlage zu realisieren. Für Netzwerktechnik-Komponenten bedeutet das unter anderem: abgesicherte Management-Zugänge, eine rollenbasierte Benutzer- und Rechteverwaltung, kryptografisch geschützte Kommunikationskanäle, Integritätsprüfungen von Firmware sowie ein nachvollziehbares Logging sicherheitsrelevanter Ereignisse. Hinzu kommen Härtungsmaßnahmen wie das Deaktivieren nicht benötigter Dienste oder Ports, die Absicherung vor Brute-Force-Angriffen und gesicherte Update-Mechanismen. Erst wenn diese Fähigkeiten auf der Geräteebene vorhanden sind, können Betreiber die in der Norm beschriebenen Zonen- und Leitungsmodelle in der Praxis effizient abbilden.

Im Maschinen- und Anlagenbau zeigt sich der Nutzen solcher Funktionen besonders deutlich. Produktionszellen werden typischerweise als eigene Security-Zonen mit streng festgelegten Kommunikationsbeziehungen ausgelegt. Managed Switches übernehmen hier nicht nur das reine Switching. Sie trennen außerdem die verschiedenen Maschinenteile über VLANs logisch voneinander, priorisieren zeitkritische Protokolle (zum Beispiel Profinet oder EtherNet/IP) und unterstützen Ring-Redundanzmechanismen für eine hohe Verfügbarkeit. Security-Router, die an der Grenze zwischen den Security-Zonen installiert sind, setzen die oben genannten streng definierten Kommunikationsbeziehungen durch integrierte Firewalls mit Stateful Inspection um. Über IPsec- oder OpenVPN-Tunnel lassen sich Remote-Servicezugriffe zeitlich begrenzt und eindeutig authentifiziert freischalten. Das schließt die Protokollierung ein, welche Verbindung wann aktiv war und welche Steuerungen adressiert wurden.

Phoenix Contact bietet ein ganzheitliches 360-Grad-Security-Konzept an

Umfänglicher Schutz von kritischen Infrastrukturen und älteren Anlagen

Noch höhere Anforderungen bestehen in öffentlichen Infrastrukturen und kritischen

Bitte umblättern ▶

Cyber Security

Sicherer Betrieb		
Deutscher IT Security Act 1.0	→	Deutscher IT Security Act 2.0
NIS 1 Richtlinie	→	NIS 2 Richtlinie

Cybersicherheit in Produkten	
EU Cyber Resilience Act	
Allg. Produktsicherheitsverordnung	EU-Maschinenverordnung
Produkthaftungsrichtlinie	Gesetz über Artificial Intelligence Act

Die europäischen Gesetzgebungen NIS 2 und CRA im Vergleich

Wenn der Cyber Resilience Act umgesetzt ist, werden alle Vorschriften und Anleitungen für Sicherheitsaspekte in Produkten umgesetzt.

Jan Aulenberg, Produktmarketing Network Technology, Phoenix Contact

Zertifizierte Cyber Security von Phoenix Contact

Phoenix Contact bietet ein umfassendes Portfolio an gemäß der IEC 62443-4-2 zertifizierten Produkten für industrielle Netzwerke. Dazu gehören die Managed Switches der Serie FL Switch 2000, Security-Router der Produktfamilie mGuard sowie industrielle Mobilfunklösungen wie die Cellulink-Router für 4G-/5G-Netze. Weitere Baureihen – wie die WLAN-Infrastrukturgeräte FL WLAN mit WiFi-6/-6E-Technologie und die Managed Switches der Serie FL Switch 5900 für die 19-Zoll-Rack-Montage – erfüllen bereits wesentliche Anforderungen der IEC 62443-4-2.

Alle Produkte entstehen in sicheren, ebenfalls zertifizierten Entwicklungsprozessen gemäß IEC 62443-4-1. Sie halten die beschriebenen Security-Funktionen für den Einsatz in anspruchsvollen OT-Umgebungen ein. Die 360-Grad-Security-Strategie von Phoenix Contact umfasst neben sicheren Produkten und Prozessen auch sichere Lösungen sowie ein aktives Schwachstellenmanagement durch ein PSIRT-Team (Product Security Incident Response Team). Damit unterstützt das Unternehmen Betreiber dabei, industrielle Netzwerke ganzheitlich abzusichern – von der Planung über den Betrieb bis zum Incident-Handling.

Versorgungsnetzen. Hier müssen die Leitstellen-, Fernwirk- und Feldebene sowohl gegen externe Angriffe als auch gegen Fehlkonfigurationen geschützt werden. Managed Switches stellen beispielsweise sicher, dass lediglich autorisierte Geräte an festgelegten Ports (zum Beispiel via Port-Security, 802.1X oder MAC-Filter) zugelassen und so Manipulationsversuche im Layer-2-Bereich erschwert werden. Zeitgestempelte Logs und die Anbindung an zentrale Syslog- oder SIEM-Systeme ermöglichen es, sicherheitsrelevante Ereignisse im Leitstand nachzuvollziehen.

Ein drittes häufiges Szenario ist das Retrofit älterer Anlagen. Viele Steuerungssysteme sind ursprünglich ohne Security-Fokus entwickelt worden. Sie arbeiten daher weder mit verschlüsselten Protokollen noch mit modernen Authentifizierungsmechanismen. Hier setzen Betreiber zertifizierte Security-Router als vorgelagerte Schutzschicht ein, um solche Komponenten in isolierten Segmenten zu betreiben. Typische Maßnahmen in diesem Kontext sind die strikte Whitelist-Konfiguration erlaubter Verbindungen, die Einrichtung definierter Engineering-Zugänge sowie die Limitierung von Fernzugriffen auf klar festgelegte Wartungsfenster. In Kombination mit Switch-Funktionen wie der oben beschriebenen Port-Security lässt sich die Angriffsfläche auf diese Weise deutlich verringern, ohne die bestehende Automatisierung grundlegend umbauen zu müssen.

Zusammenarbeit entlang eindeutiger Prozesse

Zertifizierte Einzelgeräte allein reichen jedoch nicht aus. Sie entfalten ihren Wert erst in einer abgestimmten Systemarchitektur, wie sie die IEC 62443 vorsieht: Defense-in-Depth, Zoneneinteilung, festgeschriebene Kommunikationspfade und konsistente Härtungsmaßnahmen. Entscheidend ist, dass alle beteiligten Akteure wie Betreiber, Integratoren und Hersteller entlang eindeutiger Prozesse agieren. Unternehmen wie Phoenix Contact ergänzen zertifizierte Produkte deshalb durch sichere Entwicklungsprozesse, Lösungsarchitekturen und Incident-Response-Strukturen. Für Betreiber bedeutet dies: Sie können auf durchgängige Security-Konzepte zurückgreifen, die über das einzelne Gerät hinausgehen. Darüber hinaus unterstützt die IEC 62443 Betreiber nicht nur im Aufbau ganzheitlicher Security-Konzepte, sondern ebenfalls in der Erfüllung der neuen gesetzlichen Vorgaben, wie beispielsweise dem Cyber Resilience Act (CRA). Denn zahlreichen der neuen gesetzlichen Anforderungen wird bereits heute durch die IEC 62443 Rechnung getragen.

Industrielle Cyber-Sicherheit ist ein fortlaufender Prozess. Zertifizierte Komponenten schaffen dafür eine belastbare Grundlage. Sie erlauben den Netzwerkaufbau nach anerkannten Standards, eine Minimierung der Bedrohungen sowie die Einhaltung regulatorischer Anforderungen. In Zeiten zunehmender Digitalisierung und Standardisierung sind die zertifizierten Security-Komponenten damit ein unverzichtbarer Baustein für eine stabile industrielle Wertschöpfung. GIT

Netzwerkkomponenten von Phoenix Contact sind gemäß IEC 62443 zertifiziert

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

Blåkläder fertigt künftig 98 % seiner Produkte selbst

Nahezu alle von Blåkläder verkauften Kleidungsstücke werden 2026 in den eigenen Fabriken des Workwear-Herstellers produziert. Ermöglicht wird das durch eine neue Fabrik in Bangladesch. „Die branchenübliche Praxis, keine eigenen Produktionsstätten zu besitzen, erschwert die Nachhaltigkeitsbemühungen in der gesamten Bekleidungsindustrie. Mit unseren eigenen Fabriken fällt es uns leichter, die Arbeitsbedingungen zu verbessern und unseren ökologischen Fußabdruck nachhaltig zu verringern. Deshalb sind wir sehr stolz darauf, gegen den Strom zu schwimmen“, sagt Anders Carlsson, Geschäftsführer von Blåkläder.


© Blåkläder Deutschland GmbH

Die neue Fabrik von Blåkläder, Gava, wurde 2025 in Dhaka, der Hauptstadt von Bangladesch, eröffnet und ermöglicht es dem Unternehmen, Strickwaren wie T-Shirts, Poloshirts und Unterwäsche selbst herzustellen. In Zukunft werden dadurch mindestens 98 Prozent aller vom Unternehmen verkauften Produkte in den eigenen Fabriken hergestellt.

Bei voller Auslastung wird Blåkläder in der neuen Fabrik 2.400 Mitarbeiter beschäftigen und somit insgesamt rund 8.000 Angestellte in Süd- und Südostasien. Allen Mitarbeitern werden über dem Branchenniveau liegende Löhne sowie Zugang zu medizinischer Versorgung garantiert. Blåkläder unterhält zudem einen Fond, bei dem Mitarbeiter bei Bedarf finanzielle Unterstützung beantragen können.

„Unsere Mitarbeiter sind das Herzstück des Unternehmens. Jeder, der bei uns arbeitet, soll die Möglichkeit haben, seine Fähigkeiten weiterzuentwickeln, eine Karriere im Unternehmen aufzubauen und vor allem die Gewissheit zu haben, seinen Arbeitsplatz zu behalten“, sagt Anders Carlsson.

Die Fabrik in Bangladesch ist mit Solarmodulen ausgestattet, die 40 bis 50 Prozent des Energiebedarfs der Anlage decken. Wie mehrere andere Fabriken von Blåkläder ist auch dieser Standort nach LEED Platinum zertifiziert und erfüllt zudem zwei soziale Nachhaltigkeitsstandards: Oeko-Tex STeP und SA8000. **www.blaklader.com**

Baak bringt Sicherheitsschuh-Duo für Frauen heraus


© Baak

Der Halbschuh und der knöchelhohe Stiefel von Baak sind die ersten Damenmodelle der „Adventure“-Serie. In Handwerks- und Industrieberufen ist Persönliche Schutzausrüstung meist verpflichtend. Frauen sind dort zwar in der Minderheit, aber eine relevante Zielgruppe: Laut Statistischem Bundesamt liegt ihr Anteil im Handwerk bei rund 10 Prozent, in der Industrie bei etwa 15 Prozent. Für Sicherheitsschuhe bedeutet das, Passform und Funktion stärker auf Frauenfüße auszurichten. Genau hier setzt der Hersteller mit den neuen Modellen „Alea“ und „Alessia“ an. Beide S3S-Modelle fertigt Baak auf speziellen Damenleisten und berücksichtigt dabei typische Unterschiede wie eine schmalere Ferse, einen anderen Volumenverlauf im Vorfußbereich und eine geringere Spannhöhe. So wird eine Passform erreicht, die den Fuß sicher führt und Rutschen im Schuh reduziert – ein wichtiger Faktor für Stabilität und Tragekomfort bei langen Einsätzen. **www.baak.de**

MASCHINEN- UND ANLAGENSICHERHEIT

Zukunftssicher mit ASi-5

Warum Anwender von der neuen ASi Generation vielfach profitieren

Josef Alaaddin, stellvertretender Teamleiter Technischer Support bei Bihl+Wiedemann

Einfache Installation, robuste Technik und vergleichsweise niedrige Maschinenkosten: AS-Interface gehört seit Jahren zu den verbreiteten Lösungen für die Feldebene. Mit ASi-5 hat die Technologie einen weiteren Entwicklungsschritt gemacht und ermöglicht heute höhere Datenraten, kürzere Zykluszeiten und eine einfachere Integration moderner Geräte wie Io-Link-Sensoren und -Aktoren. IO-Link ist eine standardisierte, serielle Punkt-zu-Punkt-Kommunikation zur Parametrierung und Diagnose von Feldgeräten. Josef Alaaddin, stellvertretender Teamleiter Technischer Support bei Bihl+Wiedemann, erläutert im Interview mit GIT SICHERHEIT, warum sich ASi-5 bereits in zahlreichen Anwendungen etabliert hat und welche Perspektiven sich daraus für zukünftige Automatisierungslösungen ergeben.

GIT SICHERHEIT: Herr Alaaddin, wie hat sich ASi-5 aus Sicht von Bihl+Wiedemann in der jüngeren Vergangenheit entwickelt?

Josef Alaaddin: ASi-5 und ASi-5 Safety haben sich im Markt flächendeckend etabliert. Dies beweisen u. a. die weit mehr als 250.000 ASi-5 Geräte von uns und anderen Herstellern, die bereits in Maschinen und Anlagen installiert sind. Die Technologie überzeugt dabei sowohl in reinen ASi-5 Applikationen wie als perfekte Ergänzung zu ASi-3. Und die Nachfrage insbesondere aus der Lager- und Fördertechnik, der Verpackungsautomatisierung und der Prozesstechnik bewegt sich weiterhin auf hohem Niveau. Dies liegt auch daran, dass mit ASi-5 in vielen Aufgabenstellungen aufwendige ethernetbasierte Lösungen vermieden oder ersetzt werden können. Und weil ASi-5 für uns ganz klar eine Erfolgsstory ist, entwickeln wir gerade auch einen ASi-5 Repeater, mit dem sich die mögliche Leitungslänge von ursprünglich 200 m zukünftig vervielfachen lässt.

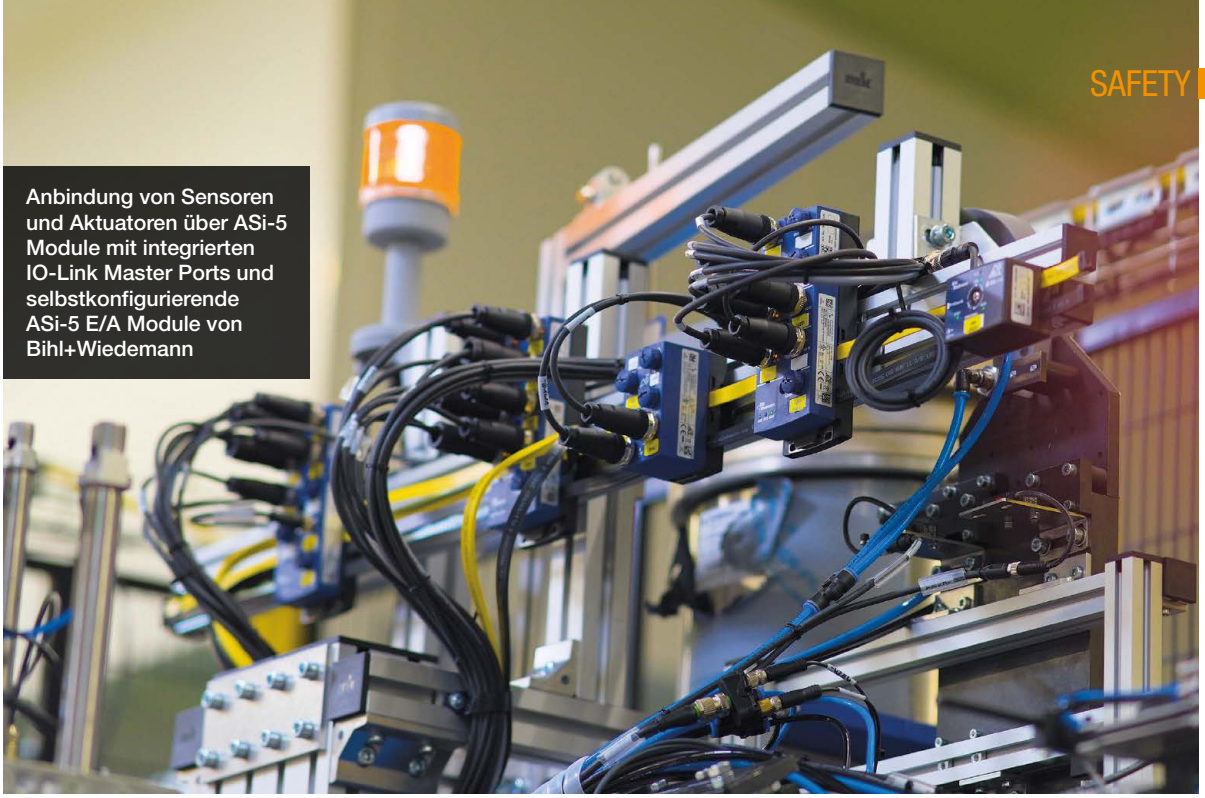
Leitungslänge ist ein Thema – welche Vorteile bietet ASi-5 denn bei der Energieverteilung im Feld?

Josef Alaaddin: ASi-5 als Feldbus der unteren Automatisierungsebene macht die Energieverteilung, eine elementare Komponente der Technologie, sehr effizient und flexibel. Energie und Daten laufen über das bekannte gelbe 1,5 mm² Profilkabel, das für eine auf acht Ampère begrenzte Übertragungsleistung völlig ausreicht. Wenn aber, etwa für Antriebe oder Ventile, Bedarf für mehr Leistung besteht, kann dieser über ein zweites, schwarzes Profilkabel realisiert werden – mit einem Leitungsquerschnitt von 2,5 mm² sogar bis 20 A. Ebenfalls umgesetzt werden kann über das schwarze Profilkabel auch passive Sicherheit bis SIL3/PLe. Die Installation in Durchdringungstechnik ohne Stecker und weitere Module spart darüber hinaus nicht nur Verdrahtungsaufwand, Materialkosten und Montagezeit, sondern macht die Installation im Vergleich zu klassischen Feldbussen oder Punkt-zu-Punkt-Verbindungen auch viel schlanker und übersichtlicher. Da ein ASi-5 Strang bis zu 62 Teilnehmer versorgen kann, kann die Energieverteilung ohne zusätzliche Verkabelungen stufenweise angepasst werden.

Was bedeuten die zusätzlichen Möglichkeiten von ASi-5 für die Konfiguration von ASi Netzwerken?

Josef Alaaddin: Grundsätzlich können, wie schon bei ASi-3, alle Netzwerke mit ASi-5 Komponenten über ein Handadressiergerät und den Master konfiguriert werden. Wie komplex die Konfiguration wird, hängt dabei ganz wesentlich von der Komplexität der angestrebten Automatisierungslösung ab. Da wir unsere Kunden dabei so gut wie möglich unterstützen möchten, bieten wir ihnen mit unseren Software-Suites eine Lösung, mit der sie ihre Konfiguration deutlich vereinfachen und beschleunigen können.

Damit lassen sich z. B. IO-Link Devices komfortabel konfigurieren oder Frequenzumrichter parametrieren, und die Parameterdaten können danach auch einfach von



Anbindung von Sensoren und Aktuatoren über ASi-5 Module mit integrierten IO-Link Master Ports und selbstkonfigurierende ASi-5 E/A Module von Bihl+Wiedemann

Modul zu Modul und sogar von Projekt zu Projekt kopiert werden. Außerdem können Anwender per Drag and Drop ihre Projekte direkt aus dem integrierten Hardwarekatalog umsetzen und auch am Bildschirm testen. Aber wir haben nicht nur die Maschinenbauer im Blick, sondern auch deren Kunden, die Anlagenbetreiber, denn sie sind es ja, die die Maschinen am Ende optimal nutzen sollen. Dafür macht es aber Sinn, dass sie unsere Produkte und Lösungen besser kennen und verstehen. Und deshalb unterstützen wir von Bihl+Wiedemann die Anwender nicht erst mit technischem Support, wenn sie ihn aktuell benötigen sollten, sondern schon von Anfang an mit Informations- und Schulungsmaterialien. Dazu zählen nicht nur unsere Installationsempfehlungen, Best Practices und der Troubleshooting Guide sowie eine Vielzahl von Schulungsvideos zu allen möglichen Themen auf unserer Webseite, sondern seit kurzem auch unsere Bihl+Wiedemann Academy.

Stichwort Installation: Inwiefern unterscheidet sich eine Installation mit ASi-5-Gateways in Bezug auf die Cybersicherheit von anderen ethernetbasierten Lösungen?

Josef Alaaddin: Bei ASi-5 ist das Gateway mit OPC UA das Bindeglied zwischen TCP/IP und der ASi Installation, es entkoppelt aber auch physisch die ethernetbasierten Schnittstellen und die Feldebene mit ASi. Durch diesen kommunikativen Bruch kann das ASi Netzwerk nicht zur Angriffsplattform für Cyberattacken werden. Wird also statt eines IO-Link Masters mit integrierter Ethernetschnittstelle ein ASi-5 Modul mit integriertem IO-Link Master eingesetzt, können mögliche Sicherheitslücken gar nicht erst entstehen. Wenn also eine Kombination cybersicher ist, dann die von ASi-5 mit IO-Link. ASi-5 spannt hier quasi den Schutzschirm auf, unter dem IO-Link dann ohne Gefahren von außen betrieben werden kann. GIT

Bihl+Wiedemann GmbH
www.bihl-wiedemann.de

Das einwandfreie Funktionieren aller Kranmotoren ist die Voraussetzung für reibungslose Prozesse; jede ungeplante Unterbrechung würde hohe Folgekosten verursachen. Daher soll der Zustand der Motoren kontinuierlich überwacht werden

MASCHINEN- UND ANLAGENSICHERHEIT

Smarte Schwingungsmessung

Fehler erkennen, bevor sie entstehen

Die Schwingungsanalyse entwickelt sich von einer reinen Zustandsüberwachung hin zu einem zentralen Baustein moderner Sicherheits- und Instandhaltungskonzepte. Durch den Einsatz hochauflösender Sensortechnik und intelligenter Datenanalyse lassen sich Fehler nicht nur erkennen, sondern bereits in ihrer Entstehung identifizieren. Damit wird Condition Monitoring zu einem entscheidenden Faktor für sichere, effiziente und zukunftsfähige Produktionsprozesse.

Ungeplante Stillstände verursachen für Betreiber erhebliche Kosten, führen zu Produktionsausfällen und können im Ernstfall sogar Risiken für Mensch und Anlage mit sich bringen. Eine frühzeitige und zuverlässige Zustandsüberwachung ist daher entscheidend, um Wartungsmaßnahmen vorausschauend zu planen und Ausfälle zu vermeiden.

Die Schwingungssensoren von Pepperl+Fuchs leisten hierzu einen wesentlichen Beitrag: Sie erkennen frühzeitig Montagefehler, Lockerungen, Resonanzen, Lagerschäden oder Unwuchten und tragen so zur hohen Anlagenverfügbarkeit bei. Für Anwendungen wie Zentrifugen, Ventilatoren, Pumpen oder Motoren bietet die DIN ISO 20816 einen etablierten Normrahmen mit klar definierten Schwingungsgrenzwerten.

Die Sensoren erfassen und verarbeiten Schwingungen im Frequenzbereich von 10 bis 1000 Hz und geben diese als RMS-Schwinggeschwindigkeit aus – eine bewährte Kenngröße zur zuverlässigen Zustandsbewertung.

Effiziente Übertragung hochaufgelöster Schwingungsdaten

Die VIM3-Serie mit einem Frequenzbereich von bis zu 12 kHz liefert die ideale Basis für anspruchsvolle Analysen. Sie ist mit einer IO-Link-Schnittstelle ausgestattet, die eine effiziente Datenübertragung ermöglicht. Pepperl+Fuchs nutzt einen zweistufigen Ansatz zur Messung von Schwingfrequenzen:

- Volle Datentransparenz: Rohbeschleunigungswerte – ungefiltert oder vorverarbeitet – werden direkt vom Sensor an die Maschinensteuerung übertragen.
- Effiziente Übertragung großer Datenmengen: Große Schwingungsdatensätze werden über das standardisierte BLOB (Binary Large Object) Profil von IO-Link übertragen. So können umfangreiche Sensordaten schnell und zuverlässig übertragen werden, die über den normalen IO-Link-Kanal nicht möglich wären.
- Besonders praktisch: Die Speichergröße ist flexibel einstellbar, sodass je nach Bedarf entweder größere Datenmengen oder schnellere Übertragungszeiten priorisiert werden können.

Vorteil für den Anwender:

- Vollständige Datengrundlage für tiefergehende Schwingungsanalysen
- Erfassung des Maschinen-Gut-Zustands schon bei der Inbetriebnahme
- Sofortige Erkennung von Abweichungen durch Verschleiß oder Beschädigungen, selbst bei kritischen Schwingungen in mehreren Frequenzbereichen

Der VIM3 Schwingungssensor wird über Schraubgewinde oder Magnetadapter am Kranmotoren befestigt. Mittels kapazitiver MEMS-Sensorik werden sowohl Geschwindigkeit als auch Beschleunigung, die bei einer Schwingungsbewegung entstehen, gemessen. Die Daten werden analog oder mittels IO-Link Kommunikation an die Steuerung übermittelt. Unwuchten, Lagerschäden und Resonanzen werden so zuverlässig angezeigt

Überall dort, wo die Zustandsüberwachung von Maschinen und Anlagen notwendig ist, helfen die Schwingungssensoren wie der VIM3 von Pepperl+Fuchs, ungeplante Stillstände zu vermeiden und den Schutz von Personal und Anlagen zu gewährleisten

Frequenzmessung und Rohdatenübertragung

In der zweiten Ausbaustufe erweitert Pepperl+Fuchs die VIM3-Serie der IO-Link-Schwingungssensoren um zusätzliche Messgrößen wie beispielsweise den Beschleunigungswert (Peak-Hold) sowie den Crest-Wert für die Lagerzustandserkennung. Diese Kennwerte werden zyklisch an die Maschinensteuerung übertragen und stehen dort unmittelbar zur Verfügung.

Darüber hinaus besteht die Möglichkeit, Rohdaten in einem breiten Frequenzspektrum von bis zu 12 kHz über das IO-Link BLOB Protokoll zu übertragen. Dabei ist zu berücksichtigen, dass die Übertragungsdauer durch die maximale Datenrate von IO-Link begrenzt ist.

Zwei Wege von der Analyse bis zur Kompaktlösung:

- **Umfassende Analyse über BLOB-Profil**

Über das BLOB-Profil können umfangreiche Rohdatenpakete bereitgestellt werden, die auf der Steuerungsseite detailliert ausgewertet werden können – beispielsweise mittels FFT-, Hüllkurven- oder Zeitbereichsanalyse.

- **Kompakte Zustandsbewertung über integrierte Kennwerte**

Wer eine schnelle und einfache Lösung bevorzugt, kann direkt auf die intern berechneten Kennwerte etwa den Crest-Wert zur Lagerzustandsbewertung zurückgreifen.

IO-Link als Basis für modernes Condition Monitoring

Die VIM3-Serie kann darüber hinaus Kenntnisse zur Zustandsbewertung liefern. Dazu gehören die Zähler- und Zeitfunktionen, mit denen erfasst wird, wie lange eine Maschine oberhalb definierter Schwingungsgrenzwerte betrieben wird.

So lassen sich Wartungsmaßnahmen direkt am Sensor zustandsabhängig steuern. Eine Überwachung über die Maschinensteuerung ist häufig nicht mehr erforderlich. Gleichzeitig entfällt die klassische Wartung nach festen Intervallen, wodurch Kosten gesenkt und die Effizienz erhöht werden.

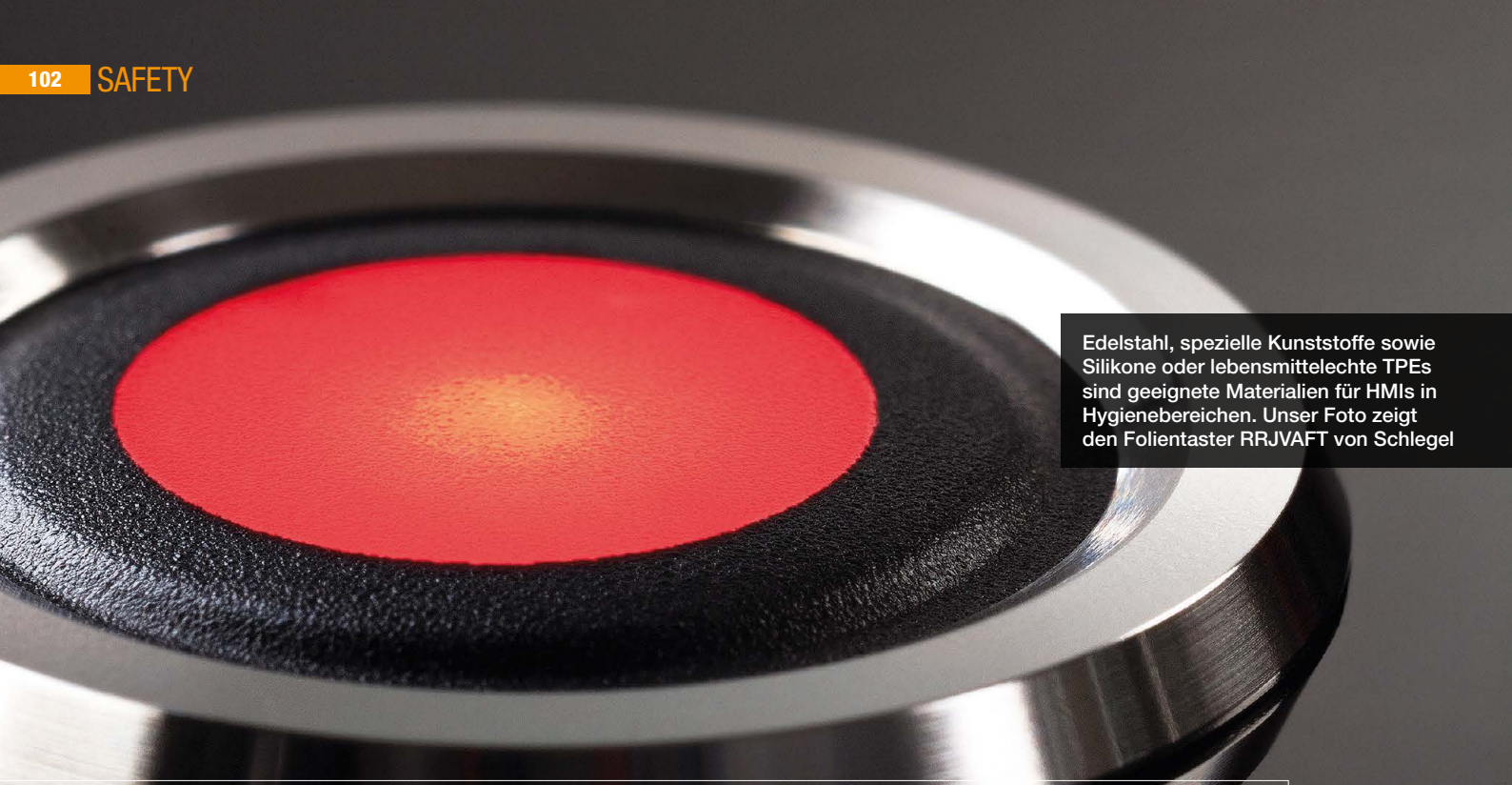
Sicherheit in allen Umgebungen

Die Kombination aus hochauflösender Messtechnik und intelligenter Datenverarbeitung leistet einen wichtigen Beitrag zur industriellen Sicherheit. Früh erkannte Abweichungen verhindern nicht nur kostenintensive Ausfälle, sondern reduzieren auch das Risiko von Folgeschäden oder gefährlichen Betriebszuständen.

Für den Einsatz in explosionsgefährdeten Bereichen oder sicherheitskritischen Anwendungen bietet Pepperl+Fuchs weitere Schwingungsgssensoren: Neben dem bewährten VIM 3 stehen der VIM 6 mit EX-Zulassung sowie der VIM 8 mit EX-Zulassung, SIL2-Zertifizierung und zwei flexibel einstellbaren Schaltausgängen zur Verfügung. GIT

Autor:
Alen Stranjik

Pepperl+Fuchs SE
www.pepperl-fuchs.com/



Edelstahl, spezielle Kunststoffe sowie Silikone oder lebensmittelechte TPEs sind geeignete Materialien für HMIs in Hygienebereichen. Unser Foto zeigt den Folientaster RRJVAFT von Schlegel

HYGIENEKRITISCHE PRODUKTIONSUMGEBUNGEN

Keine Chance für Keime

Wie sich HMI-Systeme und Bedienelemente hygienegerecht und normkonform auslegen lassen.

In hygienesensiblen Produktionsumgebungen entscheiden oft konstruktive Details darüber, ob sich Anlagen zuverlässig reinigen lassen oder Kontaminationsrisiken entstehen. Doch welche Anforderungen ergeben sich daraus für HMI-Systeme und Bedienelemente? GIT SICHERHEIT hat mit Torsten Singer, Produktmanager bei Schlegel, und Jürgen Leng, Business Development Manager bei Schlegel, darüber gesprochen.

GIT SICHERHEIT: Herr Singer, welche besonderen Anforderungen müssen HMI-Systeme und Bedienelemente in Branchen mit hohen Hygieneanforderungen erfüllen, etwa in der Lebensmittelverarbeitung, Getränkeproduktion oder Pharmaindustrie?

Torsten Singer: In hygienekritischen Produktionsumgebungen gelten für HMI-Systeme deutlich strengere Vorgaben als im klassischen Maschinenbau. Im Kern geht es darum, das Risiko einer Kontamination konsequent zu minimieren. Dabei spielen mehrere Faktoren eine Rolle: die konstruktive Gestaltung, die Wahl geeigneter Materialien und die Geometrie der Oberflächen. Auch ergonomische und funktionale Aspekte dürfen nicht vernachlässigt werden.

Was heißt das konkret? Welche konstruktiven Merkmale sind für hygienegerechte Bedienelemente zwingend notwendig?

Torsten Singer: Damit einzelne Bedienelemente oder komplette HMI-Systeme die strengen Vorgaben in Lebensmittel-, Getränke- und Pharmaanwendungen erfüllen, müssen mehrere konstruktive Grundprinzipien berücksichtigt werden. Entscheidend ist zunächst die Materialauswahl: Diese muss korrosionsbeständig, lebensmittelecht und resistent gegenüber aggressiven Reinigungs- und Desinfektionsmitteln sein.

Ein zentraler Punkt ist auch die Gestaltung der Bedienoberflächen. Fugen, Spalten oder raue Flächen sind tabu, weil sich hier Schmutz festsetzen kann. Stattdessen müssen die Oberflächen glatt und geschlossen sein, damit sie problemlos gereinigt werden können – oft sogar unter Hochdruck, mit Heißwasser oder Schaumreinigern. Ein Fehler in der Praxis sind nicht ausreichend geschlossene Übergänge zwischen Bediengerät und Gehäuse. Gerade hier entstehen oft schwer zu reinigende Bereiche, die hygienische Risiken bergen.

Das heißt, hohe Anforderungen an die Dichtheit sind unumgänglich?

Torsten Singer: Absolut. Durchgängige Dichtheit ist unverzichtbar. Hochwertige Dichtsysteme verhindern, dass Feuchtigkeit oder Reinigungsmittel eindringen. Die gängigen Schutzarten IP66, IP67 und IP69K sind also nicht nur Qualitätsmerkmale, sondern zwingende Voraussetzung. Gerade in der Fleischverarbeitung oder Milchindustrie werden Bedienelemente

häufig heiß und mit Hochdruck gereinigt, was enorme mechanische und thermische Belastungen bedeutet.

Bedienelemente müssen zudem ergonomisch und funktional sein: Sie müssen auch mit Handschuhen zuverlässig funktionieren, eindeutiges taktiles oder optisches Feedback liefern und selbst während des laufenden Reinigungsprozesses nicht beeinträchtigt werden. Viele Anlagenbetreiber setzen zusätzlich auf antibakterielle Oberflächen und spezielle Dichtkonzepte, um die Keimbelastung dauerhaft niedrig zu halten.

Welche Materialien eignen sich besonders für Bedienelemente im Hygienebereich und warum?

Torsten Singer: Edelstahl, insbesondere V4A (1.4404/316L), ist hier der Goldstandard. Er ist korrosionsbeständig, lebensmittelecht, mechanisch robust und auch resistent gegen aggressive Reinigungsmittel. Die glatte, polierte Oberfläche verhindert, dass sich Keime in Rissen oder Poren festsetzen können und Schmierfilme bilden.

Auch geeignete Kunststoffe wie PC/ABS oder spezielle PA-Arten werden verwendet, da sie leichter und kostengünstiger herzustellen sind. Silikone oder lebensmittelechte TPEs kommen dort zum Einsatz, wo flexible Komponenten oder Dichtungen benötigt werden. Alle Kunststoffe müssen chemikalienbeständig, temperaturstabil und hydrophob sein sowie die Vorgaben von FDA und EU-Verordnungen erfüllen.

Moderne HMI-Systeme nutzen zunehmend kapazitive Glasfronten. Glas ist porenfrei, leicht zu reinigen und beständig gegen Reinigungsmittel. Mit speziellen antimikrobiellen Beschichtungen lassen sich die Oberflächen zusätzlich hygienisch optimieren. Allerdings ist der Einsatz von Glas im Hygienebereich begrenzt, da in vielen Bereichen mit Handschuhen gearbeitet wird.

Torsten Singer, Produktmanager bei Schlegel

Jürgen Leng, Business Development Manager bei Schlegel

Welche Normen und Richtlinien sind für die Auswahl hygienegerechter HMI-Komponenten besonders relevant?

Jürgen Leng: Wichtig sind Normen und Richtlinien, die Hygienic Design, Materialkonformität, Reinigbarkeit und sichere Bedienung regeln. Zu den wichtigsten zählen:

- DIN EN 1672-2:2021-05 definiert grundlegende Hygieneanforderungen an Maschinen für die Lebensmittelverarbeitung, etwa zu reinigungsgerechtem Design, Oberflächenbeschaffenheit und der Vermeidung von Schmutznischen.

Bitte umblättern ▶

Auch Not-Halt-Schalter, wie der FRVK-POOI von Schlegel, müssen absolut dicht sein, wenn sie in hygienekritischen Bereichen eingesetzt werden

- EHEDG-Richtlinien geben Empfehlungen für hygienegerechtes Design, Materialauswahl und Reinigbarkeit in kritischen Bereichen. Die EHEDG (European Hygienic Engineering and Design Group) entwickelt internationale Standards für die hygienische Konstruktion von Maschinen und Prozessen in der Lebensmittelindustrie.
- DGUV-Vorgaben betreffen Arbeitssicherheit, Ergonomie und sichere Bedienbarkeit von HMIs auch unter hygienischen Bedingungen.
- FDA-Vorschriften (USA) sind relevant für international eingesetzte Anlagen, insbesondere für FDA-konforme Materialien.
- EU-Verordnung 10/2011 enthält Regelungen zu Kunststoffen mit Lebensmittelkontakt und ist damit entscheidend für die Materialwahl in der Lebensmittelproduktion und bei Verpackung.

Wie stellen Sie sicher, dass Ihre Produkte den hohen Anforderungen der Maschinenrichtlinie entsprechen?

Jürgen Leng: Wir gewährleisten die Konformität durch die konsequente Anwendung harmonisierter Normen, klar definierte interne Entwicklungs- und Qualitätsprozesse sowie externe Zertifizierungen. Dazu gehören unter anderem CE-Konformitätsbewertungen, Prüfungen durch unabhängige Stellen wie den TÜV und die Berücksichtigung relevanter Hygieneanforderungen.

Welche Branchen stellen in der Praxis die höchsten Anforderungen an hygienegerechte Bedienelemente?

Torsten Singer: Die höchsten Hygienestandards finden wir eindeutig in der Pharmaindustrie, insbesondere bei aseptischen oder sterilen Produktionsprozessen. Jede Oberfläche und jedes Bedienelement muss so gestaltet sein, dass sie keine potenzielle Kontaminationsquelle darstellt. Hier greifen auch FDA- und GMP-Richtlinien, die extrem klare Anforderungen an Material, Beschaffenheit und Reinigung stellen.

Sehr anspruchsvoll ist auch die Lebensmittelherstellung und -verarbeitung. Neben hohen Hygieneanforderungen stellt die intensive Reinigung mit aggressiven Medien hohe Anforderungen an HMI-Systeme und Bedienelemente.

Unabhängig von der Branche gilt: Überall dort, wo offene Produkte gehandhabt, abgefüllt oder verarbeitet werden, steigen die Anforderungen an Bedienelemente. HMI-Komponenten müssen also nicht nur technisch zuverlässig sein, sondern auch aktiv zur Hygienesicherheit beitragen.

Zusammengefasst: Was müssen Unternehmen bei der Auswahl von Bedienelementen im Hygienebereich beachten?

Torsten Singer: Es geht immer darum, Kontaminationsrisiken zu minimieren und gleichzeitig eine zuverlässige Bedienbarkeit sicherzustellen. Unternehmen sollten daher mehrere Punkte besonders beachten:

- Hygienisches Design: Glatte Oberflächen ohne Fugen oder Schmutzkanten.
- Reinigungsbeständigkeit: Materialien und Dichtsysteme müssen Hochdruck, Heißwasser, Schaumreiniger und aggressive Chemikalien aushalten.
- Praxisgerechte Bedienung: Auch mit Handschuhen oder nassen Händen zuverlässig nutzbar.

Zudem sollten Produkte zertifiziert sein und den gängigen Normen entsprechen, um maximale Sicherheit im hygienischen Produktionsumfeld zu gewährleisten. GIT

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

© Bilder: Schlegel

Die GIT SICHERHEIT ist für uns wichtig, weil sie für eine verlässliche und partnerschaftliche Zusammenarbeit steht und zugleich als Sprachrohr und Multiplikator zentrale Themen unserer Branche sichtbar macht. Sie greift Entwicklungen frühzeitig auf, setzt Impulse und trägt dazu bei, die Sicherheitswirtschaft in ihrer ganzen Vielfalt nach außen zu stärken.

Markus Klaedtke,
Vorstandsvorsitzender BVSW e.V.

35 JAHRE GIT SICHERHEIT

Sicherheitsschaltgerät für EX-Bereiche

Mit dem Sicherheitsrelais PSR-MC35-EXI baut Phoenix Contact sein Safety-Portfolio weiter aus. Das Produkt ermöglicht einen sicheren Betrieb in anspruchsvollen industriellen Umgebungen. Es wurde speziell für den Einsatz in explosionsgefährdeten Bereichen der Zone 2 entwickelt. Darüber hinaus hat das Gerät eine IECEx- und ATEX-Zulassung und erfüllt damit internationale Sicherheitsanforderungen. Das Sicherheitsrelais arbeitet zuverlässig unter herausfordernden Bedingungen. Eine lackierte Leiterplatte schützt vor Korrosion. Der erweiterte Temperaturbereich bis +60 °C erlaubt die Nutzung in zahlreichen Anwendungen der Prozess- und Verfahrenstechnik. Besonders hervorzuheben ist, dass die angeschlossenen Betriebsmittel sogar in Zone 0 (Gas) und Zone 20 (Staub) verwendet werden dürfen. Die kompakte Bauform spart Platz im Schaltschrank. **www.phoenixcontact.com**

Jens Delliehausen wird CSO bei Schmersal

Jens Delliehausen übernimmt die Position des Chief Sales Officer (CSO) bei der K.A. Schmersal GmbH & Co. KG und damit die globale Verantwortung für den Vertrieb. In dieser Funktion wird er die internationale Vertriebsorganisation strategisch weiterentwickeln und neue Wachstumsimpulse setzen. Jens Delliehausen berichtet direkt an den geschäftsführenden Gesellschafter Philip Schmersal sowie Managing Director Michael Ambros. Der 54-Jährige hat ausgeprägte Führungserfahrung im Vertrieb und ist spezialisiert auf die Transformation und Weiterentwicklung von Vertriebsorganisationen, erfolgreiches Change-Management sowie die nachhaltige Stärkung von Marktposition und Vertriebserfolg – national wie international. **www.schmersal.com**

MASCHINEN- UND ANLAGENSICHERHEIT

Cybersecurity in der Praxis: Was Sie jetzt wissen müssen

Bedeutung von MVO und CRA für Risikobeurteilung, OT Security und Dokumentationsprozesse im Maschinenbau

© GIT SICHERHEIT / Wiley VCH

Auf dem Bild v.l.n.r.: Wolfgang Onderka, Experte für funktionale Sicherheit und industrielle Cybersecurity bei Wieland Electric, Franca Hopf, Product Managerin Funktionale Sicherheit bei Wieland Electric und Timo Gimbel, Redakteur bei GIT SICHERHEIT, am Stand von Wieland Electric auf der SPS 2025 in Nürnberg

Mit der neuen Maschinenverordnung (MVO) und dem Cyber Resilience Act (CRA) stellt die Europäische Union die Weichen für ein neues Sicherheitsverständnis im Maschinenbau. Funktionale und digitale Sicherheit wachsen zusammen und werden zu verbindlichen Voraussetzungen für die CE-Kennzeichnung. Damit steigen nicht nur die technischen Anforderungen, sondern auch der Handlungsdruck für Hersteller, Betreiber und Systemintegratoren.

Wie können Maschinenbauer diesen Wandel strukturiert angehen? Welche konkreten Pflichten ergeben sich aus den Regelwerken und wo liegen derzeit die größten Unsicherheiten? Dazu geben Wolfgang Onderka, Experte für funktionale Sicherheit und industrielle Cybersecurity, und Franca Hopf, Product Managerin Funktionale Sicherheit, beide von Wieland Electric, praxisnahe Einblicke. Sie erklären, worauf es bei der Risikobeurteilung speziell im Kontext von Cybersecurity ankommt, wie sich die Dokumentation sinnvoll organisieren lässt und welche Unterstützung Maschinenbauer hierbei von Seiten der Hersteller erhalten können.

GIT SICHERHEIT: Welche konkreten Anforderungen stellt die neue Maschinenverordnung (MVO) an Maschinenbauer im Hinblick auf Cybersecurity und Dokumentationspflichten?

Wolfgang Onderka: Ein zentrales Element der neuen Maschinenverordnung ist der Schutz des sicherheitsrelevanten Programmteils. Es geht dabei nicht um das gesamte Steuerungsprogramm, sondern gezielt um die Absicherung jener Anteile, die sicherheitskritische Funktionen abbilden. Dieser Teil muss vor Manipulation oder unbeabsichtigter Veränderung geschützt werden.

Darüber hinaus fordert die Verordnung ein vollständiges Logging, also die Aufzeichnung aller Änderungen und Aktivitäten, die sich auf den sicherheitsrelevanten Programmabschnitt beziehen. Das schafft Nachvollziehbarkeit und ist ein wesentlicher Bestandteil der Bewertung der Cybersecurity. Die Anforderungen sind ab dem 20. Januar 2027 verpflichtend umzusetzen. Dadurch erhält der Maschinenbau ein gewisses Zeitfenster, zugleich wird aber auch deutlich, dass jetzt gehandelt werden muss.

Franca Hopf: Die MVO bringt insbesondere im Hinblick auf digitale Risiken neue Anforderungen mit sich. Externe Verbindungen – etwa über Netzwerkschnittstellen oder Fernzugriffe – dürfen auf keinen Fall zu einer gefährlichen Situation führen. Kommunikationspfade müssen daher abgesichert oder gegebenenfalls deaktiviert werden, wenn sie sicherheitsrelevante Funktionen beeinflussen können.

Zudem erweitert sich die Risikobeurteilung, denn neben klassischen physischen Risiken müssen künftig auch Cyberbedrohungen systematisch bewertet werden. Bei der Dokumentation gibt es hingegen gewisse Erleichterungen, da digitale Bereitstellung grundsätzlich zulässig ist, allerdings nur unter klar definierten Rahmenbedingungen.

Wie beeinflusst der Cyber Resilience Act (CRA) die Entwicklung und den Betrieb von Maschinen und Anlagen – insbesondere im Hinblick auf OT-Security?

Wolfgang Onderka: Mit dem CRA ist Cybersecurity kein „nice to have“ mehr, sondern Vorschrift. Das hat direkte Auswirkungen auf den Entwicklungsprozess. Bereits in der Konstruktion müssen potenzielle Schwachstellen identifiziert und durch geeignete Maßnahmen abgesichert werden. Dieses Vorgehen folgt dem Prinzip „Secure by Design“, bei dem Sicherheitsaspekte von Beginn an in die Architektur der Maschine integriert werden. Besondere Aufmerksamkeit gilt der Steuerungssoftware. Sie kann nicht länger situativ entwickelt oder verändert werden. Stattdessen verlangt der CRA eine strukturierte Herangehensweise mit dokumentierter Einflussanalyse, Change Management und durchgängiger Nachvollziehbarkeit über alle Versionen hinweg. Ziel ist es, neben der funktionalen Sicherheit auch die digitale Resilienz der Maschine sicherzustellen.

Franca Hopf: Der CE-Konformitätsprozess erweitert sich durch den CRA um eine digitale Dimension. Die Risikobewertung erfolgt nicht einmalig, sondern fortlaufend über den gesamten Lebenszyklus – von der Produktauslegung über den Betrieb bis hin zur Außerbetriebnahme.

Auch im laufenden Betrieb ergeben sich klare Anforderungen. Unternehmen müssen auf schwerwiegende Sicherheitsvorfälle reagieren, diese melden und zu Updates informieren. Das setzt ein kontinuierliches Monitoring der OT-Systeme sowie eine stärkere Verzahnung zwischen IT und OT voraus.

Welche Schritte sollten Maschinenbauer jetzt unternehmen, um die Umsetzung von MVO und CRA echtzeitig zu starten, ohne in Aktionismus zu verfallen?

Wolfgang Onderka: Zunächst einmal ist Besonnenheit wichtig. Statt sich von Schlagzeilen unter Druck setzen zu lassen, sollte man sich strukturiert mit den tatsächlichen Anforderungen der Maschinenverordnung und des Cyber Resilience Act auseinandersetzen.

Ein sinnvoller erster Schritt ist die Analyse des bestehenden Entwicklungsprozesses im Bereich funktionale Sicherheit. Eine systematische Gap-Analyse schafft Klarheit über den Handlungsbedarf und die Prioritäten. Darüber hinaus empfiehlt es sich, ein unternehmensweites Managementsystem für Cybersecurity aufzusetzen, auf dessen Basis Risikoanalysen durchgeführt werden können, deren Ergebnisse wiederum direkt in die Konstruktion und das Softwaredesign einfließen.

Franca Hopf: Bei konkreten Projekten sollte zunächst geprüft werden, ob diese unter die Regelungen des CRA fallen. Danach folgt der frühzeitige Dialog mit den Kunden: Welche Sicherheitsfunktionen werden erwartet, welches Schutzniveau ist erforderlich? Diese Informationen sollten idealerweise bereits in die Spezifikationsphase einfließen. Zudem braucht es eine enge Zusammenarbeit zwischen Konstruktion, IT und Safety, um Anforderungen konsistent umzusetzen.

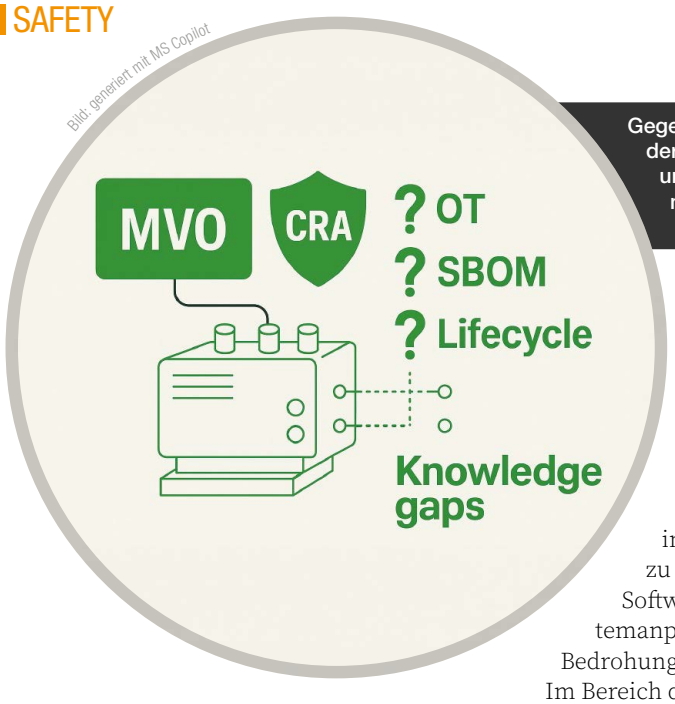
Wo liegen aktuell die größten Wissenslücken bei Maschinenbauern im Bereich OT-Security und Cyber-Resilienz?

Wolfgang Onderka: Viele Unternehmen haben verstanden, dass sie handeln müssen. Was jedoch häufig fehlt, ist das Wissen darüber, wie die Anforderungen konkret umgesetzt werden können. Das betrifft insbesondere die Risikoanalyse, aber auch die Dokumentation. Welche Anforderungen gelten an Struktur, Umfang und Format? Reicht eine sauber geführte Excel-Datei oder braucht es spezialisierte Tools?

Zudem wirft die Forderung nach einer Softwarestückliste (SBOM) viele praktische Fragen auf. Auch rechtliche Verpflichtungen, etwa die Meldepflicht bei aktiv ausgenutzten Schwachstellen, sind nicht überall bekannt oder werden unterschätzt.

Bitte umblättern ▶

Wieland Electric bietet ein umfassendes Weiterbildungsangebot rund um das Thema industrielle Cybersecurity an – viele der Kurse sind sogar kostenlos



Gegenwärtig steht der Maschinenbau vor der Frage, wie die Anforderungen aus MVO und CRA konkret umgesetzt werden können – insbesondere mit Blick auf die Risikoanalyse und die Dokumentation

Franca Hopf: Oft fehlt noch das Denken im vollständigen Lebenszyklus. Cybersecurity wird noch zu häufig punktuell betrachtet, obwohl sie ein durchgängiges Thema ist und kein einmaliges Projekt.

Wie unterstützt Wieland Electric Maschinenbauer bei der Bestandsaufnahme, Risikobeurteilung und Dokumentation?

Wolfgang Onderka: Wir unterstützen Unternehmen dabei, einen strukturierten und konformen Prozess aufzusetzen, der alle relevanten Anforderungen beinhaltet. Dabei helfen wir nicht nur bei der Frage, was zu tun ist, sondern kümmern uns auch um das Wie und den richtigen Zeitpunkt.

Ein Schwerpunkt liegt in der Risikobeurteilung. Wir begleiten die Unternehmen dabei, geeignete Herangehensweisen zu finden und sinnvoll in bestehende Prozesse zu integrieren, etwa bei Softwareänderungen, Systemanpassungen oder neuen Bedrohungsszenarien.

Im Bereich der Dokumentation bieten wir keine Einheitslösung, sondern orientieren uns an den internen Strukturen des Kunden. Entscheidend ist, dass Inhalt und Nachvollziehbarkeit stimmen und die Dokumentation über den gesamten Lebenszyklus hinweg anpassbar bleibt.

Wie sieht das Zusammenspiel von MVO und CRA in der Praxis aus?

Wolfgang Onderka: Die Maschinenverordnung fokussiert sich auf den Schutz des Menschen vor der Maschine. Der CRA betrachtet die Situation aus dem umgekehrten Blickwinkel und zielt auf den Schutz der Maschine vor Eingriffen. In beiden Fällen müssen die identifizierten Bedrohungen reduziert werden, häufig mit denselben Maßnahmen.

Dabei gilt eine klare Regel: Safety vor Security. Maßnahmen zur Cybersecurity dürfen niemals die funktionale Sicherheit beeinträchtigen.

Franca Hopf: Beide Regelwerke fordern eine nachvollziehbare, dokumentierte Risikobeurteilung. Bereits vor der Konstruktion müssen Risikoanalysen durchgeführt werden, aus denen Sicherheitskonzepte, technische Dokumentation und Prozesse zum Schwachstellenmanagement abgeleitet werden. So entsteht eine gemeinsame Linie über den gesamten Maschinenlebenszyklus.

Welche konkreten Produkte und Lösungen von Wieland kommen im Zusammenhang mit der Maschinenverordnung (MVO) und dem Cyber Resilience Act (CRA) typischerweise zum Einsatz?

Wolfgang Onderka: SamosPro, unsere modulare und programmierbare Sicherheitssteuerung mit intuitiver Software, ist so konzipiert, dass zentrale Anforderungen aus MVO und CRA bereits unterstützt werden, etwa Zugriffskontrolle, Absicherung sicherheitsrelevanter Softwarebestandteile und die Nachvollziehbarkeit von Änderungen.

Darüber hinaus verfolgen wir das Ziel, Maschinenbauer zu befähigen, zentrale Aufgaben wie Risikoanalysen, Softwarestücklisten und Dokumentation eigenständig umzusetzen.

Franca Hopf: Neben den Produktlösungen bieten wir zum aktuellen Zeitpunkt ein umfassendes Weiterbildungsangebot rund um industrielle Cybersecurity, vieles davon sogar kostenlos. Dazu zählen zum Beispiel kurzweilige Webinare zu Cybersecurity-Grundlagen, zur Umsetzung des Cyber Resilience Act, zur Norm IEC 62443 sowie zur Durchführung von Risikoanalysen gemäß MVO und CRA.

Ein wichtiger Bestandteil ist die Erstberatung. Viele Unternehmen benötigen zunächst eine fundierte Einordnung, um das Thema strukturiert anzugehen. Oft ist diese Sensibilisierung bereits der entscheidende Schritt, um intern Prozesse und Verantwortlichkeiten zu klären und genau hier setzen wir als Experten an. GIT

Wieland Electric GmbH
www.wieland-electric.com

Oliver Winzenried (r.) und Professor Dr. Jörn Müller-Quade im Gespräch in den Räumen von Wibu-Systems in Karlsruhe

Wibu-Systems beruft Professor Dr. Jörn Müller-Quade in den Aufsichtsrat

Die Wibu-Systems AG hat Professor Dr. Jörn Müller-Quade in ihren Aufsichtsrat berufen. Damit wurde die strategische Aufsicht des Unternehmens in den Bereichen Kryptografie, sicheres Computing und langfristige digitale Resilienz weiter gestärkt. Diese Entscheidung ist das Ergebnis einer langjährigen Zusammenarbeit, die auf dem gemeinsamen Ziel basiert, Sicherheitsarchitekturen zu entwickeln, die sowohl wissenschaftlich fundiert als auch operativ umsetzbar sind. Dr. Jörn Müller-Quade genießt international hohes Ansehen für seine Arbeit in den Bereichen Kryptografie und IT-Sicherheit. Seine Forschungsarbeiten umfassen sicheres Cloud Computing, sichere Mehrparteienberechnungen, formale Sicherheitsdefinitionen und Sicherheitsmodelle sowie hardwarebasierte Vertrauensanker. Dies sind Disziplinen, die für den Schutz von Software, geistigen Eigentums und digitaler Infrastrukturen in kontrollierten und unsicheren Umgebungen zunehmend an Bedeutung gewinnen.

www.wibu.com

Jan Gundermann, Managing Director Germany, Blåkläder Deutschland

© Blåkläder

PSA

Workwear, die weiterdenkt

Von Eigenproduktion, Material-Updates und der Frage, was moderne PSA wirklich leisten muss

Die Anforderungen an moderne Workwear und PSA steigen – ebenso wie der Druck auf Lieferketten, Materialinnovationen und nachhaltige Produktionsweisen. Blåkläder gehört zu den Unternehmen, die diese Entwicklungen seit Jahren aktiv mitgestalten. Im Gespräch gibt Jan Gundermann Einblicke in die Strategien, Entscheidungen und Trends, die seine Branche prägen: von Eigenproduktion und Zertifizierungsprozessen über neue Materialqualitäten bis hin zu internationalen Impulsen und der Rolle familiengeführter Strukturen. Ein Interview, das zeigt, wie vielschichtig der Weg zu funktionaler und verantwortungsvoller Arbeitskleidung heute ist.

GIT SICHERHEIT: Herr Gundermann, zur DNA von Blåkläder gehört es, möglichst viel der Wertschöpfung selbst zu kontrollieren – u. a. durch eigene Werke in Asien und kurze, transparente Lieferketten. Wieviel Prozent der Waren entstehen aus Eigenproduktion und welche Vorteile bietet das für Ihre Kunden?

Jan Gundermann: Rund 95 % unserer Produkte fertigen wir in eigenen Werken in Asien. Auch unser komplettes Schuhsortiment stammt aus eigener Produktion. Darauf sind wir besonders stolz, denn wir haben uns bewusst gegen Lohnfertigung entschieden. Wir wollen wissen, unter welchen Bedingungen produziert wird, welche Materialien eingesetzt werden und wie jeder einzelne Prozessschritt aussieht.

Für unsere Kunden zahlt sich das in mehrfacher Hinsicht aus. Zum einen sichern wir eine sehr hohe Warenverfügbarkeit, weil wir Kapazitäten langfristig planen und steuern können. Zum anderen gewährleisten wir eine gleichbleibend hohe Qualität. Wer bei uns bestellt, weiß, was er bekommt, völlig unabhängig von Saison oder Marktlage. In Zeiten fragiler Lieferketten ist diese Stabilität ein entscheidender Vorteil.

Ihre Produktionsstandorte sind u. a. Step by OekoTex zertifiziert; einzelne Werke wurden sogar nach LEED ausgezeichnet. Welche Voraussetzungen mussten für diese Zertifizierungen vorliegen?

Jan Gundermann: Die Zertifizierungen spiegeln sehr gut wider, wie wir Produktion verstehen. Bei LEED, also dem international anerkannten Standard für nachhaltige Gebäude, müssen grundlegende Standards erfüllt sein. Dazu gehört, dass sich ein Projekt an einem festen Standort befindet, klar definierte Projektgrenzen einhält und bestimmte Mindestanforderungen an Größe und Infrastruktur erfüllt. Darüber hinaus spielen Kriterien wie Energieeffizienz, Ressourcenschonung und nachhaltige Bauweise eine zentrale Rolle.

Die Step-by-Oeko-Tex-Zertifizierung geht noch stärker auf die Produktionsprozesse selbst ein. Sie bewertet unter anderem das Chemikalienmanagement, die Umweltleistung eines Standorts sowie soziale Verantwortung und Qualitätsmanagement. Gesundheit und Sicherheit der Mitarbeitenden sind ebenfalls ein zentrales Kriterium.

Für uns sind solche Zertifizierungen wichtig, weil sie unsere eigenen Ansprüche an eine verantwortungsvolle Produktion objektiv überprüfbar machen. Sie stellen sicher, dass ökologische Standards, sichere Arbeitsbedingungen und transparente Prozesse in unseren Produktionsstätten dauerhaft eingehalten werden.

Auf der A+A 2025 hat Blåkläder u. a. die Weiterentwicklung seiner Multinorm-Orange-Gewebe vorgestellt. Woher kam der Impuls für diese Weiterentwicklung und welche konkreten Vorteile bietet das neue Gewebe mit Blick auf die Nachhaltigkeit?

Jan Gundermann: Der Impuls kam aus dem Markt. Unsere Händler und Endkunden haben eine steigende Nachfrage nach leistungsfähigeren, gleichzeitig komfortablen Multinorm-Lösungen signalisiert. Solche Rückmeldungen geben den Impuls zur Produktentwicklung.

Mit der neuen Qualität 1524 ist uns ein deutlicher Schritt nach vorn gelungen. Das Material zeigt in Trageversuchen kein Fädenziehen und bleibt dadurch länger optisch und funktional intakt. Der erhöhte Polyesteranteil ist mit einer Flammschutzfunktion kombiniert. Gleichzeitig ist das Gewebe für Industriewäsche nach EN 15797 zugelassen und erfüllt die E2-Anforderungen im Bereich geschmolzenes Eisen und Stahl. Mit einem Gewicht von 315 Gramm pro Quadratmeter verbindet es Robustheit mit hohem Tragekomfort. Genau diese Balance entscheidet darüber, ob Schutzkleidung im Alltag akzeptiert und gerne getragen wird.

Blåkläder ist seit 1959 familiengeführt. Wie prägt diese Eigentümerstruktur Ihre langfristigen Entscheidungen – etwa bei Lagerhaltung/Bevorratung, Investitionen in Werke oder bei „Nein"-Entscheidungen zugunsten von Langlebigkeit statt kurzfristigem Umsatz?

Jan Gundermann: Als familiengeführtes Unternehmen denken wir nicht in Quartalszahlen, sondern in Generationen. Diese Perspektive prägt unsere Entscheidungen. Wir investieren in unsere Werke, in Lager-

kapazitäten und in die Weiterentwicklung unserer Produkte, ohne dabei kurzfristigen Renditeerwartungen zu folgen.

Das Eigentümerverständnis ist stark im operativen Geschäft verankert. Man kennt die Anforderungen der Händler ebenso wie die Bedürfnisse der Anwender. Investitionen sind deshalb immer auf das Kerngeschäft ausgerichtet und langfristig angelegt. Stabilität und Verlässlichkeit sind für uns keine Schlagworte, sondern Grundlage unseres Handelns.

Viele der Marktteilnehmer im Workwear- und PSA-Bereich treiben die Markenbildung auf dem deutschen und europäischen Markt stark voran. Wie positioniert sich Blåkläder in diesem Wettbewerb?

Jan Gundermann: Unsere Positionierung ergibt sich aus unsrem Werteverständnis. Qualität und Langlebigkeit stehen an erster Stelle. Unsere Produkte sind für anspruchsvolle Arbeitsumfelder konzipiert und müssen dort dauerhaft bestehen.

Gleichzeitig legen wir großen Wert auf Funktionalität. Ergonomische Schnitte, Stretch-Materialien oder verstärkte Nähte sind elementarer Bestandteil unserer Entwicklung. Nachhaltigkeit verstehen wir als logische Konsequenz aus Qualität und Verantwortung. Design dient nicht als Selbstzweck: Es geht uns um attraktive Lösungen, die Individualität ermöglichen. Jede unserer Kollektionen bietet eine Vielzahl an Farbkombinationen, sodass Unternehmen und Träger genau die Lösung finden, die funktional überzeugt und zugleich zur eigenen Identität passt.

Wir richten uns an professionelle Anwender mit hohen Anforderungen – im Handwerk ebenso wie in Bau, Industrie, Automotive, Service oder Logistik. Auch der Bereich Women's Workwear gewinnt zunehmend an Bedeutung, weil sich die Arbeitswelt spürbar verändert.

In Skandinavien ist Blåkläder im Bereich PSA in einer marktführenden Position. Internationalisierung ist daher ein wichtiger Baustein, um als Unternehmen weiter zu wachsen. Welche Märkte sind hierbei besonders von Interesse und welche Vorteile bietet die Internationalisierung z. B. den Kunden in Deutschland?

Jan Gundermann: Wir sind in 27 Ländern auf drei Kontinenten aktiv und beobachten die internationalen Märkte sehr genau. Aktuell richten wir ein besonderes Augenmerk auf den SOD-Markt, also die Region „South of Denmark", sowie auf Nordamerika mit Kanada und den USA. Gleichzeitig verlieren wir unsere etablierten Heimatmärkte nicht aus dem Blick.

Die internationale Präsenz bringt wertvolle Impulse. Erfahrungen aus unterschiedlichen Branchen und Regionen fließen in unsere Produktentwicklung und unsere Prozesse ein. Dieses gebündelte Know-how kommt letztlich allen Kunden zugute, auch denen in Deutschland. Internationalisierung bedeutet für uns nicht nur Wachstum, sondern auch kontinuierliches Lernen.

Ebenfalls auf der A+A 2025 hat Blåkläder mit dem ToolRig eine Taschenlösung vorgestellt, die in den skandinavischen Ländern seit vielen Jahrzehnten zum Alltag des Handwerks gehören, in Deutschland bisher aber kaum Einzug gehalten haben. Was ist das Kundennutzen-Versprechen und wie sieht der Rollout in Deutschland aus?

Jan Gundermann: In Deutschland startet der Rollout Ende des ersten Quartals, unter anderem mit einer Präsentation auf der Holz-Handwerk-Messe. Die Warenverfügbarkeit ist für Mai vorgesehen.

Das System ermöglicht eine flexible Positionierung der Taschen rund um den Körper und schafft so mehr Ergonomie und Effizienz bei der täglichen Arbeit. Gleichzeitig lassen sich die Module auch außerhalb der Kleidung einsetzen, etwa im Fahrzeug oder an der Werkbank. ToolRig versteht sich als durchdachte Systemlösung, die Arbeitsabläufe erleichtert und körperliche Belastungen reduziert.

Wohin entwickelt sich der Workwear-/PSA-Markt in Deutschland & Europa aus Ihrer Sicht? Und welches Positionierungs-Statement geben Sie Blåkläder für die nächsten drei Jahre mit?

Jan Gundermann: Der Markt ist derzeit anspruchsvoll und stark umkämpft. Gleichzeitig steigen die Erwartungen an Qualität, Nachhaltigkeit und Lieferfähigkeit deutlich. Unternehmen suchen verlässliche Partner, die nicht nur Produkte liefern, sondern langfristige Lösungen anbieten.

Unser Ziel ist es, weiter zu wachsen und unsere Rolle als einer der international führenden Anbieter im Bereich Workwear und PSA konsequent auszubauen. Dabei bleiben wir unserem Grundverständnis treu: kompromisslose Qualität, kontrollierte Wertschöpfung und eine klare Verantwortung gegenüber Kunden, Mitarbeitenden und Umwelt. GIT

Blåkläder Deutschland GmbH
www.blaklader.de

Vom Sicherheitsschuh zum Lifestyle-Produkt – die neuen Retro-Modelle von Elten sind nicht von klassischen Sneakern zu unterscheiden, bieten aber Sicherheit in den Schutzklassen S1 und S1PS

Hendrik van Elten gehört zur fünften Generation der Familie van Elten. Seit Januar 2025 bringt er sich aktiv in die Weiterentwicklung des Unternehmens ein und arbeitet dabei eng mit seinem Vater Heiner van Elten zusammen. Voraussichtlich Mitte 2027 wird er in seine Fußstapfen treten und die Geschäftsführung übernehmen

SICHERHEITSSCHUHE

„Mutig bleiben, ohne leichtfertig zu werden“

Elten im Wandel zwischen Familienwerten und Internationalisierung

Mit dem Einstieg der fünften Generation steht Elten vor einem neuen Kapitel. Hendrik van Elten spricht im Interview über den Generationenwechsel im Familienunternehmen, internationale Wachstumsstrategien und den Anspruch, Tradition, Unternehmenskultur und Mut zu bewahren. Im Fokus stehen zudem veränderte Anforderungen an Sicherheitsschuhe, die stärkere Markenpositionierung sowie die Rolle von Digitalisierung und KI bei der Weiterentwicklung von Prozessen und Produkten.

GIT SICHERHEIT: Herr van Elten, Sie steigen in Ihr wirtschaftlich sehr erfolgreiches Familienunternehmen ein. Empfinden Sie das als Rückenwind oder als Erwartungsdruck, das Niveau weiter auszubauen?

Hendrik van Elten: Eine starke wirtschaftliche Basis erzeugt Erwartungen, aber auch Möglichkeiten Dinge auszuprobieren. Ich empfinde das mehr als Ansporn und große Chance. Wir haben damit die Möglichkeit, Elten von einem nationalen zu einem europäischen Marktführer auszubauen. Mein Großvater hat den Großteil unserer Produkte an die Kohle- und Stahlindustrie in NRW verkauft. Mein Vater an diverse Industrien wie Automobil und Logistik in Deutschland. Nun wollen wir noch weiter diversifizieren, auch über Europa hinaus. Mit einem stabilen Fundament im Rücken ist das für mich eher Rückenwind als Druck. In dem Prozess möchte ich mutig bleiben, ohne leichtfertig zu werden.

Wie haben Sie den Generationenwechsel bisher erlebt – und was war für Sie persönlich die größte Herausforderung in diesem Prozess?

Hendrik van Elten: Die Zusammenarbeit funktioniert sehr gut und harmonisch. Man lernt voneinander, gibt sich gegenseitig neue Impulse und diskutiert positiv über Veränderungen. Mein Vater und ich arbeiten sehr gut zusammen. Ich sehe es schließlich als Aufgabe eines Fami-

lienunternehmens, auf den Erfolg der vorherigen Generationen aufzubauen. Wenn mein Vater sich in einigen Jahren noch in der Ausrichtung des Unternehmens wiederfinden kann, bewerte ich den Generationenwechsel als erfolgreich. Die größte Herausforderung sehe ich darin, das Vertrauen der Mitarbeitenden zu gewinnen. Aber ich denke, ich bin auf einem guten Weg. Wenn das Team, das für die bisherige Entwicklung unseres Unternehmens verantwortlich ist, auch künftig den Weg mitgeht und sich darin wiederfindet, sehe ich das als große Bestätigung.

Aus dem niederrheinischen Uedem in die Welt – Hendrik van Elten möchte das Familienunternehmen vom deutschen zum europäischen Marktführer ausbauen und sogar über die europäischen Grenzen hinauswachsen

Sie haben vor Ihrem Einstieg bei Elten u. a. vier Jahre beim Start-up Flink gearbeitet. Welche Impulse aus dieser Zeit bringen Sie nun in ein traditionsreiches Unternehmen ein?

Hendrik van Elten: Ich habe mitgenommen, wie wichtig es ist, Unternehmensprozesse regelmäßig zu hinterfragen und zu optimieren, um auf Marktveränderungen zu reagieren. Aber ich habe im Start-up auch gesehen, was ich hier nicht haben möchte: eine hohe Mitarbeiterfluktuation. Nach vier Jahren war ich bei Flink einer der Mitarbeiter mit der längsten Unternehmenszugehörigkeit. Bei Elten hingegen begleiten uns viele Mitarbeiter ihr ganzes Berufsleben und darüber hinaus. Teilweise bringen sie die nächste Generation mit ins Unternehmen. Diese Kultur will ich unbedingt beibehalten.

Wo sehen Sie das größte Wachstumspotenzial für Sicherheitsschuhe „Made by Elten“?

Das leichte Modell Tavixx XXFE lime-blue Low ESD S1 bringt weniger als 400 Gramm auf die Waage

Hendrik van Elten: Gerade der skandinavische Markt ist interessant für uns, dort bauen wir unser Vertriebsteam aus. Auch in Großbritannien sind wir aktiver als vor einigen Jahren. Ich sehe auch Potenzial, weiter über die europäischen Grenzen hinaus zu wachsen. Wir arbeiten schon seit mehreren Jahren exklusiv mit einem Handelspartner in Australien zusammen. Spannend finde ich auch den asiatisch-pazifischen Raum. Dort gibt es Märkte, die Wachstumspotenzial haben und mittlerweile auch ein Preisniveau, das passt. Und wer weiß, vielleicht wird in vier Jahren sogar der US-Markt wieder interessant.

Wir müssen stets die Trends der Branche im Blick behalten und unser Portfolio entsprechend anpassen. Allein durch die Internationalisierung kommen neue Herausforderungen auf uns zu. Schon in Großbritannien stellt sich der Kunde einen anderen Sicherheitsschuh vor als in Deutschland.

Wer sind heute die Hauptabnehmer Ihrer Produkte – und wie haben sich deren Anforderungen weiterentwickelt?

Hendrik van Elten: Eine der wichtigsten Branchen ist die Logistik- und Dienstleistungsbranche. Aber auch Bereiche wie die Rüstungsindustrie oder den technischen Dienst wollen wir stärker in den Fokus nehmen. Dabei bleibt der Technische Handel unser Hauptabnehmer. Er ist Touchpoint und Schnittstelle für den Endkunden. Das Produktportfolio kombiniert mit der Expertise des Handels ist für uns und die Kunden entscheidend. Gleichzeitig brauchen große Unternehmen oft komplette Versorgungskonzepte, weshalb der Austausch im Key Account wichtiger geworden ist. Auch der direkte Verkauf an die Endkunden über unseren Online-Store ist ein Vertriebsweg, den man heutzutage gehen muss.

Bitte umblättern ▶

Mit seinen Fußschutzkonzepten und technologischen Innovationen möchte sich Elten künftig noch internationaler aufstellen. Das abgebildete Modell Renzo Biomex GTX Boa blue Mid ESD S3 hilft, Umknickunfälle zu verhindern

Bei den Anforderungen sehe ich drei große Trends. Erstens: mehr Individualität zum Beispiel durch orthopädische Einlagesysteme oder Mehrweiten. Wir bieten seit einigen Jahren die 3-D Fußvermessung inklusive orthopädischer Beratung, um auf Fußfehlstellungen reagieren zu können. Das wirkt den Problemen des Trägers entgegen, reduziert aber auch Fehlzeiten.

Der zweite Trend ist die Vermischung von Freizeit- und Arbeitsschuhen. Viele unserer Kunden sind mehrere Kilometer täglich zu Fuß unterwegs. Da zählen vor allem Leichtigkeit und Komfort. Und das Design, denn der Sicherheitsschuh wird immer mehr zum Lifestyle-Produkt. Daher verwenden wir Materialien, die auch im Laufschuhbereich eingesetzt werden wie zum Beispiel die Dämpfungsmaterialien Super Critical Foaming oder Infinergy von BASF.

Zuletzt begleitet uns auch das Thema Kostenreduzierung bei unseren Kunden. Da ist es unsere Aufgabe, bestmöglich auf den Kunden zu reagieren. Ich bin sicher, dass die Langlebigkeit der Schuhe und geringe Ausfallzeiten der Mitarbeiter am Ende den größten Beitrag zur nachhaltigen Kostensenkung darstellen.

Welche Mehrwerte erwarten Sie durch den Einsatz von KI in der Prozessoptimierung?

Hendrik van Elten: KI spielt vor allem dort eine Rolle, wo wir repetitive Aufgaben automatisieren können – weniger in der Produktion, eher in der Verwaltung und im Vertrieb. Sie hilft, Bedarfe früher zu erkennen, Beratungen zu personalisieren und Datenanalysen zu vereinfachen. Die eingesparte Zeit können wir dann für wertvolle Interaktionen mit unseren Geschäftspartnern nutzen. Außerdem kann sich das bestehende Personal stärker spezialisieren und damit zusätzliche Mehrwerte für die Kunden schaffen. So können wir Mitarbeitern auch die Möglichkeit geben, sich weiterzuentwickeln und den Weg der Internationalisierung aktiv mitzugestalten

Eines ihrer zentralen Anliegen, ist die stärkere Etablierung von Elten als Marke. Zudem soll die Wiedererkennbarkeit der Produkte gestärkt werden. Was bedeutet das konkret?

Hendrik van Elten: Für mich bedeutet das vor allem, dass Elten als Marke klarer erkennbar wird – nach innen und nach außen. Wir wollen eine Designsprache etablieren, die unsere Qualität, Technologie und Verlässlichkeit sichtbar macht. Unsere Produkte sollen auf den ersten Blick zeigen, wofür wir stehen: moderne Sicherheitsschuhe, die funktional, komfortabel und hochwertig sind. Dafür schärfen wir unsere Linien, arbeiten an einer konsistenten Produktidentität und investieren in eine Markenwelt, die zu den Ansprüchen moderner Anwender passt. Der Kunde soll unsere Schuhe nicht nur wegen der Schutzklasse wählen, sondern weil er die Marke wiedererkennt und sich bewusst dafür entscheidet.

Elten blickt auf über 115 Jahre Unternehmensgeschichte zurück. Was waren die wichtigsten Meilensteine des Unternehmens und stehen wir aus Ihrer Sicht aktuell an einem neuen Wendepunkt in der Entwicklung?

Hendrik van Elten: Wenn man auf über 115 Jahre Unternehmensgeschichte schaut, waren die wichtigsten Meilensteine immer die Momente, in denen wir uns neu ausgerichtet haben. Ganz am Anfang standen unsere ersten Arbeitsschuhe aus Leder. Später haben wir lange Zeit auch Herren, Damen- und Kinderschuhe gefertigt, bevor wir uns Ende der 1970er Jahre bewusst auf Sicherheitsschuhe spezialisiert haben.

Ein weiterer Moment war 2011 die Einführung der L 10 Serie, unserer ersten Sicherheitsschuhe im Sneaker Style. Sie sahen aus wie Chucks – hiermit haben wir etwas gewagt, was es so im Markt nicht gab. Vielen Menschen haben wir so gezeigt, dass Sicherheitsschuhe nicht nur schützen, sondern auch gut aussehen können.

Mein Großvater hat den Großteil unserer Schuhe in den Bergbau geliefert, mein Vater später in die Automobil- und Logistikbranche. Und jetzt stehen wir wieder an einem Wendepunkt: Internationalisierung, Digitalisierung und der demografische Wandel verändern unsere Branche. Wir halten an unseren Werten Qualität und Verlässlichkeit und dem Standort Uedem fest – bleiben aber flexibel und mutig. Wenn wir diesen Balanceakt schaffen, also die Geschwindigkeit der heutigen Zeit mit der Sorgfalt eines Familienunternehmens zu verbinden, dann haben wir große Chancen. Dies möchte ich nun gestalten. GIT

Elten GmbH
https://elten.com

Infrastrukturprojekt Rheinbrücke Leverkusen an der A1 zwischen Köln und Düsseldorf

Service-Lift-Lösung für neue Rheinbrücke

Sicherheit, Ergonomie und Effizienz standen im Mittelpunkt des Beitrags von Hailo Professional zu einem wichtigen Infrastrukturprojekt in Deutschland: der Rheinbrücke Leverkusen, die als Teil der stark frequentierten A1 ein Schlüssel zur Entlastung des Verkehrsraums zwischen Köln und Düsseldorf ist.

Nachdem die alte Brücke dem Verkehrsaufkommen nicht mehr gewachsen war, begann im Jahr 2017 der Bau einer neuen Rheinüberquerung, zu der Hailo acht individuell angepasste Service-Lifte beigesteuert hat. Sie ermöglichen den sicheren, ergonomischen Zugang zu den rund 80 Meter hohen, 17 Grad geneigten Pylonen – und sind damit zentraler Bestandteil des Wartungs- und Sicherheitskonzepts der Brücke.

Das Projekt brachte eine Reihe an Herausforderungen mit sich. So mussten die Lift-Lösungen des Herstellers auf die Besonderheiten des Projekts angepasst und während des laufenden Autobahnbetriebs in die komplexe Bauwerksgeometrie integriert werden.

Lösung für außergewöhnliche Geometrien

Zum Einsatz kommen acht Service-Lifte des Typs TOPLift HP-L2, jeweils vier Stück pro Pylon. Aufgrund der sich verjüngenden Bauform wurde ein zweistufiges Konzept realisiert: In jeder Pylonseite überwindet ein unterer Lift 35 Meter, ein oberer weitere 25 Meter. Auf 35 Metern Höhe befindet sich ein Umstieg. Die Anlagen sind für zwei Personen und Material mit einer Tragfähigkeit von 250 Kilogramm ausgelegt.

Die Besonderheit: Die Pylone verlaufen dauerhaft in einem Winkel von 17 Grad. „Das bedeutet, dass sämtliche Führungen, Seile, Halterungen und Kabelführungen speziell angepasst und getestet werden mussten“, erläutert Sascha Rübsamen, Leiter Konstruktion bei Hailo Professional. „Auch die Leitern, an denen die Lifte geführt werden, verlaufen schräg. Das ist in dieser Form außergewöhnlich.“

Während die technische Basis auf einem bewährten System beruht, wurde die Lösung für diese besondere Geometrie umfassend individualisiert. Neben moderner Steuerungs- und Überwachungstechnik umfasst das Konzept eine parallele Fluchtleiter mit Steigschutzsystem. Die geschlossenen Kabinen sind mit einer kontrollierten Fahrtüberwachung, überwachten Türverriegelungen sowie Notausstieg ausgestattet.

Sicherheit und Effizienz im Wartungsalltag

Für Hailo steht dabei nicht nur die technische Machbarkeit im Fokus, sondern vor allem die Sicherheit der Wartungsteams. „Moderne Instandhaltung ist weit mehr als ein Mensch mit Werkzeug und Leiter“, betont Frank Frey, Geschäftsbereichsleiter Hailo Professional. „Ein Service-Lift ermöglicht es, in wenigen Minuten ausgeruht und mit Material in 80 Meter Höhe zu sein. Das reduziert Unfallrisiken erheblich und steigert zugleich die Effizienz.“ Die Anlagen können im Hol- und Sendebetrieb genutzt und ferngesteuert werden. Damit lassen sich Materialtransporte und Wartungsabläufe flexibel organisieren – ein deutlicher Mehrwert gegenüber rein leiterbasierten Zugangslösungen. **www.hailo-professional.de**

PSA

Sicherheit mit Hand und Fuß

Wie Ejendals Hand- und Fußschutz unter regulatorischem Druck, Lieferkettenrisiken und Nachhaltigkeitszielen weiterentwickelt

Multiple Krisen, volatile Lieferketten und steigende regulatorische Anforderungen prägen derzeit auch den Markt für persönliche Schutzausrüstung (PSA). Mit einem großen Team im DACH-Raum (Deutschland, Österreich, Schweiz), eigenen Laboren, Lösungen der Marken und einer klaren Zielsetzung positioniert sich das Ejendals als verlässlicher Akteur im Bereich persönlicher Schutzausrüstung (PSA). Im Zentrum steht dabei der Anspruch, Verletzungen an Händen und Füßen systematisch zu vermeiden.

Die neue S3S-Modelle Jalas Tempus 5705, 5725 und 5715 setzen bei den Obermaterialien auf Cordura recor, einem Gewebe aus recyceltem Polyester, ergänzt durch PFAS freie wasserabweisende Ausrüstungen

Ejendals ist ein familiengeführtes Unternehmen in dritter Generation und fokussiert sich auf Schutzlösungen für Hände und Füße. Die Vision „Zero injuries to hands and feet" beschreibt den Anspruch, Arbeitsunfälle an diesen besonders gefährdeten Körperstellen zu reduzieren – für Mitarbeitende, Unternehmen und die Gesellschaft insgesamt. Vier Werte – Kundenfokus, kontinuierliche Verbesserung, Langfristigkeit und Respekt – prägen nach eigenen Angaben Entscheidungen entlang der gesamten Wertschöpfungskette, vom Produktdesign über die Lieferkette bis zur Zusammenarbeit mit Handelspartnern.

In der DACH-Region verfügt Ejendals über ein umfangreiches Team aus Vertrieb, technischem Service und Schulung. Diese enge Verzahnung ermöglicht eine Betreuung, die von der Gefährdungsbeurteilung (systematische Analyse von Unfall- und Gesundheitsrisiken am Arbeitsplatz) bis zur passenden Produktauswahl reicht.

Forschung, Labor-Kompetenz und Krisenfestigkeit

Trotz geopolitischer Spannungen, instabiler Lieferketten und wirtschaftlicher Unsicherheiten zeigt sich der Markt für persönliche Schutzausrüstung vergleichsweise stabil, da Arbeitssicherheit eine grundlegende Voraussetzung für den Betrieb vieler Unternehmen ist. Ejendals investiert weiterhin in Forschung und Entwicklung, unter anderem in eigene Entwicklungs- und Chemikalienlabore.

„Wir bei Ejendals sind überzeugt, dass Nachhaltigkeit ein langfristiges Geschäftsmodell voraussetzt – und dass Weiterentwicklung dort entsteht, wo Qualität, Sicherheit und Umweltanforderungen gemeinsam betrachtet werden", sagt Werner Schwarzberger, Regional Sales Director DACH.

Die unternehmenseigenen Labore in Leksand sowie der erweiterte Analytikbereich in Jokipii ermöglichen Material- und Chemikalientests im eigenen Haus. Das unterstützt eine zügige Produktentwicklung und hilft, regulatorische Anforderungen zu erfüllen, etwa im Zusammenhang mit der geplanten Einschränkung von PFAS (per- und polyfluorierte Alkylsubstanzen).

Nachhaltigkeit als Bestandteil der Produktentwicklung

Nachhaltigkeit ist bei Ejendals strukturell verankert. Grundlage ist eine doppelte Wesentlichkeitsanalyse nach CSRD und ESRS (EU-Vorgaben zur Nachhaltigkeitsberichterstattung), mit Schwerpunkten wie Gesundheit und Sicherheit, Ethik, Innovation, Energieeffizienz, Chemikalienmanagement und Klimaziele.

Bei den Sicherheitsschuhen setzt Jalas messbare Kriterien um: Bis zu 100 Prozent des verwendeten Leders stammen aus Gerbereien, die nach dem Leather Working Group Standard zertifiziert sind. Mehrere Modelle tragen das EU-Ecolabel oder eine Oeko Tex Zertifizierung, die auf geprüfte Schadstoffarmut hinweist.

Bei Modellen wie Jalas Exalter kommen Obermaterialien mit biobasierten Anteilen aus nachwachsenden Rohstoffen zum Einsatz. Laufsohlen mit Anteilen aus recyceltem Nitrilkautschuk tragen zur Reduzierung des Materialfußabdrucks bei, ohne funktionale Eigenschaften wie Rutschhemmung oder Haltbarkeit wesentlich zu verändern.

Neue S3S-Modelle (Sicherheitsklasse nach EN ISO 20345 mit zusätzlichem Durchtrittschutz und verbesserter Wasserabweisung) wie Jalas Tempus 5705, 5725 und 5715 kombinieren sportliche Optik mit ergonomischen Aspekten und Nachhaltigkeitskriterien. Die Obermaterialien bestehen aus Cordura recor, einem Gewebe aus recyceltem Polyester, ergänzt durch PFAS freie wasserabweisende Ausrüstungen. Mehrlagige Sohlenkonstruktionen, dämpfende Einlegesohlen mit Poron xrd (energieabsorbierendes Material) sowie angepasste Leisten sollen die Belastung von Füßen, Knien und Rücken reduzieren.

Auch Tegera Handschuhe greifen Nachhaltigkeitsaspekte auf. Oeko Tex zertifizierte Modelle sowie Schnittschutzhandschuhe mit bioattribuierten Dyneema Fasern oder hohen Anteilen recycelter Materialien, etwa bei den Tegera Pro Winterhandschuhen, verbinden Haltbarkeit, Tragekomfort und einen bewussteren Materialeinsatz.

Chemikalien, Energie, Kreislauf: messbar und nachvollziehbar

Um Umwelt- und Nachhaltigkeitsaussagen nachvollziehbar zu machen, setzt Ejendals auf ein eigenes Chemikalienmanagement. Dazu zählen eine unternehmensweite Liste eingeschränkt zulässiger Stoffe (Restricted Substances List), Schulungen für Einkauf und Produktmanagement sowie regelmäßige Prüfungen im eigenen Labor. Ziel ist es, kritische Stoffgruppen wie bestimmte PFAS Verbindungen schrittweise zu ersetzen.

Seit 2018 konnten Strom- und Gesamtenergiebedarf pro Umsatz deutlich gesenkt werden. Die Hauptstandorte werden vollständig mit Strom aus erneuerbaren Quellen versorgt; eine Solaranlage in Jokipii liefert rund 400 MWh pro Jahr. Weitere Maßnahmen sind FSC zertifizierte Schuhkartons aus Recyclingfasern, reduzierte Kunststoffanteile in Verpackungen, optimierte Logistikprozesse sowie erste Pilotprojekte zur Rückführung von Schuh- und Textilresten. Ergänzend sind Investitionen in ein emissionsärmeres Heizsystem geplant.

Partnerschaft mit GIT, Kundennähe und Blick nach vorn

Anlässlich des Jubiläums der GIT SICHEHREIT gratuliert Ejendals einem Fachmedium, das den Arbeitsschutzmarkt im DACH Raum seit vielen Jahren begleitet. Als langjähriger Partner nutzt Ejendals die GIT SICHERHEIT bewusst als Plattform für fachliche Beiträge, Marktbeobachtungen und den Austausch mit Anwendern und Entscheidenden.

> GIT SICHERHEIT ist für uns ein Spiegel des Marktes und zugleich ein Forum für den Dialog.
>
> **Werner Schwarzberger**

„GIT SICHERHEIT ist für uns ein Spiegel des Marktes und zugleich ein Forum für den Dialog – gerade in einer Zeit, in der Sicherheit, Nachhaltigkeit und Wirtschaftlichkeit enger zusammenhängen“, so Werner Schwarzberger, Reginal Sales Director bei Ejendals.

Mit einem breit aufgestellten DACH Team, stabiler Lieferfähigkeit, einem Safety Konzept aus Produkten, Schulungen und

Sicherheitsbewertungen sowie einer klar strukturierten Nachhaltigkeitsagenda sieht sich Ejendals für kommende Anforderungen gut vorbereitet. „Unser Anspruch ist es, Hand und Fußschutz verantwortungsvoll weiterzuentwickeln und ein verlässlicher Partner für Unternehmen zu sein – auch in herausfordernden Situationen“, fasst Schwarzberger zusammen. GIT

Ejendals AB
www.ejendals.com

© Bilder: Ejendals AB

DuPont Tyvek ist ein extrem reißfester, leichter und atmungsaktiver Vliesstoff, der wasser-, bakterien- und chemikalienbeständig ist. Diese Eigenschaften machen ihn besonders geeignet für Schutzkleidung im industriellen Umfeld

HSE-MANAGEMENT

Von Transport bis Recycling

5 Wege, wie HSE-Manager nachhaltigere Entscheidungen im Bereich PSA treffen können

Manager für Gesundheit, Sicherheit und Umwelt (HSE) spielen eine entscheidende Rolle bei der Gewährleistung der Sicherheit von Mitarbeitenden und berücksichtigen dabei auch die Umweltauswirkungen ihrer Tätigkeit. Ein Bereich, in dem sie viel bewirken können, ist die Anwendung der Grundsätze der Kreislaufwirtschaft bei der Auswahl von persönlicher Schutzausrüstung (PSA). Im Folgenden finden Sie fünf Möglichkeiten, wie sich HSE-Manager für eine nachhaltigere Auswahl von PSA entscheiden können.

1. Transportwege berücksichtigen

Der Transport von PSA über verschiedene Stationen hinweg trägt zur Entstehung von Treibhausgasemissionen bei. Zur Bewertung des CO_2-Fußabdrucks gehört daher die Betrachtung der gesamten Transportkette – vom Hersteller zum zentralen Lager, weiter zu einzelnen Standorten sowie schließlich zur Verwertung oder Entsorgung. Kürzere Transportwege und effizientere Logistikkonzepte können die Umweltbelastung reduzieren. Entsprechend kann es sinnvoll sein, Lieferanten zu bevorzugen, die ihre Lieferketten regional ausrichten oder Transporte bündeln.

2. Verpackungen reduzieren und möglichst wiederverwenden

Verpackungsmaterialien verursachen Ressourcenverbrauch und Abfall. In vielen Fällen ist eine Einzelverpackung von Schutzkleidung nicht zwingend erforderlich. Großverpackungen oder Mehrfachverpackungen können eine praktikable Alternative darstellen und das Abfallaufkommen verringern. Das von DuPont 2015 eingeführte Tyvek 500 Xpert Eco Pack hat so zum Beispiel bereits 820 kg Abfall je 35.000 Kleidungsstücke vermieden, den Verbrauch von Wasser und Primärenergie reduziert und die CO_2-Emissionen gesenkt. Kreislaufwirtschaft setzt voraus, dass die notwendigen Verpackungen wiederverwertbar sind.

3. Recyclingfähigkeit der Materialien prüfen

Ob und wie PSA recycelt werden kann, hängt wesentlich von den verwendeten Materialien ab. Die meisten Einwegkleidungsstücke werden z. B. aus Kunststoffgemischen hergestellt, sodass es schwierig ist, die verschiedenen Materialien für die Wiederverwendung zu trennen. Und selbst wenn es möglich ist, die einzelnen Kunststoffe zu extrahieren, ist das Material oft von schlechter Qualität und nur begrenzt verwendbar. Das erschwert eine hochwertige

Bei Tyvek handelt es sich um ein Monomaterial aus hochdichtem Polyethylen (HDPE), das sich leicht extrahieren lässt und somit eine hohe Recyclingfähigkeit

Wiederverwertung. Monomaterialien können dagegen unter geeigneten Bedingungen einfacher recycelt werden, sofern die Produkte nicht kontaminiert sind. So ist beispielweise Tyvek von DuPont ein Monomaterial aus hochdichtem Polyethylen (HDPE), das sich leicht extrahieren lässt und ein hochwertiges Material ergibt, das in mehreren Anwendungen wiederverwendet werden kann. Bei der Auswahl von PSA ist es demnach sinnvoll zu prüfen, inwieweit eingesetzte Materialien grundsätzlich für Recyclingprozesse geeignet sind und welche Rücknahme- oder Verwertungskonzepte existieren.

4. Langlebigkeit und Materialeinsatz berücksichtigen

Ein weiterer Ansatz zur Unterstützung der Kreislaufwirtschaft besteht darin, die Nutzungsdauer von PSA zu verlängern, ohne die Schutzfunktion zu beeinträchtigen. Robuste Materialien können das Risiko von Beschädigungen verringern und die Zahl vorzeitig entsorgter Kleidungsstücke reduzieren. Gleichzeitig beeinflusst das Materialgewicht die Umweltbilanz: PSA, die aus leichteren Materialien hergestellt wird, verringert auch die Umweltauswirkungen. Je schwerer das Material ist, desto mehr Abfall fällt am Ende der Lebensdauer des Artikels an.

Kontaminierte PSA muss in der Regel thermisch entsorgt werden. Auch hier spielt die Materialwahl eine Rolle, da sich Materialien hinsichtlich ihres Energiegehalts und ihres Verhaltens bei der Verbrennung unterscheiden. DuPont Tyvek kann beispielsweise sicher verbrannt werden. Als Brennstoff liefert es mehr als den doppelten Energiewert von Kohle und so viel Energie wie Öl, gemessen in BTU, was bedeutet, dass es ein gutes Energie-aus-Abfall-Potenzial hat.

5. Nachhaltigkeitsansatz der Hersteller bewerten

In Fällen, wo die Chemikalienschutzkleidung kontaminiert wird und nicht wiederverwertet werden kann, gibt es andere Wege, um die Nachhaltigkeit zu verbessern. So hat DuPont vor kurzem mit dem Tyvek 500 Xpert BioCircle einen Overall herausgebracht, der zu 100 % aus bio-kreislauffähigem HDPE stammt und nach einem ISCC-zertifizierten Massenbilanzansatz hergestellt wurde und dadurch den Impakt auf die Umwelt um 58 % reduziert.

Die Kreislaufwirtschaft umfasst den gesamten Lebenszyklus eines Produkts. Entsprechend ist es sinnvoll, Lieferanten auszuwählen, die Nachhaltigkeit nicht nur beim Produkt, sondern auch in ihren betrieblichen Prozessen berücksichtigen. Dazu zählen etwa der Einsatz erneuerbarer Energien in der Produktion, transparente Nachhaltigkeitsziele sowie eine nachvollziehbare Berichterstattung. Informationen aus unabhängigen Bewertungs- oder Berichtsplattformen wie zum Beispiel EcoVadis können bei der Einordnung helfen. Ebenso relevant ist, ob und wie Unternehmen ihre langfristigen Umweltziele definieren und deren Umsetzung dokumentieren. Beispielsweise konnten die DuPont-Standorte im Jahr 2023 die Treibhausgasemissionen in zwei Bereichen gegenüber dem Vergleichsjahr 2019 bereits um 58 % reduzieren und damit ihr Ziel für 2030 vorzeitig übertreffen. Durch eine bewusste Auswahl von PSA können HSE-Manager dazu beitragen, Umweltbelastungen zu reduzieren – etwa durch kürzere Transportwege, geringeren Verpackungsaufwand, recyclingfähige Materialien und langlebigere Produkte. Die Zusammenarbeit mit Herstellern, die Nachhaltigkeit als übergreifendes Handlungsprinzip verstehen, kann diesen Ansatz unterstützen. So lassen sich Anforderungen an Arbeits- und Gesundheitsschutz mit ökologischen Zielen besser in Einklang bringen. GIT

Autor:
Steve Marnach,
EMEA Training Manager und
Specialist Critical Environments,
DuPont Personal Protection

Ausführlichere Ratschläge finden Sie im e-Leitfaden von DuPont, „Leitfaden für HSE-Manager*innen zu PSA mit geringerer Umweltbelastung“

DuPont Personal Protection
www.dupont.de

© Bilder: DuPont

EINSATZSTIEFEL

Jedes Gramm am Fuß zählt

Warum Komfort, Feuchtigkeitsmanagement und neue Materialien im Defence-Bereich immer wichtiger werden

Steigende Einsatzanforderungen, veränderte Bedrohungslagen und lange Tragezeiten stellen Militär- und Polizeistiefel vor neue Herausforderungen. In einer aktuellen Konzeptstudie zeigt Gore Tex, wie moderne Materialien und eine ganzheitliche Konstruktion klassische Denkweisen im Defence Footwear Bereich hinterfragen können. Im Interview mit David Bastias, Footwear Business Development Manager Military & Law Enforcement bei W. L. Gore & Associates, erläutert der Experte, warum Komfort, geringes Gewicht und Feuchtigkeitsmanagement heute entscheidende Faktoren für Einsatzfähigkeit und Durchhaltevermögen sind – und wie das Obermaterial Extraguard neue konstruktive Spielräume für zukünftige Einsatzstiefel eröffnet.

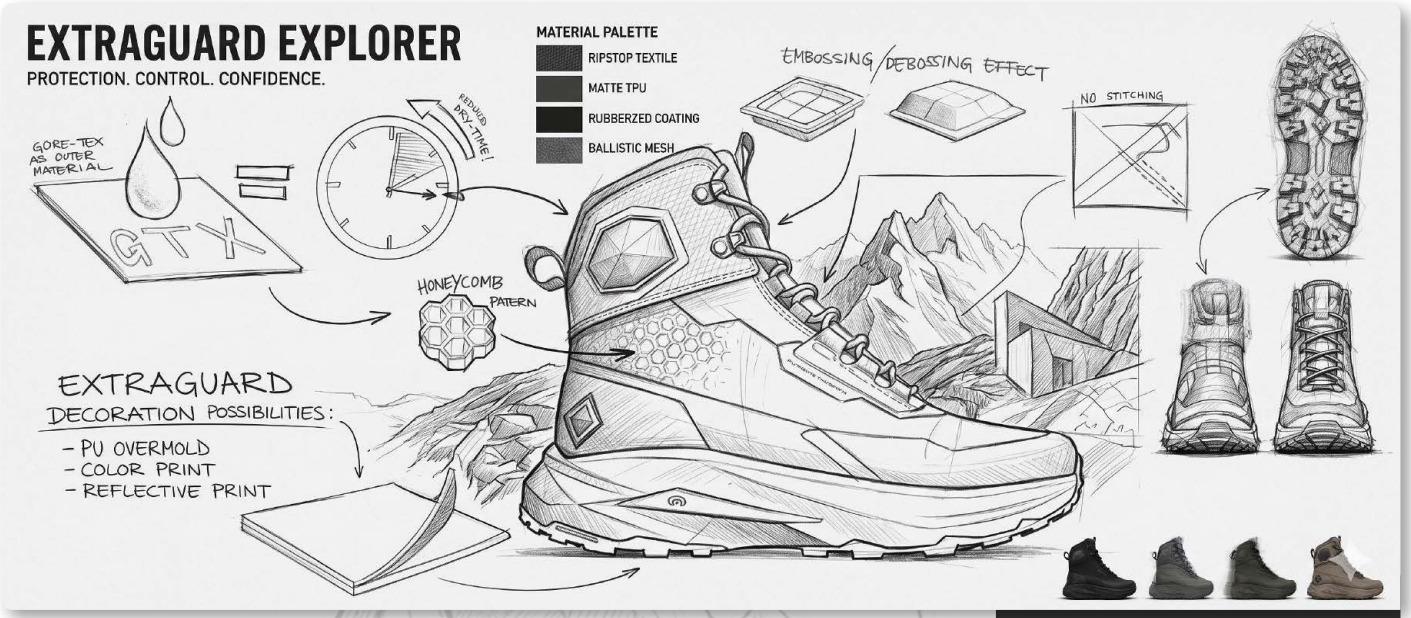
GIT SICHERHEIT: Herr Bastias, Militär- und Polizeikräfte stellen hohe Anforderungen an ihre Einsatzstiefel. Was war der Auslöser für Gore-Tex, eine eigene Konzeptstudie für diesen Bereich zu starten?

David Bastias: Wir sind stetig im Austausch mit Herstellern, Beschaffern und Endanwendern. Dabei stellen wir fest, dass sich die Einsatzprofile von Soldatinnen und Soldaten ebenso wie von Polizeikräften in den vergangenen Jahren spürbar verändert haben. Gefragt sind heute vor allem hohe Mobilität, lange Tragezeiten und ein zuverlässiges Funktionieren unter stark wechselnden klimatischen Bedingungen.

Hinzu kommt die veränderte sicherheitspolitische Lage: Landes- und Bündnisverteidigung rücken in Europa wieder stärker in den Fokus. Das bedeutet in vielen Fällen Einsätze in kalten, nassen und wechselhaften Umgebungen. Gleichzeitig orientieren sich viele Einsatzstiefel konstruktiv noch immer an sehr klassischen Mustern – schwere, sehr steife Lederstiefel.

Hier setzen wir mit Extraguard an, einem schützenden Obermaterial, das speziell für hohe mechanische Belastungen entwickelt wurde. Extraguard ist 40 Prozent leichter als Leder, sehr robust und abriebfest, nimmt kaum Wasser auf und bleibt daher auch bei Nässe dauerhaft leicht. Das Material ist marktverfügbar und hat sich unter anderem bei Sicherheitsschuhen, z. B. im Baugewerbe, im täglichen Einsatz bewährt.

Uns ging es aber bei der Konzeptstudie nicht darum, Extraguard einfach als Ersatz für Leder zu positionieren, sondern zu zeigen, welche konstruktiven Möglichkeiten entstehen, wenn man ein etabliertes Material zum Ausgangspunkt einer Neuentwicklung macht. Deshalb haben wir die Studie konsequent vom leeren Blatt aus gedacht – Material, Konstruktion und Einsatzanforderung als ein zusammenhängendes System.



▲ Die Konzeptstudie der Marke Gore-Tex veranschaulicht, welche konstruktiven Ansätze das Extraguard Obermaterial für leichtere und komfortablere Kampfstiefel ermöglicht

◀ Von Grund auf neu konstruiert, kombiniert die Konzeptstudie für Einsatzstiefel von Polizei und Militär das Extraguard-Obermaterial mit einer ETPU-Sohle aus dem Performance-Schuhbereich, um Gewicht und Tragekomfort gezielt zu verbessern

Lange Beschaffungszyklen sind bei Behörden und Militär die Regel. Warum tut sich der Defence-Bereich mit neuen Technologien oft schwer, und was bedeutet das für Innovationen wie Extraguard?

David Bastias: Der Defence- und Sicherheitsbereich ist stark reguliert – aus gutem Grund. Es geht um Sicherheit, Vergleichbarkeit und Verlässlichkeit. Gleichzeitig sind Beschaffungszyklen hier häufig deutlich länger als Innovationszyklen in der Industrie. Während Materialien und Fertigungstechnologien sich schnell weiterentwickeln, laufen Erprobung, Zulassung, Standardisierung und Einführung im militärischen Umfeld über viele Jahre.

Deshalb reicht es nicht, nur einen theoretischen Vorteil zu zeigen. Neue Lösungen müssen so ausgelegt sein, dass sie über lange Zeit konsistent bewertet, getestet und gefertigt werden können – mit reproduzierbaren Materialeigenschaften und stabilen Prozessen. Genau hier setzt unsere Konzeptstudie an. Sie veranschaulicht, welche konstruktiven Fortschritte möglich werden, wenn Materialinnovation und Konstruktion von Anfang an gemeinsam gedacht werden – statt neue Materialien lediglich für bestehende Stiefelmodellen zu verwenden.

Die Konzeptstudie betont Komfort als entscheidenden Faktor. Warum ist gerade Komfort bei Kampfstiefeln so wichtig – und was hat es mit dem Satz „Ein Gramm am Fuß ist fünf Gramm am Rücken“ auf sich?

Bitte umblättern ▶

Die Anforderungen an Einsatzstiefel haben sich hinsichtlich Mobilität, Tragezeiten sowie Design deutlich verändert

David Bastias: Komfort wird bei Einsatzstiefeln häufig unterschätzt, weil man ihn mit reiner Bequemlichkeit verwechselt. Tatsächlich ist Komfort ein zentraler Faktor für Einsatzfähigkeit. Ein Stiefel ist ein Arbeitsgerät – und jede konstruktive Schwäche wirkt sich über Stunden und Tage direkt auf den Körper aus. Unnötiges Gewicht, Steifigkeit oder ungünstige Druckpunkte kosten Energie und damit Ausdauer und Kampfkraft.

Der Satz „Ein Gramm am Fuß ist fünf Gramm am Rücken" bringt das sehr anschaulich auf den Punkt. Studien zeigen, dass zusätzliches Gewicht am Fuß den Energieverbrauch beim Gehen deutlich stärker erhöht als dieselbe Masse am Oberkörper. Der Grund ist die permanente Beschleunigung und Abbremsung bei jedem Schritt.

Komfort bedeutet dabei mehr als geringes Gewicht. Auch Passform, Dämpfung, Atmungsaktivität und ein natürliches Abrollverhalten spielen eine große Rolle. Ein weiterer wichtiger Punkt ist die Eintragezeit. Klassische Lederstiefel müssen häufig über Wochen eingelaufen werden. Extraguard ist von Beginn an flexibel – es gibt praktisch keine Break-in-Time. Das ist ein sehr konkreter Vorteil im Einsatzalltag.

Ein großes Problem herkömmlicher Einsatzstiefel sind Feuchtigkeit und lange Rücktrocknungszeiten. Warum sind diese Punkte im Einsatz so kritisch – und welche Lösungen bietet Extraguard?

David Bastias: Nässe ist im Einsatzalltag oft der härteste Gegner – gerade in europäischen Breiten mit kaltem, feuchtem und wechselhaftem Klima. Gleichzeitig stehen nicht immer Trocknungsmöglichkeiten zur Verfügung. Denken Sie an Soldaten, die tage-, manchmal wochenlang im Feld sind. Nasse Stiefel werden schwer, kühlen aus und verändern das Tragegefühl deutlich.

Extraguard wurde genau für diese Schwachstelle anders entwickelt. Das Obermaterial nimmt kaum Wasser auf, bleibt formstabil und leicht. Dies führt zu deutlich kürzeren Rücktrocknungszeiten als bei Lederstiefeln. Hinzu kommt: Extraguard benötigt keine Pflege. Im Zweifel reicht Abspülen mit Wasser – auch mit dem Hochdruckreiniger. Das ist im Einsatz nicht zu unterschätzen, denn welche Einsatzkräfte haben heutzutage noch Lederpflege dabei?

Wie wichtig wird aus Ihrer Sicht das Thema Design für Polizei- und Militärstiefel – auch im Hinblick auf Recruiting?

David Bastias: Funktion steht immer an erster Stelle. Aber Design ist das sichtbare Ergebnis guter Funktion. Und in Zeiten hohen Recruiting-Bedarfs bei Militär und Polizei wird dieser Aspekt immer wichtiger. Bewerberinnen und Bewerber schauen sehr genau hin: Wie modern ist die Ausrüstung? Wie bequem ist sie? Wer möchte seinen beruflichen Alltag mit schwerer, unbequemer und altbacken wirkender Ausrüstung bestreiten, wenn es technisch längst zeitgemäße Alternativen gibt? Das ist heutzutage ein ganz entscheidender Aspekt für die Personalgewinnung wie wir von unseren Endkunden wissen.

Die Sohle mit hoher Dämpfung gilt als weiteres zentrales Element der Studie. Welche Rolle spielt Dämpfung im täglichen Einsatz?

David Bastias: Dämpfung beeinflusst direkt, wie lange man leistungsfähig bleibt. Harte Untergründe und lange Distanzen belasten Gelenke und Muskulatur erheblich. Mit der eingesetzten ETPU-Sohle übertragen wir Know-how aus dem Performance-Schuhbereich. Ziel ist ein kontrolliertes, dauerhaft stabiles Dämpfungsverhalten. Der Stiefel trägt sich nahezu wie ein Sneaker.

Viele Verantwortliche glauben nach wie vor: „Ein robuster Einsatzstiefel muss aus Leder sein." Wie begegnen Sie dieser Haltung?

David Bastias: Leder ist ein bewährter Standard, bietet ein sehr hohes Schutzniveau und wird immer seine Berechtigung haben. Gleichzeitig bringt das Material aber Herausforderungen mit – insbesondere bei Wasseraufnahme, Gewicht und Pflegeaufwand. Pflege wird im Einsatzalltag häufig nicht konsequent durchgeführt. Extraguard setzt genau hier an: robust, leicht, kaum Wasseraufnahme, kein Fetten notwendig.

Zum Abschluss: Ist Ihr Ansatz eher ein komplett neu gedachtes Elektroauto als ein umgebauter Benziner?

David Bastias: Der Vergleich passt als Denkmodell sehr gut. Ein Elektroauto benötigt keinen großen Motorblock, kein klassisches Getriebe und keinen Tank. Baut man in die Karosserie eines Benzinmodells einen Elektromotor ein, so kann man die Vorteile dieser Antriebsart gar nicht voll ausschöpfen, also mehr Platz im Innenraum, geringere Außenmaße etc.

Ähnlich verhält es sich bei unserer Konzeptstudie, die die Vorteile von Extraguard voll ausschöpft. Das Modell wurde, ähnlich einem neu konstruierten Elektroauto, von Grund auf für Extraguard konzipiert. Sie soll Denkanstöße geben – denn Innovation hat immer mit einem Perspektivwechsel zu tun. GIT

W. L. Gore & Associates GmbH
www.gore-tex.com

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

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

Sicherheitsmanagement

deister electronic 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

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

Sicherheitsmanagement

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

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 Privatanwendern spezialisiert.

Sicherheitsmanagement

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

Sicherheitsmanagement

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

Sicherheitsmanagement

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

Sicherheitsmanagement

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

Sicherheitsmanagement

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

Sicherheitsmanagement

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

Gebäudesicherheit

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

PERIMETER SCHUTZ

Sicherheitsmanagement

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

Gebäudesicherheit

SimonsVoss Technologies GmbH
Münchner Str. 16 · 85774 Unterföhring
Tel.: 089 992280
marketing-simonsvoss@allegion.com
www.simons-voss.com
Digitale Schließanlagen mit Zutrittskontrolle, kabellose und bohrungsfreie Montage, batteriebetrieben, keine Probleme bei Schlüsselverlust.
Digital Schließen ist neu für Sie? Rufen Sie an: 089 99228-555

Perimeterschutz

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

Sicherheitsmanagement

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

VIDEO ÜBERWACHUNG

GEBÄUDE SICHERHEIT

Gebäudesicherheit

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

Videoüberwachung

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

Gebäudesicherheit

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

Gebäudesicherheit

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

Videoüberwachung

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

Gebäudesicherheit

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

Gebäudesicherheit

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

Videoüberwachung

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

Videoüberwachung

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

Zeit + Zutritt

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

Zeit + Zutritt

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

Videoüberwachung

Zeit + Zutritt

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

Zeit + Zutritt

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

Zeit + Zutritt

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

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

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

Zeit + Zutritt

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

Zeit + Zutritt

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

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

Zeit + Zutritt

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

Zeit + Zutritt

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

Zeit + Zutritt

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

Zeit + Zutritt

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

NOTRUF SERVICE LEITSTELLE

BRAND SCHUTZ

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

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, Alarmempfangsstelle DIN EN 50518, Alarmprovider, Mobile Einsatz- und Interventionskräfte, Objekt- und Werkschutz

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, Arbeitsschutz, sicherheitsrelevante Betriebsausstattung, Gefahrstoff-Leckage-Warnsystem

ARBEITS SICHERHEIT

Notruf- und Service-Leitstelle

Fernwirk-Sicherheitssysteme Oldenburg
FSO
Ihr Security-Provider

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

Brandschutz

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 Brandschutzlösungen. Branchenspezifisches Fachwissen mit hochwertigen Brandschutzkomponenten vereint zu einem sicheren und verlässlichen Brandschutz. Flankiert wird dies mit Fachschulungen und einem umfangreichen, lösungsorientierten Kundenservice.

Arbeitssicherheit

ELTEN

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

Ihr Eintrag in der Rubrik

GIT BusinessPartner
Die Einkaufsrubrik für den direkten Kontakt

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

Wir beraten Sie gerne!

Brandschutz

seTec

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

Arbeitssicherheit

Hailo

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

Bequem auf dem Sofa durch die e-Ausgabe derGIT SICHERHEIT blättern: Registrieren Sie sich auf **www.git-sicherheit.de/newsletter**

Arbeitssicherheit

KRAUSE-Werk GmbH & Co. KG
Am Kreuzweg 3 · D-36304 Alsfeld
Tel: +49 (0) 6631 / 795 - 0
info@krause-systems.de
www.krause-systems.com
Tritte, Leitern, Steigtechnik, Podestleitern, Fahrgerüste

Gefahrstoffmanagement

SÄBU Morsbach GmbH
Zum Systembau 1 · 51597 Morsbach
Tel.: 02294 694-24 · Fax: 02294 694-38
safe@saebu.de · www.saebu.de
Gefahrstofflagerung, Gefahrstoffcontainer, Auffangwannen, Bodenschutzsysteme, Gasflaschenlagerung, Gasflaschencontainer, Gasflaschenbox, Kleingebinderegale
Unser Online-Shop: www.fladafi.de

GEFAHRSTOFF MANAGEMENT

GASMESS TECHNIK

Maschinen + Anlagen

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

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- unad Arbeitsschutz, Sicherheitsschränke, Chemikalien- und Umluftschränke, Druckgasflaschenschränke, Gefahrstoffarbeitsplätze, Absauganlagen, Raumluftreiniger uvm.

Gasmesstechnik

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

Maschinen + Anlagen

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

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

MASCHINEN ANLAGEN SICHERHEIT

Maschinen + Anlagen

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

Gefahrstoffmanagement

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

Maschinen + Anlagen

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

Maschinen + Anlagen

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

WILEY

35 Jahre

GIT SICHERHEIT

Die Jubiläumsausgabe

Seit 35 Jahren begleitet GIT SICHERHEIT den Sicherheitsmarkt – kritisch, unabhängig und immer nah an den relevanten Fragen der Zeit. Dieses Jubiläum ist für uns mehr als ein Rückblick: Es ist Anlass, Entwicklungen einzuordnen, Stimmen zu Wort kommen zu lassen und den Blick nach vorn zu richten.

Auf unserer Jubiläums-Landing-Page finden Sie exklusive Interviews mit Entscheiderinnen und Entscheidern, fundierte Trendberichte, pointierte Analysen und besondere Specials, die zeigen, wie sich Sicherheitstechnologien, Strategien und Märkte verändert haben – und was heute wirklich zählt.

Entdecken Sie 35 Jahre SICHERHEIT im Kontext.

Jetzt online auf:
git-sicherheit.de/de/
35-Jahre-GIT-SICHERHEIT

DIE VIP LOUNGE

Linda Voigtländer

Leitung Gefahrenabwehr Prävention, Infraserv Höchst

- 2009 Fachkraft für Schutz und Sicherheit bei Infraserv Höchst
- Bis 2015 Berufsbegleitendes Studium Bachelor Business Administration Securitymanagement
- Studienbegleitend tätig in der kaufmännischen Abteilung während des Studiums bei gleichzeitiger Wahrnehmung sicherheitsrelevanter Aufgaben
- 2017-20 Betriebsleitung Unternehmenssicherheit mit 110 Mitarbeitern
- 2020 bis heute Abteilungsleitung Gefahrenabwehr Prävention mit 150 Mitarbeitern

Ihr Berufswunsch mit 20 war: Mit 20 war ich bereits in meiner Wunschausbildung zur Fachkraft für Schutz und Sicherheit im Industriepark Höchst bei Infraserv Höchst. Schon mit 14 hatte ich das erste Mal das klare Interesse, im Sicherheitsbereich zu arbeiten.

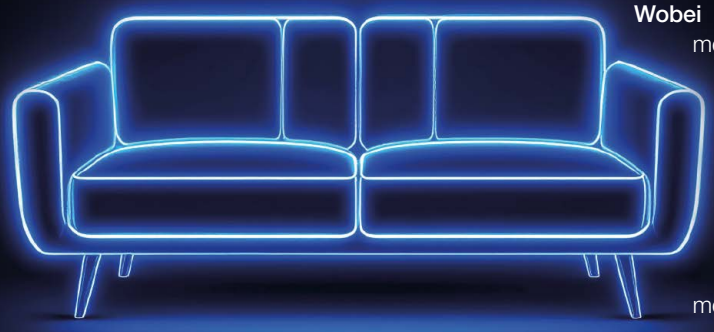
Was hat Sie dazu bewogen, eine Aufgabe im Bereich Sicherheit zu übernehmen? Der Wunsch wurde mit der Ausbildung zur Fachkraft für Schutz und Sicherheit sehr konkret. Ausschlaggebend war vor allem mein ausgeprägter Gerechtigkeitssinn. Mir waren Recht und Ordnung schon immer sehr wichtig.

Welche sicherheitspolitische Entscheidung oder welches Projekt sollte Ihrer Meinung nach schon längst umgesetzt sein? Die konsequente Vernetzung und der Informationsaustausch zwischen den relevanten Akteuren im Sicherheitsbereich. Dies gilt insbesondere auch für eine engere Zusammenarbeit zwischen Behörden und der privaten Sicherheitswirtschaft.

Die beste Erfindung im Bereich Sicherheit ist Ihrer Meinung nach: Die besten Entwicklungen sind solche, die Menschen unterstützen, die täglich Verantwortung tragen. Also Lösungen, die entlasten, Orientierung geben und im richtigen Moment die richtigen Informationen liefern.

Ein Erfolg, den Sie kürzlich errungen haben, war: Ich bin stolz, dass wir unsere Sicherheitskompetenz nicht nur am eigenen Standort einbringen, sondern auch deutschlandweit und über die Landesgrenzen hinaus Unternehmen bei Sicherheitsanalysen unterstützen. Im vergangenen Jahr konnten wir uns im Kontext von Digitalisierung, Automatisierung und den neuen KRITIS-Anforderungen sehr gut positionieren.

Wer hat Ihrer Meinung nach eine Auszeichnung verdient? Ich glaube, Auszeichnungen gehen oft an die, die sichtbar sind. Verdient hätten sie aber viel häufiger die, die im Hintergrund dafür sorgen, dass alles reibungslos funktioniert: in der Pflege, im Sicherheitsbereich, aber genauso in der Energieversorgung, im Rettungsdienst oder auch in der IT.



Wobei entspannen Sie? Bei meinem Pferd. Beim Reiten, am liebsten draußen in der Natur – durch den Wald, fern vom Alltag.

Welchen Urlaubsort können Sie empfehlen? Seit wir mit Kleinkind reisen, hat sich meine Definition von Erholung leicht verschoben: Wichtig sind ein kurzer Transfer, ein kinderfreundliches Hotel und ein Strand, zum Sandburgen bauen. Griechenland bietet traumhafte Strände – aber auch Südtirol ist eine absolute Empfehlung.

Welche Zeitschriften lesen Sie regelmäßig? Natürlich die GIT SICHERHEIT, um fachlich auf dem neuesten Stand zu bleiben und Entwicklungen in der Sicherheitsbranche einzuordnen. Darüber hinaus gehört Psychologie Heute für mich fest dazu. Nicht zuletzt lese ich täglich Tageszeitungen.

Die GIT SICHERHEIT ist wichtig für Sie, weil… sie komplexe Themen greifbar macht und das ohne unnötige Fachsimpelei. In einem Bereich, in dem sich Technologien und Anforderungen ständig weiterentwickeln, ist es entscheidend, eine verlässliche Quelle zu haben, die Trends einordnet und Orientierung gibt. Ich schätze besonders die Mischung aus fachlicher Tiefe und Praxisnähe. Man bekommt nicht nur theoretisches Wissen, sondern auch konkrete Einblicke, die im Arbeitsalltag wirklich weiterhelfen.

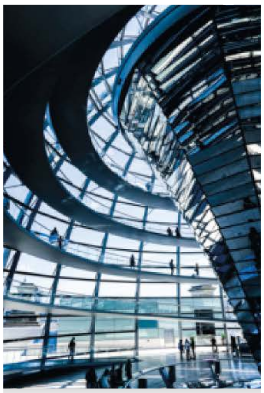
Welches Buch haben Sie zuletzt gelesen? „Factfulness“ von Hans Rosling – ein Buch, das zeigt, wie stark unsere Wahrnehmung von globalen Entwicklungen von Vorurteilen geprägt ist und wie wichtig ein faktenbasierter Blick auf gesellschaftliche Themen ist.

Welche Musik hören Sie am liebsten? Mein Musikgeschmack ist ziemlich alltagstauglich. Aber wenn ich mich entscheiden müsste, schlägt mein Herz für Rockmusik – vor allem für die von Nickelback.

Was motiviert Sie? Vor allem die Verantwortung, die mit dem Thema Sicherheit einhergeht. Zu sehen, dass Prozesse funktionieren, Risiken erkannt oder sogar verhindert werden. Das sind konkrete Erfolge, auch wenn sie oft im Hintergrund stattfinden. Genauso wichtig ist für mich das Team: Ich arbeite mit Menschen zusammen, die ihre Verantwortung ernst nehmen und auf die man sich verlassen kann.

Worüber machen Sie sich Sorgen – und was stimmt Sie zuversichtlich? Sorgen macht mir aktuell die zunehmende Unberechenbarkeit in der Sicherheitslage – sowohl durch globale Entwicklungen als auch durch Akteure, die schwer einzuschätzen sind. Zuversichtlich stimmt mich aber, dass wir in Deutschland auf sehr stabile Strukturen bauen können – funktionierende Institutionen, ein hohes Sicherheitsbewusstsein und viele Menschen, die täglich Verantwortung übernehmen.




17.–19. Juni 2026

Lakeside Security Summit 2026

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

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

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

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

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

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

ASW Baden-Württemberg

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

Wir denken Sicherheit neu.

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

Wir bündeln die verschiedenen Systeme auf einer herstellerneutralen Plattform. Qualifiziertes Personal überwacht rund um die Uhr aus unserer zertifizierten, intelligenten Leitstelle sämtliche sicherheitsrelevanten Prozesse Ihres Unternehmens.

www.klueh.de

KI-generiert durch Frank Maagh, NT-Medien GmbH