EURO SECURITY

Das Sicherheitsmagazin für Planer, Errichter und Anwender für die DACH-Region



KENTIX
ASSA ABLOY

Sicherheit auf einer Plattform

Strategien

Made in Germany ist ein Versprechen für Sicherheit; Ein Interview mit CEO Thomas Dallmeier

Unternehmen

SALTO-Story: Salto feiert 25 Jahre voller Innovation und inspirierender Zutritts-lösungen

KRITIS

Wenn die Tür in den Serverraum eine Schwachstelle ist: Was bedeutet NIS-2 wirklich für Ihre physische Zutrittskontrolle?

ISSN 09481249 • 12-2025 • ZKZ 16724 Postvertriebsstück bezahlt • 80383 BAY Germany ©SEC Global • euro-security.de

Inhalt



Unser Titelbild

Kentix GmbH
Carl-Benz-Straße 9
D-55743 Idar-Oberstein
Telefon +49 6781 562510
www. kentix.com

Impressum 2
Inhaltsangabe 2
Editorial 4

TITELSTORY

Sicherheit optimal vernetzt ASSA ABLOY und Kentix orchestrieren Sicherheit neu 6
Mit der Integration von Kentix setzt ASSA ABLOY ein starkes Zeichen für vernetzte Sicherheitslösungen. Die Kombination aus IoT-Plattform, physischer Sicherheit und globaler Marktpräsenz schafft ein integriertes Sicherheitsökosystem für Rechenzentren und kritische Infrastrukturen – skalierbar, effizient und zukunftsorientiert.

DIGITALE WELT

Jahresrückblick 2025 der Euro Security Redaktion 53
IT-Sicherheit, Rechenzentrumssicherheit und Künstliche Intelligenz

2025 zeigte, wie eng IT-Security, Rechenzentren und KI verflochten sind. Ganzheitliche Sicherheitskonzepte, nachhaltige und automatisierte Infrastrukturen sowie verantwortungsvoll eingesetzte KI werden zum Schlüssel für Resilienz, Innovation und digitale Souveränität.

IT-Sicherheit 2025: Fünf zentrale Trends 53

2025 erfordern hybride Bedrohungen ein Umdenken: Ganzheitliche Sicherheitsstrategien verbinden Cyber-, physische Sicherheit und Resilienz. Passwordless Authentifizierung, kontinuierliche Tests und KI-gestützte Abwehr werden zum Standard – vom Konzern bis zum Mittelstand.

Rechenzentrumssicherheit: Fünf Trends im Data-Center-Bereich 55

KI treibt 2025 den massiven Ausbau von Rechenzentren voran – mit stark steigendem Energiebedarf. Nachhaltigkeit, Automatisierung und Edge Computing werden zu Pflichtaufgaben. Wer AI-ready, effizient und souverän agiert, sichert Wettbewerbsfähigkeit im Datacenter-Zeitalter.

Künstliche Intelligenz 57
Fünf Trends zwischen Chance und Risiko

2025 wurde KI zum zweischneidigen Schwert der Cybersicherheit: Sie stärkt Abwehr, automatisiert Prozesse und steigert Produktivität – wird aber zugleich von Angreifern genutzt. Entscheidend sind menschliche Kontrolle, Transparenz und verantwortungsvolle KI-Nutzung.

Sicherheitslage 2025 61
Zehn kritische Trends im Spiegel der Euro-Security-Kommentare

Im Jahr 2025 nutzte Euro Security seine Kommentare, um der Sicherheitsbranche die systemische Dimension von Sicherheit näherzubringen. Ziel war eine Debatte über Technologie, Regulierung und Organisation zu versachlichen, operative Präzision, gesellschaftliche Akzeptanz und Governance. Denn die Weiterentwicklung belastbarer Sicherheitsstrategien für Staat und Gesellschaftstehen im Fokus von Fachjournalismus.

Jahreschronik 2026 64
Themen im Verlauf des Jahres 2025

Technik, Regulierung und gesellschaftliche Anforderungen zusammenwirken. Vertrauen, Resilienz und Akzeptanz werden zur Währung, Sicherheit wandelt sich vom Einzelprodukt zum integrierten System.

KÜNSTLICHE INTELLIGENZ

PagerDuty 12
KI bestimmt den Takt: Die wichtigsten IT-Trends für 2026

Telekom, FH IAS 51
KI-Agenten sollen helfen, in der Notaufnahme Leben zu retten

MARKT & ZAHLEN

Genetec Report: Die Lage der physischen Sicherheit 22
Wie Modernisierung, KI und Partnerschaften einen neuen strategischen Sicherheitsrahmen setzen

Allianz 28
D&O-Haftungsrisiken 2026: Allianz-Analyse zeigt ein deutlich verschärftes Risikoumfeld für Führungskräfte

ESET 32

Impressum

Euro Security Fachmedien (Verlagsvertretung); Grabenfeldstrasse 25, 83083 Riedering, Tel: +49 (0)8036 3035071; Email: redaktion@euro-security.de
Redaktion: ***Dr. Claudia Mrozek, Chefredak. (V.i.S.d.P., Herausgeber)****, Caroline Best, Angela Kloose, Dirk Lehmanski, Maria Lehmen, Anne, Schneider, Heiko Scholz, Patricia Ovo, Cathy Thomens, Sophie Mrozek, Alexander Mrozek, Mariam Nassreddin; Marcus Smid, Angela Thorn*
Druckerei *D+L Print, Dorsten / Schmidl & Rotaplan Druck, Regensburg*
Aboverkauf *DCMN Marketing Agentur, Email: abo@sec-global.org*
Anzeigenverwaltung/-vertretung *DCMN Marketing Agentur Oberbayern, Bestellungen und Druckvorlagen: anzeigen@euro-security.de*

Copyright: *Der Markenverwerter SEC Global ist urheberrechtlich verantwortlich für Inhalt, Design und die Herstellung von Druckmaterialien/-erzeugnissen für die Fachzeitschriften Euro Security, Middle East Security und African Security. Ebenfalls betreffen allgemeine Copyrightrechte und -pflichten die Webseite ‚www.eurosecglobal.de' und alle angeschlossenen Seiten, digitalen Services und Publikationen. Ohne Zustimmung des Verlags können weder ganze Artikel noch große Teile von Texten per E-Mail, über ‚Social Media'-Netzwerke oder auf andere Weise veröffentlicht werden. Eine wirtschaftliche Verwertung oder eine andere kommerzielle Benutzung ist nicht zulässig. In Verbindung mit der gedruckten Zeitschrift oder den veröffentlichten Texten auf der Website bzw. digitalen Anwendungen ist das Reproduzieren oder die Vervielfältigung von Marken/ Logos (wie "Euro Security" [ES] oder "Middle East Security" [MES] Name genauso wie andere verlagseigene Logos oder Handelsnamen nur mit schriftlicher Genehmigung der Verlagsleitung möglich. Das Kopieren oder die Verlinkung ganzer Textpassagen unter eigenem Namen sind ausschließlich für den persönlichen und nicht-kommerziellen Gebrauch zulässig. Der Ausdruck eines Artikels auf Papier ist zulässig, eine Vervielfältigung nicht. Genauso ist eine Speicherung für den privaten Gebrauch zulässig. Eine Verwendung, die über den nicht-kommerziellen Gebrauch hinausgeht, ist nicht erlaubt. Digitale Anwendungen sind pro Lizenz nur auf bis zu fünf getrennten Geräten zu verwenden. Auch aus diesen Quellen ist eine Reproduktion, Veränderung oder eine kommerzielle Verwendung nicht gestattet. Die Übertragung der Inhalte auf andere Webseiten, Newsgroups, Mailinglisten, elektronische Bulletins, Servern oder andere Medien, die mit einem Netzwerk verbunden sind oder regelmäßig oder systematisch Inhalte in elektronischer (einschließlich der im Rahmen jeder Bibliothek, Archiv oder ähnliche Dienstleistung) speichern, ist nicht gestattet. Jede Verwendung der im Druck oder Online publizierten Inhalte sind ausdrücklich untersagt. Anfragen auf Genehmigung bitte an einen unserer SEC Global unter copyright@sec-global.org senden. Eine Freigabe oder ein kostenpflichtiges Angebot wird Ihnen umgehend zugehen. © Sec Global*

EURO SECURITY Fachverlage und - medien ist förderndes Mitglied im BHE/Deutschland. BHE-Mitglieder erhalten im Rahmen ihrer Mitliedschaft regulär erscheinende Ausgaben der Euro Security DACH kostenlos.

Inhalt







Von Drohnenspionage bis Cyberkrieg: Welche Risiken die digitale Sicherheit im Jahr 2026 prägen werden

Globale Markt für Videoüberwachung 2025-2030 87
Technologie, Geopolitik und neue Geschäftsmodelle formen eine Branche im Wandel

MARKTBERICHTE

Die Zukunft des Alarms 38
Elektronische Alarmsysteme in der DACH-Region: Marktentwicklung: Neue Spieler und Konsolidierung

Der Markt für elektronische Alarmsysteme in Deutschland, Österreich und der Schweiz (DACH) steht vor einem Wandel. Während der Gesamtmarkt für Sicherheitstechnik 2024 trotz schwacher Baukonjunktur um 3,4 % wuchs, stagnierten klassische Einbruchmeldesysteme und blieben hinter dem Durchschnitt zurück. Etablierte Anbieter stehen unter Innovations- und Preisdruck, während neue Hersteller wie Ajax Systems (Ukraine) und Satel (Polen) mit modernen, funkbasierten Systemen traditionelle Platzhirsche herausfordern. Das Segment befindet sich an einer Weggabelung, geprägt durch Digitalisierung und den Kampf gegen veraltete Technologien.

MESSENKALENDER

Sicherheitsmessen 2026: Rund um die Welt 84
Trends, Technologien und Treffpunkte der globalen Sicherheitsbranche

NIS2

primion 10
Was bedeutet NIS-2 wirklich für Ihre physische Zutrittskontrolle?

Compliance-Beauftragte kennen das Szenario: Sie investieren Millionen in Netzwerksicherheit, implementieren ausgefeilten Endpunktschutz und richten eine Zero-Trust-Architektur ein – doch all das nützt nichts, wenn jemand durch eine unverschlossene Tür in den Serverraum gelangt.

PROGNOSEN

IFS 34
Blindflug ist keine Strategie

Cycode 34
Programmierende KI: Die generierte Gefahr

IT-Sicherheit und digitale Souveränität 35
Herausforderungen, Risiken und Perspektiven im Jahr 2026

SICHERHEITSSTRATEGIEN

Cloud, Compliance und KI 18
Wie Verkada die Sicherheitsbranche in Europa neu definiert

Cloud, Compliance und KI: Verkada gestaltet die Sicherheitsbranche in Europa neu. Am Rande des Verkada Security Summit 2025 in München sprach Euro Security mit CEO Filip Kaliszan über die beschleunigte Expansion des Unternehmens, innovative cloudbasierte Lösungen und die Stärkung der Marktposition in der DACH-Region und darüber hinaus.

Dallmeier electronic 24
Made in Germany ist ein Versprechen für Sicherheit -

„Made in Germany" ist für Dallmeier mehr als ein Label – es ist ein Sicherheitsversprechen. CEO Thomas Dallmeier erklärt im Interview, warum das Unternehmen Hardware und Software konsequent in Deutschland entwickelt, wie Datenschutz, Cybersecurity und KI praxisnah umgesetzt werden und warum Kunden weltweit gezielt auf echte deutsche Qualität setzen..

TÜRLÖSUNGEN

Assa Abloy 30
„Hilfe, da fehlt ein Kabel!": Schnittstellenprobleme in der Gebäudeplanung

UNTERNEHMENSPORTRAIT

Die SALTO-Story 14
Ein Vierteljahrhundert Zugang neu gedacht

25 Jahre Innovation: Salto Systems hat aus einem kleinen spanischen Start-up einen globalen Vorreiter für smarte Zutrittslösungen gemacht. Mit kabellosen, vernetzten Systemen, Cloud-Technologie und dem SALTO WECOSYSTEM setzt das Unternehmen neue Maßstäbe in Sicherheit, Design und Nutzererlebnis – und öffnet die Türen für die Zukunft der Zutrittskontrolle.

WISSENSCHAFT

Hochschule Lausanne 33
Robotergreifer aus Langusten-Exoskeletten

euro-security.tv euro-security.de

Editorial

Rückblick und Ausblick



Das Jahr neigt sich dem Ende zu – Zeit, zurückzublicken und zugleich nach vorn zu schauen. Die europäische Sicherheitsbranche steht an einem entscheidenden Punkt: Konsolidierung durch Übernahmen nimmt Fahrt auf, Marktführer werden größer, kleinere Anbieter werden aufgekauft oder integriert. Doch stellt sich die Frage: Dient diese Konzentration wirklich der Sicherheit? In manchen Segmenten drohen marktbeherrschende Strukturen, die Innovation erstikken und die Vielfalt der Lösungen einschränken. Die Branche muss sich fragen, ob wachsende Dominanz einzelner Unternehmen langfristig dem Schutz der Gesellschaft dient oder vor allem wirtschaftlichen Interessen.

Übernahmen: Fluch oder Segen

Die zunehmende Konsolidierung bringt zwar Effizienz und Skaleneffekte, gleichzeitig entsteht das Risiko, dass einzelne Anbieter marktbeherrschend werden. Innovation könnte dadurch gebremst werden, und die Vielfalt der Sicherheitslösungen leidet. Gerade in Bereichen kritischer Infrastruktur ist es entscheidend, dass Wettbewerb erhalten bleibt, um neue Ideen und praxisnahe Sicherheitskonzepte nicht zu blockieren. Die Branche steht vor der Aufgabe, Wachstum und Konzentration bewusst zu steuern und die Balance zwischen Marktlogik und gesellschaftlicher Verantwortung zu wahren.

Digitalisierung: Chancen und Risiken

Technologische Durchbrüche in Überwachung, Zutrittskontrolle und Gefahrenabwehr eröffnen enorme Chancen. Gleichzeitig wächst die Verantwortung: Digitale Systeme können den Menschen unterstützen, dürfen aber nicht die Freiheit oder Privatsphäre einschränken. Algorithmen und KI sind nur so zuverlässig wie die Menschen, die sie bedienen. Im Spannungsfeld zwischen Dienstleister und möglichem Sicherheitsrisiko bleibt der Faktor Mensch zentral – als Anwender, Kontrollinstanz und auch als potenzieller Risikofaktor. Technik darf nicht überall den Menschen ersetzen, besonders in Bereichen, in denen Vertrauen, Intuition und situatives Urteilsvermögen unverzichtbar sind.

Mensch und Technik

Nicht alles, was finanziert werden kann, ist auch der richtige Weg. Im Zivilschutz, wo Budgets knapp sind, drohen Defizite, die jeden Einzelnen betreffen. Eine aufmerksame, couragierte Gesellschaft bleibt die natürliche Grundlage jeder effizienten Sicherheitsstrategie. Gleichzeitig zeigt die Praxis: Drohnen, Sensorik und automatisierte Systeme sind unverzichtbar, wenn Bereiche zu gefährlich oder schwer zugänglich sind. Der Schlüssel liegt im intelligenten Zusammenspiel von Mensch und Maschine – Technologie unterstützt, ersetzt aber nicht die menschliche Verantwortung.

Zivilschutz: Defizite vorhanden

Die Kluft zwischen digitalen Innovationen und bewährten „alten" Technologien darf nicht weiter wachsen. Die Branche muss Brücken schlagen – unabhängig von momentanen Wachstumsraten. Deutschland und Europa müssen die Weichen für die Zukunft stellen und die Innovationskraft vergangener Jahrzehnte wiederentdecken. Ausbildung in IT-Sicherheit, Technischer Gebäudeausrüstung, Ingenieurwissen, Softwarekompetenzen und technischer Kreativität muss intensiviert werden. Start-ups sollten wieder stärker in den Mittelpunkt rücken, im Dialog mit etablierten Marktgrößen, und junge Talente einbinden. Weniger Fokus auf kurzfristige Umsatzmaximierung, mehr auf langfristige Ausbildungspotenziale und technologische Zu- kunftsfähigkeit.

Digital und Analog verbinden

Die Dominanz asiatischer Hersteller darf nicht als Schicksal hingenommen werden. Europa hat die Chance, vorhandene Führungspositionen in der Sicherheitstechnik zu behaupten und auszubauen – mit klarem Bekenntnis zu Qualität, Innovation und Unabhängigkeit. Gleichzeitig muss die Branche die Kluft zwischen digitalen Innovationen und traditionellen Methoden überwinden, um widerstandsfähige, gesellschaftlich verantwort- bare Lösungen zu gewährleisten, die Technik und Mensch sinnvoll verbinden.

Start-ups und Innovation fördern

Zukunftsfähige Sicherheitslösungen entstehen nur, wenn Ingenieurwissen, Softwarekompetenzen und technisches Kreativpotenzial stärker in Start-ups, Planungsinstanzen und Ausbildungsprogrammen gefördert werden. Der Dialog mit jungen Talenten ist entscheidend – weniger Vertriebsseminare zur Umsatzmaximierung, mehr langfristige Entwicklungsstrategien und praxisnahe Ausbildung. Start-ups sind dabei nicht nur Ideengeber, sondern zentrale Partner im Innovationsnetzwerk der Branche und Bindeglied zwischen technologischem Fortschritt und gesellschaftlicher Verantwortung.

Europäische Sicherheit bewahren

Europa muss seine technologische Führungsrolle sichern und den eigenen Sicherheitsmarkt stärken. Die Branche ist gefordert, die Balance zwischen Digitalisierung, Innovation und menschlicher Kontrolle herzustellen. Nur so lassen sich nachhaltige, vertrauenswürdige und unabhängige Sicherheitslösungen entwickeln, die den Schutz des Einzelnen und der Gesellschaft gleichermaßen gewährleisten.

Frohe Festtage!

Euro Security wünscht allen in der Branche frohe Festtage. Mögen wir in den kommenden Wochen Kraft schöpfen, um im neuen Jahr gemeinsam an einem unabhängigen, sicheren Europa zu arbeiten und die Sicherheitsbranche als wachstumsstarkes Segment auch in Krisenzeiten zu erhalten. Innovation, Menschlichkeit, Mut und die verantwortungsvolle Nutzung digitaler Möglichkeiten sind die Bausteine, auf denen wir die Sicherheit von morgen gestalten können. **[Dr Claudia Mrozek]**

Verkada



Die führende Lösung für physische Sicherheit

Scannen Sie den QR-Code, um eine personalisierte Demo zu vereinbaren.



Sicherheit optimal vernetzt

ASSA ABLOY und Kentix orchestrieren Sicherheit neu

„Wir bündeln Zutritt, Brand-, Umwelt- und Netzwerküberwachung – in einer einzigen Plattform."

Mit der Integration von Kentix setzt ASSA ABLOY ein strategisches Signal im Markt für hochvernetzte Sicherheitslösungen. Beide Unternehmen vereinen ihre Stärken zu einem technologischen Gesamtansatz, der physische Sicherheitsanforderungen in Rechenzentren und kritischen Infrastrukturen ganzheitlich adressiert. Kentix bringt eine ausgereifte IoT-Plattform mit, die zentrale Sicherheitsfunktionen in einer einzigen Architektur konsolidiert und dadurch Komplexität, Kosten und Aufwand deutlich reduziert. ASSA ABLOY erweitert dieses technologische Fundament um globale Präsenz, etablierte Vertriebskanäle und langjährige Erfahrung in der Absicherung sensibler Umgebungen. Für Betreiber entsteht ein integriertes Sicherheitsökosystem, das frühe Gefahrenerkennung, hohe Skalierbarkeit und konsistente Compliance-Prozesse ermöglicht. Gleichzeitig bleibt Kentix als Standort, Team und Innovationsmotor bewusst erhalten – und wird so zum zentralen Baustein einer gemeinsamen, zukunftsorientierten Sicherheitsstrategie.

Wie lassen sich komplexe Sicherheitsanforderungen in Rechenzentren und kritischen Infrastrukturen effizient bündeln? Im Gespräch mit Euro Security geben die Verantwortlichen Joachim Mahlstedt, Chief Commercial Officer DAS bei ASSA ABLOY / Managing Director Kentix GmbH, und Thomas Fritz, Managing Director Kentix GmbH, spannende Einblicke: Sie erklären, welche Vorteile die Integration von KentixONE für Kunden bringt, wie die Technologie in das globale Portfolio von ASSA ABLOY eingebunden wird und welche Perspektiven sich für Mitarbeitende und Märkte ergeben. Ein Blick hinter die Kulissen einer Partnerschaft, die Sicherheit neu definiert.



ES: Herzlichen Glückwunsch zur Übernahme: Warum hat sich ASSA ABLOY für Kentix entschieden – und warum gerade jetzt?
Mahlstedt: „Vielen Dank. Die Übernahme von Kentix passt genau zur strategischen Ausrichtung von ASSA ABLOY, unsere Position im Bereich digitaler Sicherheitslösungen für Rechenzentren und kritische Infrastrukturen zu stärken. Kentix verfügt über eine hervorragende IoT-Plattform-Expertise sowie agile Innovationskraft – genau diese Technologiekompetenz wollten wir zusätzlich ins Portfolio holen. Zudem eröffnet die Integration neue Märkte und Vertriebskanäle in der EMEIA-Region, was zu einem sehr guten Zeitpunkt kommt. Kunden profitieren jetzt von einem umfassenden Portfolio aus innovativen ASSA ABLOY- und Kentix-Lösungen."



ES: Welche konkreten Ziele verfolgen Sie mit der Integration von Kentix in die ASSA ABLOY Gruppe?
Mahlstedt: „Zum einen möchten wir die technologische Exzellenz und Agilität von Kentix bewahren – diese Werte haben wir als sehr wichtig identifiziert. Zum anderen wollen wir gemeinsam mit Kentix die Skalierung vorantreiben: Wir sehen enormes Potenzial in Data-Center-Lösungen, in verteilten Infrastrukturen (Edge, PoP-Sites) sowie im Umfeld kritischer Infrastrukturen



(KRITIS), und durch die globale Ausrichtung von ASSA ABLOY können wir diese Lösungen international schneller ausrollen."

ES: Was ändert sich für Kunden und Mitarbeitende von Kentix durch die Übernahme – bleibt z. B. der Standort erhalten, bleibt das Team bestehen?

Mahlstedt: „Ja – wir haben ausdrücklich betont, dass der Standort in Idar-Oberstein erhalten bleibt und das bestehende Kentix-Team weitergeführt wird. Für unsere Kunden heißt das: Bewährte Ansprechpartner bleiben bestehen, und wir schaffen zugleich zusätzliche Ressourcen und Entwicklungsmöglichkeiten. Für Mitarbeitende ergeben sich neue Chancen durch den internationalen Rahmen von ASSA ABLOY."

ES: Kommen wir zur technologischen Seite: KentixONE wird als „8-in-1" Physical SecurityPlattform bezeichnet – können Sie erläutern, welche acht Sicherheitsfunktionen damit gemeint sind?

Fritz: „Gerne. Die Plattform KentixONE bündelt acht herkömmliche Sicherheits- bzw. Überwachungssysteme in einer IoT-Lösung. Dazu zählen unter anderem die Zutrittskontrolle, Einbruchalarmierung, Videoüberwachung, Netzwerk-Monitoring, Umgebungs- bzw. Umwelt-Monitoring, Brandfrüherkennung, Leistungsüberwachung sowie externe Störmeldungen. Das sind im Wesentlichen die Systeme, die

zur Überwachung kritischer digitaler Infrastrukturen am wichtigsten sind, z. B. Edge Data Center, verteilte Infrastrukturen in Telekommunikation und Versorgung, aber auch industrielle Anwendungen.

ES: Welche Rolle spielt KentixONE konkret im Data-Center-Umfeld – und welche Anforderungen lassen sich damit adressieren?
Fritz: „Im Data-Center-Umfeld ist physische Sicherheit genauso wichtig wie IT-Sicherheit. Mit KentixONE können wir über 40 physische Gefahren proaktiv überwachen – angefangen bei unbefugtem Zutritt, Brandrisiken, Umgebungsbedingungen bis hin zu Ausfällen in der Stromversorgung. Zudem unterstützt die Plattform Standards wie ISO 27001, EN 50600 oder gesetzliche Vorgaben wie NIS-2 oder CER – also genau das Umfeld, in dem Betreiber von Rechenzentren und kritischen Infrastrukturen agieren."

Im Umfeld von Data Centern und kritischen Infrastrukturen bietet KentixONE eine sehr zielgerichtete, kosteneffiziente und leicht integrierbare Lösung mit vielen relevanten Funktionen für die physische Sicherheit. Im Gegensatz zu den großen „All-Purpose"-PSIM-Systemen, die eine extrem breite Basis und Tiefe bieten, ist KentixONE speziell auf solche Umgebungen zugeschnitten – und damit weniger komplex, teuer und aufwändig.

ES: Integration in vorhandene IT/OT-Infrastrukturen ist ja oft eine Herausforderung – wie adressiert KentixONE diese Herausforderung?
Fritz: „Bei KentixONE wird großer Wert auf eine nahtlose Integration gelegt. Die Software kann on-premise als Hardware-Appliance oder Docker-Container ausgeführt werden, bietet offene Schnittstellen (REST-API) und ist mit bestehenden Systemen kompatibel. Die Software-defined-Hardware-Architektur (SDH) ermöglicht zudem eine flexible Skalierung und Resilienz. Selbst bei Ausfall einzelner Netzwerksegmente bleiben zentrale Sicherheitsfunktionen aktiv. Als Kentix bieten wir zudem einen kompletten Systembaukasten mit IoT-basierter Sensorik und Aktorik für nahezu jede Anforderung zur Absicherung kritischer Infrastrukturen an. Damit wird die Integration in die Infrastruktur unserer Kunden sehr einfach. Wir sind seit vielen Jahren Vorreiter im Bereich integrierter physischer Sicherheitslösungen. Mit unserem Kentix MultiSensor haben wir die Überwachung von IT-, Technik- und Infrastrukturräumen revolutioniert und erheblich vereinfacht. In den letzten 15 Jahren hat der Kentix MultiSensor viele Unternehmen vor Ausfällen und Totalverlusten bewahrt.

ES: : Wie sieht der Nutzen für Kunden konkret aus – etwa in Bezug auf Kosten, Betrieb oder Effizienz?
Fritz: Mit KentixONE können KRITIS- und Data-Center-Betreiber ihre Kosten deutlich reduzieren, da mehrere Sicherheitssysteme in einer einzigen Plattform zusammengeführt werden.
Der Betrieb wird einfacher, da alle Alarme und Gewerke zentral in einer Oberfläche verwaltet werden und weniger Aufwand für Wartung und Integration entsteht.
Gleichzeitig erhöht sich die Effizienz: Gefahren werden früher erkannt, Einsätze können zielgerichteter geplant werden und die Zahl der Fehlalarme sinkt.
Für verteilte Standorte bietet KentixONE ein einheitliches Bedien- und Sicherheitskonzept, das Rollouts und Erweiterungen spürbar beschleunigt.
Zudem erleichtert die Plattform die Erfüllung von Compliance- und Audit-Anforderungen, da physische Sicherheitsnachweise zentralisiert und konsistent bereitgestellt werden. Insgesamt profitieren Betreiber kritischer Infrastrukturen somit von einer sichereren, transparenteren und deutlich schlankeren Betriebsführung bei stark reduzierten Kosten.

ES: Welche Rolle spielt die Übernahme von Kentix für das Gesamtportfolio von ASSA ABLOY im Sicherheitsbereich?
Mahlstedt: „Die Integration von Kentix ergänzt unser Zutritts- und Zugangslösungsportfolio um digitalisierte IoT-Überwachungsfunktionen – insbesondere für Rechenzentren und kritische Infrastrukturen. Damit können wir unseren Kunden nicht nur mechanische oder elektronische Tür- bzw. Zutrittskontrollen bieten, sondern ein gesamtheitliches Monitoring- und Sicherheits-Ökosystem. Kurz gesagt: Wir erweitern unser Angebot vom Zugang hin zur umfassenden physischen Infrastruktur-Sicherheit."

ES: Welche Innovationsfelder oder Weiterentwicklungen sehen Sie mit dieser Kombination von ASSA ABLOY + Kentix in der Zukunft?
Mahlstedt: „Wir sehen mehrere spannende Felder:
Erstens die Skalierung in neue Märkte – Edge-Data-Center, verteilte Infrastrukturen, internationales Wachstum.
Zweitens die Weiterentwicklung der KentixONE-Plattform – z. B. erweiterte Visualisierung (Gebäude-, Anlagenpläne), KI/-Analytics-Funktionen, noch tiefere Integration in OT/IT-Umgebungen.
Drittens sehen wir das Zusammenspiel mit Zutritts- und Zugangslösungen von ASSA ABLOY – also ein ganzheitlicher „Physical & Digital Security" Ansatz."

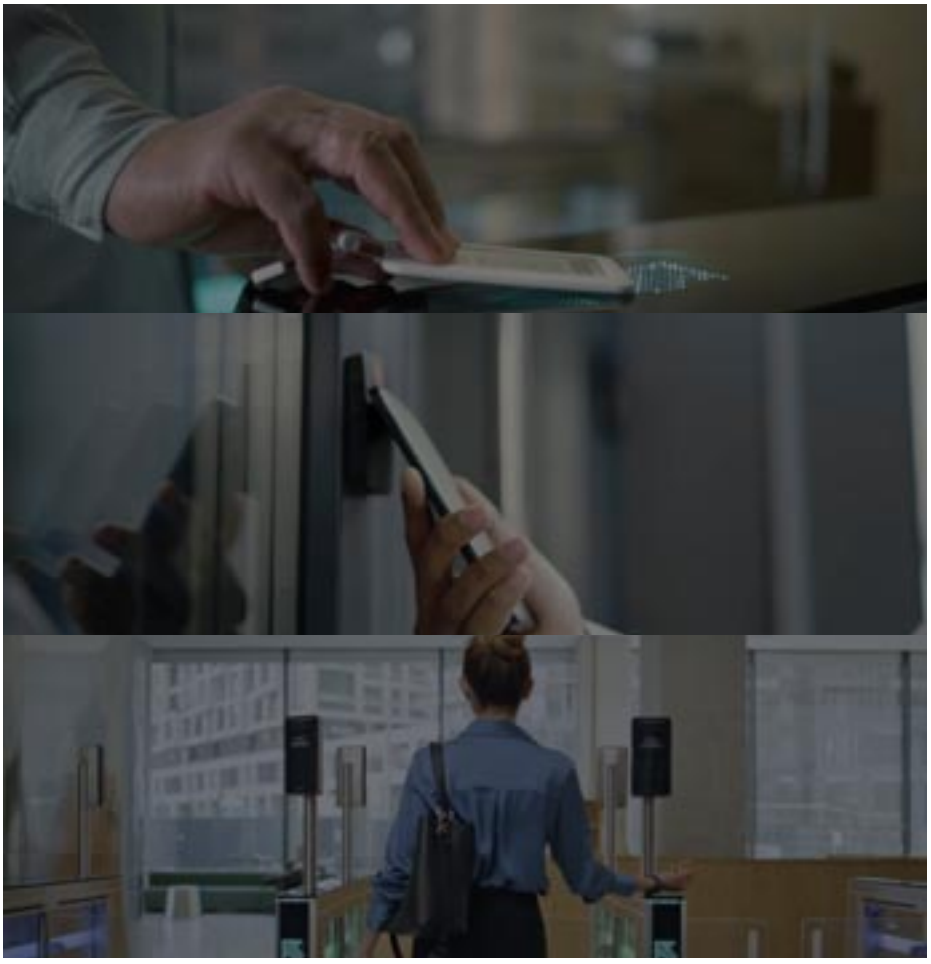
ES: Zum Schluss: Welche Botschaft möchten Sie den Lesern von Euro Security mitgeben – insbesondere jenen Verantwortlichen für Sicherheit in Rechenzentren und kritischen Infrastrukturen?
Fritz: „Mein Appell lautet: Physische Sicherheit und digitale Überwachung wachsen zusammen – wer heute Rechenzentren oder kritische Anlagen betreibt, darf dieses Zusammenspiel nicht ignorieren.
Mit der Bündelung von Zutritt, Brand-, Umgebungs- und Netzwerk-Überwachung in einer einzigen Plattform setzen wir mit KentixONE ein klares Zeichen für Zukunftsfähigkeit, Skalierbarkeit und Effizienz. Und mit ASSA ABLOY als Partner verfügen Betreiber über ein internationales Netzwerk und Ressourcen. Nutzen Sie diese Entwicklung, um Ihre Infrastrukturen resilient und sicher aufzustellen."

ES: Danke für das Gespräch.

Was bedeutet NIS-2 wirklich für Ihre physische Zutrittskontrolle?

Compliance-Beauftragte kennen das Szenario: Sie investieren Millionen in Netzwerksicherheit, implementieren ausgefeilten Endpunktschutz und richten eine Zero-Trust-Architektur ein – doch all das nützt nichts, wenn jemand durch eine unverschlossene Tür in den Serverraum gelangt.

Die NIS-2-Richtlinie greift genau diese Realität auf. Gemäß Artikel 21 ist die physische Zutrittskontrolle keine Aufgabe der Haustechnik mehr, sondern eine Cybersicherheitsaufgabe mit dem gleichen regulatorischen Gewicht wie Firewall-Richtlinien. Unternehmen müssen physische Sicherheitsmaßnahmen implementieren, die unbefugten Zutritt zu kritischen Infrastrukturen, Rechenzentren und operativen Technologieumgebungen verhindern.



Für CISOs und Facility Manager in wesentlichen und wichtigen Einrichtungen der EU bedeutet dies nicht nur eine Richtlinienaktualisierung. Es handelt sich um eine vollständige Neudefinition von Sicherheitsstrategie, Budgetbefugnissen und Managementverantwortlichkeiten.

Warum NIS-2 die physische Zutrittskontrolle als wesentliche Cybersicherheit behandelt

Seit Jahrzehnten galt: IT sichert das Netzwerk, Facility Management sichert das Gebäude. Diese klare Trennung wird nun zu einer regulatorischen Haftung.

Das Ende der physisch-digitalen Sicherheitstrennung

Artikel 21 der NIS-2-Richtlinie hebt die Unterscheidung zwischen physischen und digitalen Sicherheitsmaßnahmen auf. Die Richtlinie verlangt ausdrücklich „Sicherheitsmaßnahmen für die physische Sicherheit der Gebäude und Einrichtungen der Unternehmen“ als Teil eines umfassenden Cybersicherheits-Risikomanagements. Dies ist keine Empfehlung, sondern eine gesetzliche Verpflichtung, unterstützt durch obli-

gatorische Audits, grenzüberschreitende Zusammenarbeit von Regulierungsbehörden und erhebliche finanzielle Sanktionen.

Die Logik ist einfach: Unbefugter physischer Zutritt zu einem Rechenzentrum, Serverraum oder industriellen Steuerungssystem macht alle Investitionen in digitale Sicherheit wertlos. Wer physischen Zutritt hat, muss keine Verschlüsselung knacken oder Multi-Faktor-Authentifizierung überwinden – er geht einfach durch die unbewachte Tür.

Was ist NIS-2 Artikel 21?

Artikel 21 schreibt physische Sicherheitsmaßnahmen als Bestandteil des Cybersicherheits-Risikomanagements vor.

Unternehmen müssen den unbefugten Zutritt zu kritischen Bereichen mit derselben Sorgfalt verhindern, wie sie digitale Sicherheitsmaßnahmen umsetzen.

Die versteckten Compliance-Lücken für CISOs und Facility Manager

Viele Unternehmen glauben, dass sie ausreichend physisch geschützt sind. Sie verfügen über Ausweislesegeräte, verschlossene Türen und Sicherheitspersonal. Dennoch zeigen Audits regelmäßig drei kritische Schwachstellen:

1. Standalone-Systeme ohne Nachweisbarkeit: Viele Zutrittskontrollsysteme sind noch isoliert und können keine Daten an zentrale Critical Event Management (CEM)-Plattformen weiterleiten. Protokolle existieren, sind aber in proprietären Formaten oder lokalen Datenbanken gespeichert – nicht zentralisiert oder analysierbar.
Für Auditoren bedeutet dies ein Problem: NIS-2 verlangt protokollierte und überprüfbare Zutrittsereignisse. Unternehmen mit Standalone-Systemen können diese Anforderungen oft nicht effizient erfüllen, obwohl physische Kontrollen technisch vorhanden sind.

2. Fragmentierte Zuständigkeiten zwischen IT und Facility Management: CISOs verantworten IT-Sicherheit, Facility Manager die physische Sicherheit. NIS-2 verlangt jedoch die Integration physisch-digitaler Sicherheitsmaßnahmen. Ohne klare Zuständigkeiten entstehen Risiken bei Budget, Incident Response und Schulungen:

- Budgetanträge fallen zwischen Abteilungen durch
- Notfallpläne berücksichtigen keine physischen Sicherheitsverstöße
- Sicherheitsbewusstsein fokussiert nur auf digitale Bedrohungen, Tailgating oder Credential Sharing werden vernachlässigt

3. Überwachungs- und Dokumentationslücken
NIS-2 verlangt Protokollierung, Echtzeitüberwachung und Meldung innerhalb von 24 Stunden bei Sicherheitsverstößen. Digitale Systeme erfüllen dies oft über SIEM oder SOCs. Ältere Zutrittskontrollen hingegen speichern Daten isoliert, Fehlversuche und Zugriffe außerhalb der Bürozeiten werden nicht aktiv überwacht.

Das Risiko: Auch bei vorhandenen Kontrollen kann Compliance nicht nachgewiesen werden. Dokumentationslücken gelten als Verstöße.

Zero-Trust-Framework für physische Zutrittskontrolle

Das Prinzip „nie vertrauen, immer überprüfen" sollte auf jede physische Zugangskontrolle angewendet werden. Jeder Zugang wird in Echtzeit geprüft, jeder Zugangspunkt kontinuierlich überwacht.

Jede Zutrittsanfrage überprüfen
Im Zero-Trust-Modell reicht der Besitz einer gültigen Ausweiskarte nicht mehr. Moderne Zutrittskontrollen kombinieren MFA, Biometrie oder mobile Authentifizierung.

Vorteile:
- Gestohlene oder geklonte Ausweise sind nutzlos
- Credential Sharing wird verhindert
- Verlorene Ausweise stellen kein Risiko mehr dar

Least-Privilege-Zutritt
Zutritt wird nach Jobfunktion und Zeitfenstern beschränkt. Zeitarbeiter oder Auftragnehmer erhalten nur temporären Zugang. Auch Führungskräfte unterliegen denselben strengen Verifizierungs- und Überwachungsprotokollen.

Kontinuierliche Überwachung und Protokollierung

Alle Zutritte – erfolgreich oder fehlgeschlagen – werden zentral protokolliert und in SIEM- oder CEM-Plattformen integriert. Echtzeitwarnungen erkennen:

* Mehrfache Nutzung einer Karte an verschiedenen Orten
* Zutritte zu ungewöhnlichen Zeiten
* Wiederholte Fehlversuche
* Unbefugten Zutritt zu eingeschränkten Bereichen
* Tailgating

So lassen sich Vorfälle proaktiv verhindern und Audit-Anforderungen sofort erfüllen.

Physische Sicherheit ist Cybersicherheit unter NIS-2

Die Prämisse ist klar: digitale Sicherheitsmaßnahmen allein reichen nicht aus. Eine unbewachte Tür kann jede Firewall und Verschlüsselung außer Kraft setzen.

CISOs müssen physische Sicherheitsrisiken in Risikobewertungen einbeziehen, Notfallpläne anpassen und physische Zutrittsprotokolle in digitale Sicherheitsüberwachung integrieren. Facility Manager müssen physische Zutrittskontrollen nach denselben Standards überwachen, dokumentieren und auditen wie IT-Systeme.

Unternehmen, die diese Konvergenz erfolgreich umsetzen, schaffen widerstandsfähigere Sicherheitsstrukturen, reduzieren Risiken und erfüllen regulatorische Anforderungen.

Fazit
Ihre Serverraumtür ist jetzt ein Cybersicherheits-Objekt. Die zentrale Frage lautet: Verwalten Sie sie entsprechend?

[www.primion.io]

KI bestimmt den Takt: Die wichtigsten IT-Trends für 2026

Die Dynamik in der IT-Welt schafft ein Umfeld, in dem Chancen und Risiken enger denn je miteinander verwoben sind. Vor diesem Hintergrund entstehen neue Möglichkeiten – von deutlich gesteigerter Produktivität bis hin zu vollständig neu gedachten Geschäftsmodellen – aber auch ernstzunehmende Herausforderungen für die Sicherheit, Governance und Ethik. Im Jahr 2026 erreicht der Einsatz von künstlicher Intelligenz eine neue Reifephase, in der KI nicht mehr als separate Technologie betrachtet wird, sondern als grundlegende Ebene moderner IT-Architekturen. Eduardo Crespo, Vice President EMEA bei PagerDuty, sieht diese Entwicklung als Ausgangspunkt für die wichtigsten Prognosen, die das IT-Jahr 2026 bestimmen werden:

Europa wird erneut zum Wachstumsmotor

Auch wenn die Wachstumsprognosen für 2026 moderat ausfallen – Europa hat durchaus die Chance, wieder zum Wachstumsmotor zu werden und der Dominanz der USA etwas entgegenzusetzen. Wenn sich die Inflation weiterhin stabilisiert und wie prognostiziert in den nächsten zwei Jahren bei ca. zwei % einpendelt, dann werden europäische Unternehmen ihre bislang aufgeschobenen Investitionsentschei- dungen in neue Technologien wie GenAI und KI-Agenten in die Tat umsetzen. Damit wird die digitale Transformation auch in Europa noch mehr an Fahrt gewinnen. Europa kann 2026 und in den darauffolgenden Jahren wieder Wachstumsimpulse setzen und eine führende wirtschaftliche Rolle einnehmen, wenn es gelingt, die politischen Rahmenbedingungen für eine bessere Wettbewerbsfähigkeit zu schaffen, Investitionen zu steigern und externe Risiken wie Handelskonflikte zu minimieren.

Unternehmen korrigieren ihre Personalstrategie

Der Einsatz von KI verändert die Anforderungen an Mitarbeitende grundlegend. Die Technologie stellt unsere Arbeitswelt, wie wir sie jahrzehntelang kannten, in einem atemberaubenden Tempo auf den Kopf. Doch 2026 wird sich zeigen, dass manche Unternehmen vorschnell gehandelt und wertvolle Arbeitskräfte übereilt entlassen haben. Sie werden einen Teil der Mitarbeitenden wieder zurückholen und eventuell neue Kandidaten mit spezifischen KI-Kenntnissen neu einstellen, um ihre ambitionierten Ziele bei der Implementierung von KI-gestützten Systemen zu realisieren und auszuweiten. Dabei kommt der kontinuierlichen Weiterbildung und -entwicklung der Mitarbeitenden eine Schlüssel- rolle zu.

DORA-Verstöße – von der Überwachung zum Vollzug

Die seit Januar 2025 EU-weit geltende DORA-Verordnung (Digital Operational Resilience Act) legt für Akteure im Finanzsektor klare Regeln für das Management von IT-Risiken fest – auch durch Drittanbieter, die Meldung von Vorfällen, die Durchführung von Sicherheitstests sowie den Austausch von Informationen zum Schutz vor Cyberrisiken.

DORA stellt sicher, dass Verstöße gegen die digitale operationale Widerstandsfähigkeit konsequent geahndet werden, um die Stabilität des Finanzsektors zu gewährleisten und Reputationsschäden zu vermeiden. Die Verordnung sieht ein strenges Sanktionssystem und empfindliche Geldbußen vor. Für die Einhaltung und den Vollzug ist in Deutschland die BaFin zuständig. Deutsche und europäische Unternehmen müssen sicherstellen, dass ihre operative Resilienz nicht nur dem Standard entspricht, sondern auch reaktionsfähig ist. Seit Inkrafttreten von DORA wurde zunächst auf Überwachung, Prüfung und Verwarnung gesetzt. Das dürfte sich im kommenden Jahr jedoch ändern: Im Wiederholungsfall und bei schwerwiegenden Verstößen werden die Behörden 2026 mehr und mehr dazu übergehen, den Sanktionsrahmen auch konsequent zu nutzen und u.a. Geldbußen zu verhängen.

Ethik und Regulierung prägen die nächste Phase der KI-Einführung

Je vernetzter Unternehmen agieren und je tiefer KI-gestützte Systeme in den Arbeitsalltag integriert werden, umso klarer wird die Notwendigkeit, die weitere Entwicklung verstärkt unter ethischen Aspekten voranzubringen. Europäische Regierungen und Unternehmen werden 2026 ihren Fokus zunehmend auf den ethischen Einsatz von KI legen, um das Vertrauen ihrer Kunden zu sichern. Auch wenn KI-Modelle zunehmend autonom handeln, muss jederzeit nachvollziehbar sein, welche menschliche Instanz für Entscheidungen haftet und wie Fehlverhalten oder Verzerrungen korrigiert werden.

Unternehmen werden sicherstellen, dass Mitarbeitende über ausreichende KI-Kompetenz verfügen, um Risiken verantwortungsvoll zu managen: Transparenz, Fairness, Datenschutz und Schutz vor Diskriminierung müssen gewährleistet sein, da KI-Systeme bestehende Biases verstärken oder sensibelste Daten verarbeiten können. Regulierungen wie der EU AI Act setzen dafür Mindeststandards, doch die Vorschriften werden sich weiterentwickeln, um den immer neu entstehenden Herausforderungen gerecht zu werden.

Der Weg zum vollständig KI-gesteuerten Unternehmen

Eine Prognose, die über das Jahr 2026 hinausgeht, nimmt Bezug auf die Frage, wie

weit der Einsatz von KI-Tools in Unternehmen gehen wird. KI-Agenten, die immer enger mit Menschen zusammenarbeiten und sich dadurch täglich verbessern, werden in naher Zukunft alle zentralen operativen Geschäftsabläufe orchestrieren – von der Produktentwicklung über die Robotersteuerung bis hin zu Kundeninteraktionen.

Doch nicht nur operativ, sondern auch strategisch wird KI eine immer größere Rolle spielen, wie z.B. bei der Entwicklung von Innovationen oder der Gestaltung der Kundenerfahrung. Das Vertrauen in die KI bleibt jedoch auch in den kommenden Jahren essenziell für erfolgreiche, KI-gesteuerte Unternehmen.

Eduardo Crespo ist VP EMEA bei PagerDuty. Er verfügt über mehr als 20 Jahre Erfahrung im Investment Banking, in der Strategieberatung und innovativen Cloud- und Softwarelösungen. Zuletzt war Eduardo Crespo Teil der Management-Teams von Medallia, einem führenden SaaS-Unternehmen im Bereich Experience Management, und begleitete das Unternehmen von der Serie-C-Finanzierung bsi zum Börsengang an der NYSE.





Die SALTO-Story

Ein Vierteljahrhundert Zugang neu gedacht

Salto feiert 25 Jahre voller Innovation und inspirierender Zutrittslösungen

Salto Systems, ein weltweit führender Anbieter von smarten Zutrittstechnologien, feiert im Jahr 2025 sein 25-jähriges Bestehen. Seit der Gründung im Jahr 2000 revolutioniert Salto, wie Menschen Türen öffnen und Räume sichern – aus einem kleinen Start-up in Nordspanien wurde ein globaler Technologieführer, der mit seinem intelligenten Zutritts-Ökosystem Türen zu neuen Chancen, Verbindungen und Wachstum öffnet. Gegründet mit der Vision, universell einsetzbare, kabellose und vernetzte Schließsysteme zu schaffen, ist Salto heute zu SALTO WECOSYSTEM gewachsen – einer globalen Unternehmensgruppe, die die Branchenpioniere Gantner, Salto und Vintia unter einem Dach vereint. Gemeinsam bieten diese Marken hochmoderne Lösungen für Zutrittskontrolle, Ticketing, Identitätsmanagement und elektronische Schließtechnik.

Heute sind Salto-Technologien in über 100.000 Installationen und an 10 Millionen Zutrittspunkten im Einsatz und ermöglichen täglich mehr als 40 Millionen Menschen sicheren Zugang – verteilt über mehr als 40 Länder weltweit. Mit über 1.850 Mitarbeitenden steht Salto für kontinuierliche Innovationskraft und nutzerzentriertes Design und ist ein vertrauenswürdiger Partner für zahlreiche Branchen. „Unser Jubiläum ist sowohl eine Feier unserer bemerkenswerten Reise als auch ein Bekenntnis zu einer ambitionierten Zukunft. Wir werden weiterhin mit modernsten Technologien intelligente Zutrittslösungen vorantreiben, um unseren Anwendern weltweit sichere und smarte Erlebnisse zu ermöglichen“, sagt Marc Gomez, CEO von SALTO WECOSYSTEM, anlässlich des 25-jährigen Jubiläums.

Von der ersten Idee zum Technologieführer

Was im Jahr 2000 mit der radikalen Idee eines völlig kabellosen, batteriebetriebenen Türschlosses begann, hat die Zutrittskontrolle grundlegend verändert. Salto entwickelte eines der ersten eigenständigen elektronischen Schlösser, das ohne mechanischen Schlüssel auskommt. Bereits 2002 folgte mit dem SALTO Virtual Network der nächste Meilenstein: Diese Daten-auf-Karte-Technologie ermöglichte es, Zutrittsrechte kontaktlos auf RFID-Smartcards zu speichern und Türen offline zu vernetzen. Schlüsselkarten wurden dadurch zu intelligenten Datenträgern, die Zutrittsdaten beim Vorhalten an Türlesern austauschen konnten. Spätestens mit der Vorstellung von SALTO Wireless im Jahr 2008 verabschiedete sich Salto vollständig von verkabelten Lösungen – erstmals ließ sich ein Zutrittssystem in Echtzeit steuern, ohne dass irgendwelche Kabel zu den Türen gelegt werden mussten. Dieses erste funkvernetzte Zutrittssystem verband autonome batteriebetriebene Türschlösser online mit zentraler Steuerung – ein Durchbruch in der Branche.

In den 2010er-Jahren wandelte sich Salto vom reinen Hardwarehersteller zum Lösungsanbieter mit einer offenen Plattform-Strategie. Statt isolierter Schließgeräte entwickelte Salto umfassende Systeme aus Türhardware, Software und Cloud-Diensten. So war Salto ein Vorreiter bei cloud-



2001 - Die Saltogründer (v.l.n.r.): Marc Handels und Javier Roquero. Alle Fotos ©Salto



Gründung von Salto Systems Deutschland im Jahr 2010: v.l.n.r. Saltogründer Javier Roquero, Thomas Schmidt, Geschäftsführer DACH und Saltogründer Marc Handels

Historische Meilensteine

2000 Gründung von Salto Systems in Spanien mit dem Ziel, kabellose, batteriebetriebene und vernetzte Zutrittssysteme zu entwickeln.

2002 Einführung des SALTO Virtual Network (SVN) – ein Daten-auf-Karte-System, das eine sichere virtuelle Vernetzung von Türschlössern ohne kabelgebundene Verbindung ermöglicht.

2008 Präsentation von SALTO Wireless, dem ersten funkvernetzten Zutrittssystem für kabellose Echtzeit-Zutrittskontrolle.

2014 Launch von Clay by Salto (heute SALTO KS), einer der ersten cloudbasierten Zutrittsplattformen (Access-Control-as-a-Service) für ortsunabhängiges Schlüsselmanagement.

2015 Einführung von JustIN Mobile – Salto gehört zu den ersten Anbietern, die Mobile Access per Smartphone (via App, NFC/Bluetooth oder Wallet) ermöglichen.

2020 Übernahme des österreichischen RFID-Spezialisten Gantner Electronic, Erweiterung des Portfolios um Ticketing-, Bezahlsysteme und Schrankschließtechnik; die kombinierte Produktionskapazität steigt auf über 1 Million Zutrittspunkte jährlich.

2024 Neupositionierung als SALTO WECOSYSTEM – ein gemeinsamer Markenauftritt für Salto, Gantner und Vintia. Marc Gómez übernimmt ab April 2024 als Group-CEO, während Mitgründer Javier Roquero in den Vorstand wechselt[Gleichzeitig entsteht die Salto-Stiftung zur Förderung sozialer Initiativen.

2025 Markteinführung neuer Lösungen wie XS4 Face (Gesichtserkennung mit mobiler Nutzerverwaltung) und das ID-Management-System Salto IDM; Salto begeht sein 25-jähriges Jubiläum als Innovationsführer der Zutrittsbranche.

basierten Zutrittslösungen: Bereits 2014 wurde mit Clay by Salto (später Salto KS) eine Access-Control-Cloud eingeführt, lange bevor „Access as a Service" zum Branchenstandard wurde. Die Online-Verwaltung von Zutrittsrechten in Echtzeit – ohne lokale Server – erlaubte es insbesondere Betreibern moderner Gebäude, Büros und Co-Working-Spaces, ihre Anlagen flexibel und ortsunabhängig zu steuern. 2015 gehörte Salto außerdem zu den ersten Unternehmen mit Mobile Access: Über JustIN Mobile konnten Nutzer per Smartphone Türen öffnen, was in Hotels und Büroumgebungen schnell auf große Resonanz stieß. Parallel legte Salto verstärkt Wert auf Design und Nutzererlebnis. Die elektronischen Beschläge und Leser wurden in modernen, schlanken Designs und verschiedenen Farben angeboten, sodass sie sich nahtlos in Hotel- oder Wohnumgebungen einfügen. Diese Kombination aus Ästhetik und Funktionalität trug dazu bei, die Akzeptanz elektronischer Schließsysteme in Bereichen wie Hotellerie und Wohnen deutlich zu erhöhen. Salto etablierte sich so als Anbieter, der Sicherheitstechnik und Architekturdesign erfolgreich vereint.

Globale Expansion und strategische Übernahmen

Mit dem technologischen Erfolg einher ging eine konsequente internationale Expansion. Salto verfolgte das Prinzip „Global denken, lokal handeln" und baute ein weltweites Vertriebs- und Servicenetz auf. Lokale Tochtergesellschaften und Niederlassungen wurden in den Schlüsselregionen Europas, Amerikas, Asiens und Ozeaniens gegründet, um Kunden vor Ort besser betreuen zu können. Bereits in den 2000er-Jahren eröffnete Salto erste Auslandsbüros; bis 2020 war das Unternehmen mit eigenen Niederlassungen in über 30 Ländern präsent, und Mitte der 2020er-Jahre stieg diese Zahl auf fast 50 Länder an. Die lokalen Teams kümmerten sich um Vertrieb, Installation und Support, was nicht nur den kulturellen und marktbezogenen Besonderheiten gerecht wurde, sondern auch das Vertrauen der Kunden stärkte – denn sie hatten stets regionale Ansprechpartner. Diese globale Präsenz trug maßgeblich dazu bei, Salto als Weltmarke für Zutrittslösungen zu etablieren.





Um das Wachstum weiter zu beschleunigen und technologische Synergien zu nutzen, setzte Salto ab 2015 verstärkt auf strategische Übernahmen. Ein entscheidender Schritt war die Eingliederung der österreichischen Gantner Electronic im Jahr 2020. Gantner, ein Spezialist für elektronische Zugangs- und Abrechnungssysteme (u. a. in Freizeiteinrichtungen, Hochschulen und Unternehmen), ergänzte das Salto-Portfolio ideal – etwa durch Lösungen für Schließfächer, bargeldloses Bezahlen, Ticketing und Besuchermanagement.

Durch die Übernahme konnte Salto seine



Foto oben: Die ersten Beschläge wurden vor 25 Jahren präsentiert und begründeten unter anderem die Erfolgsstory von Salto **Foto mitte:** Das ExperienceCenter im Headquarter im Jahr 2023. **Foto unten:** Das Gruppenfoto auf der Security in Essen zeigt den Erfolg, die bedeutung und das Wachtumspotential des Unternehmens. Wichtig für das Salto-Team ist die die Vision: Fortschrift istkein Produkt. Es ist eine Haltung! Fotos: @SaltoSystems

Position als ganzheitlicher Lösungsanbieter ausbauen: Gemeinsam verfügte man nun über eines der umfangreichsten Produktportfolios am Markt und die Fähigkeit, über eine Million Zutrittspunkte pro Jahr auszuliefern. Gleichzeitig wuchs das Team und vereinte geballtes Know-how in Forschung und Entwicklung. Weitere Akquisitionen – wie die früheren Zukäufe des niederländischen Start-ups Clay (2017) und des dänischen Smartlock-Herstellers Danalock (2017) sowie Conlan (2019) – hatten bereits den Weg in Richtung Cloud und Mobilität geebnet. Mit Gantner aber erreichte Salto eine neue Größenordnung und machte einen großen Schritt hin zu einem ganzheitlichen Ökosystem, das alle Aspekte von Zutritt und Benutzererlebnis abdeckt. Zudem entstand 2020 mit Vintia eine neue Konzernmarke (aus Gantner Tikketing hervorgegangen), die sich auf Ticketing- und Buchungssysteme für Freizeitanbieter und Veranstaltungen konzentriert.

Neue Marken-DNA: SALTO WECOSYSTEM

Pünktlich zum 25-jährigen Jubiläum leitete Salto 2024 einen umfassenden Marken- und Strukturwandel ein. Unter der neuen Dachmarke SALTO WECOSYSTEM wurden die drei Kerngeschäfte – Zutrittskontrolle (Salto), Identifikations- und Bezahllösungen (Gantner) sowie Ticketing- und Besuchermanagement (Vintia) – in einer gemeinsamen Plattform zusammengeführt. Diese ganzheitliche Markenidentität spiegelt den Anspruch wider, den Kunden ein nahtlos integriertes Ökosystem zu bieten, in dem alle Komponenten perfekt aufeinander abgestimmt sind.

Im Zuge der Neuausrichtung gab es auch personelle Veränderungen an der Unternehmensspitze: Seit April 2024 führt Marc Gómez als Group CEO die Salto-Gruppe, während Mitgründer Javier Roquero nach 23 Jahren die operative Leitung abgab und in den Board of Directors wechselte. Roquero bleibt dem Unternehmen als strategischer Berater verbunden und engagiert sich insbesondere in der neu gegründeten SALTO Foundation, die soziale Projekte – etwa im Bereich Sport und Inklusion – fördert. Mit der SALTO WECOSYSTEM-Struktur wurden zudem globale Teams für Vertrieb, Innovation, Service und Cybersecurity geschaffen, um die Zusammenarbeit innerhalb der Gruppe zu stärken und effizienter auf Marktanforderungen reagieren zu können. Die Firmenführung betont, dass der neue Markenauftritt die Grundlage für eine vielversprechende Zukunft legen soll – geprägt von noch mehr Innovation, Kundennähe und nachhaltigem Wachstum.

Menschen als Schlüssel zum Erfolg

Trotz aller technologischen Meilensteine betont Salto, dass der wahre Schlüssel zum Erfolg in den Menschen liegt, die hinter der Technologie stehen. Von Anfang an waren es leidenschaftliche und hartnäckige Mitarbeitende und Partner, die an die Vision glaubten und sie vorantrieben. Hinter jedem Produkt, jedem Projekt und jedem Innovationssprung stehen Menschen, die Herausforderungen meistern, Ideen einbringen und gemeinsam Lösungen finden. Diese Unternehmenskultur – geprägt von Teamwork, Pioniergeist und der Offenheit, aus Fehlern zu lernen – hat es Salto ermöglicht, sich immer wieder agil an Veränderungen im Markt anzupassen und ambitionierte Ziele zu erreichen.

„The real key to Salto's success goes beyond products or technology – it's about people and partners" („Der echte Schlüssel zum Erfolg liegt nicht in Produkten oder Technik – sondern in den Menschen und Partnerschaften"), heißt es dazu treffend von Seiten Saltos.

Die 25-jährige Geschichte von Salto ist somit auch die Geschichte eines Teams und eines Partnernetzwerks, das gemeinsam Grenzen verschoben und Innovationen möglich gemacht hat. Dieses Bewusstsein spiegelt sich im Leitsatz „Our People" wider, mit dem Salto die Leistungen seiner Belegschaft und seiner Partner ausdrücklich würdigt.

Ausblick: Zugangslösungen der nächsten Generation

Nach einem Vierteljahrhundert Innovationsführerschaft ruht sich Salto nicht auf seinen Lorbeeren aus. Die Weichen für die Zukunft sind gestellt: Bis 2030 soll das Unternehmen in Größe und Reichweite mindestens verdoppelt werden, indem neue Märkte erschlossen und das bestehende Portfolio weiter ausgebaut wird. Technologisch will Salto sein Zutritts-Ökosystem noch enger mit den Smart-Building- und IoT-Welten verknüpfen. Themen wie KI-gestützte Zutrittsanalyse, vorausschauende Sicherheitssysteme und noch stärker personalisierte Nutzererlebnisse stehen auf der Agenda. Ebenso spielt Nachhaltigkeit eine wachsende Rolle – von energieeffizienten, batterielosen Schloss-Technologien bis zur klimaneutralen Produktion am Firmenstandort. Die WECOSYSTEM-Strategie bildet dabei das Fundament, um dieses zukünftige Wachstum zu tragen. Sie soll nicht nur technische Innovation begünstigen, sondern auch die Kundenorientierung und die kulturelle Zusam- menführung der Teams weltweit fördern. Salto sieht in dem neuen ganzheitlichen Ansatz den Schlüssel, die eigene Position als führende Marke für smarte Zutrittslösungen zu festigen und auch künftig als Taktgeber für Innovationen in der Sicherheits- und Gebäudeautomation zu dienen.

Die 25-jährige Erfolgsgeschichte von Salto Systems zeigt eindrucksvoll, wie langfristige Vision, kontinuierliche Innovation und strategische Flexibilität eine Branche verändern können. Aus der bahnbrechenden Idee eines kabellosen, vernetzten Schlosses entstand Schritt für Schritt ein umfassendes Zutritts-Ökosystem, das heute weltweit Millionen von Menschen verbindet.

Salto steht im Jahr 2025 nicht nur für High-Tech-Schließsysteme, sondern für ein intelligentes Zusammenspiel von Menschen, Räumen und digitalen Services. Mit dieser Kombination aus technologischer Exzellenz und einer auf Menschen fokussierten Kultur ist Salto bestens gerüstet, um auch in den kommenden Jahrzehnten die Standards in der Zutrittskontrolle neu zu definieren und die Türen zu einer sicheren, vernetzten Zukunft weit aufzustoßen.

[Begeben Sie sich auf die Reise 25 Jahre Salto Systems: www.salto-systems.com/de-de/25-jahre-salto]

Cloud, Compliance und KI

Wie Verkada die Sicherheitsbranche in Europa neu definiert

Marktstrategische Perspektive aus München

Am Rande des Verkada Security Summit 2025 in München führte Euro Security im Oktober ein ausführliches Gespräch mit Filip Kaliszan, Mitgründer und CEO von Verkada. Die Unterhaltung fand vor dem Hintergrund einer Phase beschleunigter Expansion in Europa statt, in der Verkada seine Position als innovativer Anbieter cloudbasierter Sicherheitslösungen in der DACH-Region und darüber hinaus weiter festigt.

Im Gespräch wurden fünf marktstrategisch relevante Kernpunkte deutlich: Europa gilt als Schlüsselmarkt, dessen heterogene Länderstrukturen und strenge Regulierung ihn komplex machen, zugleich aber zu einem der attraktivsten Wachstumsmärkte für Cloud-basierte Sicherheitslösungen. Deutschland fungiert als Compliance-Labor. Vollständig entwickelte Tools und zertifizierte Prozesse verschaffen Verkada einen Wettbewerbsvorteil, der in anderen europäischen Märkten direkt skaliert werden kann. Der Software-first-Ansatz nutzt die Standardisierung der Hardware, um Kamera-, Zutritts-, Alarm- und Sensoriksysteme zu integrieren und technologischen Vorsprung gegenüber Hardware- zentrierten Mitbewerbern auszuspielen.

Mit KI-basierten Lösungen werden Sicherheitsvorfälle proaktiv erkannt, Fehlalarme reduziert und Kosten minimiert, während operative Effizienz gesteigert wird. Schließlich garantiert Verkada durch strikte Trennung von Kundendaten, länderspezifische Funktionskontrolle und klare Abgrenzung von Massenüberwachung marktführende Ethik und Vertrauen in der DACH-Region.

Europa als Flickenteppich – technologische Chance statt Hürde

Viele US-Unternehmen betrachten Europa als homogenen Markt. Kaliszan betont dazu: „In den USA betrachten viele Europa als einen einzigen Markt. Aber Europa besteht aus verschiedenen Ländern, Kulturen und gesetzlichen Rahmenbedingungen. Man muss jedes einzelne wirklich verstehen."

Für Verkada zeigte sich schnell, dass technologische, kulturelle und regulatorische Unterschiede in jedem Land berücksichtigt werden müssen. Datenschutz, nationale Sicherheitsanforderungen und unterschiedliche Integrationsstandards machen Europa komplex – eröffnen aber zugleich Chancen, frühzeitig marktführende Lösungen zu etablieren.

Das Unternehmen wurde 2016 im Silicon Valley gegründet und fokussierte zunächst den US-Markt. 2019 folgte die erste europäische Niederlassung in London. Die weitere Expansion verzögerte sich durch COVID, da Kaliszan Kunden und Partner zwei Jahre lang nicht persönlich treffen konnte.

Marktdynamik: In Europa dominiert Enterprise statt Mittelstand

In den USA wuchs Verkada zunächst stark im Mittelstand, einem Segment, das neue Technologien schnell adaptierte. In Europa jedoch verhielten sich mittelständische Unternehmen zurückhaltender, insbesondere gegenüber Cloud- und KI-basierten Sicherheitslösungen.

Kaliszan stellte klar: „In Europa verstehen die großen Unternehmen den Wert sehr schnell, gerade in Deutschland, wo Compliance einen so hohen Stellenwert hat".

Diese Marktsegmentierung prägte die europäische Expansionsstrategie maßgeblich.

Deutschland als Testlabor: Strenge Regeln werden zum Wettbewerbsvorteil

Der deutsche Markt ist stark reguliert. Verkada nutzte dies strategisch, indem das Unternehmen alle Compliance-Tools, technischen Richtlinien und Dokumentationen selbst entwickelte. Dies entlastet Partner und Kunden erheblich. Kaliszan erläutert: „Viele Länder sagen schlicht: Wenn es in Deutschland funktioniert, reicht uns das als Nachweis."

Damit avancierte Deutschland nicht nur zu einem Absatzmarkt, sondern zum Innovationsmotor für die gesamte europäische Expansion.



Filip Kaliszan, Mitgründer und CEO von Verkada. Foto: ©Verkada

Cloud in der physischen Sicherheit: Vom Misstrauen zur operativen Effizienz

Als Verkada 2016 begann, klassische On-Premise-Systeme durch Cloud-Lösungen zu ersetzen, stieß das Unternehmen auf Skepsis – selbst in den USA. Kaliszan beschreibt die Strategie, wie Pilotprojekte mit Testhardware und Übernahme der Evaluierungskosten den Einstieg erleichtern. „Nach ein paar Wochen des Testens erkennen die Kunden den Mehrwert. Dann wollen sie es standardisieren. Der Aha-Effekt ist sehr stark."

Technologischer Unterschied: Software-first statt Hardware-zentriert

Der Hardware-Wettlauf der letzten Jahrzehnte – Megapixel, Sensoren, Objektive – sei weitgehend gelöst. Verkada setzt stattdessen auf integrierte Plattformen aus Kamera-, Zutritts-, Alarm- und Umweltsensorik, gesteuert über Cloud-Software. „Kameras sind heute ein relativ gelöstes Hardware-Problem. Durch iPhones und Smartphones treibt der Konsumentenmarkt die Innovation. Aber niemand hat sich ernsthaft der Software angenommen."



Ein Messebesucher brachte es treffend auf den Punkt: „Der Unterschied ist: Die KI von Verkada funktioniert wirklich", berichtet Kaliszan.

Europäische Standards: Integrationen sind Pflicht, nicht Kür

Deutsche BDS-Normen, EN-Standards oder nationale Datenschutzanforderungen stellen internationale Anbieter vor Herausforderungen.

Verkada übernimmt diese Arbeit selbst: Unerlaubte Funktionen wie Gesichtserkennung werden deaktiviert, länderspezifische Dokumentationen bereitgestellt, Datenhoheit technisch und organisatorisch gesichert. „Früher haben Hersteller Produkte gebaut und die Compliance den Kunden überlassen. Das funktioniert heute nicht mehr. Wir müssen die Last abnehmen – nicht die Kunden", ist sich Kaliszan sicher.

Proaktive Sicherheit durch KI: Von reaktiv zu prädiktiv

KI transformiert physische Sicherheit von der reaktiven Analyse hin zu proaktiver Prävention. Verkada-Systeme erkennen unter anderem unbefugtes Überklettern von Zäunen, Stürze, frühzeitige Warnungen bei Rauch oder Wasserschäden sowie atypische Bewegungsmuster. „Viele Schäden entstehen nachts. Ein geplatztes Rohr kann Hunderttausende Euro kosten. Wenn ein System das erkennt und meldet, bevor es eskaliert, spart das enorm viel Geld", fasst Kaliszan die Bedrohnungslage zusammen.
Neue Aktivitätserkennungen werden nur veröffentlicht, wenn sie außergewöhnlich zuverlässig arbeiten – das Motto: „nichts versprechen, was sich in der Praxis nicht bewährt", Kaliszan.

Ethik und Verantwortung: Keine Zukunft wie in China

Kaliszan hebt hervor, dass KI-gestützte Sicherheitssysteme klaren ethischen Leitlinien folgen müssen. Reduktion von Kriminalität darf nicht mit Massenüberwachung einhergehen. Kundendaten werden strikt getrennt, Tracking unterbleibt, Technologien werden nicht für staatliche



Überwachung entwickelt. „Freiheit bedeutet Sicherheit – nicht Überwachung."

Innovation durch Kundendialog

Neue Funktionen erscheinen kontinuierlich über die Cloud, flankiert von jährlichen Produktkonferenzen. Entscheidender sei jedoch der direkte Austausch mit Kunden. „Wenn wir das tun, was für unsere Kunden richtig ist, wird unser Unternehmen automatisch besser", bewertet Kaliszan den Dialog mit Verkada Kunden. Verkada bleibt damit schnell, innovativ und softwaregetrieben – mit klarem Fokus auf Compliance, proaktive Sicherheit und ethisch verantwortliche KI-Lösungen in Europa.

[DCM]

INFOBOX: KERNTHEMEN

Cloud: Verkada verlagert physische Sicherheitslösungen von On-Premise zu Cloud-basierten Plattformen. Pilotprojekte und Testhardware ermöglichen die schnelle Evaluierung. Vorteile: einfache Implementierung, Skalierbarkeit, Echtzeit-Überwachung, Standardisierung über mehrere Standorte.

Compliance: Strikte Einhaltung lokaler Standards (BDS, EN, Datenschutz) wird von Verkada zentral umgesetzt. Unerlaubte Funktionen werden deaktiviert, Dokumentationen bereitgestellt, Datenhoheit technisch und organisatorisch gesichert. Vorteil: Entlastung für Partner und Kunden, Skalierbarkeit in anderen europäischen Märkten.

KI: Echtzeit-Detektion von Sicherheitsvorfällen, frühzeitige Warnungen bei Stürzen, Wasserschäden oder unbefugtem Zutritt. Reduktion von Fehlalarmen, proaktive Prävention, Kostenersparnis. Ethik: keine Massenüberwachung, strikte Trennung der Kundendaten.



Report

Die Lage der physischen Sicherheit

Wie Modernisierung, KI und Partnerschaften einen neuen strategischen Sicherheitsrahmen setzen

Die physische Sicherheit verändert sich tiefgreifend: Mit zunehmender Systemintegration, einer immer stärkeren Verflechtung mit der IT, datengetriebenen Prozessen sowie der wachsenden Bedeutung von KI wird Sicherheit zum Faktor für betriebliche Effizienz und Resilienz. Der Report „Die Lage der physischen Sicherheit 2026" von Genetec zeigt, dass Unternehmen physische Sicherheit zunehmend nicht nur als Schutz für Menschen und Vermögenswerte ansehen, sondern als eine Unternehmensfunktion, die den Geschäftswert verbessert. Für die weltweite Studie hat Genetec 7.368 Fachleuten für physische Sicherheit aus Unternehmen verschiedener Größen und Branchen befragt.

Die Sicherheitsverantwortlichen in Unternehmen erkennen zunehmend, wie neue Technologien die Schutzfunktion und das Reaktionsvermögen ihrer Sicherheitssysteme verbessern können und sind deshalb offen für Investitionen. Angesichts neuer Sicherheitsbedrohungen sind sie im Bereich der physischen Sicherheit auf solide technologische Kompetenzen angewiesen. Deshalb arbeiten sie intern mit der IT-Abteilung und extern mit Partnern und Anbietern eng zusammen. Gemeinsam können sie die Komplexität meistern, Lücken schließen, Systeme vereinheitlichen und intelligentere, widerstandsfähigere Schutzkonzepte erarbeiten.

Physische Sicherheit beeinflusst Geschäftserfolg

Die Ergebnisse der Umfrage zeigen eine rasante Veränderung in der Arbeitsweise und der Wertschöpfung von Abteilungen für physische Sicherheit. Sie ermöglichen nicht nur Schutz, sondern unterstützen Entscheidungsprozesse, betriebliche Abläufe und die organisationsweite Zusammenarbeit.

Sicherheit wird damit zur strategischen Steuerungsgröße. Über 70 Prozent der Befragten nutzen bereits integrierte oder vereinheitlichte Systeme für Videomanagement und Zutrittskontrolle. Die wichtigsten Gründe für die Modernisierung alter Lösungen in den Bereichen Videomanagement und Zutrittskontrolle sind dabei Integration in neue Technologien (60 Prozent) und der Zugriff auf neue Funktionen (51 Prozent). Folgende Systeme wurden 2025 am häufigsten ersetzt: Kameras (61 Prozent), Zutrittskontrolle (56 Prozent), Videomanagementsysteme (40 Prozent), Lesegeräte und Karten für die Zutrittskontrolle (36 Prozent).

Cyberrisiken durch Vereinheitlichung minimieren

Die Grenzen zwischen digitalen und physischen Bedrohungen verschwimmen zunehmend. Die Umfrageergebnisse legen nahe, dass mit der immer stärkeren Vernetzung physischer Sicherheitssysteme der Schutz von IoT- und Edge-Geräten mittlerweile eine zentrale operative Anforderung ist.

Angesichts immer neuer Sicherheitsbedrohungen steigt die Nachfrage nach vereinheitlichten Plattformen für physische Sicherheit, Cybersicherheit und Business Intelligence. 37 Prozent der befragten Unternehmen melden eine Zunahme physischer oder digitaler Zwischenfälle, bei großen Unternehmen sogar 48 Prozent. Die häufigsten Cyberangriffe sind Phishing (50 Prozent), Malware (41 Prozent), Geräte-Hacking (40 Prozent) und Social Engineering-Angriffe (36 Prozent).

Durch die zunehmende Vernetzung physischer Sicherheitssysteme ist eine Kooperation mit der IT-Abteilung nicht nur sinnvoll, sondern unverzichtbar. Physische Sicherheitsmaßnahmen müssen kontinuierlich weiterentwickelt werden, um Netzwerke sowie Personen und Sachwerte zu schützen. Vereinheitlichte und integrierte Systeme ermöglichen ein ganzheitliches Sicherheitsmanagement sowie eine verbesserte Entscheidungsfindung.

KI: Großes Interesse, begleitet von Unsicherheit

Das Brancheninteresse an KI hat sich laut Report gegenüber dem Vorjahr verdoppelt. Durchschnittlich 21 Prozent der befragten Unternehmen nutzen KI/LLM-basierte Funktionen und im Schnitt 26 Prozent Analyse- und Visualisierungstools.

KI kann die physische Sicherheit effizienter gestalten, indem sie Anomalien erkennt, Vorfälle vorhersagt und eine schnellere, sicherere Entscheidungsfindung ermöglicht. Allerdings muss die Technologie mit Bedacht eingesetzt und verwaltet werden. KI-gestützte Analysen beispielsweise bieten nur dann einen Mehrwert, wenn sie mit verantwortungsvoller Datennutzung und klaren operativen Zielen einhergehen. Um das KI-Potenzial auszuschöpfen, sind vernetzte Systeme und ein bruchloser Datenaustausch erforderlich. Die Hauptziele der KI-Integration sind laut dem Report die automatische Auslösung von Ereignissen (55 Prozent), die vollständige Automatisierung repetitiver Aufgaben (48 Prozent) und die automatische Filterung und Klassifizierung von Ereignissen sowie die automatische Koordination von Notfallaufgaben (jeweils 46 Prozent).

Während das Vertrauen in KI wächst, bestehen jedoch weiterhin Unsicherheiten hinsichtlich der Implementierung. Nur 29 Prozent der befragten Endnutzer gaben an, keine Bedenken hinsichtlich KI zu haben. Gleichzeitig sind 70 Prozent über die Konzeption und Implementierung von KI-Systemen besorgt. Bedenken bestehen insbesondere hinsichtlich der Verwendung der Daten und wegen des mangelnden Verständnisses der Technologie.

Cloud und Hybridmodelle: Flexibilität statt Dogma

Unternehmen verfolgen heute primär das Ziel, Workloads flexibel zu steuern. Infolgedessen gewinnt die Einführung der Cloud in Form von Hybridmodellen an Dynamik. Cloudbasierte Appliances und Edge-Geräte verändern die Art und Weise, wie Sicherheit implementiert und aufrechterhalten wird. Diese Komponenten sorgen für einfache Konnektivität über Anwendungen und Standorte hinweg, erleichtern die Skalierung und verbessern die Agilität durch automatische Softwareupdates, Ferndiagnosen und weniger Serviceeinsätze. Als wichtigste Gründe für den Cloud-Einsatz nennen die Unternehmen automatische Updates und einfache Implementierung sowie leichtere Wartung von Systemen und Servern im Netzwerk.

Im Vergleich zu 2024 ist der Einsatz von Hybrid-Cloud für physische Sicherheitsumgebungen um 2 Prozent auf 45 Prozent gestiegen. 48 Prozent setzen noch auf reine On-Prem-Lösungen und 7 Prozent auf reine Cloudlösungen.

61 Prozent der Planer erwarten in den nächsten zwölf Monaten eine steigende Cloud-Migration und 72 Prozent erwarten in den kommenden fünf Jahren überwiegend Hybridmodelle.

Zusammenarbeit als Innovationstreiber

Mit zunehmender Komplexität benötigen Unternehmen langfristige, verlässliche Partner. Technologiepartner begleiten heute nicht nur Projekte, sondern Modernisierungsprogramme, KI-Implementierungen und Cloudtransformationen. Systemintegratoren und Hersteller gelten inzwischen als vertrauenswürdige Partner, die sinnvolle Veränderungen ermöglichen und Technologieinvestitionen langfristig schützen können.

Fachwissen in den Bereichen Design und Bereitstellung sowie aktives Engagement für verantwortungsbewusste Innovation sind besonders gefragt. 73 Prozent der Unternehmen geben an, dass die Zukunftsfähigkeit und Stabilität des Anbieters von physischen Sicherheitssystemen entscheidend sind. Produktleistung (45 Prozent) und Preisgestaltung (43 Prozent) folgen ebenfalls als zentrale Kriterien.

Vom Schutz zur Wertschöpfung: Die Zukunft der physischen Sicherheit

Der Genetec Report zeigt, dass physische Sicherheit längst mehr als eine Schutzfunktion erfüllt und sich zu einem strategischen Erfolgsfaktor für Unternehmen entwickelt hat. Zentrale Treiber dieser Entwicklung sind vereinheitlichte Plattformen und integrierte Systeme für ein ganzheitliches Sicherheitsmanagement sowie die zunehmende Zusammenarbeit zwischen IT- und Sicherheitsteams und externen Partnern.

Ein weiterer wichtiger Baustein ist der gezielte Einsatz von Cloud-Technologien für eine bessere Zusammenarbeit und Resilienz. KI-basierte Lösungen reduzieren darüber hinaus Fehlalarme und sorgen für Automatisierung und eine bessere Entscheidungsfindung.

Am erfolgreichsten werden die Organisationen sein, die Technologie zielgerichtet, vernetzt und mit Fokus auf den Menschen einsetzen – und dabei Sicherheit als integralen Bestandteil der Unternehmensstrategie verstehen.

Den vollständigen Report „Die Lage der physischen Sicherheit 2026" von Genetec hier herunterladen:
[www.tinyurl.com/4cfyncau]

Autor: Andreas Flemming, Area Sales Director DACH, Genetec Deutschland



Thomas Dallmeier, CEO von Dallmeier electronic
Foto ©Dallmeier

Made in Germany

ist ein Versprechen für Sicherheit

Interview mit Thomas Dallmeier: Dallmeier electronic ist seit Jahrzehnten ein führender Anbieter von Videoüberwachungs- und Videoinformationstechnologie. Im Gespräch erklärt CEO Thomas Dallmeier, warum das Gütesiegel „Made in Germany" für sein Unternehmen weit mehr als ein Marketingversprechen ist – und weshalb internationale Kunden gezielt nach Produkten aus Deutschland verlangen.

Euro Security: Herr Dallmeier, Ihr Unternehmen entwickelt und produziert seit jeher in Deutschland. Warum halten Sie so konsequent am Standort fest?
Dallmeier: Für uns ist „Made in Germany" seit jeher eine Verpflichtung, keine Werbefloskel. Unsere Kunden verlangen Qualität, und sie sind auch bereit, dafür zu zahlen. Gerade in der Sicherheitstechnik geht es nicht nur um Funktionalität, sondern vor allem um Vertrauen.

Euro Security: Viele asiatische Anbieter locken mit günstigen Preisen. Was unterscheidet Dallmeier davon?
Dallmeier: Preis ist nicht alles. Bei sicherheitsrelevanten Produkten kann ein vermeintlich günstiger Einkaufspreis sehr teuer werden – zum Beispiel, wenn Daten unbemerkt ins Ausland abfließen oder versteckte Hintertüren im System existieren. Solche Fälle sind bekannt. Unsere Kunden – von Flughäfen über Stadien bis hin zu Industrieanlagen – wissen: Mit Dallmeier haben sie die volle Kontrolle über Hard- und Software.

Euro Security: Was bedeutet „volle Kontrolle" konkret?
Wir entwickeln und produzieren sämtliche Kernkomponenten selbst – von der Kamera über die Aufzeichnungssoftware bis zur intelligenten Auswertung. Rund 50 % unserer Entwicklungsressourcen fließen allein in Sicherheitsaspekte. Damit machen wir die Sicherheitstechnik selbst sicher – Stichwort Cybersecurity und „Secure by Design". Nur so können wir garantieren, dass unsere Produkte frei von Manipulationen sind.

Euro Security: Wie sieht ein echter „Secure by Design"-Ansatz in der Praxis aus?
Dallmeier: Ein echter „Secure by Design"-Ansatz beginnt bei Dallmeier wie gesagt bereits bei der Produktentwicklung: Durch eigene Softwareentwicklung und Fertigung in Deutschland gewährleisten wir eine vollständige Transparenz in der Lieferkette und minimieren das Risiko von Hintertüren. Technisch setzen wir auf mehrere Schutzebenen: sichere Datenübertragung, strenge Zugriffskontrollen, abgeschottete Betriebssysteme und integrierte Sicherheitsvorkehrungen gegen unbefugten Zugriff. Regelmäßige Updates sowie Penetrationstests ergänzen das Konzept und sorgen dauerhaft dafür, dass unsere Kunden maximale Sicherheit bei minimalem Administrationsaufwand erhalten.

Euro Security: Sind Datenschutzvorgaben eher Herausforderung oder Chance für die Entwicklung von Sicherheitstechnologie?
Dallmeier: Beides – aber vor allem eine Chance. Vorschriften wie die DSGVO bringen zweifellos technische und organisatorische Herausforderungen mit sich. Gleichzeitig fördern sie aber Transparenz,



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

Qualität und Verantwortungsbewusstsein. Wer Datenschutz nicht als Hürde, sondern als festen Bestandteil der Systemarchitektur versteht, schafft Vertrauen – insbesondere im Umfeld von Behörden, kritischer Infrastruktur oder international agierenden Unternehmen. Am Ende ist Compliance keine Last – sie ist eine Stärke, die Vertrauen und Differenzierung schafft.

Euro Security: Andere Unternehmen verlagern aus Kostengründen ins Ausland. Warum kommt das für Sie nicht infrage?
Dallmeier: Weil man damit Vertrauen verspielt. Wenn ich nicht mehr weiß, was in einer Komponente steckt, kann ich meinen Kunden keine hundertprozentige Sicherheit versprechen. Made in Germany bedeutet für uns: Jeder Entwicklungsschritt ist nachvollziehbar, überprüfbar und transparent.

Gerade im Bereich der Hochtechnologie ist in der Vergangenheit bereits viel wertvolles Know-how aus Deutschland abgewandert – etwa im Bereich der Kameraoptik. Wir sehen darin eine Verpflichtung: Dallmeier investiert gezielt in die Entwicklungstiefe am Standort Regensburg, um genau dieses Wissen zu sichern und weiter auszubauen.
Unser Anspruch ist es, nicht nur fertige Komponenten zu integrieren, sondern Schlüsseltechnologien selbst zu beherrschen – für mehr Transparenz, Qualität und langfristige Innovationsfähigkeit.

Euro Security: Welche Rolle spielt dabei die Nachfrage der Kunden?
Dallmeier: Eine entscheidende. Unsere Kunden fragen gezielt nach Made in Germany, weil es für Qualität, Datenschutz und Compliance steht. In internationalen Ausschreibungen ist es häufig sogar das ausschlaggebende Kriterium.

Euro Security: Wird das Gütesiegel künftig noch wichtiger werden?
Dallmeier: Ganz klar: ja. Cyberangriffe, Industriespionage und geopolitische Unsicherheiten nehmen zu. Vertrauen in Herkunft und Integrität von Produkten wird immer wichtiger. Wer Made in Germany kauft, investiert nicht nur in Technik, sondern in Zukunftssicherheit.

Euro Security: Wie relevant ist das Thema KI in Ihren Entwicklungen – und wie stellen Sie hier Qualität und Transparenz sicher?
Dallmeier: Künstliche Intelligenz ist für uns kein Trend, sondern ein zentraler Bau-



Auch das patentierte Multifocal-Sensorsystem Panomera® entsteht in Deutschland. Foto ©Dallmeier

stein 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.
Der Vorteil liegt auf der Hand: Bei vielen am Markt verfügbaren Netzen ist unklar, mit welchen Daten sie trainiert wurden. Genau hier lauern Risiken – von Verzerrungen in den Ergebnissen bis hin zu nicht nachvollziehbaren Fehlerquellen. Wir dagegen schaffen unsere Trainingsdaten selbst, exakt abgestimmt auf die Anforderungen unserer Kunden. So behalten wir die volle Kontrolle über den Input und können garantieren, dass unsere Netze praxisnah, zuverlässig und transparent arbeiten. Dieser Ansatz steigert nicht nur die Präzision und Verlässlichkeit, sondern schafft eine klare Grundlage für Vertrauen in die Technologie. Kurz gesagt: Wir setzen auf „AI made in Germany".

Euro Security: Andere Hersteller werben auch mit „Made in Germany". Wo liegt der Unterschied zu Dallmeier?
Dallmeier: Leider ist es in unserer Branche oft so, dass „Made in Germany" oft nur die Endmontage in Deutschland umfasst. Dabei werden Komponenten teilweise aus sensiblen oder sicherheitskritischen Regionen eingekauft. Das mag formaljuristisch reichen, hat mit echtem „Made in Germany" aber wenig zu tun.

Noch kritischer ist allerdings der Software-Bereich: Bei vielen Herstellern stammen die zentralen Software-Komponenten nicht aus Deutschland. Kunden können daher kaum nachvollziehen, wer tatsächlich Zugriff auf ihre sensiblen Videodaten hat – oder ob im schlimmsten Fall Hintertüren eingebaut sind.

Bei Dallmeier ist das anders: Wir entwickeln und produzieren unsere Hardware in Deutschland, und genauso entsteht unsere Software hier – inklusive aller Themen rund um Datenschutz und Datensicherheit. Das heißt: Von der ersten Schraube bis zur letzten Codezeile unterliegt alles deutschen Qualitäts- und Rechtsstandards. Das ist für unsere Kunden nicht nur ein Qualitätsversprechen, sondern vor allem ein entscheidender Faktor für Vertrauen.
Euro Security: Sie haben Rechtsstandards



Made in Germany ist für Dallmeier ein Versprechen für Sicherheit. Foto ©Dallmeier

erwähnt… Wie können Organisationen die DSGVO einhalten, ohne die Effizienz ihrer Systeme zu gefährden?
Dallmeier: Datenschutz und Effizienz schließen sich nicht aus – im Gegenteil: Unsere Systeme sind so konzipiert, dass sie beides vereinen. Ein integriertes Rechtemanagement sorgt beispielsweise für eine präzise Steuerung von Benutzergruppen und Zugriffsrechten. Funktionen wie Privacy Zones ermöglichen es, sensible Bereiche dauerhaft oder ereignisbasiert zu verpixeln.

Ein besonders praxisnahes Beispiel ist das Panomera® Privacy Shield: Die fernsteuerbare Abdeckung für unsere Multifocal-Sensorkameras unterstützt nicht nur die Einhaltung von Datenschutzvorgaben, sondern erhöht durch die Remote-Bedienung gleichzeitig die Effizienz.

Euro Security: Wie sollten Entscheider den langfristigen Wert von Sicherheitssystemen jenseits des Anschaffungspreises bewerten?
Dallmeier: Der reine Anschaffungspreis sagt wenig aus. Eine fundierte Bewertung berücksichtigt die Total Cost of Ownership (TCO) über den gesamten Lebenszyklus – inklusive Installation, Wartung, Integrationsfähigkeit, Betrieb, Schulungsbedarf, Support und Ersatzteilverfügbarkeit.

Am Beispiel von Panomera® zeigt sich das besonders deutlich: Zwar liegt der Stückpreis mitunter zunächst höher als bei klassischen Kameras, doch durch die großflächige Abdeckung mit wenigen Installationspunkten sinken Infrastruktur-, Verkabelungs- und Wartungskosten erheblich. Die intuitive Bedienung entlastet zudem die Leitstellen. Über mehrere Jahre betrachtet, erweisen sich diese Systeme als deutlich wirtschaftlicher.

Euro Security: Ihr Fazit, Herr Dallmeier?
Dallmeier: Made in Germany ist für uns kein Label, sondern ein Versprechen – an unsere Kunden, an unsere Mitarbeiter und an den Standort Deutschland. In der Sicherheitstechnik darf es keine Kompromisse geben. Und genau dafür stehen wir.

Euro Security: Vielen Dank für das Interview.

D&O-Haftungsrisiken 2026

Allianz-Analyse zeigt ein deutlich verschärftes Risikoumfeld für Führungskräfte

Das Haftungsumfeld für Vorstände, Geschäftsführer und Aufsichtsräte entwickelt sich so dynamisch und komplex wie selten zuvor. Unternehmen weltweit befinden sich in einem Spannungsfeld aus geopolitischen Unsicherheiten, wirtschaftlichen Belastungen, technologischen Umbrüchen und wachsendem gesellschaftlichem Druck. In dieser Situation geraten nicht nur Organisationen als Ganzes, sondern zunehmend auch die handelnden Personen in den Fokus von Regulierungsbehörden, Aktionären, Aufsichtsorganen und der Öffentlichkeit.

Der neue Allianz-Bericht zu Directors-and-Officers-Risiken (D&O) für 2025/2026 zeigt eindrucksvoll, wie stark sich die Risikolandschaft verändert hat, welche Treiber besonders relevant sind und welche Herausforderungen Führungskräfte künftig beherrschen müssen. D&O-Versicherungen, einst vor allem als Schutz vor klassischen Managementfehlern gedacht, haben sich dabei zu einem zentralen Instrument moderner Corporate Governance entwickelt und stehen an der Schnittstelle zwischen strategischer Steuerung, regulatorischer Verantwortung und technologischem Wandel.

Geopolitische Entwicklungen rücken inzwischen ganz oben auf die Tagesordnung vieler Unternehmen. Konflikte, politische Instabilität, Handelsstreitigkeiten und Sanktionen entfalten weitreichende Konsequenzen für globale Geschäftsmodelle. Während früher vor allem wirtschaftliche Indikatoren im Vordergrund standen, bestimmen heute geopolitische „Schockwellen" operative Herausforderungen, regulatorische Neuausrichtungen und Reputationsrisiken.

Der Bericht macht deutlich, dass Führungskräfte zunehmend dafür haftbar gemacht werden können, wenn sie die Auswirkungen geopolitischer Veränderungen falsch einschätzen, Sanktionsregime nicht einhalten oder regulatorische Anpassungen in wichtigen Märkten zu spät umsetzen. In einer Welt, in der globaler Wettbewerb und politische Realignments eng verwoben sind, entsteht ein Geflecht aus Risiken, das D&Os in ganz neuer Form herausfordert. Fehlentscheidungen können schnell in Aktionärsklagen, aufsichtsrechtliche Maßnahmen oder internationale Rechtsstreitigkeiten münden. Geopolitische Intelligenz und systematisches Monitoring globaler Hotspots sind deshalb nicht mehr nur eine Option, sondern ein elementarer Bestandteil moderner strategischer Führung.

Parallel zu den geopolitischen Risiken wachsen die Herausforderungen im Bereich der Cybersicherheit. Cyberrisiken haben sich in den vergangenen Jahren rasant zu einem der häufigsten Auslöser für D&O-Schäden entwickelt. Mit einer deutlichen Zunahme von Datenpannen, Ransomware-Angriffen und technischen Störungen steigt der Druck auf das Management, ein belastbares Cyberrisikomanagement zu etablieren.

Der Allianz-Bericht zeigt, dass Vorstände und leitende Angestellte zunehmend für Versäumnisse haftbar gemacht werden können, wenn sie Cyberbedrohungen nicht angemessen adressieren. Besonders relevant wird dies im Zusammenhang mit gesetzlichen Vorgaben wie der europäischen NIS2-Richtlinie, die nicht nur strengere Sicherheitsstandards fordert, sondern auch die persönliche Verantwortung von D&Os für die Überwachung der Cybersicherheit und der Reaktionsfähigkeit eines Unternehmens auf Cybervorfälle hervorhebt. Die Schwelle für Klagen sinkt, während die Bereitschaft, Ansprüche geltend zu machen, sowohl von Aktionären als auch von Regulierungsbehörden zunimmt. Selbst wenn Führungskräfte nicht unmittelbar verantwortlich sind, entstehen im Rahmen von Cybervorfällen oft hohe Verteidigungs- und Untersuchungskosten, die das Risiko weiter erhöhen. Der Bericht unterstreicht, dass Investitionen in Cyberabwehr, Business-Continuity-Management und Datenschutz nicht nur operative Resilienz fördern, sondern auch entscheidend für die Prävention haftungsrelevanter Situationen sind.

Ein weiterer Schwerpunkt des Allianz-Berichts liegt auf den rasant wachsenden Risikofeldern der künstlichen Intelligenz (KI). Der globale KI-Markt wird sich in den kommenden Jahren nahezu vervielfachen, gleichzeitig steigt die Wahrscheinlichkeit haftungsrelevanter Ereignisse. KI-Systeme versprechen Effizienzgewinne, neue Geschäftsmodelle und Innovationsschübe, bergen jedoch erhebliche rechtliche und regulatorische Herausforderungen.

Der Bericht verweist darauf, dass die Zahl KI-bedingter Rechtsstreitigkeiten – insbesondere im Bereich der „Securities Class Actions" – deutlich zugenommen hat. Aktionäre und Aufsichtsbehörden beobachten sehr genau, ob Unternehmen AI-Risiken korrekt einschätzen, ob Leistungsversprechen realistisch sind oder ob sogenanntes „AI-Washing" betrieben

wird, also übertriebene oder irreführende Darstellungen von Fähigkeiten und Chancen. Fehlerhafte Modelle, algorithmische Verzerrungen, Datenschutzverletzungen oder fehlerhafte Offenlegungen können zu erheblichen Kursverlusten führen – und damit zu direkten Haftungsansprüchen gegen D&Os. Für Führungskräfte bedeutet dies, dass die Integration von KI nicht nur ein technologisches Projekt ist, sondern auch ein Governance-Thema mit erheblichen Offenlegungspflichten und Compliance-Anforderungen.

Neben Technologie und Geopolitik spielen auch Umwelt- und Produkthaftungsfragen eine wachsende Rolle, insbesondere im Zusammenhang mit per- und polyfluorierten Alkylsubstanzen (PFAS), den sogenannten „Forever Chemicals". Diese langlebigen Stoffe, die seit den 1940er-Jahren in zahlreichen Produkten eingesetzt wurden, sind mittlerweile Gegenstand umfangreicher internationaler Gerichtsverfahren. Da PFAS mit Gesundheits- und Umweltproblemen in Verbindung stehen, entwickeln sich daraus erhebliche Haftungsrisiken.

Der Allianz-Bericht weist darauf hin, dass allein in den USA Kosten in Höhe von über 100 Milliarden US-Dollar möglich sind. Für D&Os entsteht Verantwortung, wenn Risiken nicht erkannt oder unzureichend offengelegt werden. Aktionäre werfen Vorständen zunehmend vor, potenzielle Umwelt- oder Produktrisiken zu spät kommuniziert oder falsch eingeschätzt zu haben. Dies kann insbesondere dann relevant werden, wenn negative Nachrichten zu Kursrückgängen führen und Haftungsansprüche begründet werden. Der Bericht betont, dass Unternehmen frühzeitig erkennen müssen, welche neuen Risiken am Horizont entstehen, und diese transparent kommunizieren sollten. Fehlende oder verspätete Offenlegung wird immer häufiger Grundlage für finanzielle Ansprüche gegen Führungskräfte.

Auch private Unternehmen gehören mittlerweile zu den zentralen Verursachern und Betroffenen von D&O-Risiken. Steigende Kosten, volatile Märkte, neue regulatorische Anforderungen und der Druck der digitalen Transformation belasten die Verantwortlichen erheblich. Besonders Handels- und Zollrisiken sowie geopolitische Einflüsse machen privaten Unternehmen zu schaffen. Wenn Unternehmen die Auswirkungen von Zöllen falsch einschätzen, fehlerhafte Angaben machen oder Preisüberwälzungen nicht transparent kommunizieren, kann dies zu regulatorischen Untersuchungen, zivilrechtlichen Klagen oder Vorwürfen der Verletzung von Treuepflichten führen.

Der Bericht empfiehlt privaten Unternehmen daher, verstärkt in Szenarioplanung zu investieren und Risiken in Lieferketten sowie tarifbezogene Abhängigkeiten systematisch zu analysieren. Eine robuste Governance-Struktur, klare Dokumentation und proaktive Risikokommunikation sind entscheidend, um Haftungsansprüche zu vermeiden.

Hinzu kommt ein deutlicher Anstieg der weltweiten Insolvenzen. Prognosen zufolge sollen die globalen Unternehmensinsolvenzen 2025 um 6 % und 2026 um weitere 5 % steigen, womit fünf aufeinanderfolgende Jahre mit Zuwächsen erreicht werden.

Besonders kritisch ist jedoch die wachsende Zahl sogenannter „Mega-Insolvenzen", bei denen Unternehmen mit Ver- mögenswerten über einer Milliarde US-Dollar betroffen sind. Für D&Os steigt damit das Risiko erheblich: Sobald ein Unternehmen in finanzielle Schwierigkeiten gerät, erweitern sich die Treuepflichten, und jede Entscheidung unterliegt strengster ex-post-Bewertung durch Behörden, Gläubiger und Insolvenzverwalter. Schlechte Dokumentation, verspätete Reaktionen oder interne Interessenkonflikte können zu erheblichen Haftungsansprüchen führen.

Selbst der bloße Verdacht finanzieller Schieflagen kann Auslöser für Rechtsstreitigkeiten sein, da Stakeholder versuchen, ihre eigenen Interessen abzusichern. Der Bericht macht deutlich, dass Führungskräfte im Vorfeld einer möglichen Insolvenz besonders sorgfältig agieren, ihre Entscheidungsprozesse dokumentieren und rechtliche Beratung frühzeitig einbeziehen sollten.

Insgesamt zeigt die Allianz-Analyse, dass sich die Zahl der D&O-Schäden weltweit seit drei Jahren kontinuierlich erhöht und inzwischen wieder das Niveau – oder sogar darüber – der Vor-Pandemie-Zeit erreicht. Während Nordamerika weiterhin führend bei der Schwere der Schadenfälle ist, steigen auch in Europa und Asien die Anspruchsbereitschaft und Komplexität der Verfahren deutlich an. Das Zusammenspiel aus geopolitischer Unsicherheit, Cyberrisiken, KI-bezogenen Rechtsstreitigkeiten, Umweltverfahren und wirtschaftlicher Instabilität bildet eine Risikolandschaft, die Führungskräfte erheblich fordert und hohe Anforderungen an Governance, Compliance und strategisches Risikomanagement stellt.

Der Allianz-Bericht verdeutlicht somit, dass 2026 ein Schlüsseljahr für D&O-Haftung und Corporate Governance sein wird. Die Risiken entstehen zunehmend aus externen Schocks, technologischen Fehlentwicklungen und regulatorischen Veränderungen – weniger aus klassischen Fehlentscheidungen. Unternehmen müssen ihre Governance- und Risikostrukturen anpassen, ihre Überwachungssysteme stärken und die Kompetenzen ihrer Führungsgremien erweitern.

Ebenso wichtig ist es, frühzeitig mögliche Belastungsszenarien zu erkennen und interne Prozesse so auszurichten, dass Transparenz und Verantwortlichkeit gewährleistet sind. D&O-Versicherungen werden damit nicht nur zu einem essenziellen Schutzmechanismus, sondern auch zu einem strategischen Begleiter, der Impulse für professionelles Management und nachhaltige Risikosteuerung setzt.

[Download: tinyurl.com/4ax84mzx]



„Hilfe, da fehlt ein Kabel!“

Schnittstellenprobleme in der Gebäudeplanung

In vielen Bauprojekten gibt es einen Moment der Ernüchterung: Türen sind falsch dimensioniert, Verkabelungen fehlen, Schnittstellen wurden übersehen. Doch warum passiert das immer wieder? Und wie lassen sich diese Probleme vermeiden? Sebastian Ott, Objektberater und Experte für ganzheitliche Türlösungen bei ASSA ABLOY, kennt die Antworten.

? Wann treten Schnittstellenprobleme rund um Türen besonders häufig auf?

Ott: Immer dann, wenn Projekte komplexer werden – und das ist heute fast die Regel. Besonders im Neubau und in sicherheitskritischen oder stark frequentierten Gebäuden gibt es kaum noch „einfache“ Türen. Türlösungen müssen vielfältige Anforderungen erfüllen und dabei reibungslos zusammenspielen – von der Barrierefreiheit über den Brandschutz bis hin zur Fluchtwegsteuerung.

Und obwohl Türen oft nur einen kleinen Teil der Projektkosten ausmachen, stecken hier die meisten Bauch- und Kopfschmerzen. Deshalb begleiten wir Bauvorhaben häufig schon in sehr frühen Leistungsphasen.

? Welche Akteure müssen bei der Türplanung zusammenarbeiten?

Ott: Im Idealfall arbeiten die vier Gruppen eng zusammen:

1. Architekten, die festlegen, welche Tür wo benötigt wird und welche Funktionen sie erfüllen muss.
2. Elektroplaner, die definieren, welche elektrischen Komponenten notwendig sind, z. B. für Zutrittskontrolle oder Fluchtwegtechnik.
3. Türbauer, die die mechanische Ausführung verantworten – inklusive Schlossansteuerung.
4. Errichter bzw. Integratoren, die am Ende alles funktionsfähig zusammenbringen.

Letztere werden oft zu spät eingebunden – nicht zuletzt, weil entsprechende Leistungen gar nicht ausgeschrieben werden oder weil eine koordinierende Instanz fehlt.

? Warum wird der Errichter oft erst so spät eingebunden?

Ott: Weil die entsprechenden Leistungen gar nicht oder nur sehr vage ausgeschrieben werden. Bei der hohen Sicherheits-

anforderungen wie bei den Kritischen Infrastrukturen erfolgen Ausschreibungen oft nicht öffentlich – oder nur in Teilen.

Dabei sind es genau hier die besonders anspruchsvollen Schnittstellen: Zutrittskontrolle, Einbruchmeldeanlage, Videoüberwachung – all das muss im Zusammenspiel funktionieren.
Theoretisch wären Sicherheitsfachplaner: oder Schnittstellenkoordinatoren gefragt, um genau diese Verzahnung zu planen. Doch häufig gibt es niemanden, der offiziell beauftragt wurde, diese übergreifende Kommunikation zu übernehmen.

? Zwar existieren für einzelne Türen oft sogenannte Funktionsbeschreibungen – aber wer koordiniert, dass diese auch über alle Gewerke hinweg sinnvoll zusammengeführt werden?

Ott: Gerade wenn Architekten nur in der Entwurfsphase tätig sind und lediglich die Visualisierung übernehmen, bleiben Schnittstellenfragen oft ungeklärt. Spätestens in der Ausführungsplanung wird es dann kritisch – vor allem, wenn unterschiedliche Fachplaner beteiligt sind und keine saubere Übergabe stattfindet. Das Risiko für Lücken, Missverständnisse und Planungsfehler ist enorm.

? Wer ist im Normalfall für die Funktionsbeschreibung einer Tür zuständig?

Ott: In der Regel erstellt der Architekt die Funktionsbeschreibung – also eine klare Definition, was die jeweilige Tür leisten muss. Diese Anforderungen fließen dann in die Türenliste ein, die Teil der Planungsunterlagen wird.
Spannend wird es bei den Zuständigkeiten in den verschiedenen Leistungsphasen: In Leistungsphase 3 sieht die HOAI vor, dass Architekten die Koordination der beteiligten Fachplaner übernehmen – allerdings primär auf konzeptioneller Ebene.

In Leistungsphase 5 kommt zwar auch die Integration dieser Fachplanungen hinzu, doch auch hier geht es nicht um die technische Detailkoordination.

? Und der Elektroplaner?Welche Leistungen bringt der?

Der bringt in den Leistungsphasen 3 bis 5 lediglich seine Grundleistungen ein – also ebenfalls keine übergreifende Abstimmung. Eine systematische Abstimmung zwischen Türsystem, Zutrittskontrolle, Brandmeldetechnik und Co. ist also formal gar nicht vorgesehen.
Das Ergebnis: Genau an den kritischen Schnittstellen fehlt es an klarer Verantwortung. Und damit steigt das Risiko für spätere Reibungsverluste erheblich.

? Woran liegt es, dass die Koordination so oft scheitert?

Ott: Die HOAI sieht diese Schnittstellenabstimmung nicht explizit vor. Architekten und TGA-Planer schieben sich oft gegenseitig die Verantwortung zu. Die Elektroplanung enthält zwar Koordinationsleistungen, aber keine übergreifende Abstimmung von Türsystemen, Zutrittskontrolle und Brandmeldetechnik. Das Ergebnis: fehlende Zuständigkeit und unklare Kommunikation.

? Und wie wird das dann in der Praxis gelöst?

Ott: Das lösen wir als Objektberater: wir bringen alle Beteiligten frühzeitig ins Gespräch. Wenn zum Beispiel feststeht, dass eine Tür mit Rettungswegtechnik ausgestattet werden soll, sprechen wir dies bereits in der Konzeptphase mit den Fachplanern an. Je genauer das im Vorfeld definiert ist, umso besser ist die Ausschreibung und die Übergabe ans TGA-Gewerk. Mit dieser klaren Abstimmung gibt es auf der Baustelle keine unangenehmen Überraschungen.

? Was passiert, wenn diese Koordination fehlt?

Ott: Dann stehen am Ende aus einem Schloss Kabel heraus – aber niemand weiß, wo sie angeschlossen werden sollen. Das kann vorkommen, wenn es nicht richtig koordiniert ist.

? Gerade bei öffentlichen Bauprojekten entsteht oft zusätzliche Unsicherheit: Wer wird letztlich den Auftrag für den Türbau erhalten? Welche Produkte kommen konkret zum Einsatz – welches Schloss, welche Technik?

Ott: In Deutschland ist die Ausschreibung im öffentlichen Bereich grundsätzlich nicht produktspezifisch. Es dürfen lediglich die funktionalen Anforderungen und Eigenschaften der Tür beschrieben werden. Welche konkreten Komponenten am Ende verbaut werden, bleibt lange offen.
Genau an dieser Stelle setzen wir als Objektberater an: Sobald klar ist, welches Unternehmen den Auftrag erhalten hat, nehmen wir Kontakt auf und stimmen uns eng mit dem Türbauer ab. So stellen wir sicher, dass beispielsweise Rettungswegtechnik von ASSA ABLOY korrekt berücksichtigt wird – ohne zusätzlichen Abstimmungsaufwand auf Seiten des Türbauers. Die Planung wird einfacher, reibungsloser und effizienter.

? Wie sähe der ideale Ablauf aus Ihrer Sicht aus?

Ott: Perfekt wäre ein Prozess, bei dem alle Beteiligten – von Architekten über TGA- und Elektroplaner bis hin zu Türbauer und Errichter – frühzeitig eingebunden werden. Wir haben dazu eine Checkliste entwickelt, der alle Schritte übersichtlich darstellt.
Außerdem unterstützen wir bei Ausschreibungstexten und bei der Schnittstellenkoordination – kostenfrei. Das erleichtert nicht nur die Planung, sondern vermeidet auch spätere Konflikte.
Klar, die Planung lässt sich auch ohne Objektberater stemmen. Doch mit unserer Unterstützung läuft's deutlich entspannter – ohne unnötige Schleifen, Missverständnisse oder Bauchschmerzen. Wenn wir frühzeitig eingebunden werden, begleiten wir den gesamten Prozess: von der Idee über die Planung bis zur Umsetzung. Und zwar im Schulterschluss mit allen Beteiligten – Architekt, TGA-Planer, Metallbauer, Schreiner, Errichter und Systemintegrator.
Dieser enge Austausch ist der Schlüssel: Wenn alle früh ins Gespräch kommen, ist auch sichergestellt, dass am Ende alles so zusammenpasst, wie es gedacht war – funktional, technisch und organisatorisch.



Download: www.tinyurl.com/3ejn84wf

Von Drohnenspionage bis Cyberkrieg

Welche Risiken die digitale Sicherheit im Jahr 2026 prägen werden

2026 wird zu einem Wendepunkt der digitalen Sicherheit. Das prognostizieren die Experten des europäischen IT-Sicherheitsherstellers ESET. Sie zeichnen das Bild eines Jahres, in dem geopolitische Spannungen, KI-Missbrauch und professionelle Cyberbanden die Schlagzeilen bestimmen werden. Die Lage bleibt brisant und betrifft Staaten, Unternehmen und Verbraucher gleichermaßen. Weitere Trends hat der Hersteller in seinem aktuellen Blogpost " Von Drohnen, Desinformation & Datenklau – neue Cybergefahren in 2026*)" zusammengefasst.

"Die geopolitische Lage spiegelt sich heute eins zu eins im digitalen Raum wider", sagt ESET Cybersicherheitsexperte Thorsten Urbanski. "Cyberangriffe sind längst ein fester Bestandteil internationaler Konflikte – und genau deshalb gewinnt 'Made in EU' in der IT-Sicherheit enorm an Bedeutung. Europa braucht vertrauenswürdige Technologien, die unabhängig, transparent und souverän entwickelt werden."

Drohnen-Branche wird zum neuen Spionageziel

Die weltweite Aufrüstung im Drohnensektor entfacht eine Dynamik, die 2026 nicht nur militärisch, sondern auch cybertechnisch wirkt. Staaten wie China, Russland, Iran und Nordkorea setzen verstärkt auf digitale Spionage, um sich in einem strategischen Zukunftsmarkt Vorteile zu verschaffen. Einen besonders perfiden Fall (https://tinyurl.com/mu76c9ce) von Industriespionage hat ESET im Oktober 2025 aufgedeckt. Vor allem China beobachtet Taiwans militärische Modernisierung kritisch und versucht, technologische Entwicklungen frühzeitig auszuspähen. Russland wiederum richtet seinen Fokus weiter auf die Drohnenprogramme der Ukraine, die sich im Krieg schnell weiterentwickeln.

"Die großen staatlichen Akteure suchen immer dort nach Schwachstellen, wo technologische Innovation am schnellsten voranschreitet", sagt Jean-Ian Boutin, Director of Threat Research bei ESET. "2026 wird der Drohnensektor deshalb stärker denn je im Fadenkreuz stehen."

Europa bleibt im Visier russischer Hacker

Der russische Angriffskrieg gegen die Ukraine bleibt der zentrale geopolitische Treiber für Cyberangriffe auf Europa. Selbst ein möglicher Waffenstillstand würde diese digitale Offensive wahrscheinlich nicht stoppen. Russische Gruppen werden sich 2026 voraussichtlich stärker auf europäische Militärprogramme, Energieinfrastrukturen und die Lieferketten westlicher Modernisierungsprojekte konzentrieren. Gleichzeitig rückt die engere digitale Kooperation zwischen Russland und Belarus in den Fokus, die ihre Fähigkeiten im Cyberkrieg zusammenbringen werden.

KI wird zum geopolitischen Risikofaktor

Künstliche Intelligenz verschärft diese Entwicklungen erheblich. Staaten nutzen KI-Modelle, um ihre Operationen zu skalieren, sei es für Spionage, Desinformation oder Sabotage. Gleichzeitig entsteht ein unübersichtlicher Markt für Modelle unbekannter Herkunft, die manipuliert oder kompromittiert sein können. Betrüger profitieren enorm von diesem Wandel: Deepfakes, perfekt formulierte Nachrichten und täuschend echte Online-Profile lassen sich in Sekunden generieren und global verbreiten. Gerade in Zeiten politischer Spannungen kann dies das Vertrauen in öffentliche Debatten massiv untergraben.

"Digitale Agenten verbreiten sich immer stärker – sowohl auf der 'guten' als auch auf der 'bösen' Seite", warnt Juraj Janosik, Head of AI bei ESET. "Ohne starke IT-Sicherheit gefährden sich Unternehmen unnötig selbst und öffnen Cyberkriminellen Tür und Tor."

Ausblick: Keep calm (and safe)

Vor diesem Hintergrund kommt es jetzt vor allem darauf an, die eigene IT-Sicherheit zu stärken. China, die USA sowie andere Länder und Regionen haben in vielen Bereich bereits eine Vorreiterrolle eingenommen. Das heißt aber nicht, dass die Europäische Union ihr Licht unter den Scheffel stellen muss: Auch Europa ist in verschiedenen Branchen Technologieführer. Insbesondere in der Cybersicherheit haben sich in der EU starke Hersteller herauskristallisiert, die auf technischer Ebene maßgebend sind und gleichzeitig höchsten Datenschutzanforderungen entsprechen. Mit dem richtigen Hersteller an der Seite sind Unternehmen wie Privatnutzer vor den meisten Cyberbedrohungen effektiv geschützt.

Weitere Trends für 2026 gibt es im aktuellem Blogpost von ESET: "Von Drohnen, Desinformation & Datenklau – neue Cybergefahren in 2026 [www.tinyurl.com/4z3tanx7]

Robotergreifer aus Langusten-Exoskeletten

Natürliche Gelenke von EPFL-Wissenschaftlern übertreffen die künstlich hergestellten deutlich

Forscher der Ingenieurschule der Eidgenössischen Technischen Hochschule Lausanne (www.epfl.ch) (EPFL) haben einen bioinspirierten experimentellen Robotermanipulator entwickelt, der auch Original-Biobauteile hat - und zwar ein Paar Exoskelette aus Langustenschalen. Die Kombination biologischer Elemente mit synthetischen Komponenten habe nicht nur ein erhebliches Potenzial für die Verbesserung der Robotik, sondern unterstütze auch nachhaltige Technologiesysteme.

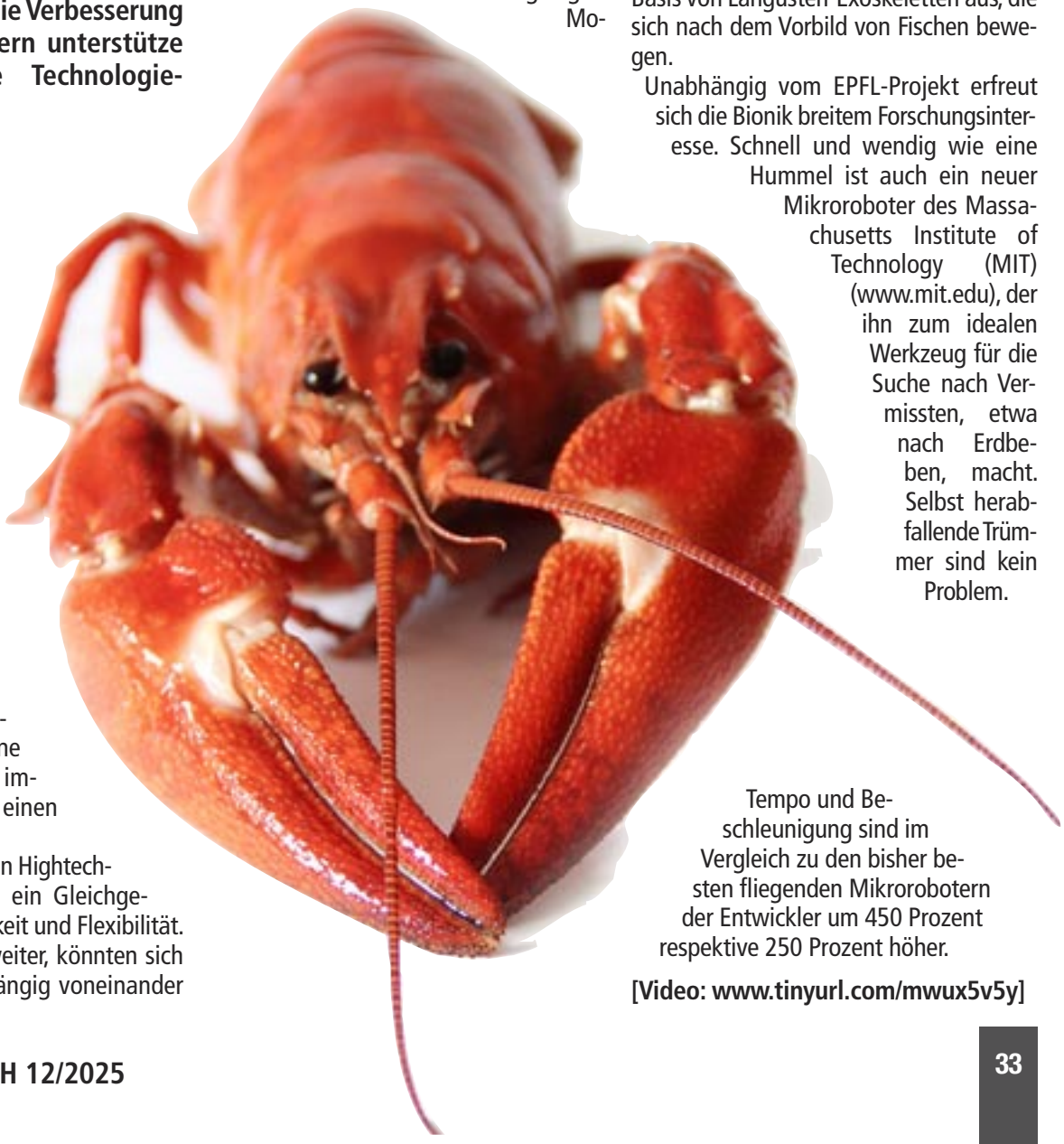
Schnell und hohes Drehmoment

Forschungsleiterin Josie Hughes und ihr Team haben drei Roboteranwendungen realisiert, bei denen die Exoskelette von Langusten mit synthetischen Komponenten verstärkt und erweitert worden sind: einen Manipulator, der Objekte mit einem Gewicht von bis zu 500 Gramm handhaben kann, einen Greifer, der sich verbiegen und verschiedene Objekte zu greifen imstande ist, und einen Schwimmroboter.
Der Expertin nach bieten Hightech-Exoskelette wie diese ein Gleichgewicht zwischen Steifigkeit und Flexibilität. Dadurch, so Hughes weiter, könnten sich ihre Segmente unabhängig voneinander bewegen. Diese Eigenschaften ermöglichten den Tieren schnelle Bewegungen mit hohem Drehmoment im Wasser, könnten aber auch für die Robotik sehr nützlich sein.

Vom Textmarker bis zur Tomate

Um die Eigenschaften des Langusten-Exoskeletts zu verbessern und zu verstärken, haben die Ingenieure ein Elastomer eingebaut, damit jedes seiner Segmente mithilfe von zugefügten Motoren beweglich ist. Schließlich überzog das Team das Exoskelett mit einer Silikonbeschichtung, um es zu verstärken und Abnutzung zu verhindern.
Die Wissenschaftler kombinierten letztlich zwei dieser Exoskelette zu einem Greiferpaar, das eine Vielzahl von Objekten unterschiedlicher Größe und Form packen kann, vom Textmarker bis hin zur Tomate, ohne die teilweise empfindlichen Objekte zu zerdrücken. Und einen Schwimmroboter statteten die Forscher mit Flossen auf der Basis von Langusten-Exoskeletten aus, die sich nach dem Vorbild von Fischen bewegen.

Unabhängig vom EPFL-Projekt erfreut sich die Bionik breitem Forschungsinteresse. Schnell und wendig wie eine Hummel ist auch ein neuer Mikroroboter des Massachusetts Institute of Technology (MIT) (www.mit.edu), der ihn zum idealen Werkzeug für die Suche nach Vermissten, etwa nach Erdbeben, macht. Selbst herabfallende Trümmer sind kein Problem.



Tempo und Beschleunigung sind im Vergleich zu den bisher besten fliegenden Mikrorobotern der Entwickler um 450 Prozent respektive 250 Prozent höher.

[Video: www.tinyurl.com/mwux5v5y]

Blindflug ist keine Strategie

Von Sebastian Spicker, Managing Director DACH bei IFS

Viele Unternehmen haben in den letzten Jahren viel Geld in ihre Digitalisierung investiert. Wo neue Plattformen und KI-Lösungen in Sachen Produktivität, Effizienz und Flexibilität riesiges Potenzial versprechen, tappen allerdings nicht wenige Betriebe immer noch im Dunkeln. Und warum? Weil sie längst den Überblick über ihre Assets, Prozesse und Daten verloren haben – und damit auch die Grundlage für eine nachhaltig erfolgreiche Digitalisierung. Die Konsequenz ist ein strategischer Blindflug, der den Rückstand gegenüber Wettbewerbern nur noch vergrößert.

Gerade im Manufacturing zeigt sich dieses Dilemma deutlich. Wer nicht weiß, wann Maschinen ausfallen, welche Ersatzteile wann verfügbar sind oder wie Lieferketten zusammenspielen, handelt immer reaktiv statt proaktiv. Predictive Maintenance war lange das Schlagwort, doch inzwischen reichen reine Vorhersagen von isolierten Systemen allein kaum noch aus. Wettbewerbsfähige Effizienz entsteht erst, wenn Unternehmen aktiv das beste Wartungsfenster berechnen können – inklusive Faktoren wie Auslastung, Wetter oder Personalverfügbarkeit der Techniker. Wer diese Informationen besitzt, erreicht weniger Downtime und einen echten Boost an Produktivität. Szenarien wie diese sind längst keine Zukunftsmusik mehr, sondern gelebte Praxis. Vorausgesetzt, die Datenbasis stimmt und Systeme können miteinander kommunizieren.

Ein ähnliches Bild zeigt sich im Field Service Management. Viele Unternehmen und Dienstleister planen ihre Außendiensteinsätze heute mit KI-Unterstützung. Doch wirklich intelligent wird die Planung erst dann, wenn sie mit Asset-Management-Systemen verbunden ist. Nur so fließen alle relevanten Informationen ein, vom Wartungsplan über Ersatzteile bis hin zu den individuellen technischen Voraussetzungen des Personals. Ohne diese Transparenz bleibt auch die neueste KI-Lösung ein stumpfes Werkzeug.

Dafür muss sich in erster Linie die grundlegende Erwartungshaltung gegenüber KI und Technologie verändern. Denn allein lösen auch sie nicht alle Fragen, die Wirtschaft und Industrie aktuell beschäftigen. Sie sind mächtig und wirkungsvoll, keine Frage. Aber nur dann, wenn Unternehmen den Mut haben, ihre Prozesse neu zu denken und über die notwendige Datengrundlage verfügen. Natürlich klingt das nach einer Mammutaufgabe. Doch die Alternative ist gefährlicher: Wer an alten Prozessen festhält, verliert nicht nur Effizienz, sondern auch Wettbewerbsfähigkeit. Märkte stellen neue Anforderungen in immer kürzeren Zyklen, Technologien entwickeln sich schneller, als viele Entscheider handeln.

Was also tun?

Erstens: Unternehmen müssen Transparenz über Assets und Datenflüsse schaffen sowie Prozesse ganzheitlich digital betrachten.

Zweitens: Sie müssen dafür auf praxisnahe KI-Lösungen setzen, die branchenspezifisch erprobt sind, statt sich in der Vielfalt an Standardsoftware zu verlieren.

Drittens: Führungskräfte sollten ein AI-First-Mindset entwickeln und ihre Mitarbeitenden in die Transformation einbinden. Nur wer versteht, welchen Mehrwert Technologie bietet, wird sie auch annehmen und nutzen.

Am Ende geht es nicht darum, blind Technologien einzukaufen und sie irgendwie an die eigene IT-Landschaft zu nageln, sondern zunächst das Licht in den eigenen Systemen anzuschalten. Wem das gelingt, der gewinnt Klarheit, Effizienz und Handlungsspielräume. Alle anderen bleiben wohl oder übel im Dunkeln – und riskieren, von der Konkurrenz überholt zu werden.

Programmierende KI: Die generierte Gefahr

Von Jochen Koehler, Vice President Sales EMEA bei Cycode

Large Language Modells schreiben Code in Sekunden. Was nach einem neuen Level an Effizienz klingt, hat allerdings auch eine Schattenseite. Das Problem: Sicherheit ist bislang kein integraler Bestandteil von KI-basierter Softwareentwicklung.

Programmieren ist dank GenAI so einfach wie noch nie. Fast jeder kann damit im Handumdrehen mehr oder weniger guten Code erzeugen – allerdings schlagen Studien bereits Alarm: Ganze 62 % aller KI-generierten Codes sind fehlerhaft oder verwundbar. Noch gravierender: Nach nur fünf Iterationen von KI-unterstützten Verbesserungen steigt die Zahl kritischer Sicherheitslücken um fast 38 %.

Wird Code also immer unsicherer, je häufiger KI im Entwicklungsprozess eingesetzt wird? Das ist sicherlich immer abhängig von Modell und Entwickler. Eins ist aber sicher: Ohne eine Sensibilisierung und entsprechende Gegenmaßnahmen kann das Versprechen der Effizienz schnell in ein enormes Risiko umschlagen.

Schließlich optimiert GenAI auf Funktionalität, nicht auf Sicherheit und Resilienz. Damit verschiebt sich das Gleichgewicht zwischen Innovation und Sicherheit weiter zulasten der Stabilität digitaler Systeme. Künstliche Intelligenz kann ein mächtiges Tool sein – aber nur, wenn wir Sicherheit von Anfang an mitdenken. Dazu gehören strukturierte Code-Reviews, automatisierte Schwachstellenanalysen und Security-by-Design-Prin- zipien. Nur wer trotz automatisierter Code-Generierung das letzte Wort behält, kann die Vorteile von KI nutzen, ohne neue Risiken zu schaffen.

IT-Sicherheit und digitale Souveränität

Herausforderungen, Risiken und Perspektiven im Jahr 2026

Auch im Jahr 2026 stehen die Bereiche IT-Sicherheit, Datenschutz, digitale Souveränität und Cyber-Resilienz erneut vor tiefgreifenden Veränderungen. Die zunehmende Professionalisierung cyberkrimineller Akteure, neue regulatorische Anforderungen sowie der rasante technologische Fortschritt – insbesondere im Bereich der Künstlichen Intelligenz – verschärfen die Bedrohungslage für Unternehmen und Organisationen aller Größenordnungen. Gleichzeitig eröffnen innovative Sicherheitsansätze neue Möglichkeiten, um komplexen Angriffsszenarien wirksam zu begegnen und digitale Infrastrukturen widerstandsfähiger zu gestalten.

Im Fokus stehen dabei unter anderem KI-gestützte Angriffe und Deepfake-Desinformation, die Vertrauen, Identitäten und Entscheidungsprozesse gezielt untergraben. Ebenso gewinnen identitätsbasierte Sicherheitsarchitekturen und die Absicherung von BYOD-Umgebungen weiter an Bedeutung, da klassische Perimeter-Modelle zunehmend an ihre Grenzen stoßen.

Nicht zuletzt rücken Supply-Chain-Risiken im KI-Zeitalter und die Frage nach digitaler Souveränität stärker in den Vordergrund, da Abhängigkeiten von Technologien, Daten und Anbietern strategische Risiken darstellen können. Nachfolgend finden Sie Einschätzungen und Statements von Experten verschiedener Unternehmen aus diesen Branchen, die diese zentralen Themen aus ihrer jeweiligen Perspektive beleuchten.



Andreas Süß, CEO DACH bei aDvens GmbH ©aDvens

aDvens

KI-gestützte Angriffe und Desinformationskampagnen mittels Deepfakes werden uns im kommenden Jahr herausfordern

„Künstliche Intelligenz wird 2026 nicht nur verstärkt in der Abwehr von Cyberattacken eingesetzt, sondern auch zur professionellen Erstellung neuer Angriffsmethoden. Wir werden eine Zunahme hochpersonalisierter, überzeu- gender Phishing-Mails erleben, die in Echtzeit auf Verteidigungsmaßnahmen reagieren können. Ebenfalls werden wir im kommenden Jahr noch häufiger Desinformationskampagnen sehen, die auf KI-generierten Deepfakes basieren. Diese werden gezielt darauf abzielen, das Vertrauen in Medien, Institutionen und digitale Kommunikation zu untergraben. Da solche Kampagnen häufig von staatlich gesteuerten Akteuren ausgehen, wird uns auch das Thema der digitalen Souveränität weiter beschäftigen. Wir müssen in der Lage sein, unsere Gesellschaft auch technisch unabhängig zu schützen."

Axis Communication

NIS-2 und Cybersicherheit: Videosicherheit als Treiber der Cyber-Resilienz



Jochen Sauer, Architect & Engineering Manager bei Axis Communications ©Axis Communications

„Mit dem NIS-2-Umsetzungsgesetz übernimmt Deutschland verschärfte EU-Cybersecurity-Standards – mit mehr Pflichten, mehr Nachweisen und mehr Verantwortung für Hersteller und Betreiber. Das betrifft auch Videosysteme, denn sie sind längst keine simplen Kameranetzwerke mehr, sondern cyber-physische Plattformen.

Für Hersteller bedeutet das: Es reicht nicht mehr, nur ‚Kameras plus Rekorder' zu liefern. Gefordert sind Plattformen mit End-to-End-Verschlüsselung, Cloud-Edge-Verteilung, KI-basierter Anomalie-Erkennung, standardisierten APIs und automatischer Integritätsprüfung. Systeme müssen Vorfälle nicht nur erkennen, sondern kontextualisiert an SOCs

melden – inklusive Forensik-Daten. Parallel dazu stehen Betreiber unter Dokumentations-, Melde- und Auditpflichten. Jede Komponente muss prüfbar sein, jede Entscheidung nachvollziehbar. Videosicherheit wird daher künftig nicht mehr nur an Auflösung und Bildqualität, sondern an Cyber-Resilienz, Compliance und Integrationsfähigkeit gemessen. Wer frühzeitig investiert, sichert sich einen strategischen Vorsprung. 2026 markiert dabei den Wendepunkt: Video wird nicht länger als reine Sicherheitstechnik betrachtet, sondern als fester Bestandteil der Cybersicherheit."



Létitia Combes, Co-Gründerin und MD bei BxC Security ©BxC Security

BxC Security

Identität ist der neue Perimeter – Die Absicherung von Netzwerken alleine reicht nicht mehr aus

„In modernen OT-Umgebungen verliert der klassische Perimeterschutz alleine mit Firewalls und Air Gaps rasant an Bedeutung. In Zeiten von Remote-Zugriff, Cloud-Konnektivität oder mobilen Diagnosetools zielen Angreifer immer häufiger auf Identitäten ab, um sich lateral in Systemen bewegen zu können. Gleichzeitig steigt die Zahl von Maschinenidentitäten geradezu explosionsartig an.

Ein moderner Perimeterschutz auf Grundlage von Identitäten nutzt digitale Zertifikate, die von einer Public Key Infrastructure automatisiert ausgestellt und gemanagt werden. Dann können sich Maschinen gegenseitig authentifizieren, bevor sie miteinander kommunizieren, Zugriff ist mit der Identität und nicht der IP verknüpft und Vertrauen kann überprüft, widerrufen oder eingefordert werden."

Jamf

Bedrohung von innen: 2026 führt kein Weg an sicherer Containerisierung von BYOD-Geräten vorbei



Henrik Nitsche, Security Solution Manager bei Jamf ©Jamf

„Böswillige oder unwissende Insider entwickeln sich zunehmend zur größten Bedrohung für Unternehmen, da sie bereits über legitimen Zugang zu sensiblen Daten, Systemen und Kommunikationswegen verfügen. Während externe Angriffe meist durch etablierte Sicherheitsmechanismen wie Firewalls, IDS/IPS oder Zero-Trust-Modelle erkannt und abgewehrt werden können, agieren Insider oft unerkannt innerhalb der Vertrauensgrenzen des Unternehmensnetzwerks.
Deshalb wird die Kontrolle über BYOD-Geräte 2026 ein wichtiger Schwerpunkt für Sicherheitsteams sein. Immer mehr Unternehmen werden eine Containerumgebung für ihre Mitarbeiter einrichten, um geschäftliche Daten strikt von privaten Bereichen zu trennen und Insider-Bedrohungen zu minimieren."

Malwarebytes

Supply-Chain-Angriffe: 2026 wird die Zahl der Attacken auf KI-Trainingsdaten massiv steigen



Pieter Arntz, Malware Intelligence Researcher bei Malwarebytes © Pieter Arntz

„Die rasante Verbreitung von Künstlicher Intelligenz (KI) eröffnet nicht nur neue Möglichkeiten, sondern schafft auch Angriffsflächen, die bisher kaum beachtet wurden. Cyberkriminelle werden im kommenden Jahr verstärkt die Trainingsprozesse von KI-Systemen ins Visier nehmen. Dabei manipulieren sie heimlich Trainingsdaten oder fügen subtile, aber persistente Hintertüren ein, die erst unter bestimmten Bedingungen aktiv werden.
Diese neue Art von „Supply-Chain-Angriff" instrumentalisiert den KI-Entwicklungsprozess selbst und stellt eine bisher unbekannte Dimension der Cyberbedrohung dar. Die Herausforderung für Unternehmen und Entwickler liegt darin, Transparenz und Integrität

über den gesamten Lebenszyklus der KI zu gewährleisten – von der Datensammlung bis zum Deployment. Nur durch robuste Überwachung, unabhängige Audits und innovative Abwehrstrategien lässt sich dieser Bedrohung begegnen."

Object First

Digitale Souveränität ist nicht mehr eine Frage der Compliance, sondern der Macht



Daniel Fried, SVP EMEA bei Object First ©Object First

„Unternehmen verstehen, dass die Kontrolle über ihre Daten ein entscheidender strategischer Hebel ist, und Cloud-Giganten müssen ihre Angebote überdenken: Die Labels „Trusted Cloud" und „Sovereign Data" werden zu wichtigen Auswahlkriterien. So wird vor dem Hintergrund anhaltender geopolitischer Spannungen das Wissen darüber, wo Daten gehostet werden, zunehmend zu einer wirtschaftlichen Waffe. Auch investieren Unternehmen massiv in Datenkartierung und Rückverfolgbarkeit, immutable Backups und transparente Datenflüsse. Das Ziel: Angriffe und Vorfälle sollen für eine lückenlose Kontrolle über die eigenen Systeme nicht mehr hingenommen, sondern vorweggenommen werden. Europa etabliert sich als Kontinent der vernünftigen digitalen Sicherheit."

Scrive

Europa muss in seine eigene digitale Souveränität investieren



Monir Gueblaoui, CPO bei Scrive © Scrive

„Die jüngsten Ausfälle bei Amazon Web Services und Microsoft Azure zeigen erneut, wie abhängig wir von außereuropäischen Infrastrukturen sind. In ganz Europa stehen Organisationen vor derselben Frage: Können wir wirklich Datensicherheit und Compliance-Konformität gewährleisten, wenn unsere kritischsten Daten in ausländischen Gerichtsbarkeiten vorgehalten werden? In Schweden sind beispielsweise zwei der wichtigsten Behörden des Landes, die Agentur für Sozialversicherung und das Zentralamt für Finanzwesen, zu gegensätzlichen Einschätzungen gekommen, ob die Nutzung von Cloud-Diensten aus den USA überhaupt rechtmäßig ist. Dies ist ein klares Zeichen dafür, dass Europa dringend ein eigenes, sicheres digitales Ökosystem aufbauen muss. Bei Scrive sind wir davon überzeugt, dass die Sicherheit und Innovationsfähigkeit Europas von digitaler Souveränität abhängt – von der Entwicklung einer eigenen digitalen Infrastruktur, Standards und SaaS-Lösungen, mit denen unsere Daten keinen Außeneinflüssen unterliegen. Bei der Stärkung der digitalen Souveränität Europas geht es nicht nur um Compliance, sondern um Resilienz, Vertrauen und langfristige



Claus Gründel, General Manager Security Solutions bei Swissbit ©Swissbit

Swissbit

Post-Quantum-Sicherheit und vertrauenswürdige Lieferketten

„2026 wird Post-Quantum-Kryptografie zum bestimmenden Security-Thema. Auch wenn Quantencomputer noch nicht marktreif sind, müssen Unternehmen ihre Systeme jetzt auf die Post-Quantum-Ära vorbereiten. Das reicht von PQC-fähigen FIDO-Authentifikationslösungen mit hybriden Credentials bis zum Schutz langlebiger Embedded- und IoT-Geräte.

Gerade in industriellen Umgebungen, in denen Hardware selten erneuert wird, sind modulare Sicherheitsarchitekturen und agile Kryptografie essenziell. Parallel steigt die Bedeutung einer transparenten, kontrollierbaren Lieferkette – nicht nur durch regulatorische Vorgaben, sondern auch als entscheidendes Differenzierungsmerkmal in einer zunehmend geopolitisch geprägten Welt."

Die Zukunft des Alarms

Elektronische Alarmsysteme in der DACH-Region

Marktentwicklung: Neue Spieler und Konsolidierung

Der Markt für elektronische Alarmsysteme in Deutschland, Österreich und der Schweiz (DACH) steht vor einem spannenden Wandel. Während der Gesamtmarkt für Sicherheitstechnik 2024 trotz schwacher Baukonjunktur um 3,4 % wuchs, stagnierten klassische Einbruchmeldesysteme und blieben hinter dem Marktdurchschnitt zurück. Dies deutet darauf hin, dass etablierte Anbieter unter Innovations- und Preisdruck stehen. Gleichzeitig drängen neue Hersteller mit frischen Ideen in den Markt: Ajax Systems aus der Ukraine und Satel aus Polen etwa gelten als Innovationstreiber, die mit modernen, funkbasierten Systemen traditionelle Platzhirsche herausfordern. Dieses Marktsegment befindet sich genau an einer Weggabelung, geprägt durch Digitalisierung und im Kampf gegen Markthemmnisse durch veraltete Technologien oder Denkweisen. Aber auch in diesem Markt ist die Branche hoffnungsfroh im Aufwind. Wachstumszahlen demonstrieren diese positiven Trends.

Auf der Anbieterseite findet zugleich eine Marktkonsolidierung statt. Große Konzerne strukturieren um: So wurde 2025 der Geschäftsbereich von Carrier Fire & Security (zu dem auch die Marke Aritech gehört) an einen Investor verkauft und unter Kidde Global Solutions (KGS) neu aufgestellt. Traditionsmarken wie Aritech bleiben zwar erhalten, sind nun aber Teil größerer Plattformgesellschaften, was zu gebündelter Expertise, aber auch weniger Vielfalt an unabhängigen Herstellern führt. Ähnlich haben frühere Zusammenschlüsse (etwa die Integration von Bentel, DSC und Visonic unter dem Dach von Tyco/Johnson Controls) den Markt geprägt. Für Errichter und Systemhäuser bedeutet dies einerseits Zugang zu kompletten Lösungsportfolios aus einer Hand, andererseits aber auch die Gefahr, sich von wenigen Großanbietern abhängig zu machen.



International spielen chinesische Anbieter eine ambivalente Rolle. Firmen wie Hikvision oder Dahua bieten zunehmend eigene Alarm- und Smart-Home-Systeme an, meist zu aggressiven Preisen. Gerade im Einstiegssegment und DIY-Bereich haben asiatische Importprodukte den Markt geflutet. Gleichzeitig wächst in sensiblen Bereichen das Misstrauen gegenüber chinesischer Hardware. So wird in den USA und Teilen Europas der Verzicht auf chinesische Kameratechnik forciert – ein Trend, der Wettbewerbern Chancen eröffnet. Ajax Systems etwa hat angekündigt, verstärkt im Kamera-Segment mit KI-Funktionen anzutreten und will damit gezielt Marktanteile gewinnen, die chinesische Hersteller durch Vertrauensverluste einbüßen. Insgesamt ist zu erwarten, dass Technologietrends wie künstliche Intelligenz, Videoüberwachung und Smart-Home-Integration die Branche antreiben – wer hier innovationsfähig ist, kann sich vom Wettbewerb abheben.

Ajax Systems: Funk-Technologie als Game-Changer

Ajax Systems aus der Ukraine gilt als Vorreiter einer neuen Generation von Alarm-

systemen. Das Unternehmen setzt vollständig auf drahtlose Funktechnik und kombiniert diese mit einer benutzerfreundlichen App-Plattform. Sämtliche Sensoren – von Bewegungsmeldern über Öffnungskontakte bis zu Rauch- und Wassermeldern – kommunizieren per verschlüsseltem Funkprotokoll mit der Zentrale. In den vergangenen Jahren hat Ajax konsequent die Leistungsfähigkeit dieser Funktechnik ausgebaut und ging nun Ende 2025 einen entscheidenden Schritt. Nach Angaben des Herstellers Ajax Systems stellte das Unternehmen das erste vollständig kabellose Alarmsystem mit EN 50131-Grade-3-Zertifizierung vor – ein Schutzgrad, der bislang primär verkabelten Systemarchitekturen vorbehalten war.

Die Vorteile liegen auf der Hand: Installation und Nachrüstungen werden drastisch vereinfacht – es müssen keine Kabel gezogen oder Wände aufgestemmt werden, was Zeit und Kosten spart. Projekte lassen sich so deutlich schneller umsetzen, selbst in Bereichen mit höchsten Sicherheitsanforderungen (etwa Juweliere, Banken oder Rechenzentren).

Auch bei der Vertriebsstrategie beschreitet Ajax teils neue Wege. Das System wird zwar professionell installiert, aber der Hersteller pflegt einen nahezu consumer-orientierten Markenauftritt mit regelmäßigen Produkt-Events, umfangreicher Online-Präsenz und intuitiven Tools für Errichter und Endkunden. In der DACH-Region baut Ajax auf Distributionspartner und veranstaltet Ajax Business Days, um Facherrichter mit der Technik vertraut zu machen. Die Ajax-App und Cloud spielen eine zentrale Rolle: Endkunden können ihre Anlage bequem per Smartphone steuern, inklusive Alarmbenachrichtigung und Videoverifikation.

Für Errichter bietet Ajax einen Partner-Webzugang mit Überblick über installierte Anlagen, Wartungszustände und Updates, was den Service erleichtert. DIY-Tauglichkeit ist offiziell nicht das Ziel – Ajax positioniert sich als Profi-System – doch die einfache Konfiguration und der Verzicht auf Verdrahtung ermöglichen es technisch versierten Nutzern durchaus, kleinere Anlagen selbst in Betrieb zu nehmen. Im Vergleich zu klassischen Anbietern verzichtet Ajax gänzlich auf fest verdrahtete Bus-Komponenten und setzt stattdessen auf eigene Funk-Repeater, um auch größere Objekte (bis zu 200-250 Sensoren) abdecken zu können. Interessant ist, dass Ajax trotz Cloud-Anbindung keine laufenden Nutzungsgebühren für die App erhebt – ein Unterschied zu manchem etablierten Anbieter.

Satel: Polnischer Allrounder mit Hybrid-Ansatz

Der polnische Hersteller Satel verfolgt einen etwas anderen Ansatz: Er bietet Hybrid-Systeme an, die sowohl Draht- als auch Funktechnik unterstützen. Satel unterteilt Alarmanlagen ausdrücklich in drahtgebundene, drahtlose oder kombinierte Installationen. Damit kann je nach Projekt flexibel entschieden werden, ob z.B. Bewegungsmelder per Bus-Leitung angeschlossen oder per Funk eingebunden werden – viele Satel-Zentralen (z.B. aus der INTEGRA-Serie) erlauben beides. Das kommt vor allem in Bestandsgebäuden zum Tragen, wo Funklösungen eine schnelle Nachrüstung ermöglichen, während im Neubau oft Bus-Technik bevorzugt wird. In puncto Vertriebskanal setzt Satel auf klassische Fachherrichter und den Elektrogroßhandel.
In der DACH-Region kann die Marke ihre Position noch weiter ausbauen, durch Kooperationen mit Sicherheitstechnik-Distributoren und durch professionelle Messepräsenzen (z.B. auf der Security Essen) hat sich Satel einen festen Platz bei vielen Installateuren erarbeitet.

Technologisch punktet Satel mit einer breiten Plattformstrategie: Die Alarmzentralen lassen sich meist nicht nur für Einbruchmeldungen nutzen, sondern auch für Zutrittskontrolle und einfache Gebäudeautomation. So wirbt Satel mit „Intelligent Security Solutions" – Lösungen, die Sicherheits-, Zugangs- und Smart-Building-Funktionen vereinen. Ein Beispiel ist die Integration mit dem Gebäudeautomations-Standard KNX: Über ein optionales KNX-Modul kann eine Satel-Alarmanlage mit dem Smart-Home-System kommunizieren, etwa um im Alarmfall Lichter einzuschalten oder Rollläden hochzufahren. Diese Offenheit für offene Standards hebt Satel von manch proprietärer Konkurrenz ab.



©Satel

Bei der Cloud-Anbindung zeigt sich Satel eher konservativ: Fernzugriff für Benutzer und Remote-Konfiguration für Techniker sind zwar möglich (via Apps und PC-Software), laufen aber meist über eigene Ser-


©Satel bewave

ver oder VPN-Verbindungen, nicht über eine ständig aktive IoT-Cloud. Das System erfordert daher etwas mehr Konfigurationsaufwand und Fachkenntnis, was die DIY-Tauglichkeit einschränkt – Satel-Anlagen werden typischerweise von geschulten Errichtern projektiert und eingerichtet. Im Vergleich zu Ajax Systems positioniert sich Satel somit als Allrounder, der moderne Funktechnik bietet, aber zugleich das klassische Errichter-Handwerk und etablierte Standards wie VdS-Grade, EN-Normen und KNX-Bus fest im Blick behält.

Jablotron: Tschechischer Komplettanbieter mit Cloud-Fokus


©Jablotron

Der tschechische Hersteller Jablotron geht einen etwas anderen Weg und gilt als Vorreiter bei cloudverbundenen Alarmsystemen. Ähnlich wie Satel setzt Jablotron zwar auf Hybrid-Systeme, die sowohl Draht- als auch Funktechnik unterstützen – die aktuelle Jablotron 100+ Zentrale kombiniert kabelgebundene Bus-Komponenten und Funkmelder für eine hohe Installationsflexibilität.

In Bestandsgebäuden ermöglicht die Funkanbindung eine schnelle Nachrüstung, während im Neubau Bus-Leitungen für stabile Vernetzung sorgen. Anders als manch anderer Anbieter hat Jablotron jedoch früh auf Cloud-Konnektivität gesetzt: Bereits 2011 führte Jablotron als erster Alarmhersteller Cloud-Dienste ein, um Alarmsysteme rund um die Uhr online zu halten. Nutzer können ihre Alarmanlage permanent per MyJablotron-App überwachen und steuern, und auch Alarmempfangsstellen (Leitstellen) sind 24/7 mit dem System verbunden. Diese permanente IoT-Anbindung bietet stets aktuelle Statusinformationen und hohen Bedienkomfort, erfordert aber die Infrastruktur des Herstellers.

Im Vertrieb setzt Jablotron – trotz seiner IoT-Affinität – auf ein klassisches Facherrichter-Modell. Die Systeme werden ausschließlich von zertifizierten Jablotron-Partnern geplant, installiert und per PC-Software (F-Link) programmiert. Endkunden profitieren anschließend von einer intuitiven Bedienung: Jablotron-Anlagen gelten als äußerst benutzerfreundlich. Die Steuerung erfolgt optional über schlichte Bedienteile mit Ampel-LED-Anzeigen oder komfortabel via Smartphone-App. Über die App lassen sich Alarme einsehen, das System scharf/unscharf schalten und sogar Hausautomationsfunktionen bedienen. Jablotron verfolgt den Ansatz einer umfassenden Lösung aus einer Hand: Das System vereint Einbruchmeldeanlage, Gefahrenmelder (z.B. Rauch, Wasser, CO) und einfache Smart-Home-Funktionen in einer Plattform. So können beispielsweise Beleuchtung, Heizung oder Garagentore über Ausgänge der Alarmzentrale automatisiert und ferngesteuert werden. Eine Integration in offene Gebäudeleittechnik ist ebenfalls möglich – etwa über ein optionales KNX-Interface, das Jablotron-Anlagen bidirektional mit einer KNX-Smart-Home-Installation kommunizieren lässt.

Insgesamt bietet Jablotron somit ein rundes Gesamtpaket, das Sicherheit und Komfort vereint, allerdings innerhalb seines proprietären Ökosystems bleibt. Bei der Cloud-Anbindung zeigt sich Jablotron deutlich progressiver als konservative Mitbewerber: Fernzugriff und -wartung sind fester Bestandteil des Systems und laufen über die eigenen europäischen Jablotron-Server. Jablotron ist überzeugt, dass jedes Alarmsystem idealerweise an eine Leitstelle aufgeschaltet sein sollte – das System unterstützt daher von Haus aus die Aufschaltung auf Alarmempfangsstellen (über Jablotrons Cloud ARC). Im Alarmfall können so Interventionen durch Wachdienste unmittelbar eingeleitet werden. Diese Architektur erfordert zwar etwas mehr initiale Konfiguration durch den Fachmann und bindet den Kunden an Dienste des Herstellers, ermöglicht aber auch einen hohen Grad an Service (z.B. automatische Funktionstests, Firmware-Updates und 24/7-Verbindung) ohne dass der

Endnutzer sich technisch kümmern muss. DIY-Tauglichkeit steht folglich nicht im Vordergrund .
Im Vergleich zu Ajax Systems positioniert sich Jablotron als Komplettlösung, die moderne Funktechnik und permanente App-Anbindung bietet, dabei aber stärker auf professionelle Installation und Überwachung setzt. Wie Ajax nutzt auch Jablotron hauptsächlich proprietäre Funkprotokolle im 868-MHz-Band und bietet stylish designte Komponenten, doch Jablotron erlaubt zusätzlich eine Verkabelung von Geräten und verfolgt einen „Service"-Ansatz: Alarmanlagen werden meist mit Wartungsvertrag und Aufschaltung verkauft, weniger als reines Gadget. Zudem erfüllt Jablotron die gängigen europäischen Normen (EN 50131 Grad 2, entsprechend VdS-Klasse A und setzt auf zertifizierte Cloud-Sicherheit (ISO-zertifizierte Rechenzentren in der EU. Nationale Zertifizierungen wie das deutsche VdS-Siegel stehen dabei weniger im Fokus – ähnlich wie andere internationale Hersteller orientiert man sich an pan-europäischen Standards.
Insgesamt bedient Jablotron damit einen Mittelweg: Der Hersteller vereint die Vorteile neuer, cloudbasierter Alarmsysteme mit der klassischen Facherrichter-Philosophie und etablierten Sicherheitsstandards. Installateure schätzen die vielseitige All-in-One-Plattform und Endanwender die einfache Bedienung – eine Win-win-Situation, die Jablotron in der Sicherheitsbranche einen festen Platz verschafft hat

Telenot: Deutsche Qualität mit Zertifikat

Wenn es um traditionelle Alarmtechnik in Deutschland geht, fällt fast zwangsläufig der Name Telenot. Der mittelständische Hersteller aus Aalen steht seit Jahrzehnten für verkabelte Profi-Anlagen, hat aber mittlerweile ebenfalls leistungsfähige Funkkomponenten im Programm. Telenot verfolgt dabei strikt einen Hybrid-Ansatz: Die aktuelle Alarmzentrale compact easy smart&safe vereint alle Installationsarten – bis zu 100 Melder können wahlweise per Funk, per klassischer Drahtlinie oder via



moderner Bus-Technik angeschlossen werden. Diese Flexibilität erlaubt es, Bestandsbauten ohne großen Aufwand nachzurüsten, aber auch Neubauten vollverdrahtet auszustatten, wo gewünscht. Telenot betont, dass dank dieses Baukastenprinzips praktisch jedes Objekt passend ausgerüstet werden kann, vom Einfamilienhaus bis zum Gewerbebetrieb.

Ein Alleinstellungsmerkmal von Telenot ist der Vertriebskanal: Das Unternehmen verfügt über ein einzigartiges Partnernetz mit rund 450 autorisierten Telenot-Stützpunkten im deutschsprachigen Raum. Nur zertifizierte Facherrichter dürfen Telenot-Anlagen installieren, was eine gleichbleibend hohe Qualität sicherstellen soll. Endkunden erhalten Planung, Montage und 24/7-Service aus einer Hand über diese Partnerbetriebe.

Ein DIY-Verkauf an Endverbraucher findet nicht statt – Telenot positioniert sich klar als Premium-Anbieter „mit Brief und Siegel". Diese Strategie unterstreicht Telenot auch durch kompromisslose Zertifizierungen: Sämtliche Komponenten tragen Gütesiegel wie das VdS-Home oder EN Grad 2/3, sind polizeilich empfohlene Anlagen und KfW-förderfähig. Für sicherheitssensible Kunden und Versicherer behalten solche Prüfsiegel einen hohen Stellenwert.
Trotz seines konservativen Rufs hat Telenot bei Cloud und Apps aufgeholt. Die hauseigene SmartApp (BuildSec 4.0) ermöglicht Smartphone-Bedienung und Statuskontrolle der Anlage.

Besonderen Wert legt Telenot dabei auf Datensicherheit: Die Kommunikation zwischen App und Alarmzentrale läuft ausschließlich über die firmeneigene hochsichere Plattform „hiXser- ver" und ist Ende-zu-Ende verschlüsselt. So bleiben alle sensiblen Daten unter Kontrolle des Herstellers bzw. des Errichters – ein bewusstes Gegenmodell zu Cloud-Diensten außerhalb Europas. Allerdings ist für die App-Nutzung eine Freischaltung durch den betreuenden Telenot-Partner nötig, der damit weiterhin als Bindeglied zwischen Technik und Endkunde fungiert. Konfigurationsaufwand und Inbetriebnahme sind bei Telenot-Lösungen deutlich höher als etwa bei Ajax oder Lupus, was aber vom Zielpublikum – professionelle Errichter und anspruchsvolle Gewerbekunden – in Kauf genommen wird für maximale Zuverlässigkeit.
In Summe bleibt Telenot ein Benchmark für Qualität und Sicherheit „Made in Germany". Die Unternehmenstreue ihrer Partner und Kunden ist hoch, doch im Wettbewerb mit agileren Funk-Newcomern muss Telenot zeigen, dass traditionelle Stärken wie Zertifizierung und langlebige Technik auch in Zukunft kaufentscheidend bleiben.

Aritech (Kidde/Carrier): Integrierte Lösungen über den Errichter

Aritech ist eine traditionsreiche Marke, die vor allem Branchenkennern geläufig ist. Ursprünglich in den 90er Jahren als europäische Alarmtechnik-Marke bekannt, war Aritech später Teil von GE Security und zuletzt unter dem Dach von Carrier Fire & Security angesiedelt. Seit 2025 gehört Aritech zur neuen Kidde Global Solutions (KGS) Plattform, bleibt aber als Produktname bestehen. Aritech steht sinnbildlich für klassische Einbruchmeldetechnik im gewerblichen Bereich: Verkabelte oder hybride Zentralen mit hoher Skalierbarkeit, oft kombiniert mit Brandmelde- und Zutrittskontrolltechnik. In der DACH-Region sind Aritech-Systeme vor allem in größeren Liegenschaften (Bürokomplexe, industrielle



©aritech

Anlagen) im Einsatz, wo sie von zertifizierten Errichtern projektiert werden.

Die Vertriebs- und Produktstrategie von Aritech (bzw. KGS) setzt auf Praxisnähe und Weiterentwicklung bewährter Lösungen. Laut KGS soll der deutsche Markt konsequent mit den bewährten Marken weiterentwickelt werden – inklusive praxisnaher Unterstützung für Planer, Errichter und Endanwender. Das deutet darauf hin, dass Aritech-Produkte auch künftig über den klassischen Errichterkanal verkauft und betreut werden. DIY- oder Retail-Angebote existieren praktisch nicht; stattdessen liegt der Fokus auf Ausschreibungen und Systemlösungen, bei denen z.B. eine Alarmzentrale in ein Gesamtsicherheitskonzept (inkl. Video, Zutritt, Gebäudeleittechnik) integriert wird.

Technologisch hat Aritech in den letzten Jahren sein Portfolio modernisiert, z.B. mit der interaktiven Touch-Bedienung RisControl und IP-fähigen Hybridzentralen (der ATS Advanced-Reihe). Funktechnik spielt eher eine untergeordnete Rolle – zwar gibt es Funkmelder und Erweiterungsmodule, doch Aritech-Anlagen werden in der Regel drahtgebunden errichtet, um höchste Stabilität und EMI-Resistenz zu gewährleisten.

Bei Cloud-Anbindung bleibt Aritech konservativ: Fernüberwachung erfolgt meist über Leitstellen-Protokolle oder VPN, weniger über Endkunden-Apps (obwohl Fernsteuer-Apps vorhanden sind). Diese zurückhaltende Plattformstrategie unterscheidet Aritech von den agilen Newcomern, ist aber in sicherheitskritischen Umgebungen oft erwünscht. Unterm Strich bedient Aritech weiterhin vor allem Sicherheitsprofis, die robuste, integrierbare Systeme suchen – im Vergleich mit Ajax oder Abus also eher kein Massenmarkt-Produkt, aber ein stabiler Pfeiler im High-End-Segment der Sicherheitstechnik.

Silentron: Italiens Funk-Pionier



Silentron aus Italien nimmt eine besondere Rolle ein, denn das Unternehmen war einer der ersten Hersteller weltweit, der auf kabellose Alarmtechnik setzte. Bereits seit den 1970er Jahren entwickelt Silentron drahtlose Alarmanlagen und gilt damit als erster italienischer Pionier auf diesem Gebiet.

Das Produktangebot umfasst heute ein vollständiges Sortiment professioneller Alarmtechnik – von Zentralen über Melder bis zu Sirenen – und setzt durchgängig auf Funkkommunikation. Anders als Ajax, das Funk erst in jüngerer Zeit mit neuester Technologie einführte, kann Silentron auf jahrzehntelange Erfahrung zurückgreifen. Allerdings basierten frühe Silentron-Systeme auf proprietären Funksignalen mit begrenzter Reichweite und ohne die modernen Verschlüsselungsstandards – hier haben neuere Wettbewerber technologisch aufgeholt und teils überholt. Silentron vertreibt seine Systeme vorwiegend in Südeuropa über autorisierte Errichter und seit einigen Jahren auch über die Nice-Gruppe (ein italienischer Smart-Home-Konzern, zu dem Silentron mittlerweile gehört).

In der DACH-Region ist Silentron eher ein Nischenanbieter, der v.a. über Importeure vereinzelt Projekte ausstattet. Vertriebskanal ist klassisch der Installateur-Fachbetrieb; ein Endkundengeschäft existiert kaum. Die DIY-Tauglichkeit der Systeme ist gering – zwar sind sie funktechnisch relativ simpel aufzubauen, aber die Programmierung der Zentralen erfolgt meist über Codes und PC-Software, was Fachwissen erfordert.

In puncto Cloud und Plattform hält sich Silentron zurück: Einige neuere Modelle bieten eine App-Anbindung und Fernwartung, doch ein umfassendes Cloud-Ökosystem fehlt. Hier spiegelt sich die DNA als klassischer Alarmhersteller wider. Immerhin können neuere Silentron-Alarmzentralen in Smart-Home-Systeme eingebunden werden (z.B. über I/O-Module oder proprietäre Schnittstellen), aber offene Standards wie KNX werden – anders als bei Satel – nicht direkt unterstützt.

Funktechnik vs. Draht ist bei Silentron kein Entweder-Oder, sondern die Unternehmensphilosophie: Man vertraut vollständig auf Funk. Für Installateure mag das ungewohnt sein, doch Silentron be-

tont die professionelle Zuverlässigkeit seiner Funklösungen, die sich in tausenden Installationen bewährt hätten.

zonen, können aber auch via Funkempfänger drahtlose Melder einbinden. Einen reinen Funkansatz wie Ajax verfolgt man nicht



©Technoalarm



©Bentel Security/Johnson Controls

Im Vergleich zu Ajax fehlen Silentron allerdings einige moderne Features (z.B. Videoverifikation oder smarte App—Steuerung), sodass der einstige Pionier heute eher im Mittelfeld des Innovationsrankings liegt. Für bestimmte Einsatzfälle – etwa in historischen Gebäuden mit Denkmalschutz, wo keine Kabel verlegt werden dürfen – bleiben Silentron-Anlagen eine interessante Option.

Tecnoalarm: High-End-Security made in Italy

Tecnoalarm ist ein weiterer italienischer Hersteller, der sich einen Namen vor allem im High-End-Segment gemacht hat. Seit der Gründung 1977 verfolgt Tecnoalarm mit großer Leidenschaft ein Ziel: höchste Zuverlässigkeit und frühzeitige Detektion (Zitat aus einem Unternehmensprofil). Das Unternehmen hat einige technisch ausgefeilte Lösungen entwickelt, zum Beispiel besondere Bewegungsmelder mit Doppler-Radar-Technologie und fokussierbarer Abdeckung, die in kunstvollen Pininfarina- Designgehäusen stecken. Tecnoalarm-Anlagen werden oft dort eingesetzt, wo hochwertige Objekte (Villen, Museen, Juweliergeschäfte) geschützt werden müssen und wo false Alarms minimiert werden sollen.

Bei der Technik kombiniert Tecnoalarm überwiegend verkabelte Systeme mit optionalen Funkerweiterungen. Die Zentralen (z.B. TP8-Serie) unterstützen Bus-Module und Kabel– Tecnoalarm vertraut primär auf Kabel für die Kernsensorik und nutzt Funk meist nur ergänzend. Die Vertriebsstruktur ist klar auf professionelle Errichter ausgerichtet. In DACH arbeitet Tecnoalarm mit spezialisierten Partnerfirmen, die oft auf Luxus-Sicherheitstechnik spezialisiert sind. DIY oder Massenmarkt spielt keine Rolle.

Interessant ist Tecnoalarms Plattform- und Service-Strategie: Mit der firmeneigenen RSC®-Technologie (Remote Sensitivity Control) können Installateure die Empfindlichkeit der Sensoren aus der Ferne justieren und regelmäßige Fernwartungen durchführen, ohne vor Ort sein zu müssen. Damit war Tecnoalarm ein Vorreiter in Sachen Remote-Service, lange bevor Cloud-Plattformen üblich waren. Heute bietet Tecnoalarm Apps für Alarmierung und Statusanzeige an, doch die Kernsteuerung läuft lokal und ohne Cloud-Zwang. Das System richtet sich an Fachleute, die eine feine Abstimmung der Melder vornehmen – so gesehen ist der Konfigurationsaufwand hoch, aber das Resultat sehr individuell optimiert.

Im Vergleich mit Ajax und Satel positioniert sich Tecnoalarm als Boutique-Anbieter. Funk vs. Draht ist hier keine ideologische Frage, sondern eine des Einsatzortes – man bietet beides an, rät aber bei höchster Sicherheit oft zu Draht. Der Vertriebskanal bleibt exklusiv: Tecnoalarm-Installateure durchlaufen spezielle Schulun- gen, um die Technik auszureizen. Für Endkunden (und Errichter) mit höchsten Ansprüchen an Alarmreaktion und Falschalarm- sicherheit bleibt Tecnoalarm eine feste Größe, auch wenn der Hersteller in puncto Smart-Home-Integration und Cloud eher zurückhaltend agiert.

Bentel Security: Italienische Marke im globalen Verbund

Bentel Security aus Italien hat eine doppelte Identität: Zum einen ist Bentel ein traditionsreicher Hersteller von Alarmanlagen mit eigener Geschichte; zum anderen ist Bentel heute Teil der Produktfamilie von DSC/Tyco (inzwischen Johnson Controls). Das bedeutet, dass Bentel-Produkte in Technik und Strategie eng mit den weltweit vertriebenen Systemen von DSC/Visonic verzahnt sind. So gilt Bentel als Security-Benchmark und bietet ein komplettes Sortiment an Einbruchmeldetechnik und Brandmeldesystemen an. Besonders bekannt ist die KYO-Panelserie und die neuere ABSOLUTA-Zentrale, die modular erweiterbar ist.

Technologisch folgt Bentel dem Kurs des Mutterkonzerns: Die aktuellen Bentel-Alarmzentralen sind Hybrid-Systeme, die sowohl kabelgebundene Zonen als auch modernste Funkmelder unterstützen. Hier kommt oft die PowerG-Funktechnologie zum Einsatz – ein hochreichweiten, verschlüsseltes Funkprotokoll, das von Visonic/DSC entwickelt wurde.

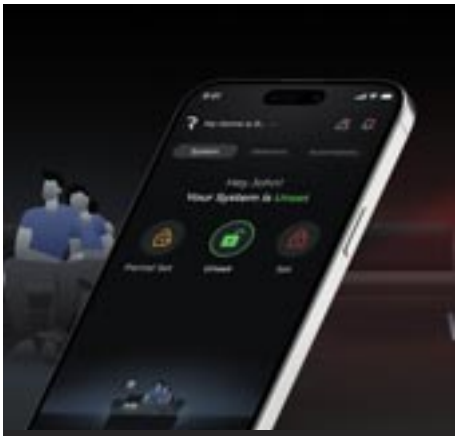
Eine Bentel ABSOLUTA Plus mit Funkmodul kann z.B. bis zu 48 Zonen überwachen, verkabelt oder kabellos, und eignet sich damit für mittelgroße Wohn- und Gewerbeobjekte. Im Gegensatz zu reinen Funkanbietern hat Bentel also die Flexibilität, dem Kunden beides zu bieten.

Vertriebskanal und Plattformstrategie sind stark vom internationalen Konzern geprägt. Bentel-Produkte werden über Sicherheits-Großhändler und Installateure vertrieben, oft als Teil eines größeren Portfolios (inkl. Kameras, Zutritt etc. von JCI). Bentel-Alarmanlagen lassen sich in viele Überwachungsplattformen integrieren; es gibt Apps und IP-Module, die z.B. eine App-Steuerung via Cloud ermöglichen. So existiert die ABSOLUTA-App, mit der Nutzer ihr System aus der Ferne bedienen können – allerdings setzt dies ein aktuelles Panel-Firmware-Update voraus und die Nutzung erfolgte in der Vergangenheit teils über kostenpflichtige Services. Bentel selbst kommuniziert gegenüber Endkunden relativ wenig; die Marke tritt oft im Hintergrund auf, während Errichter oder Distributoren den Support übernehmen. Für DIY-Kunden ist Bentel nicht gedacht, auch wenn Alarmlösungen technisch versierte Käufer über Online-Shops erreichen könnten.

Im Vergleich zu Ajax oder Lupus fehlt Bentel etwas der Glamour – man setzt eher auf bewährte Sicherheitstechnik als auf Lifestyle-Features. Dafür profitieren Bentel-Kunden von der Kontinuität und globalen Unterstützung durch einen Großkonzern: Ersatzteile, langfristige Updates und Kompatibilität über Generationen hinweg sind meist gegeben. Bentel Security vereint somit italienische Alarm-Expertise mit internationaler Konzern-Power, was im DACH-Markt v.a. professionelle Anwender anspricht, die Wert auf Zuverlässigkeit und Integration in komplexe Systeme legen.

Rokonet/RISCO:
Israeli Innovation mit Cloud-Fokus

Rokonet war einst ein bekannter Name für Bewegungsmelder und Alarmanlagen aus Israel. Heute firmiert das Unternehmen unter RISCO Group und hat sich zu einem global aktiven Anbieter mit starker Cloud-Orientierung gewandelt. RISCO bietet mehrere Alarmserien (Agility – Funk, LightSYS – Hybrid, ProSYS – verkabelt) und hat früh auf die Verzahnung mit Internetdiensten gesetzt. So betreibt RISCO eine eigene Cloud-Plattform, über die Endanwender per iRISCO-App ihre Alarmanlagen steuern können und Installateure Fernwartungen durchführen.


iRISCO – Version 6.1.0 ©RISCO

Dieses Konzept wurde kontinuierlich ausgebaut: 2024 erhielt die RISCO-Cloud ein Update auf Version 6.2, das die zweiseitige Kommunikation zwischen Installateur und Endkunde verbessert und nun Push-Benachrichtigungen mit Antwortmöglichkeiten ermöglicht. Konkret kann der Alarmbenachrichtigung jetzt z.B. ein Button beigefügt werden ("Hilfe rufen" o.ä.), der direkt eine vordefinierte Aktion auslöst – eine clevere Verknüpfung von Alarm und Service für den Nutzer.

RISCOs Vertriebsstrategie bleibt trotz Cloud-Fokus im Kern beim Facherrichter. Allerdings versucht das Unternehmen, seine Partner mit neuen Geschäftsmodellen zu unterstützen: Über ein Cloud Revenue Program können Errichter z.B. laufende Einnahmen generieren, indem sie ihren Kunden die App-Nutzung und Cloud-Dienste als Abo verkaufen. Dies zeigt, wie sehr RISCO auf die Cloud setzt – sie ist nicht nur technische Drehscheibe, sondern auch Teil des Geschäftsmodells. Für Endkunden bedeutet das einerseits komfortable Funktionen (Fernzugriff, visuelle Verifikation via vernetzter Kameras, Smart-Home-Features wie Szenensteuerung), andererseits aber auch laufende Kosten und die Abhängigkeit von der RISCO-Cloud-Verfügbarkeit. Technologisch hat RISCO in den letzten Jahren vor allem an Integration gearbeitet. Das Touch-Bedienteil RisControl fungiert als Smart-Home-Panel: In Version 1.7 lässt es sich sogar mit dem Multiroom-System Sonos koppeln, sodass z.B. Musik oder Durchsagen angesteuert werden können. Zudem können RISCO-Alarmanlagen mit IP-Kameras verknüpft werden (Stichwort Videoverifikation). Funk vs. Draht: RISCO hat hier mit der LightSYS+ eine Hybridlösung im Portfolio, die bis zu 128 Zonen unterstützt – kabelgebunden oder per Funk (die LightSYS Air-Melderlinie). Rein drahtlose Systeme bedient die Agility-Reihe, die v.a. im Privatbereich beliebt ist.
DIY-Lösungen bietet RISCO offiziell nicht an, obgleich findige Kunden auch RISCO-Kom- plettpakete online erwerben und selbst installieren könnten. Der Konfigurationsaufwand ist jedoch höher als bei typischen DIY-Systemen, und viele Funktionen (z.B. Cloud-Einbindung) setzen eine Einrichtung durch einen registrierten Installer voraus.
In der DACH-Region hat RISCO eine solide Präsenz, besonders in Österreich und der Schweiz über lokale Partner.

Gegenüber Ajax oder Abus positioniert sich RISCO als innovationsgetrieben mit starker Cloud und breitem Portfolio. Für Errichter, die offen für Cloud-Services sind, bietet RISCO eine ausgereifte Plattform, die Wartungsaufwand reduziert (durch Remote-Zugriff) und sogar Zusatzgeschäfte erlaubt. Endanwender profitieren von einer stetig erweiterten App und neuen Smart-Home- Funktionen – sofern sie bereit sind, ihre Sicherheitslösung in die Hände einer Cloud zu legen.



Lupus Electronics: Smarte Alarmanlagen zwischen Profi und DIY

Lupus Electronics aus Deutschland nimmt im Alarmanlagensegment eine Sonderstellung ein. Das Unternehmen aus Landau (Pfalz) hat sich auf Alarm- und Smarthome-Kombinationen spezialisiert und spricht dabei gleichermaßen technikaffine Endanwender wie auch professionelle Installateure an. Die LUPUSEC-Systeme (XT1 Plus, XT2 Plus, XT3 etc.) sind funkbasiert und modular erweiterbar – bis zu 80 Sensoren pro Zentrale – und verbinden klassische Sicherheitsfunktionen mit Smart-Home-Features in einer einzigen Plattform. Über 80 eigene Sensoren und Aktoren (von Bewegungsmeldern über Heizkörperthermostate bis Sirenen) stehen zur Verfügung; zusätzlich lassen sich zahlreiche Drittprodukte integrieren, etwa Philips-Hue-Leuchten, Nuki-Türschlösser und seit neuestem auch Sonos-Lautsprecher. Lupus verfolgt damit konsequent eine offene Plattformstrategie für das vernetzte Zuhause, bei der Alarmanlage, Videoüberwachung und Hausautomation verschmelzen.



Eine Besonderheit von Lupus ist die Cloud-Philosophie – oder vielmehr das Feilen daran. Die Alarmzentralen besitzen eine eingebaute Web-Oberfläche und können im lokalen Netzwerk betrieben werden, ohne Daten an externe Server zu senden („Keine Cloud – keine Datenkrake. Ihre Daten bleiben zu Hause", wirbt ein Anbieter). Die Systemsicherheit wird dabei jährlich von AV-Test geprüft, um Cybersecurity zu gewährleisten. Gleichzeitig bietet Lupus aber auch Cloud-Dienste an: Über die Lupus-App können Nutzer von unterwegs auf ihre Anlage zugreifen, wobei die Verbindung über gesicherte Lupus-Server läuft. Dieser hybride Ansatz erlaubt dem Kunden zu wählen, ob er maximale Privatsphäre (lokaler Betrieb) oder maximalen Komfort (Cloud-Zugriff) möchte.

In der Vertriebspraxis zeigt sich Lupus äußerst flexibel. Die Produkte können direkt im Online-Shop des Herstellers oder über Elektronik-Fachhändler von Endkunden gekauft und in Eigenregie installiert werden. Für weniger versierte Nutzer bietet Lupus aber auch ein Partnernetz von Errichtern an, welche Installation und Wartung übernehmen. Diese Dual-Strategie

(Profi- und DIY-Kanal) ist in der Alarmbranche eher selten und hat Lupus eine treue Fangemeinde eingebracht. DIY-Tauglichkeit ist definitiv gegeben: Die XT-Zentralen werden einfach per LAN/WLAN ans Heimnetz angebunden, die Sensoren funken alle an diese Zentrale, und die Konfiguration erfolgt über eine menügeführte Weboberfläche bzw. App, die von vielen Kunden als sehr verständlich gelobt wird.

Natürlich hat dieser Komfort auch Grenzen: Bei VdS-zertifizierten Hochsicherheitsinstallationen spielt Lupus kaum eine Rolle, und wirklich große Objekte (mit mehr als 100 Meldern, komplexen Zutrittskontrollen etc.) sind besser mit klassischen Systemen bedient. Doch für Eigenheime, Büros und kleinere Gewerbe bietet Lupus eine Plug-&-Play-Sicherheit, die den Installations- und Wartungsaufwand minimiert. Updates kommen automatisch übers Internet, neue Komponenten lassen sich in Minuten anlernen, und durch die Einbindung von Smart-Home-Komponenten entsteht ein Mehrwert über die reine Einbruchmeldung hinaus (etwa Alarmanlagen-Sensorik, die auch zur Lichtsteuerung oder Heizungsabsenkung genutzt wird). Im Vergleich zu Ajax Systems ist Lupus noch lokal verwurzelt und etwas kleiner aufgestellt, braucht sich technisch aber nicht zu verstecken – insbesondere wer eine Datensouveränität schätzt, findet hier eine interessante Alternative. Für Errichter bedeutet Lupus, dass sie einerseits einen preislich attraktiven Baukasten anbieten können, der wenig Support erfordert, andererseits aber Konkurrenz durch Selbstinstaller in Kauf nehmen müssen. Dieser Spagat zwischen Profi- und DIY-Markt ist Teil der Zukunft, die Lupus in der Branche sichtbar macht.

Abus: Breit aufgestellt von DIY bis High-End

ABUS (August Bremicker und Söhne) ist in Deutschland vor allem als Traditionsmarke für Sicherheit bekannt – Schlösser, Beschläge und seit langem auch Alarmanlagen gehören zum Portfolio. ABUS deckt mit seiner Alarmtechnik sowohl den Endverbraucher- als auch den Profimarkt ab. Im Zentrum stehen dabei zwei Produktlinien: die Secvest-Alarmanlage und die Smartvest/Smartvest Pro.

Secvest ist das professionelle Funkalarmsystem von ABUS. Es handelt sich um eine VdS-zertifizierte Funkalarmanlage für Heim und Gewerbe, die mit zuverlässiger Technik und einfacher Bedienung wirbt. Secvest zeichnet sich durch ein in der Branche einzigartiges Merkmal aus – die Verbindung von Mechatronik und Elektronik. Spezielle Secvest-Fenstergriffe und -Fenstersicherungen von ABUS enthalten Sensorik, die bei einem Einbruchsversuch nicht nur Alarm auslöst, sondern auch mechanisch den Fensterflügel verriegelt. Diese Kombination erhöht den Einbruchschutz physisch und detektiert gleichzeitig den Angriff. Damit besetzt ABUS Secvest eine Nische, die weder Ajax noch Telenot so abdecken.

Technisch ist Secvest eine hybride Funklösung: Die meisten Sensoren arbeiten kabellos, aber es können auch Drahtmelder und verkabelte Bedienteile integriert werden (daher spricht ABUS von einem Hybrid-System). Secvest-Zentralen erreichen EN Grad 2 und sind bei Versicherern für Wohnobjekte anerkannt. Der Vertrieb erfolgt über Fachinstallateure und den ausgewählten Fachhandel; zwar findet man Secvest-Komponenten auch online, doch ABUS empfiehlt die Installation durch geschulte Partner.

Cloud-Anbindung ist gegeben – die Anlage kann per App (Secure@Home) gesteuert werden – jedoch legt ABUS Wert darauf, dass keine Pflicht zur Cloud besteht und die Kernfunktionen lokal funktionieren. Die Einrichtung einer Secvest erfordert Fachwissen, gerade wenn mechatronische Komponenten eingebunden werden. Entsprechend ist die DIY-Eignung begrenzt; diese Anlage richtet sich an qualitätsbewusste Kunden, die einen Errichter hinzuziehen.

Smartvest Pro hingegen wurde gezielt für den Consumer-Markt entwickelt. Diese neue Funk-Alarmanlage (seit Juni 2025 im Handel) richtet sich an private Haushalte, die eine einfache Selbstinstallation wünschen. Die Smartvest Pro kommt als Starter-Kit mit Zentrale (inkl. Innensirene) und kann kabellos um zahlreiche Sensoren erweitert werden. Die Einbindung ins Heimnetz erfolgt per LAN oder WLAN, und die Steuerung läuft über eine kostenlose Smartphone-App. Wichtig: Es fallen keine Abogebühren an – ein starkes Argument



gegenüber manch anderen Smart-Home-Alarmen.
ABUS betont die schnelle, unkomplizierte Inbetriebnahme, die vom Kunden selbst durchgeführt werden kann. Damit wagt ABUS den Spagat, einer breiten Käuferschicht Sicherheitslösungen zugänglich zu machen, ohne einen Profi zu benötigen. Technisch bietet die Smartvest Pro moderne Features wie Alexa/Google-Sprachsteuerung, Szenariensteuerung, Kameraeinbindung und optional ein Mobilfunkmodul für redundante Alarmierung. Im Grunde vereint sie Alarmanlage und Smart Home Zentrale (ähnlich wie Lupus es tut), jedoch mit dem Markenvorteil von ABUS und dessen Vertriebsnetz im Hintergrund.
Verglichen mit Ajax und Satel: ABUS agiert breitflächiger. Während Ajax auf ein Produktkonzept fokussiert und primär die professionelle Schiene fährt, besetzt ABUS mehrere Marktsegmente.
Funktechnik nutzt ABUS in beiden Linien intensiv – verkabelte Lösungen hat ABUS (bis auf alte Terxon-Anlagen) kaum noch im Programm, was den Zeichen der Zeit entspricht. Der Vertriebskanal ist zweigleisig: Secvest über Errichter, Smartvest teils im Einzelhandel/Online. In Sachen Cloud/-Plattform hat ABUS eine eigene „Smart Security World" etabliert, zu der neben Alarmanlagen auch Kameras, Türschlösser und weitere Komponenten gehören, steuerbar über die ABUS-App. Anders als einige Wettbewerber kann ABUS durch seine breite Aufstellung (inkl. Fahrradschlösser, Fenstertechnik, etc.) auch markenfremde Kunden anlocken, die beim Baumarkt vielleicht erst ein Türschloss kaufen und dann eine Alarmanlage derselben Marke in Betracht ziehen.

Standards und Zertifizierungen nutzt ABUS gezielt als Verkaufsargument, etwa VdS Home für Secvest oder Gütesiegel von AV-Test für die IT-Sicherheit der Smartvest. Unterm Strich vermittelt der Name ABUS Vertrauen. Die Produkte selbst müssen sich aber gegen Newcomer wie Ajax behaupten. ABUS setzt auf Usability und vermarktet Produkte mit Blick auf 'bewährte Sicherheit'.


©Honeywell Security

Honeywell/Resideo: Amerikanischer Riese mit Profilsuche

Honeywell Security gehört global zu den großen Namen im Alarmgeschäft. In der DACH-Region ist Honeywell vor allem im gewerblichen Umfeld und bei spezialisierten Errichtern bekannt – etwa durch die MB-Secure Alarmzentralen oder früher die Galaxy-Reihe. Honeywell/Resideo verfolgt eine klare Zwei- gleisigkeit: Für den professionellen Markt gibt es modulare Hybridsysteme (z.B. Vista-Serie, MB-Secure), die verkabelte und Funk-Zonen kombinieren und sich in umfassende Sicherheitssysteme integrieren lassen. Für den Smart-Home-Consumer-Markt in den USA brachte Honeywell hingegen All-in-One-Funkalarmpanels wie die ProSeries auf den Markt – ein 7-Zoll-Touchpanel mit Sicherheits- und Automationsfunktionen, das professionell im Haus installiert wird. In Europa ist diese Linie allerdings weniger präsent.
Vertriebskanal ist bei Honeywell/Resideo traditionell der professionelle Errichter und Großhändler (Resideo betreibt etwa die ADI-Großhandelskette).

DIY-Produkte waren eher die Ausnahme – ein Versuch mit einer direkt an Endkunden verkauften Smart Home Security Base (einer Art Alarmanlagen-Kamera-Hub) wurde 2024 eingestellt. Offenbar besinnt sich Resideo darauf, dass seine Stärke im professionellen Segment liegt. Hier bietet das Unternehmen vernetzte Sicherheitslösungen an, die leicht in Gebäudeleittechnik und Monitoring integriert werden können. So sind Honeywell-Alarmanlagen oft Teil eines Bündels aus Brandmelde-, Zutritts- und Video-Systemen bei Großkunden.

Technologisch setzt Honeywell/Resideo auf konservative Zuverlässigkeit mit modernen Ergänzungen. Die Vista/MB-Secure Panels sind hybridfähig – man kann Draht und Funk nutzen – und vor allem modular erweiterbar. Für die Enduser-Bedienung hat Resideo Connect-Apps und Touch-Keypads eingeführt, um die Systeme smarter zu machen. Außerdem bietet Resideo zahlreiche Funk-Sensoren (Bewegungsmelder, Glasbruch, Rauchmelder etc.), um ältere Drahtanlagen nachträglich kabellos auszubauen. Cloud-Dienste (Total Connect) ermöglichen Fernzugriff und Alarmbenachrichtigung, werden aber primär von professionellen Wachdiensten genutzt oder über Errichter bereitgestellt.
In der DACH-Region ist Honeywell Security

insgesamt etwas im Schatten von Marken wie Telenot oder Abus, die lokal präsenter sind. Doch in bestimmten Bereichen – etwa bei großen kommerziellen Sicherheitssystemen – behalten Honeywell-Lösungen einen festen Platz. Standards wie VdS oder EN werden selbstverständlich erfüllt, und Honeywell engagiert sich in Branchenverbänden (z.B. BHE) mit. Für Errichter kann Honeywell/Resideo vor allem dann interessant sein, wenn integrierte Lösungen gefragt sind, die über das reine Einbruchmelden hinausgehen (Stichwort Gebäudeautomation, Klimasteuerung – hier hat Resideo mit Thermostaten etc. ebenfalls Angebote).
Im Wettbewerb muss Resideo zeigen, dass es innovativ bleibt – die Konkurrenz durch Ajax und Co. zwingt auch die US-Größe dazu, mehr auf Benutzerfreundlichkeit und smarte Features zu setzen, ohne die angestammte Klientel zu verlieren.

Technologietrends: Cloud-Plattformen vs. lokale Systeme

Ein zentrales Thema für die Zukunft der Alarmbranche ist der Umgang mit Cloud-Plattformen. Viele der oben betrachteten Anbieter setzen heute auf Cloud- oder Webdienste, um ihren Kunden mehr Komfort und sich selbst neue Geschäftschancen zu eröffnen. Beispielsweise erlauben Cloud-Lösungen wie die von RISCO oder Ajax, dass Installateure Alarmanlagen komplett aus der Ferne konfigurieren und warten können – ohne zeitaufwändige Vor-Ort-Termine. Updates werden online eingespielt, Sensorzustände lassen sich remote prüfen. Für die Errichter bedeutet das Zeit- und Kostenersparnis, für Endkunden schnellere Hilfe im Servicefall. Auch die Möglichkeit, Alarmbilder oder -videos in der Cloud zu verifizieren, erhöht die Attraktivität solcher Systeme. Allerdings geht damit eine Abhängigkeit von Internet und den Servern des Herstellers einher.

Ein Gegenmodell verfolgen Hersteller wie Lupus oder (in Teilen) Abus: Sie bieten lokale Steuerungsmöglichkeiten an, sodass die Kernfunktionen der Alarmanlage auch ohne Cloud verfügbar sind. Lupus wirbt explizit damit, dass bei seinen Systemen sämtliche Daten auf der Zentrale vor Ort bleiben und der Nutzer entscheiden kann, ob er die optionalen Cloud-Funktionen nutzen will. Diese Strategie spielt vor allem in der DACH-Region, wo das Thema Datenschutz einen hohen Stellenwert hat, vielen Kunden in die Karten. Auch Telenot setzt statt einer öffentlichen Cloud lieber auf eine geschlossene eigene Plattform (hiX-server) mit streng kontrolliertem Zugriff.

In Zukunft wird sich zeigen, ob Cloud-Plattformen oder lokale Lösungen die Oberhand gewinnen. Wahrscheinlich ist eine Koexistenz: Professionelle Systeme werden weiterhin einen lokalen Basiskern haben (schon aus Redundanzgründen, falls das Internet ausfällt), aber mit Cloud-Diensten angereichert werden.

Wichtig für Endkunden ist die Transparenz: Welche Daten fließen wohin? Sind Services kostenlos oder mit Abo verbunden? Hier zeichnet sich eine Segmentierung ab: Im DIY- und Smart-Home-Segment sind kostenlose Apps ohne Folgekosten beinahe ein Muss (Ajax, Abus Smartvest Pro, Lupus etc.), da Kunden andernfalls zu Konkurrenz ohne Gebühren wechseln.

Im professionellen Segment hingegen sind Kunden eher bereit, für Mehrwertdienste zu zahlen – etwa eine professionelle Aufschaltung auf eine Notrufleitstelle oder besondere Versicherungspakete. Hersteller wie RISCO haben dies erkannt und binden Errichter in ein Modell ein, bei dem Cloud-Services kostenpflichtig verkauft werden.

Offene Standards: Bleibt KNX relevant?

Die Frage nach offenen Standards wie KNX im Alarmbereich ist komplex. KNX ist in der Gebäudeautomation fest etabliert – für Licht, Heizung, Jalousien. Die klassische Alarmanlage war lange ein separiertes System ohne Schnittstellen dazu. Doch mit dem Siegeszug des Smart Home wuchsen die Anforderungen, Alarmtechnik zu integrieren. Einige Hersteller haben reagiert: Satel bietet ein KNX-Integrationsmodul an, Telenot und Abus ermöglichen zumindest eine potentialfreie Kopplung an externe Systeme (z.B. scharf/unscharf-Status an die Haussteuerung geben). Ganz offen ist der Alarmmarkt aber noch nicht. Ein Grund: Sicherheitsanforderungen kollidieren teils mit Offenheit – eine Alarmanlage muss manipulationssicher sein und soll nicht durch beliebige Bus-Kommandos deaktivierbar sein. Daher sind KNX-Anbindungen oft nur ein Weg: Die Alarmzentrale kann Befehle ins KNX-Netz senden (z.B. Licht ein bei Alarm), aber nicht umgekehrt sicher von KNX gesteuert werden, ohne den Schutzgrad zu gefährden. Trotzdem bleibt KNX relevant, vor allem im gehobenen Wohnbau. Viele Bauherren wünschen ein einheitliches Bedienen – und sei es nur, dass am zentralen Touchpanel auch der Alarmstatus sichtbar ist.
Ein weiterer aufkommender Standard im Smart-Home-Umfeld ist Matter (siehe Infobox Seite 49). Matter ist ein offener, IP-basierter Verbindungsstandard für Smart-Home- und IoT-Geräte, der lokale Kommunikation ermöglicht und Cloud-Abhängigkeiten reduziert und von der Connectivity Standards Alliance (CSA) getragen wird. Bisher spielt dieser in der professionellen Alarmbranche keine Rolle, könnte aber zukünftig für DIY-Systeme interessant werden, um Sensoren herstellerübergreifend kompatibel zu machen. Momentan kocht jedoch jeder Anbieter sein eigenes Süppchen, vor allem aus Sicherheitsgründen (proprietäre Funkprotokolle sind schwerer zu hacken als generische).

Zertifizierungen und Standards: Kaufkriterium oder Auslaufmodell?

In der DACH-Region waren VdS-Zertifizierungen und Normeinstufungen lange Zeit entscheidende Verkaufsargumente – gerade im B2B-Geschäft. Ein VdS-Siegel signalisiert geprüfte Zuverlässigkeit; für Versicherungen ist es oft Voraussetzung, um im Schadenfall zu zahlen. Anbieter wie Telenot, Abus oder Honeywell statten daher ihre Systeme mit den entsprechenden Zertifikaten (VdS Home, EN 50131 Grade 2/3 etc.) aus und nutzen dies aktiv im Marketing. Auch Satel und RISCO haben in vielen Ländern Zulassungen nach

INFOBOX - Standards

Matter – Der neue Verbindungsstandard für das Smart Home

Matter ist ein herstellerübergreifender Smart-Home-Standard, der entwickelt wurde, um Geräte unterschiedlicher Anbieter einfach, sicher und zuverlässig miteinander kompatibel zu machen. Ziel ist es, die bislang stark fragmentierte Smart-Home-Landschaft zu vereinheitlichen und die Integration neuer Geräte deutlich zu vereinfachen.

Im Kern ist Matter ein offener, IP-basierter Kommunikationsstandard für Smart-Home- und IoT-Geräte. Er ermöglicht eine direkte, lokale Kommunikation zwischen Geräten und reduziert die Abhängigkeit von Cloud-Diensten. Damit adressiert Matter zentrale Schwachstellen bisheriger Systeme: komplexe Inbetriebnahme, Herstellerbindung, Latenzzeiten und Datenschutzbedenken.

Getragen wird der Standard von der Connectivity Standards Alliance (CSA), einem internationalen Industriekonsortium. Zu den maßgeblichen Mitgliedern zählen unter anderem Apple, Google, Amazon, Samsung sowie zahlreiche Industrie- und Technologieunternehmen wie Bosch oder Siemens. Der politische und wirtschaftliche Anspruch ist klar: Ein gemeinsamer Standard soll proprietäre Insellösungen ablösen.

Technisch setzt Matter konsequent auf IP-Kommunikation. Als Übertragungsmedien kommen Ethernet, Wi-Fi und das energieeffiziente Funknetz Thread zum Einsatz. Diese Architektur macht Matter zukunftsfähig und kompatibel mit bestehenden Netzwerkinfrastrukturen.

Ein zentraler Vorteil: Ein Matter-fähiges Gerät kann parallel in mehreren Ökosystemen betrieben werden – etwa mit Apple Home, Google Home, Amazon Alexa oder Samsung SmartThings.

Ein weiteres Kernmerkmal ist die lokale Steuerung. Grundfunktionen laufen innerhalb des Heim- oder Gebäudenetzes, ohne permanente Cloud-Anbindung. Das reduziert Latenzen, erhöht die Ausfallsicherheit und stärkt den Datenschutz. Die Cloud wird primär für Fernzugriffe oder Software-Updates benötigt.

Sicherheit ist integraler Bestandteil des Standards. Matter nutzt Ende-zu-Ende-Verschlüsselung, Geräteauthentifizierung und ein sicheres Onboarding, etwa per QR-Code oder NFC.

Unterstützt werden aktuell unter anderem Leuchten, Steckdosen, Thermostate, Türschlösser, Jalousien sowie verschiedene Sensoren. Der Funktionsumfang wird schrittweise erweitert.

Für die Sicherheits- und Gebäudetechnik ist Matter vor allem als Integrationsstandard relevant. Er erleichtert die Anbindung von Smart Locks, Sensorik und Aktoren an übergeordnete Automationsplattformen und reduziert Herstellerabhängigkeiten. Gleichzeitig gilt: Matter ist kein Sicherheitsstandard im Sinne von EN 50131. Für professionelle Einbruch- oder Gefahrenmeldeanlagen ist Matter eine ergänzende Technologie – kein normativer Ersatz.

Kurz gesagt: Matter ist der Versuch, das „USB-C des Smart Homes" zu etablieren – ein gemeinsamer technischer Nenner, der Interoperabilität schafft, ohne bestehende Systeme vollständig zu ersetzen.

EN-Standards. Spannend ist der Umgang der Newcomer damit: Ajax Systems, anfangs als „hippes" Alarm-Startup belächelt, hat erkannt, dass man ohne Zertifizierung im professionellen Segment an Grenzen stößt. Das Unternehmen hat seine Produkte daher nachträglich prüfen lassen – mit Erfolg.

In Österreich etwa erhielt Ajax das VSÖ-Zertifikat, womit die Systeme nun offiziell von allen Versicherern anerkannt sind. Und europaweit konnte Ajax 2023/24 viele Kernkomponenten nach EN Grad 2 zertifizieren lassen. Mit dem Schritt zum EN Grad 3 (höchste Stufe für zivile Einbruchmeldesysteme) hat Ajax 2025 schließlich neue Maßstäbe gesetzt.

Die Beispiele zeigen: Zertifizierungen bleiben relevant, wandeln sich aber. Für technikbegeisterte Privatkunden mag ein VdS-Siegel weniger zählen als App-Features – hier entscheidet oft das Nutzererlebnis über den Kauf. Doch spätestens, wenn es um offizielle Stellen, gewerbliche Objekte oder Versicherungsrabatte geht, kommen Standards ins Spiel.
Ein interessanter Aspekt ist die Frage, ob neue Kriterien wie Cybersecurity-Zertifikate (z.B. vom BSI oder unabhängigen Instituten) in Zukunft klassische Prüfsiegel ergänzen. Lupus geht hier einen Weg, indem es von AV-Test seine Systeme auf IT-Sicherheit prüfen lässt, um Vertrauen in die Cloud- und App-Komponenten zu schaffen.

Auch Ajax und andere werben mit Penetrationstests und Bug-Bounty-Programmen, um die digitale Sicherheit zu gewährleisten. Denkbar ist, dass in einigen Jahren neben "VdS-geprüft" auch "BSI-geprüft" ein Qualitätsmerkmal für Alarmanlagen wird, gerade da diese immer mehr vernetzt sind.

Installation und Wartung: Von der Handwerkskunst zum Plug-and-Play

Traditionell waren Alarmanlagen eine Domäne des spezialisierten Handwerks: Jedes Kabel einzeln ziehen, Kontakte verdrahten, Widerstände berechnen, regelmäßige Vor-Ort-Wartung – das alles gehörte zum Tagesgeschäft eines Errichters. Die neuen Plug-&-Play-Systeme verändern dieses Bild

drastisch. Funkbasierte Komponenten lassen sich in Minuten anlernen, Klebestrips ersetzen oft das Bohren, und Konfiguration erfolgt per Software-Assistent statt DIP-Schaltern. Das spart enorm Zeit und Installationsaufwand.
Ein Zwei-Mann-Team kann heute ein Einfamilienhaus in wenigen Stunden mit einem kompletten Funksystem absichern, wo früher vielleicht zwei Arbeitstage veranschlagt wurden. Das wirkt sich auf die Kostenstruktur aus und erweitert den Kundenkreis – auch Mietwohnungen oder temporäre Installationen (Baustellenüberwachung, Event-Security) werden praktikabel, weil rückstandslos montier- und demontierbar.

Auch die Wartungsintervalle verändern sich. Früher musste ein Techniker jährlich zur Anlage, Batterien tauschen und alles durchmessen. Moderne Sensoren haben Batterie-Lebensdauern von 5+ Jahren und melden frühzeitig ihren Status. Über die Cloud kann der Errichter viele Prüfungen remote vornehmen (Signalstärken, Sabotagekontakte etc.).

Software-Updates kommen „over the air". Einige Systeme, wie etwa das neue Ajax-Grade-3-Funksystem, preisen explizit an, dass nun selbst Hochsicherheitsbereiche ohne die bisher aufwändigen Verkabelungsarbeiten geschützt werden können – was Installations- und Wartungskosten reduziert und Projekte beschleunigt.

Für Errichter bedeutet das einerseits Effizienzgewinne, andererseits aber auch die Notwendigkeit, ihr Geschäftsmodell anzupassen. Wenn der reine Montageaufwand sinkt, verlagert sich der Wertschöpfungsanteil mehr Richtung Beratung, Konzeption und Service.

Manche Fachfirmen setzen daher verstärkt auf Serviceverträge oder zusätzliche Dienstleistungen (z.B. Netzwerkbetreuung, Smart-Home-Integration), um Umsatz zu generieren. Durch Plug-and-Play drängen zudem branchenfremde Installateure (Elektrobetriebe, IT-Firmen) in den Sicherheitsmarkt, da die Einstiegshürden geringer sind. Der klassische Alarmerrichter muss sich also verstärkt durch Expertise und Zusatznutzen profilieren – beispielsweise Beratung zu objektspezifischen Risiken, Integration komplexer Gewerke oder 24/7-Bereitschaftsdienste.

Für Endanwender ist die Entwicklung eindeutig positiv: Alarmanlagen werden einfacher und zuverlässiger. Wo früher Fehlalarme durch Verkabelungsfehler oder falsch justierte Melder häufig waren, sorgen heute voreingestellte, selbstkalibrierende Sensoren für Ruhe. Die Bedienung per App und Sprachsteuerung reduziert Anwenderfehler (keine vergessenen PIN-Codes mehr). Und sollte doch mal etwas sein, kann per Fernzugriff oft schneller geholfen werden, als bis dato mit einem vor Ort Termin.

Fazit: Ausblick für Errichter, Systemhäuser und Endkunden

Die Alarmbranche in der DACH-Region steht an der Schwelle zu einer neuen Ära. Für Errichter bedeutet dies, Tradition und Innovation in Einklang zu bringen. Einerseits bleiben bewährte Werte – hohe Zuverlässigkeit, sabotagefeste Installationen, anerkannte Zertifikate – ein Fundament ihres Geschäfts.

Andererseits müssen sie die neuen Technologien (Cloud, Funk, Smart Home) aktiv annehmen, um nicht von agile Konkurrenz überrollt zu werden. Hersteller wie Ajax Systems zeigen, wie rasant sich der Markt drehen kann, wenn man kundenorientierte Lösungen bietet.

Errichter sollten die Chance nutzen, mit diesen neuen Lösungen ihr Portfolio zu erweitern, ohne jedoch die Qualität zu vernachlässigen. Die Weiterbildung in IT-Themen, Netzwerk und Datenschutz wird dabei ebenso wichtig wie die klassische VdS-Fachkenntnis.

Systemhäuser und Integratoren profitieren von der stärkeren Vernetzung der Gewerke. Alarmanlagen sind nicht länger isolierte Kästen, sondern Teil des IoT im Gebäude. Das erlaubt neue Geschäftsmodelle: vom Komplettpaket "Sicherheit & Smart Home" bis zum laufenden Monitoring-Service. Allerdings erfordert es auch, sich mit verschiedenen Ökosystemen auszukennen – sei es KNX, sei es die Cloud-APIs der Hersteller – um Systeme miteinander sprechen zu lassen. Hier könnten offene Standards in Zukunft Erleichterung bringen; bis dahin ist viel Integrationsarbeit individuell zu leisten.

Endanwender schließlich stehen vor einer größeren Auswahl denn je. Vom günstigen DIY-Set aus dem Baumarkt bis zur zertifizierten High-End-Alarmanlage vom Profi ist alles verfügbar. Wichtig wird sein, Aufklärungsarbeit zu leisten: Welche Lösung passt zu welchem Sicherheitsbedürfnis? Nicht jeder braucht Grade-3-Schutz mit Polizeiaufschaltung – aber grundlegende Zuverlässigkeit und Datenschutz sollte auch ein DIY-System erfüllen. Offen bleibt, wie sich die Preisgestaltung entwickelt.

Chinesische Anbieter werden weiter mit niedrigen Preisen locken, während europäische Hersteller versuchen, mit Qualität und Datenschutz zu punkten. Der Endkunde in der DACH-Region ist tendenziell qualitätsbewusst, aber auch preis- und komfortorientiert – ein Spannungsfeld, in dem die Anbieter ihre Strategien fein austarieren müssen.

Insgesamt lässt sich sagen: Elektronische Alarmsysteme haben Zukunft, doch sie werden anders aussehen als noch vor zehn Jahren. Mehr Funk, mehr Cloud, mehr Integration – aber auch neue Herausforderungen bei Sicherheit (Cyber!) und Standardisierung.

Die DACH-Region mit ihren hohen Ansprüchen könnte hier einmal mehr zum Taktgeber werden: Ein Markt, der Innovation annimmt, aber an kritischen Punkten (Datenschutz, Qualität, Zertifizierung) eigene Maßstäbe setzt.

Hersteller und Errichter tun gut daran, diese Besonderheiten zu berücksichtigen, um in der Zukunft des Alarmmarkts erfolgreich zu sein.

[**ML/DCM/AM**]



KI-Agenten sollen helfen, in der Notaufnahme Leben zu retten

- **Telekom, FH IAIS und Kliniken der Stadt Köln entwickeln KI-Agenten für Unterstützung im Schockraum**
- **Struktur nach medizinischen Prioritäten und Basis der Dokumentation**
- **Blaupause für hochsichere KI-Lösungen in den AI Foundation Services**

Im Notfall-Eingriffsraum in Kliniken, dem sogenannten Schockraum, kümmern sich bis zu zehn Ärzt*innen und Pflegekräfte um die schnelle und sichere Versorgung von Schwerstverletzten. Deutsche Telekom, das Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme IAIS und das Krankenhaus Merheim von den Kliniken der Stadt Köln entwickeln aktuell anhand von Schockraum-Simulationen eine KI-gestützte Live-Anzeige: Die KI dokumentiert und verfolgt die Gespräche des medizinischen Personals im Schockraum. Auf Basis dessen ordnet ein KI-Agent die genannten Informationen nach medizinischen Prioritäten ein. Diese Liste wird laufend aktualisiert und die Daten werden gleichzeitig für die Dokumentation der Behandlung gespeichert. So sollen die Fachkräfte im Schockraum entlastet, Fehler reduziert – und Leben gerettet werden.

Die KI-Anwendung kann im sogenannten Cloud-Edge-Kontinuum direkt im Krankenhaus auf eigenen Rechnern ohne Verbindung zum Internet oder über die Cloud betrieben werden.

Die Daten können so streng geschützt und nur im europäischen Raum nach europäischen Standards für Datensicherheit abgelegt werden. Das einjährige Projekt zur Entwicklung eines Prototyps anhand von Schockraum-Simu- lationen startete im September. Grundlage ist ein modularer Software-Baukasten für die KI-Lösungen.

Wie KI im Schockraum unterstützen und Dokumentationen erleichtern soll

Das medizinische Team im Schockraum steht unter immensem Druck: Während der Übergabe der Patient*innen vom Rettungsdienst an das Schockraum-Team, im Verlauf des Behandlungsprozesses im Schockraum und bei der Übergabe von Patient*innen an die Intensivstation oder den OP werden sämtliche medizinisch relevanten Informationen verbal kommuniziert. Informationen müssen blitzschnell erfasst, ausgetauscht und verarbeitet werden, während Diagnostik und Therapie parallel ablaufen. Die zu entwickelnde Lösung nutzt Künstliche Intelligenz, um die Gespräche automatisch mitzuschneiden, in Echtzeit auszuwerten, anzureichern und strukturiert grafisch aufzubereiten. Der sich aktuell in der Entwicklung befindliche KI-Agent soll dabei helfen.

Struktur für den Notfall: Das ABCDE-Schema rettet Leben

Die Behandlung folgt dem sogenannten ABCDE-Schema, Lebensbedrohliches wird zuerst behandelt: Atemwege (Airways), Beatmung (Breathing), Kreislauf (Circulation), neurologisches Defizit (Disability), erweiterte Informationen (Exposure). Sind die Atemwege frei, liegen starke innere oder äußere Blutungen vor, ist der Stoffwechsel entgleist? Aber auch: Nimmt der/die Verletzte Gerinnungshemmer und kann deshalb schneller verbluten? Ziel der KI ist folgendes: Die KI erkennt, welche Be-

funde, Maßnahmen und Entscheidungen genannt werden. Spricht der Arzt von einem „grobblasigen Rassel-Geräusch" bei der Atmung, ermittelt der KI-Agent die Kategorie und erstellt ein Live-Bild in Ampellogik nach dem ABCDE-Schema. Darüber hinaus überführt der KI-Agent die Daten automatisch in die Formulare für Dokumentation und Qualitätssicherung.

Modellfall für sichere und flexible Cloud-Edge-Infrastrukturen

Die Lösung entsteht derzeit im Rahmen des europäischen Förderprogramms IPCEI-CIS. Ziel ist eine standardisierte, übertragbare Infrastruktur im Cloud-Edge-Kontinuum. Das System verfügt über eine erhebliche Resilienz gegenüber Infrastruktur-Ausfällen, weil es sowohl lokal als auch offline über den Super-Minicomputer DGX Spark von NVIDIA ebenso wie über die AI Foundation Services in der Open Telekom Cloud (OTC) betrieben werden kann.

Die OTC ist wesentlicher Bestandteil des T Cloud Angebots der Deutschen Telekom und entspricht sämtlichen europäischen Datenschutzvorgaben. Schlüsselkomponen- ten des Systems wie der modulare Software-Baukasten für KI-Lösungen, das Edge-Agent-Framework, die schlanken KI-Modelle sowie automatisierte Workflows für Datenverarbeitung und Training können bei der Entwicklung anderer KI-Agenten-basierter Cloud-Edge-Infrastrukturen „wiederverwendet" werden.

Fortschritt durch eine starke Partnerschaft

„Mit der Entwicklung eines vielseitig einsetzbaren Multi-Agenten-Frameworks und seiner Anpassung an die Anforderungen in der Notfallmedizin schaffen wir die Grundlage für eine Entlastung des Personals bei der Versorgung Schwerstverletzter. Wichtige Bausteine dafür sind eine gut durchdachte Systemarchitektur, die Einbindung vertrauenswürdiger Komponenten für Sprachverarbeitung und Datenmanagement sowie die Edge-Fähigkeit für den Betrieb direkt vor Ort", sagt Stefan Rüping, Abteilungsleiter am Fraunhofer IAIS.

„Indem wir medizinisches Fachwissen und realistische Schockraum-Simulationen einbringen, verzahnen wir Forschung und Praxis und tragen dazu bei, dass KI-Agenten im Schockraum künftig einen spürbaren Fortschritt für die Notfallversorgung bringen könnten", ergänzt Jerome Defosse, Leitender Oberarzt der Klinik für Anästhesiologie und operative Intensivmedizin der Kliniken der Stadt Köln.

„KI hilft bereits heute, Leben zu retten. Unser KI-Agent für die Notfallmedizin hat auch für andere Branchen Vorbildcharakter. Mit dieser praxisnahen Lösung zeigen wir den Nutzen souveräner digitaler Infrastruktur für die Wirtschaft und das Gemeinwohl", sagt Ferri Abolhassan, CEO T-Systems und Vorstandsmitglied Deutsche Telekom AG.

Das Bundeswehrkrankenhaus Berlin und das Florence-Nightingale-Krankenhaus in Düsseldorf unterstützen das Projekt in einer beratenden Rolle. Ein vor Ort im Krankenhaus laufender Prototyp, der auch offline voll funktionsfähig ist, wird voraussichtlich im Sommer 2026 einsatzfähig sein.

Thorsten Tjardes, Direktor der Klinik für Unfallchirurgie und Orthopädie Septische und Rekonstruktive Chirurgie am Bundeswehrkrankenhaus Berlin: „Für uns hat die Resilienz der KI-Assistenz oberste Priorität – sie muss auch in der Cloud und lokal, also offline, absolut zuverlässig und sicher funktionieren, um die hohen Anforderungen der Notfallmedizin zu erfüllen."

Martin Pin, Chefarzt Klinik für Notfall- und Akutmedizin am Florence Nightingale Krankenhaus Düsseldorf, ergänzt: „Als beratender Partner bringen wir unsere Expertise ein, um die innovative KI-Technologie praxisgerecht zu gestalten und eine optimale Balance zwischen technischer Exzellenz und der Nutzbarkeit im klinischen Betrieb zu gewährleisten."

Profil des aktuellen Projekts

Das aktuelle Vorhaben baut auf dem vom Bundesministerium für Gesundheit geförderten Projekt „TraumAInterfaces" auf. Um die dort gewonnenen Erkenntnisse weiterzuentwickeln und dem Gesundheitswesen zur Verfügung zu stellen, wurde eine Anschlussförderung durch das europäische Förderprogramm IPCEI-CIS zur Verfügung gestellt.

Die AI Foundation Services sind eine zentrale Plattform für sichere KI-Anwendungen. Unternehmen finden dort eine große Auswahl an Open-Source- und kommerziellen KI-Modellen. Die Open-Source-Modelle werden von T-Systems nach höchsten Sicherheitsstandards in eigenen Rechenzentren betrieben.

Das IPCEI-CIS-Programm der EU zielt darauf ab, ein „Multi-Provider Cloud-Edge Kontinuum" zu schaffen: Eine vernetzte, souveräne digitale Infrastruktur für Europa von Europa. Edge-Cloud Computing platziert leistungsstarke Rechenkapazitäten am Netzwerkrand („at the Edge") mit minimaler Latenz.

Bereits heute arbeiten zwölf EU-Mitgliedstaaten und rund 150 Partner, darunter Branchenriesen wie SAP, Siemens, Bosch, Telefónica, Orange und Airbus an diesem offenen, europäischen Betriebssystem.

Jahresüberblick 2025: IT-Sicherheit, Rechenzentrumssicherheit und Künstliche Intelligenz

Das Jahr 2025 war von tiefgreifenden Entwicklungen in der digitalen Sicherheitslandschaft geprägt. In den Bereichen IT-Sicherheit, Rechenzentrumssicherheit sowie Künstliche Intelligenz zeigten sich deutliche Trends, die Unternehmen und Institutionen vor neue Chancen und Herausforderungen stellen. Nachfolgend werden für jeden Bereich die fünf wichtigsten Trends des Jahres 2025 vorgestellt – von der Abwehr hybrider Bedrohungen und dem Paradigmenwechsel in Datacenter-Strategien bis hin zu KI als Gamechanger der Arbeitswelt.

IT-Sicherheit 2025: Fünf zentrale Trends

Hybride Bedrohungen erfordern ganzheitliche 360-Grad-Sicherheitskonzepte – Cyberangriffe und physische Risiken verschmelzen zunehmend.



Ganzheitliche Sicherheitsstrategien gegen hybride Risiken

Angesichts immer komplexerer hybrider Bedrohungen – der Kombination aus Cyberangriffen und physischen Attacken – setzen Unternehmen verstärkt auf 360-Grad-Sicherheit. Studien zeigen, dass die Schäden durch Cyberkriminalität 2025 weltweit auf über 10 Billionen US-$ steigen könnten, begleitet von vermehrten Sabotageakten vor Ort.
Punktuelle Maßnahmen reichen nicht mehr aus – statt separater Lösungen sind integrierte Sicherheitskonzepte gefragt, die IT-Security, Objektschutz und Notfallmanagement vereinen. So verfolgt etwa das Sicherheitsunternehmen KÖTTER einen ganzheitlichen Ansatz, der von Risikobewertung über Security Operations Center (SOC) bis zu Werkschutz und Brandschutz alle Bereiche abdeckt. Diese Vernetzung aller Sicherheitsgewerke aus einer Hand erhöht die Resilienz deutlich und spiegelt einen branchenweiten Trend wider: 2025 war das Jahr der unternehmensweiten Sicherheitsplattformen und IT/OT-Konvergenz, um analoge und digitale Gefahren gleichermaßen abzuwehren.

Starke Authentifizierung statt Passwörter

Ein weiterer Schwerpunkt 2025 war die Abkehr vom klassischen Passwort hin zu phishing-resistenten Authentifizierungsverfahren. Zum Welt-Passwort-Tag im Mai prophezeiten Experten gar dessen Abschaffung: So argumentiert Sophos, dass herkömmliche Passwörter und selbst simple Zwei-Faktor-Codes nicht mehr genügen angesichts immer raffinierterer Phishing-Methoden.

Im Trend liegen FIDO2-konforme Login-Methoden wie Passkeys, die in Smartphones und Browsern bereits integriert sind und mittels Fingerabdruck oder Gesichtserkennung funktionieren. Für Hochsicherheitsumgebungen empfehlen Fachleute den Einsatz von Smartcards oder Hardware-Token mit PIN/biometrischer Entsperrung[6]. Die breite Verfügbarkeit solcher Technologien führte dazu, dass 2025 viele Unternehmen Pilotprojekte zum Passwordless Login starteten.

Gleichzeitig wurden klassische Passwort-Tipps (einzigartige, komplexe Kennwörter und Passwortmanager) weiter propagiert – doch der allgemeine Tenor lautet: Das Ende des Passwort-Zeitalters naht, und Multi-Faktor-Authentifizierung mit sicheren, benutzerfreundlichen Verfahren wird zum neuen Standard.

Proaktive Resilienz und kontinuierliche Tests

Cyber Resilience rückte 2025 stärker in den Fokus, mit Betonung auf präventive Prüfungen und Reaktionsfähigkeit im Ernstfall. Regulierung spielte hier eine Rolle: Der neue EU-Rechtsrahmen (z.B. DORA für Finanzinstitute) fordert zwar periodische Sicherheitstests – doch Experten halten die bisherigen Intervalle für unzureichend. So schreibt DORA alle drei Jahre einen Penetrationstest vor, was jedoch viel zu selten sei: Bei ~70 neu entdeckten Software-Schwachstellen täglich (über 25.000 pro Jahr) würde in drei Jahren ein kritischer Berg von 11.000 Sicherheitslücken entstehen[9]. Dennis Weyel von Horizon3.ai plädiert deshalb dafür, monatliche oder sogar wöchentliche Penetrationstests durchzuführen.
Viele Firmen setzten 2025 verstärkt auf automatisierte Angriffs-Simulationen und Red-Teaming-Übungen, um ihre Abwehr laufend auf die Probe zu stellen. Wichtig ist dabei die Priorisierung gefundener Lücken – veraltete Software, schwache Passwörter, überzogene Zugriffsrechte und Software-Lieferkettenrisiken erwiesen sich als häufigste Einfallstore
Neben der Prävention wuchs auch die Aufmerksamkeit für Incident Response: Unternehmen etablierten Notfallpläne und übten die Fähigkeit, erfolgreiche Angriffe rasch zu erkennen, einzudämmen und Geschäftsbetrieb wiederherzustellen. Dieser Trend zu „Immer bereit" spiegelt die Erkenntnis wider, dass 100%iger Schutz illusorisch ist – Cyber-Resilienz wird zur Kernkennzahl moderner IT-Sicherheit.

Hochentwickelte Bedrohungen und neue Angriffsmaschen

Die Bedrohungslandschaft entwickelte sich 2025 dynamischer denn je. Ransomware-Gruppen professionalisierten ihr Geschäftsmodell als „Crime-as-a-Service"- Ökosystem – von Ransomware-as-a-Service über Datenhehlerei bis zu Doppel- und Triple-Extortion (Erpressung mit Verschlüsselung und Veröffentlichungsdrohung). Laut Berichten stieg die Zahl der Cyberangriffe in Deutschland Anfang 2025 um 55 % gegenüber dem Vorjahr, Ransomware-Attacken sogar um 126 %.

Besonders im Visier waren Bildungseinrichtungen, Behörden und Telekommunikation. Staatlich gelenkte Akteure und Hacktivisten nutzten geopolitische Konflikte (etwa den Ukrainekrieg) für vermehrte Angriffe auf kritische Infrastruktur, was westliche Staaten in Alarmbereitschaft versetzte.
Zugleich beobachteten Sicherheitsexperten einen Boom an KI-gestützten Angriffen. Deepfake- und KI-Technologien mach- ten Phishing & Social Engineering erschreckend überzeugend: Mit automatisch generierten Boss-Deepfake-Anrufen oder täuschend echten Spam-Mails gelingt es Kriminellen immer häufiger, menschliche Mitarbeiter hinters Licht zu führen. KI-Algorithmen helfen außerdem, Schwachstellen schneller auszunutzen und Attacken zu automatisieren. Diese Entwicklung senkt die Einstiegshürde für Cybercrime drastisch – auch technisch wenig versierte Täter können fertige KI-Tools nutzen, um Angriffe zu skalieren.

Insgesamt wurde 2025 klar: Cyberangriffe werden raffinierter, schneller und zahlreicher, was defensive Strategien laufend anpassen muss. Die Security-Branche reagier- te mit intensiver Threat Intelligence (etwa Einblicke in den russischsprachigen Untergrund) und dem vermehrten Einsatz von KI zur Angriffserkennung – ein Wettrüsten, das sowohl Angreifer als auch Verteidiger mit neuen Technologien aufrüsten ließ.

Cybersecurity für alle – Fokus auf KMU und Nutzer

Wo früher vor allem Großunternehmen im Zentrum standen, richtet sich der Sicherheitsblick 2025 stärker auf kleine und mittlere Unternehmen (KMU) sowie die Allgemeinheit. Angreifer machen längst keinen Halt mehr vor dem Mittelstand – im Gegenteil, immer mehr KMU geraten ins Fadenkreuz professioneller Hacker. Entsprechend starteten Behörden Initiativen, um die Widerstandsfähigkeit breiter zu erhöhen. Ein Beispiel ist Baden-Württemberg: Dort wurde der „CyberSicherheits-Check" – ein kostenloses Beratungsangebot – von Industrie- und Handelskammern nun auch auf Handwerkskammern und Branchenverbände ausgerollt, um kleine Betriebe für Cyberrisiken zu sensibilisieren. Innerhalb eines einstündigen Checks analysieren geschulte Berater die IT eines Handwerksbetriebs, identifizieren Schwachstellen und geben konkrete Handlungsempfehlungen. Solche niedrigschwelligen Angebote sollen das Rückgrat der Wirtschaft (die KMU) vor existenzbedrohenden Angriffen schützen.

Parallel betonten Experten die Bedeutung der Sicherheitskultur und Awareness unter Mitarbeitenden. Social-Engineering-Angriffe wie CEO-Fraud, die vermehrt auf menschliche Fehler zielen, erfordern gut geschulte und wachsame Angestellte. Auch 2025 blieb der Fachkräftemangel ein Problem: Über drei Millionen Cyber-Experten fehlen weltweit, was Unternehmen vor Herausforderungen stellt. Viele mittelständische Firmen greifen daher auf Managed Security Services zurück.

Unterm Strich zeichnete sich 2025 der Trend ab, Cybersecurity breit in der Fläche zu verankern – von der Chefetage bis zum Azubi, vom DAX-Konzern bis zum Familienbetrieb. Nur mit alle Beteiligten umfassenden Strategien (inklusive externer Unterstützung, wo nötig) lässt sich die ständig wachsende Bedrohungslage effektiv meistern.

Rechenzentrumssicherheit

Fünf Megatrends im Data-Center-Bereich



Digitale Welt 2025

KI als Treiber von Kapazität und Energiebedarf

Die rasante Entwicklung künstlicher Intelligenz wirkt 2025 wie ein Turbo auf Rechenzentren – allerdings ein stromhungriger. Generative AI verändert die IT-Landschaft grundlegend und lässt den Energieverbrauch von Datacentern explosionsartig ansteigen. Prognosen der Internationalen Energieagentur weisen darauf hin, dass Rechenzentren bis 2030 weltweit 945 Terawattstunden Strom jährlich benötigen könnten – mehr als der heutige Jahresverbrauch Japans. Goldman Sachs erwartet bis 2030 einen +165 % höheren Strombedarf gegenüber 2023. Selbst in kurzer Frist sind die Auswirkungen spürbar: In den USA könnte der Anteil der Rechenzentren am nationalen Stromverbrauch von 3 % (2025) auf 10 % in 2028 steigen. Für Rechenzentrumsbetreiber und Managed Service Provider (MSP) bedeutet das zweierlei: Zum einen werden Hochleistungs-Hardware (GPUs für KI) und entsprechende Kühlkapazitäten zum kritischen Erfolgsfaktor; zum anderen steigen die Betriebskosten durch Energie rasant. 2025 erkannten viele Anbieter hierin eine Herausforderung und Chance: Durch neue Kühltechnologien (z.B. Flüssigkeitskühlung) und Standortwahl mit günstigerer Energie versuchten sie, die KI-Welle zu bewältigen. Der Megatrend ist klar – „AI-ready" Rechenzentren müssen sowohl enorme Rechenlasten stemmen können als auch energetisch effizient arbeiten, um im KI-Zeitalter wettbewerbsfähig zu bleiben.

Nachhaltigkeit und Regulierung als Imperativ

Green IT ist im Datacenter-Umfeld längst kein Nice-to-have mehr, sondern 2025 zur harten Compliance-Anforderung geworden. Stichworte wie ESG-Vorgaben, die EU-Taxonomie oder die Corporate Sustainability Reporting Directive (CSRD) zwingen Betreiber, CO-Reduktion und Ressourceneffizienz nachzuweisen. Kunden fragen aktiv nach nachhaltig betriebenen Infrastrukturen und bevorzugen Dienstleister, die Klimaziele einhalten. Dabei zeigt sich jedoch eine Ambivalenz: Einerseits sollen die Systeme umweltfreundlich sein, andererseits erwarten Kunden regelmäßige Erneuerung der IT-Hardware. Ein Lösungsansatz, der 2025 an Bedeutung gewann, ist die Kreislaufwirtschaft im Rechenzentrum: Die Wiederverwendung von Geräten kann bis zu 20-fach mehr CO einsparen als reines Recycling – und senkt zugleich Kosten. IDC-Studien bestätigen, dass ganzheitliches Asset Lifecycle Management sowohl Produktivität steigert (bei 42 % der Unternehmen) als auch Kundenzufriedenheit erhöht. Betreiber, die auf Refurbishing, längere Nutzungszyklen und Stromsparmaßnahmen setzen, schaffen also ökologische und ökonomische Win-Win-Effekte. Parallel verschärfen sich gesetzliche Vorgaben.
In Europa trat etwa die NIS2-Richtlinie in Kraft, und in Deutschland wurde ein KRITIS-Dachgesetz vorbereitet, das Mindeststandards für die Resilienz kritischer Infrastrukturen (inklusive Rechenzentren) definiert. Zertifizierungen nach DIN EN 50600 oder ISO/IEC 22237, die Sicherheit und Energieeffizienz bescheinigen, wurden 2025 zum Gütesiegel. Kurzum: Nachhaltigkeit avancierte vom PR-Schlagwort zum entscheidenden Wettbewerbsfaktor in der Datacenter-Branche.

Automatisierung für Ausfallsicherheit und Effizienz

Menschliches Versagen ist laut Studien weiterhin Ursache von rund 80 % aller gravierenden Rechenzentrums-Störungen. 2025 reagierte die Branche darauf mit einem starken Schub in Richtung Automatisierung und smarter Betriebsführung, um Fehler zu minimieren und die Resilienz zu erhöhen. Moderne Monitoring-Systeme, KI-unterstützte Betriebsassistenten und Augmented Reality (AR) wurden eingesetzt, um Wartungsprozesse zu verbessern. Beispielsweise ermöglichen AR-Brillen dem Techniker vor Ort, schrittweise Anleitungen oder Echtzeit-Überwachung einzublenden, was Fehlerquoten senkt. Gartner identifizierte modulare Micro-Datacenter als zukunftsweisend: Kleine, vorgefertigte Einheiten, die weitgehend automatisiert betrieben werden können, verringern die Komplexität und erhöhen die Verfügbarkeit. Der Grundsatz lautet: „Wer nur reagiert, wird überrollt" – daher müssen MSPs und Betreiber proaktiv in die richtige Technologie von Anfang an investieren, um Betriebsausfälle zu vermeiden. Best Practices umfassen etwa predictive maintenance (KI-Modelle sagen voraus, wann ein Bauteil ausfallen könnte), Digital Twins des Rechenzentrums zur Simulation von Änderungen und Robotik für Routineaufgaben. Dass sich diese Investitionen lohnen, zeigt eine Kennzahl des Uptime Institute: 66–80 % aller Downtimes könnten durch integriertes Asset-Management und Automatisierung vermieden werden. 2025 markierte somit den Übergang vom traditionell manuellen Rechenzentrumsbetrieb hin zum „Self-driving Datacenter", in dem Software und KI viele Aufgaben übernehmen, die früher fehleranfällig in Menschenhand lagen.

Edge Computing und verteilte Infrastruktur

Mit der fortschreitenden Digitalisierung wurde 2025 die Dezentralisierung der Rechenzentren immer greifbarer. IoT-Geräte, 5G-Netze und latenzkritische Anwendungen treiben Edge Computing voran: Statt einem riesigen zentralen Rechenzentrum entstehen zahlreiche kleine Edge-Standorte – sogenannte Micro-DCs oder Points of Presence – nahe bei Endgeräten und Nutzern. Gartner prognostiziert bis 2030 eine drastische Zunahme solcher Edge-Deployments, da Unmengen von IoT-Daten lokal verarbeitet werden müssen. Dieser Trend bringt neue Sicherheits- und Managementanforderungen: Die Asset-Anzahl vervielfacht sich, die Komplexität steigt enorm. Für Dienstleister und Betreiber heißt das, sie brauchen einen zentralen, automatisierten Überblick über alle verteilten Standorte, sonst drohen blinde Flecken und Inkonsistenzen in der Konfiguration.

2025 investierten viele in zentralisierte Management-Plattformen und Monito-

ring, um hunderte Mini-Rechenzentren aus der Ferne steuern zu können. Standardisierung und Infrastruktur-as-Code-Ansätze halfen, an allen Knoten einheitliche Sicherheitspolitiken durchzusetzen.

Zudem gewann die Frage der Physische Sicherheit an verteilten Orten an Bedeutung (Zugangsschutz für Edge-Schaltschrank etc.). Der Edge-Trend geht Hand in Hand mit Cloud: Unternehmen überdenken ihre Cloud-Strategien – Resilienz schlägt Exklusivität, d.h. anstatt alles in eine Cloud zu stecken, setzen viele auf verteilte, multi-lokale Lösungen. In der Praxis bedeutet das: Hybrid- und Multi-Cloud Architekturen kombiniert mit regionalen Edge-Rechenzentren. Der Vorteil ist eine bessere Ausfallsicherheit und geringere Latenzen; der Nachteil sind mehr verteilte Angriffsflächen, was 2025 zu verstärkter Netzwerksegmentierung und Zero-Trust-Architekturen in weit verteilten Umgebungen führte.

Cybersecurity und digitale Souveränität im Datacenter

Rechenzentrumssicherheit umfasst 2025 nicht nur die physische Zutrittskontrolle oder Brandschutz – Cybersecurity ist genauso entscheidend, insbesondere da Rechenzentren oft kritische Daten und Workloads Dritter hosten. Ein Megatrend war hier das Thema Daten-Souveränität. Geopolitische Spannungen und strenge Datenschutzgesetze führten zu einer „Repatriierung" von Daten: Unternehmen holen sensible Daten aus globalen Hyperscale-Clouds zurück in regionale oder lokale Rechenzentren. Gartner prägte dafür den Begriff „Geopatriation" – aus Sorge vor ausländischem Zugriff und zwecks Einhaltung europäischer Standards akzeptieren Firmen im Zweifel sogar etwas weniger Performance, solange die Daten in vertrauenswürdigen Hoheitsgebieten liegen. Dieser Trend beflügelt europäische Anbieter und sogenannte Sovereign Cloud-Konzepte. Gleichzeitig stehen MSPs und Datacenter-Betreiber in der Pflicht, höchste Compliance- und Security-Standards zu garantieren, um dieses Vertrauen zu rechtfertigen. 2025 wurden daher vermehrt auditable Asset-Management-Systeme, Verschlüsselungslösungen und Zero-Trust-Netzwerke in Rechenzentren implementiert, um Datenschutz und Abwehr von Cyberangriffen sicherzustellen.

Auch digitale Souveränität als Strategie gewann an Gewicht: In Europa diskutierte man „Buy European" – also bevorzugt europäische Technologie und Cloud-Dienste einzusetzen – nicht nur aus Industriepolitik, sondern als Sicherheitsstrategie. Letztlich fließen die Megatrends Security & Souveränität zusammen: Ein „Next-Gen Data Center" muss KI, Nachhaltigkeit, Automatisierung, Edge und Security vereinen. Wer als Anbieter diese Klaviatur beherrscht, kann sich 2025 und darüber hinaus als zuverlässiger, vertrauenswürdiger Partner positionieren.

Künstliche Intelligenz

Fünf Trends zwischen Chance und Risiko

KI als zweischneidiges Schwert in der Cybersicherheit

Die allgegenwärtige künstliche Intelligenz ist 2025 Gamechanger und Beschleuniger für Cybersecurity – im positiven wie negativen Sinne. Auf der einen Seite ermöglichen KI-Systeme den Verteidigern enorme Fortschritte: Bedrohungserkennung in Echtzeit, Anomalie-Detection im Netzwerkverkehr und intelligente Security-Orchestrierung helfen, Angriffe schneller zu identifizieren und zu blockieren Security-Teams werden durch KI-Tools entlastet, Routineanalysen laufen automatisiert, Alarmfluten werden durch machine learning priorisiert. So bestätigen 80 % der befragten deutschen IT-Führungskräfte, dass KI die Ergebnisse im Remote-Betrieb – etwa in Security Operations – bereits messbar verbessert. Aber: Dieselbe Technologie nutzen auch die Angreifer. 2025 häuften sich Berichte über KI-generierte Malware, automatisierte Phishing-Kampagnen und schwer erkennbare Deepfake-Betrugsmaschen. Hacker setzen KI für Social Engineering ein (z.B. täuschend echte gefälschte Stimmen von Vorgesetzten, um Mitarbeiter zur Überweisung zu bewegen) und um Schadcode zu verschleiern.

Dadurch entstand ein Katz-und-Maus-Duell: KI gegen KI. So nutzten etwa Ransomware-Gruppen wie RansomHouse oder Scattered Spider automatisierte Angriffs-Tools, während Unternehmen im Gegenzug KI-basierte Abwehr einführen. Die Zahlen untermauern die Dramatik: Fast 47 % der Organisationen weltweit waren laut WEF bereits von KI-ermöglichten Cyberattacken betroffen, doch nur 37 % haben besondere Sicherheitsprüfungen für KI-Tools etabliert.

Die Lehre 2025 lautet folglich: KI ersetzt nicht den Menschen in der Sicherheit, sondern macht ihn unverzichtbarer. Da KI sowohl Schutz als auch Angriff verstärkt, kommt es mehr denn je auf menschliche Urteilskraft, Kreativität und schnelle Reaktion an, um ungewöhnliche Muster zu erkennen und übergreifende Strategien anzupassen.

Dieses „Duell" wird uns auch über 2025 hinaus begleiten und verlangt, dass Unternehmen KI als Werkzeug einsetzen, aber immer mit menschlicher Aufsicht und ethischen Leitplanken.

KI-gestützte Geschäftsmodelle und neue Produktivität

Abseits der Security rückte 2025 die wertschöpfende Nutzung von KI im Unternehmen in den Vordergrund. Viele Firmen experimentierten nicht mehr nur, sondern implementierten KI konkret, um Geschäftsprozesse zu optimieren und neue Services zu entwickeln.

Ein Trendthema war KI im Kundenservice

Hier sorgen Chatbots und Conversational AI in Self-Service-Portalen für schnellere Antworten – moderne Service-Architekturen binden KI-Module ein, um Anfragen vorzuselektieren und zu beantworten. Unternehmen berichteten von verbesserter Effizienz und Qualität im Kundenservice durch KI-gestützte Self-Service-Kanäle, die 24/7 ansprechbar sind (wichtig etwa bei Online-Banken oder E-Commerce).

Ebenso hält KI Einzug in den Field Service

Agentenbasierte KI-Lösungen helfen Außendienst-Teams, indem sie Termine und Routen optimieren oder Wissen zu Maschinen via App bereitstellen. So prognostiziert IFS, dass KI-Agenten den technischen Kundendienst revolutionieren, indem Routineaufgaben und Datenauswertungen automatisch erfolgen – Monteure können sich auf komplexe Probleme fokussieren.

Neue Geschäftsmodelle entstanden teils erst durch KI

Auf einem AI-Partnertag demonstrierten etwa Mittelständler, wie sie mit Predictive Analytics oder intelligenten IoT-Geräten ganz neue Services anbieten und Umsatzquellen erschließen. In Bayern entstand ein Projekt „AI Alcatraz", das KI-basierte Gesichtserkennung nutzt, um Universitätsgelände sicherer zu machen. Marketing und Vertrieb setzten ebenfalls auf KI – beispielsweise wurde ein KI-Marketing-Tool vorgestellt, das personalisierte Kampagnen automatisiert (CyberLink zusammen mit AMD).

Insgesamt lässt sich feststellen: 2025 schafften es Unternehmen zunehmend, KI von der Vision in die Praxis zu überführen. Gerade dort, wo KI direkt den Geschäftszweck unterstützt (etwa Predictive Maintenance in der Produktion oder Absatzprognosen im Handel), wurde sie zu einem echten Werttreiber. Dieser Trend wird sich fortsetzen, denn KI wird immer mehr zum Enabler für Produktivität und Innovation in praktisch allen Branchen.

KI-Adoption: Von der Pilotfalle zur skalierenden Anwendung

Trotz aller erfolgreichen Beispiele offenbarte 2025 auch die Hürden bei der KI-Einführung, vor allem im Mittelstand. Viele KI-Pilotprojekte scheitern leider oder verpuffen ohne nachhaltigen Nutzen. Eine vielzitierte MIT-Studie stellte fest, dass 95 % aller generativen KI-Piloten in Unternehmen ins Leere laufen – sprich, keine echten Mehrwerte liefern. Gründe dafür sind selten die KI-Technologie an sich, sondern oft mangelhafte Datenqualität, fehlende technische Integrationen oder organisatorische Hindernisse. Gerade in industriellen Umgebungen treffen moderne KI-Anforderungen auf veraltete Legacy-Systeme. Ältere ERP- oder Produktionssysteme bieten nicht die nötigen Schnittstellen, Daten sind in Silos gefangen, und es fehlen interne KI-Kompetenzen. 79 % der deutschen Unternehmen leiden laut Umfragen an eklatanten KI-Kompetenzdefiziten, obwohl 86 % der Führungskräfte großes ungenutztes Potenzial sehen. Um aus dieser „Pilotfalle" herauszukommen, setzt sich ein Trend zu „Industrial AI Apps" durch. Das sind vorgefertigte KI-Lösungen für konkrete Anwendungsfälle (etwa in Produktion, Logistik oder Personalplanung), die sich leicht in bestehende Prozesse einbetten lassen.

Statt von Grund auf eigene KI zu entwickeln – was Zeit und Know-how erfordert – greifen Mittelständler vermehrt zu Plug-and-Play-KI von spezialisierten Anbietern. Laut Experten funktionieren solche Ready-to-use-Lösungen deutlich besser als aufwendige Eigenprojekte. Die Erfolgsbeispiele in 2025 untermauern das: Unternehmen, die etwa KI-basierte Bestandsplanung oder Wissenssuche als fertige Module integrierten, konnten sofort messbare Verbesserungen erzielen. Zudem erkannten viele, dass KI-Projekte Chefsache sein müssen – und zwar interdisziplinär: Nicht die IT-Abteilung allein, sondern die Fachbereiche sollten KI-Initiativen treiben, damit Lösungen wirklich die Pain Points adressieren.

Raus aus der Experimentierphase

Die Zukunft von KI in Unternehmen liegt also darin, aus der Experimentierphase herauszukommen und skalierende Anwendungen zu etablieren. 2025 war hier ein Wendepunkt: Erfolgsfaktoren wie Integration vor Innovation, Anpassung der Sicherheitsarchitektur und intensives Change-Management wurden identifiziert, um KI vom Hype zum echten Produktivitätsbooster zu machen.

KI prägt Arbeitswelt und öffentliche Sicherheit

Jenseits der direkten Geschäftsprozesse veränderte KI 2025 auch die Art, wie wir arbeiten und für Sicherheit sorgen. Eine aufschlussreiche GoTo-Studie in Deutschland ergab, dass über die Hälfte der Arbeitnehmer (51 %) glaubt, KI mache physische Büros zukünftig überflüssig. KI-Tools ermöglichen in der Tat ein Arbeiten von überall, ohne Produktivitätseinbußen – 59 % der Mitarbeiter sagen, dank KI können sie ortsunabhängig genauso effizient arbeiten.

Die Work-Life-Balance verbessert sich laut 64 % der Befragten durch KI (etwa durch Wegfall von Pendelzeiten und smarte Arbeitsplanung). KI wird damit zum Enabler für flexible Arbeitsmodelle: Sie überwindet Distanzen via Übersetzungs- oder Collaboration-Tools, übernimmt Routineaufgaben im Hintergrund und personalisiert digitale Arbeitsumgebungen. Interessant ist, dass 80 % der IT-Leiter meinen, ihr Unternehmen nutze KI bereits effektiv für verteilte Teams – aber nur 49 % der Mitarbeiter stimmen dem zu.

Hier klafft noch eine Wahrnehmungslücke,



die zeigt: Unternehmen müssen Usability und Einbindung der KI-Lösungen verbessern, damit der Nutzen wirklich bei allen ankommt. Ein weiterer Bereich, wo KI 2025 richtungsweisend war, ist die öffentliche Sicherheit. KI-gestützte Videoanalyse wurde in ersten Polizeiprojekten eingesetzt, um z.B. in Überwachungsbildern vermisste Personen oder Täter schneller zu finden. Hessen etwa hat als erstes Bundesland KI offiziell für die Polizeiarbeit zugelassen und startete im Juli 2025 einen Pilot im Frankfurter Bahnhofsviertel: KI-Systeme werten riesige Videodaten in Echtzeit aus und haben bereits geholfen, vermisste Kinder aufzuspüren. Solche Anwendungen zeigen den Mehrwert moderner Technologie, stoßen aber auch Debatten an über Datenschutz und algorithmische Verantwortung. Insgesamt wird KI als Partner der öffentlichen Sicherheit gesehen, um etwa Terrorgefahren früher zu erkennen, aber immer mit der Maßgabe „der Mensch entscheidet am Ende".

Die Arbeitswelt wiederum erlebt KI weniger als Bedrohung von Jobs, sondern als Transformation. KI treibt den Trend zu Remote Work weiter, macht Assistenzfunktionen allgegenwärtig (von KI-Meetingprotokollen bis zu automatisierter Terminplanung) und verändert, welche Skills gefragt sind. Mitarbeiter fordern mittlerweile, dass Unternehmen mindestens so in KI investieren wie in Tischkicker und Kaffeemaschinen – über 55 % sagen, KI-Investitionen seien genauso wichtig wie klassische Büro-Benefits. 2025 setzten Unternehmen daher stärker auf KI-Weiterbildung ihrer Belegschaft und neue Arbeitskonzepte. Der Konsens: KI wird das Herzstück des neuen, flexiblen Arbeitsmodells – und wer hier frühzeitig die richtigen Weichen stellt, gewinnt im Kampf um Talente und Effizienz.

Regulierung, Transparenz und menschliches Urteilsvermögen

Mit der wachsenden Durchdringung von KI ging 2025 auch die Frage einher: Wer zähmt die KI? Während die EU am umfassenden AI Act arbeitete (voraussichtlich

voll wirksam ab 2027), entstand ein Spannungsfeld zwischen Innovationsfreiheit und Regulierung. Einerseits möchte Europa hohe Sicherheits- und Ethikstandards setzen, andererseits warnen Stimmen, eine Überregulierung könne uns ins Hintertreffen bringen. Tatsache ist: Bis verbindliche Regeln greifen, wird sich eine neue Generation KI-gestützter Cyberangriffe entwickelt haben, die heutige Gesetze überfordert.

2025 plädierten Experten deshalb für verantwortungsbewusste Selbstregulierung: Unternehmen sollten nicht auf Gesetze warten, sondern jetzt schon KI-Einsatzrichtlinien, Bias-Prüfungen und Security-Checks für KI einführen. Ebenfalls zentral ist die Transparenz von KI-Modellen. „Vertrauen ist gut, Verständnis ist besser" lautete die Devise – Firmen, die KI nutzen, müssen deren Entscheidungen erklärbar machen, um Akzeptanz bei Kunden und Mitarbeitern zu gewinnen. Kaspersky und andere riefen zu mehr Einblick in KI-Systeme auf, damit Anwender nachvollziehen können, wie z.B. ein KI-Kundendienst zu seiner Antwort kommt.

Menschliche Expertise bleibt unentbehrlich

2025 wurde klar, dass KI-Systeme zwar schnell und datengetrieben arbeiten, aber Kontext und Moral nicht „fühlen" können. So braucht es weiterhin Menschen im Loop, die Ergebnisse validieren, Fehlalarme einschätzen und ethische Grenzen setzen. Der Fachkräftemangel in KI-nahen Berufen (von Data Scientists bis Ethik-Experten) machte dabei Sorge – doch gleichzeitig entstehen neue Rollen, etwa „Prompt Engineers" für die optimale Steuerung von KI oder KI-Trainer, die Systeme auf Bias prüfen. Governance-Boards für KI wurden in großen Organisationen eingerichtet, um Fragen der Verantwortung und Compliance zu klären.

In der öffentlichen Diskussion drehte sich 2025 vieles um KI-gefertigte Fake-Inhalte, Deepfakes und Desinformation. Hier arbeitet die Industrie an technischen Gegenmitteln (Wasserzeichen für KI-Medien, Deepfake-Erkennung), aber auch an Aufklärung der Nutzer.

Fazit: 2025 war für KI ein Jahr der Reifung

Die Technologie hat unbestreitbar Nutzen gebracht – von effizienteren Geschäftsabläufen bis zu neuen Möglichkeiten in Sicherheit und Medizin. Doch zugleich wurden ihre Gefahren deutlicher sichtbar. Vertrauenswürdige KI erfordert klare Regeln und mündige Anwender. Unternehmen, die dies beherzigten, konnten KI 2025 erfolgreich als Renditefaktor einsetzen (Stichwort ROI von AI in IT-Security). Andere wiederum wurden durch KI-Lücken kalt erwischt. Der Schlüssel für die Zukunft liegt darin, KI bewusst, transparent und mit menschlichem Augenmaß einzusetzen – dann wird sie zum Motor von Innovation, nicht zum unkontrollierten Risiko.

Schlussbemerkung

Das Jahr 2025 hat deutlich gemacht, wie eng IT-Security, Rechenzentrumsinfrastruktur und KI-Entwicklung miteinander verzahnt sind. Sicherheitsstrategien müssen ganzheitlich gedacht werden, da Bedrohungen sowohl virtuell als auch physisch auftreten. Data Center als Rückgrat der Digitalisierung stehen vor dem Wandel hin zu mehr Nachhaltigkeit, Automatisierung und Verteilung. Und die Künstliche Intelligenz erweist sich als geopolitischer Gamechanger und zugleich als Alltagshelfer – sie bringt Lösungen für alte Probleme, schafft aber auch neue Herausforderungen. Für Unternehmen und Gesellschaft gilt es nun, diese Trends mitzunehmen: Resilienz aufbauen, Chancen nutzen und Risiken verantwortlich managen, um auch 2026 in einer sicheren, innovativen digitalen Welt agieren zu können.

Einordnung & Überblick: Sicherheitslandschaft 2025 im Fokus

Die folgende Übersicht bündelt die zentralen Unternehmen, die Euro Security im Jahr 2025 im Kontext von Cybersecurity, Künstlicher Intelligenz und Rechenzentrumssicherheit begleitet und analysiert hat. Sie bildet damit das inhaltliche Rückgrat eines Jahres, das wie kaum ein anderes von digitaler Verwundbarkeit, regulatorischem Druck, technologischer Beschleunigung und wachsender Resilienzanforderung geprägt war. Auffällig ist: Sicherheit wird 2025 nicht mehr in Silos gedacht. Cyber-, KI- und physische Sicherheitsarchitekturen wachsen zusammen – organisatorisch, technisch und strategisch. Genau an dieser Schnittstelle positionieren sich viele der hier aufgeführten Unternehmen: als Plattformanbieter, Integratoren oder strategische Enabler für ganzheitliche Sicherheitsmodelle.

Top-10-Relevanz über alle Themenfelder hinweg

Aus der redaktionellen Bewertung von Euro Security kristallisieren sich über alle Cluster hinweg Top-10-Akteure heraus, die den Markt 2025 besonders stark geprägt haben – sei es durch technologische Innovation, Marktdurchdringung, regulatorische Relevanz oder strategische Weichenstellungen. Diese Unternehmen tauchen häufig clusterübergreifend auf (z. B. Cloud-, KI- und KRITIS-Bezug) und stehen exemplarisch für den Trend zur integrierten Sicherheitsökonomie.

Cloud, Compliance & Resilience Stack – vertiefende Einordnung

Viele der genannten Unternehmen sind Teil dessen, was Euro Security redaktionell als Cloud/Resilience Stack beschreibt: ein Zusammenspiel aus • Cloud-Infrastrukturen; • Compliance- und Regulierungsfähigkeit (NIS2, KRITIS-DG, CRA); • Daten- und Identitätssicherheit; • physischer Schutz- und Zutrittstechni; • KI-gestützter Analyse und Entscheidungsunterstützung

Weiterführende Analysen dazu – inklusive Marktstrategien, Architekturmodelle und Praxisbeispiele – finden sich in den Hintergrundbeiträgen des Euro-Security-Teams „Cloud & Resilience", die insbesondere online vertieft wurden.

Mehr als Print

Exklusive Online-Inhalte: Ein erheblicher Teil der Berichterstattung zu diesen Unternehmen erschien ausschließlich digital auf www.euro-security.de.

Cybersecurity
8com GmbH & Co. KG [www.8com.de]
CyberLink [www.cyberlink.com]
Cycode [www.cycode.com]
Datadog [www.datadoghq.com]
G DATA CyberDefense AG [www.gdata.de]
GIGAMON [www.gigamon.com]
Goaco GmbH [www.goaco.com]
Google Cloud [cloud.google.com]
HID Global [www.hidglobal.com]
Horizon3.ai [www.horizon3.ai]
Kaspersky [www.kaspersky.com]
KÖTTER Services [www.koetter.de]
Matrix42 [www.matrix42.com]
NTT DATA [www.nttdata.com]
secunet Security Networks [www.secunet.com]
SentinelOne [www.sentinelone.com]
Sophos [www.sophos.com]
TeleTrusT [www.teletrust.de]
Thales [www.thalesgroup.com]
Vodafone Deutschland [www.vodafone.de]

Künstliche Intelligenz
AMD [www.amd.com]
Axis Communications [www.axis.com]
CyberLink [www.cyberlink.com]
Datadog [www.datadoghq.com]
Dallmeier electronic [www.dallmeier.com]
FLIR / Teledyne FLIR [www.flir.com]
Genetec [www.genetec.com]
Google Cloud [cloud.google.com]
Hanwha Vision [www.hanwhavision.com]
Hexagon [hexagon.com]
IFS [www.ifs.com]
KIOXIA [www.kioxia.com]
Kaspersky [www.kaspersky.com]
Kentix [www.kentix.com]
Memoori [www.memoori.com]
Milestone Systems [www.milestonesys.com]
OpenAI [www.openai.com]
SentinelOne [www.sentinelone.com]
Thales [www.thalesgroup.com]
SYPAQ Systems [www.sypaq.com]

Rechenzentrumssicherheit
ASSA ABLOY [www.assaabloy.com]
Datadog [www.datadoghq.com]
DEHN SE [www.dehn.de]
Genetec [www.genetec.com]
GIGAMON [www.gigamon.com]
Google Cloud [cloud.google.com]
HID Global [www.hidglobal.com]
Kentix [www.kentix.com]
NTT DATA [www.nttdata.com]
Rittal [www.rittal.com]
Senstar [www.senstar.com]
Thales [www.thalesgroup.com]
TÜV SÜD [www.tuvsud.com



Sicherheitslage 2025

Zehn kritische Trends im Spiegel der Euro-Security-Kommentare im Jahr 2025

2025 war kein Jahr der punktuellen Krisen, sondern ein Jahr struktureller Verschiebungen

Sicherheit wurde politischer, technischer – und gleichzeitig fragiler. Die Kommentare der Euro-Security-Redaktion zeigen über das Jahr hinweg ein klares Muster: Viele Entwicklungen, die einzeln sinnvoll erscheinen, entfalten im Zusammenspiel neue Risiken. Regulierung, Digitalisierung, gesellschaftliche Spannungen und Marktmechanismen greifen ineinander – nicht immer zum Vorteil der realen Sicherheitslage.

Regulierung ohne Präzision: Wenn KRITIS zum Unsicherheitsfaktor wird

Mit dem KRITIS-Dachgesetz erreicht die Regulierung der physischen Sicherheit in Deutschland erstmals eine neue Verbindlichkeit.
Was über Jahre als Empfehlung, Branchenstandard oder freiwillige Selbstverpflichtung galt, wird nun gesetzlich eingefordert: Perimeterschutz, Zutrittskontrolle, Videotechnik sowie organisatorische Sicherheitsmaßnahmen werden für Betreiber kritischer Infrastrukturen verpflichtend. Politisch markiert dies einen Paradigmenwechsel – Sicherheit wird nicht länger nur als betriebliche Verantwortung verstanden, sondern als staatlich legitimiertes Schutzgut.

Doch genau an dieser Stelle offenbart sich ein strukturelles Defizit der Regulierung. Die neue Verbindlichkeit geht nicht mit operativer Präzision einher. Während Gesetzgeber und Aufsichtsbehörden die Verantwortung für Selbsteinstufung, Risikobewertung und Maßnahmenauswahl weitgehend auf die Betreiber übertragen, fehlen belastbare Mindeststandards, klare Referenzarchitekturen oder abgestufte Schutzklassen. Für Unternehmen entsteht damit ein regulatorischer Schwebezustand, in dem Investitionsentscheidungen unter erheblicher Rechts- und Planungunsicherheit getroffen werden müssen.

Ökonomisch führt dies zu einer paradoxen Dynamik. Aus Angst vor Sanktionen oder Reputationsschäden investieren manche Betreiber überdimensioniert und ineffizient, andere setzen bewusst auf Minimalerfüllung in der Hoffnung, formalen Anforderungen zu genügen. Sicherheit wird zur Interpretationsfrage – nicht zum messbaren Ziel. Statt eines vergleichbaren Resilienzniveaus entsteht ein Flickenteppich aus Über-, Unter- und Fehlabsicherung. Regulierung erhöht damit nicht automatisch Sicherheit, sondern verlagert Risiken in die Management- und Planungsebene.

Bürokratie statt Resilienz: Wenn Dokumentation die Umsetzung verdrängt

Parallel zur wachsenden Regulierungsdichte zeigt sich 2025 eine zunehmende Verschiebung von operativer Sicherheitsarbeit hin zur formalen Nachweisführung. Betreiber kritischer Infrastrukturen berichten, dass erhebliche personelle und finanzielle Ressourcen in Risikoanalysen, Berichte, Dokumentationen und Audits fließen – Ressourcen, die für praktische Schutzmaßnahmen fehlen.

Der strukturelle Zielkonflikt ist offensichtlich: Sicherheit wird zunehmend prüfbar, aber nicht zwingend wirksam. Wo Dokumentationslogiken dominieren, geraten reale Schwachstellen aus dem Fokus – etwa ungesicherte Nebenbereiche, fehlende Redundanzen oder unzureichend qualifiziertes Personal.
Besonders kleinere Betreiber stehen unter Druck, formale Compliance herzustellen, ohne die organisatorische und technische Resilienz tatsächlich zu erhöhen. Bürokratie wird damit selbst zum Sicherheitsrisiko, weil sie Reaktionsfähigkeit bindet, operative Flexibilität einschränkt und Innovationsprozesse lähmt.

IT/OT-Konvergenz: Mehr Vernetzung, mehr Verwundbarkeit

2025 ist endgültig das Jahr, in dem physische Sicherheit ohne IT-Sicherheit nicht mehr denkbar ist. Zutrittssysteme, Videoanalyse, Leitstellen, Sensorik und Perimeterschutz sind vernetzt, cloudfähig und datengetrieben. Politisch wird diese Konvergenz vorausgesetzt – technisch und organisatorisch ist sie vielerorts noch nicht vollzogen.

Gerade im Bereich der Operational Technology zeigen sich erhebliche Defizite. Energieanlagen, Verkehrssysteme und industrielle Infrastrukturen arbeiten häufig mit veralteten Protokollen, unzureichender Segmentierung und geringer Transparenz. Betreiber wissen oft nicht, welche Systeme aktiv sind, welche Datenflüsse bestehen oder wo potenzielle Angriffspunkte liegen.

Der Trend ist besonders kritisch, da neue Regulierungen wie NIS2 oder das KRITIS-Dachgesetz IT-Sicherheitsniveaus voraussetzen, die operativ noch nicht flächendeckend erreicht sind. Ohne echte IT/OT-Integration bleibt Sicherheit fragmentiert – und damit strukturell verwundbar.

KI im Sicherheitsbetrieb: Effizienzgewinn mit wachsender Governance-Schuld

Künstliche Intelligenz ist 2025 kein Experiment mehr, sondern fester Bestandteil des Sicherheitsbetriebs. Videoanalyse, Mustererkennung, Drohnensteuerung, Cyberabwehr und Entscheidungsunterstützung versprechen Effizienzgewinne, schnellere Reaktionszeiten und Entlastung knapper Personalressourcen – ein attraktives Angebot in Zeiten von Fachkräftemangel und Kostendruck.

Doch parallel wächst eine neue, oft unterschätzte Hypothek: Governance-Schuld.

Fragen der Zweckbindung, Nachvollziehbarkeit, Bias-Kontrolle, Mitbestimmung und Auditfähigkeit werden häufig erst nach der technischen Implementierung adressiert.

KI-Systeme funktionieren technisch – sind aber organisatorisch und rechtlich unvollständig eingebettet. Der kritische Trend: Systeme verlieren Akzeptanz und erzeugen im Ernstfall rechtliche Unsicherheit, weil Verantwortlichkeiten nicht klar definiert sind.

Akzeptanz als Sicherheitsressource: Technik allein genügt nicht

Ob Bodycams bei Einsatzkräften, Videoüberwachung im öffentlichen Raum oder datenbasierte Analyseverfahren im Handel – 2025 zeigt sich deutlich: Sicherheit ist nicht nur eine technische oder rechtliche, sondern eine gesellschaftliche Frage. Technik kann deeskalieren, schützen und aufklären. Ohne transparente Regeln, klare Kommunikation und nachvollziehbare Zweckbindung kippt Schutz jedoch schnell in Misstrauen.

Akzeptanz wird damit zu einer strategischen Ressource. Wo sie fehlt, sinkt die Kooperationsbereitschaft von Mitarbeitern, Kunden und Bürgern. Sicherheitsmaßnahmen verlieren ihre Wirkung, selbst wenn sie technisch ausgereift sind. In einer politisch polarisierten Gesellschaft wird Sicherheit damit auch zur Frage von Legitimation und Vertrauen.

Gewalt im öffentlichen Raum: Wenn das Sicherheitsgefühl erodiert

Ein ernüchternder Befund des Jahres 2025: Trotz moderner Sicherheitstechnik sinkt in vielen deutschen Städten das subjektive Sicherheitsgefühl. Messerkriminalität, aggressive Übergriffe und eskalierende Konflikte prägen den urbanen Alltag – insbesondere in stark frequentierten öffentlichen Räumen.

Technische Maßnahmen allein können diese Entwicklung nicht auffangen. Fehlende Prävention, überlastete Justiz, soziale Fragmentierung und Personalmangel bei Polizei und kommunalen Sicherheitsdiensten verschärfen die Lage. Der Trend ist kritisch, weil Sicherheitsarbeit zunehmend reaktiv wird – während strukturelle Ursachen politisch nur zögerlich adressiert werden.

Resilienz der Alltagsinfrastruktur: Analoge Redundanz als politische Lektion

Blackouts, Systemausfälle und Cybervorfälle führen 2025 zu einer Neubewertung grundlegender Infrastrukturfunktionen. Bargeldversorgung, manuelle Prozesse und Notstromsysteme gelten nicht länger als Anachronismen, sondern als essenzielle Bestandteile nationaler Resilienz.

Der kritische Trend: Viele Systeme sind auf Effizienz optimiert, nicht auf Ausfallsicherheit. Ohne belastbare Fallback-Konzepte wird Digitalisierung selbst zum Risiko. Resilienz entsteht nicht allein durch Innovation, sondern durch bewusste Redundanz – eine Erkenntnis, die zunehmend auch in politische Strategien einfließt.

Preisdruck in der Sicherheitswirtschaft: Wenn Vergabepolitik Sicherheit aushöhlt

Ausschreibungen, Mindestlohndebatten und Tarifkonflikte verdeutlichen 2025 ein strukturelles Problem der Sicherheitswirtschaft. Sicherheit wird häufig nach Preis vergeben, nicht nach Qualität oder Nachhaltigkeit.

Das untergräbt Ausbildung, Professionalität und Mitarbeiterbindung. Der Markt öffnet sich für Billiganbieter, mit direkten Folgen für Verlässlichkeit und Sicherheitsniveau.

Der Trend wirkt schleichend, ist aber gefährlich: Sicherheitslücken entstehen nicht durch Technikversagen, sondern durch systematische Unterfinanzierung – politisch gewollt oder billigend in Kauf genommen.

Technikboom ohne Betriebskonzepte: Wenn Sicherheit nicht gemanagt wird

Mobile Videotürme, Drohnen, Sensorfusion und KI-basierte Analyse – der Sicherheitsmarkt erlebt einen technologischen Boom. Doch ohne klare Prozesse bleibt Technik wirkungslos.

Alarmketten, Wartung, Leitstellenintegration und Schulung entscheiden über den tatsächlichen Nutzen. Viele Projekte scheitern nicht an der Hardware, sondern an fehlender Betriebsreife. Der Trend ist eindeutig: Sicherheit wird beschafft, aber nicht systematisch gemanagt.

Staatliche Handlungsfähigkeit: Investitionen ohne Umsetzungskraft

2025 stellt der Staat erhebliche Mittel für IT-Sicherheit, Digitalisierung und Schutz kritischer Infrastrukturen bereit. Doch Investitionsvolumen allein ersetzt keine Governance.

Unklare Zuständigkeiten, langwierige Entscheidungsprozesse und fragmentierte Verantwortlichkeiten bremsen die Umsetzung. Externe Beratung kompensiert häufig strukturelle Defizite, ohne sie zu lösen. Der Engpass bleibt die staatliche Handlungsfähigkeit.

Ohne klare Rollen, schlanke Prozesse und messbare Ziele verpuffen Investitionen – mit direkten Folgen für die Sicherheitslage.

Sicherheit 2025: Komplex, politisch – und verletzlich

Sicherheit ist 2025 zur Systemfrage geworden. Technik, Regulierung, Wirtschaft und Gesellschaft sind enger denn je miteinander verflochten. Genau darin liegt die Herausforderung: Komplexe Systeme sind leistungsfähig, aber hochgradig störanfällig.

Die zentrale Frage lautet nicht mehr, ob investiert wird, sondern wie. Nicht mehr, welche Technologie eingesetzt wird, sondern wie sie organisatorisch, rechtlich und gesellschaftlich eingebettet ist.

Sicherheit 2025 entscheidet sich nicht an Kameras, Gesetzen oder KI-Modellen – sondern an Struktur, Klarheit und Verantwortlichkeit.

[**DCM**]

01/2025 Jahresauftakt in der Sicherheitsbranche: Vertrauen wird zur Währung

Wenn ein Jahr in der Sicherheitsbranche startet, beginnt es selten leise. Der Januar 2025 setzt den Ton mit einer Mischung aus Messe-Momentum, Regulatorik-Druck und einem klaren Signal an alle Entscheider: Sicherheit wird 2025 weniger über Einzelprodukte definiert – sondern über belastbare Ökosysteme aus Technik, Prozessen, Nachweisen und Verantwortung.

Innovationsbühne Dubai: Intersec Awards als Trendbarometer

Mit den Intersec Awards 2025 bekommt der Jahresauftakt einen internationalen Taktgeber. Die Auszeichnungen wirken wie ein Frühwarnsystem: Welche Technologien werden skalierbar, welche Lösungen wandern aus Pilotprojekten in den Regelbetrieb?

Der Tenor der prämierten Innovationen: Effizienz und Digitalisierung sind nicht mehr „Nice-to-have", sondern die Eintrittskarte in den Markt. Remote-Testing, automatisierte Prüf- und Serviceprozesse, KI-gestützte Analyse – all das zielt auf ein Ziel: weniger Reibung in der Umsetzung, mehr Verlässlichkeit im Betrieb. In einer Branche, die jahrzehntelang hardwaregetrieben war, markieren die Awards vor allem eines: Der Wert verschiebt sich Richtung datengetriebener Services.

KRITIS als Bühne: Dallmeier und die Logik des Reputationsprojekts

Parallel dazu zeigt der Monat, wie sehr KRITIS und Hochrisiko-Umfelder zur Schaufensterfläche für Hersteller werden. Dallmeier rückt mit der Absicherung der 61. Munich Security Conference in genau dieses Licht. Der Subtext ist unüberhörbar: Wer Sicherheitsarchitektur in einem Umfeld aus Politik, Diplomatie und sensiblen Lagen stabil hält, verkauft nicht nur Kameratechnik – sondern Glaubwürdigkeit.

Solche Einsätze sind weniger Marketing als Stresstest unter Live-Bedingungen. Und sie sind die Blaupause für das, was Betreiber 2025 häufiger verlangen werden: Nachweise, robuste Prozesse, klare Verantwortungsmodelle – nicht nur Features.

Zutritt wird Plattform: dormakaba und die KRITIS-Tauglichkeit als Wachstumsfeld

Ein zweites, ebenso deutliches Signal kommt aus der Zutrittswelt. dormakaba positioniert sich früh im Jahr entlang der KRITIS-Frage: Wie werden Zutrittslösungen auditfähig, skalierbar und in Standards übersetzbar? In der Praxis heißt das: Zutritt ist nicht mehr „Tür + Zylinder", sondern ein System aus Rollenlogik, Nachweisführung, Updates, Schnittstellen – und dem Versprechen, dass das Ganze auch in regulierten Umgebungen stabil funktioniert. Wer 2025 in kritischen Bereichen liefert, muss nicht nur Sicherheit erhöhen, sondern sie dokumentierbar machen.

Regulatorik wird Betrieb: DORA als Budgettreiber, Dynatrace als Übersetzer

Während die physische Sicherheit ihre Plattformlogik schärft, drückt die digitale Resilienz von der anderen Seite in die Entscheideretagen. Der Januar macht klar: DORA (digitale Betriebsresilienz) ist nicht nur ein Rechtsrahmen, sondern ein Betriebsmodell. Dynatrace steht exemplarisch für Anbieter, die diese Bewegung in operative Sprache übersetzen: Monitoring, Observability, Tests, Nachweise, Kennzahlen.

In vielen Unternehmen verschiebt sich damit das Gespräch von „ob wir compliant sein müssen" zu „wie wir Compliance in messbare Prozesse gießen". Das ist der Moment, in dem Regulierung zum Produktivitäts- und Budgettreiber wird – und Security-Teams zu Prozessarchitekten.

Tech-Kompass 2025: Axis und die neue Rolle von Video

Auch Axis Communications liefert im Januar eine Orientierung, die weit über Produktneuheiten hinausgeht. Sechs Technologietrends für den Sicherheitssektor markieren eine Realität, die viele Projekte längst spüren: Video ist nicht mehr nur Bild – es ist Datenquelle. Damit wird Videotechnik Teil von IT-Architektur, Governance und Cyber-Hygiene. Wer Video als „reines Kamerathema" behandelt, verliert 2025 Zeit und Geld: an Integrationsprobleme, an ungeklärte Verant- wortlichkeiten, an unsaubere Update- und Zugriffsmodelle. Axis' Trendblick ist deshalb weniger Prognose als Spiegel: Die Branche muss ihre technischen Gewerke enger verzahnen.

Risikobild mit klarer Nummer eins: Cyber dominiert

Zum Jahresauftakt prägt zudem ein übergeordnetes Risikonarrativ die Agenda: Der Allianz Risk Barometer 2025 setzt Cyber-Risiken an die Spitze der Unternehmensgefahren – noch vor Klima und geopolitischer Unsicherheit. Für die Sicherheitsbranche ist das kein Überraschungseffekt, sondern eine Verstärkung. Der Barometer-Effekt liegt woanders: Er bringt das Thema aus der IT-Ecke endgültig in Vorstandssprache. Resilienz wird 2025 zur Managementdisziplin – und die Schnittstelle zwischen physischer Sicherheit, IT-Security, BCM und Compliance wird zum eigentlichen Spielfeld.

Flughafensicherheit als Business Case: Outsourcing und Skalierung

Dass Sicherheitsbetrieb zunehmend als ska-

lierbarer Service gedacht wird, zeigt der Monat am Beispiel Luftverkehr: Securitas gewinnt einen großen Auftrag für Passagier-Sicherheitschecks am Flughafen BER. Das ist mehr als ein einzelner Deal. Es steht für eine strukturelle Verschiebung: Betreiber und öffentliche Auftraggeber lagern komplexe Sicherheitsprozesse aus, weil Skalierung, Personalsteuerung, Standardisierung und Nachweisführung immer anspruchsvoller werden. Flughäfen sind dabei wie ein Brennglas: hohe Taktung, hohe Regulierung, hohe Erwartung – und kaum Fehlertoleranz.

Cloud-Security rückt nach vorn: weg vom Firewall-Denken

Während die physische Sicherheitsbranche ihre Plattformen integriert, wird in der IT-Welt das Schutzmodell neu sortiert. Eine Cloud-Security-Studie (im Euro-Security-Umfeld als State-of-Cloud-Security diskutiert) beschreibt den Trend weg von klassischen Perimeter-Ansätzen hin zu kontextsensitiver Absicherung: Identität, Datenzugriff, Workload-Schutz, Monitoring – statt „Firewall als Hauptwahrheit".
Für Sicherheitsverantwortliche bedeutet das: Cloud-Sicherheit ist weniger Gerät, mehr Architektur. Und sie entscheidet 2025 mit darüber, wie zuverlässig Sicherheitsdaten, Videoanalytik, IoT und Leitstellen-Integrationen funktionieren.

Identitäten für Dinge: PKI und IoT werden zum Infrastrukturthema

Der Januar setzt außerdem ein langfristiges Signal: Der Markt für PKI-basierte IoT-Sicherheitslösungen wird auf Wachstumskurs gesehen – bis 2030 in Richtung mehrerer Milliarden Dollar. Hinter dieser Zahl steht eine technische Grundfrage, die 2025 immer öfter projektrelevant wird: Wie authentifizieren wir Geräte, Sensoren und Systeme zuverlässig – über Lebenszyklen, Updates, Betreiberwechsel und Lieferketten hinweg? Wer Smart Buildings, Sensorik, Edge und Cloud ernst meint, kommt an Geräteidentität nicht vorbei. PKI wird damit nicht Spezialthema, sondern Infrastruktur.

Wichtige Themen des Monats

- Intersec als Innovationsdossier: Die prämierten Lösungen zeigen, wohin sich Standards bewegen – Remote-Testing, Automatisierung und KI-gestützte Analyse sind nicht mehr Experiment, sondern Marktlogik.
- KRITIS-Dachgesetz als politischer Rahmen: Der Diskurs um Pflichten, Mindeststandards und Bürokratie wirkt als Startsignal: Betreiber brauchen compliance-fähige Sicherheitskonzepte, Integratoren mehr Dokumentations- und Nachweisfähigkeit.
- Sensorik & Früherkennung in der Praxis: Müdigkeits- und Waldbrandsensorik verlagern Security in Prävention und Arbeitsschutz – inklusive neuer Fragen nach Alarmketten, Verantwortlichkeiten und Datenqualität.

Monatsfazit für Januar

Der Januar 2025 macht in einem Satz klar, worum es im Rest des Jahres gehen wird: Sicherheit wird zur integrierten Betriebsdisziplin – und Vertrauen entsteht dort, wo Technik, Prozesse und Nachweise zusammenpassen. Innovationspreise, KRITIS-Projekte, Regulatorik und Cloud-Architekturen zeigen dieselbe Richtung. Wer 2025 gewinnt, liefert nicht nur Lösungen. Er liefert Betriebssicherheit.

JANUAR IM ÜBERBLICK

Wissenschaft & Forschung

Sicherheitsforscher deckten im Januar gravierende Schwachstellen im vernetzten Fahrzeugbereich auf. So gelang es dem US-Hacker Sam Curry, über offene Subaru-APIs Fernzugriff auf Millionen vernetzter Autos zu erlangen – bis hin zum Entriegeln und Starten der Fahrzeuge.

Dieser Vorfall unterstreicht den Innovationsdruck in der IT-Sicherheitsforschung: Vernetzte Systeme müssen dringend robuster gegen Cyberangriffe werden.

Auch im KI-Bereich gab es Bewegung: Seit dem 15. Januar 2025 wird allen gesetzlich Versicherten automatisch eine elektronische Patientenakte (ePA) eingerichtet, ein Meilenstein der Digitalmedizin. Experten betonen, dass damit auch Datenschutz und IT-Sicherheit im Gesundheitswesen an Bedeutung gewinnen.

Techniktrends

Der Digitalverband Bitkom begrüßte den Start der ePA am 15. Januar als „Herzstück des digitalen Gesundheitssystems". Bitkom-Hauptgeschäftsführer Dr. Bernhard Rohleder hob hervor, dass 71 % der Deutschen die ePA nutzen wollen.
Parallel zeigte eine Bitkom-Umfrage, dass große Unternehmen verstärkt auf KI setzen, um den IT-Fachkräftemangel zu mildern. 21 % der Firmen ab 250 Beschäftigten nutzen bereits KI-Lösungen, etwa Chatbots im IT-Support. Bitkom-Präsident Ralf Wintergerst betonte, KI könne IT-Teams entlasten, aber kein Allheilmittel sein. Insgesamt signalisieren die Januar-Trends: Digitalisierung und KI bleiben Treiber – vom Gesundheitswesen bis zur Personalstrategie.

Verbände

Die private Sicherheitswirtschaft in Deutschland verzeichnet nun knapp 290.000 Beschäftigte, wie der BDSW am 16. Januar mitteilte.

Laut Statistischem Bundesamt wuchs die Branche 2024 um rund 5.000 Beschäftigte – ein Indikator für das steigende Sicherheitsbedürfnis. Besonders gefragt sind digitale Sicherheitstechnik und „Smart Security"-Lösungen, die Fachkräfte erfordern.

Branchenvertreter betonen den wichtigen Beitrag privater Sicherheitsdienste für Schutz und Stabilität. Diese aktuellen Zahlen verdeutlichen den anhaltenden Wachstumstrend in der Sicher- heitswirtschaft und bilden den Auftakt für zahlreiche Personal- und Verbandsentwicklungen des Jahres.

02/2025 Sicherheitstechnik im Wandel: Von der Plattform zum Betriebskonzept

Nach dem politischen und regulatorischen Auftakt im Januar verschiebt sich der Fokus im Februar 2025 deutlich in Richtung Umsetzung. Die Sicherheitsbranche diskutiert weniger über Visionen, dafür umso konkreter über Architekturen, Betriebsmodelle und Akzeptanzfragen. Technik wird erwachsen – und muss sich im Alltag bewähren: im Einzelhandel, in industriellen Umgebungen, im Luftraum und in der Alarmtechnik.

Generationenwechsel in der Alarmtechnik: Telenot setzt auf Langfristigkeit

Mit der Einführung der hiplex 8400H markiert Telenot einen klaren Schnitt in der eigenen Produktgeschichte. Die Abkehr von der complex-400H-Plattform ist mehr als ein Modellwechsel: Sie steht für einen strategischen Umbau hin zu hybriden, modularen Architekturen. Verdrahtete und funkbasierte Komponenten werden nicht mehr parallel gedacht, sondern systemisch integriert. Für Facherrichter bedeutet das neue Spielräume bei komplexen Projekten, für Betreiber vor allem eines: Planungssicherheit. Längere Update-Zyklen, bessere Skalierbarkeit und die Fähigkeit, Alarmtechnik in größere Sicherheits- und Gebäudemanagementsysteme einzubetten, machen die hiplex-Plattform zum Baustein für größere Gewerbeobjekte, öffentliche Einrichtungen und KRITIS-nahe Anwendungen. Alarmtechnik rückt damit näher an IT-Logiken – ohne ihre Robustheit zu verlieren.

KI im Handel: Securitas macht Akzeptanz zur Projektbedingung

Während Telenot die technische Basis neu definiert, adressiert Securitas im Februar eine andere Schlüsselfrage: Wie wird KI im Sicherheitsbetrieb gesellschaftlich akzeptiert? Im Einzelhandel konkretisiert das Unternehmen seine Leitlinien zur KI-gestützten Videoanalyse. Der Fokus liegt auf Diebstahlprävention, aber der entscheidende Punkt ist nicht die Technik, sondern ihre Einbettung. Klare Zweckdefinitionen, transparente Kommunikation gegenüber Kunden und Mitarbeitenden sowie technische Begrenzungen bei der Personenerkennung werden zur Voraussetzung für den Projekteinsatz. Securitas macht damit deutlich: KI lässt sich nicht „installieren", sie muss organisatorisch eingeführt werden – mit Betriebsräten, Datenschutzkonzepten und klaren Governance-Regeln. Februar 2025 zeigt damit einen Reifegrad, den viele KI-Diskussionen noch vermissen lassen.

Drohnen raus aus dem Showroom: XPONENTIAL Europe als Positionsbestimmung

Auch die Drohnenbranche nutzt den Februar zur Standortbestimmung. Rund um die Berichterstattung zur XPONENTIAL Europe positionieren sich Anbieter wie Aerial UAS, AIR6 Systems, Alpha Unmanned Systems und Avilus klar als industrielle Lösungsanbieter. Der Tenor: Drohnen sind keine Demonstratoren mehr, sondern Werkzeuge für reale Anwendungen – von BVLOS-Inspektionsflügen über Dual-Use-Szenarien (MedEvac, Logistik, ISR) bis hin zu Sicherheits- und Infrastrukturaufgaben. Entscheidend ist dabei nicht allein das Fluggerät, sondern die Fähigkeit, regulatorische Anforderungen zu erfüllen und stabile Betriebsmodelle zu liefern. Der Markt verlangt weniger „Innovation um der Innovation willen", sondern belastbare Gesamtsysteme.

Konnektivität als Engpass: Wenn Funk über Einsatzfähigkeit entscheidet

Ein wiederkehrendes Motiv des Monats ist die Erkenntnis, dass Sensorik ohne Kommunikation wertlos bleibt. Beiträge zu ACAL BFI und Doodle Labs machen deutlich: Sichere Funkverbindungen, private Netze und robuste Datenpfade werden zum limitierenden Faktor unbemannter Systeme. Gerade im industriellen und sicherheitskritischen Umfeld entscheidet Konnektivität darüber, ob Systeme zuverlässig arbeiten oder im Ernstfall versagen. Funk wird damit nicht nur technische Voraussetzung, sondern eigenständiges Marktsegment – mit direkten Auswirkungen auf Drohnen, Robotik und vernetzte Sicherheitssysteme.

Forschung rückt näher an den Einsatz

Parallel dazu unterstreichen Fraunhofernahe Forschungspartner ihren Praxisbezug. Projekte zu LiDAR-Sensorik, autonomen Robotern und Gefahrenzonen-Erkundung zielen auf Anwendungen, bei denen Menschen bewusst aus riskanten Situationen herausgehalten werden sollen. Ob Inspektionen in kontaminierten Bereichen, Rettungseinsätze oder industrielle Wartung: Forschung liefert nicht mehr nur Konzepte, sondern einsatznahe Lösungen. Der Februar zeigt damit, wie stark sich Sicherheitsforschung an realen Betriebsanforderungen orientiert.

Monatsfazit für Februar

Der Februar 2025 markiert einen Wendepunkt: Sicherheitstechnik wird systemisch gedacht. Plattformen ersetzen Einzelkomponenten, Akzeptanz wird zur Projektbedingung, und Betriebskonzepte

rücken in den Vordergrund. Ob Alarmtechnik, KI im Handel oder Drohnen – entscheidend ist nicht mehr, was technisch möglich ist, sondern wie es dauerhaft, rechtskonform und zuverlässig betrieben werden kann.

Wichtige Projekte des Monats

Telenot hiplex 8400H – Alarmtechnik für komplexe Liegenschaften



Die hiplex-Plattform adressiert gezielt modulare, wachsende Strukturen: Unternehmensstandorte, öffentliche Einrichtungen und kritische Infrastrukturen. Ziel ist es, Alarmtechnik langfristig wartbar und integrativ zu gestalten – inklusive Anbindung an übergeordnete Sicherheits-, Leitstellen- und Gebäudemanagementsysteme.

Securitas – KI-gestützte Videoanalyse im Retail-Betrieb



Im Mittelpunkt stehen reale Filialumgebungen. Securitas setzt auf KI zur Ereigniserkennung, kombiniert mit klaren Zweckbindungen, eingeschränkter Personenerkennung und transparenten Informationskonzepten. Der Projekterfolg wird nicht an Algorithmen gemessen, sondern an Rechtskonformität, Betriebsratstauglichkeit und Skalierbarkeit im Filialnetz.

Drohnen: Öffentlich oder gewerblich – vom Gerät zum Betriebskonzept

Projekte von Airial UAS, AIR6 Systems, Avilus und Alpha Unmanned Systems zeigen den Übergang zur Betriebspraxis: Inspektionen kritischer Infrastruktur, logistische Sondermissionen und unterstützende Einsätze für Sicherheits- und Rettungskräfte. Neben dem Luftfahrzeug stehen sichere Funkanbindungen, Sensorintegration und definierte Betriebsprozesse im Fokus.



FEBRUAR IM ÜBERBLICK

Wissenschaft & Forschung

Im Februar traten neue EU-Vorgaben für Künstliche Intelligenz in Kraft. Seit dem 2. Februar müssen bestimmte KI-Praktiken mit „unannehmbarem Risiko" – etwa manipulative Psychotricks oder Social Scoring – vom EU-Markt verbannt sein.

Kurz darauf veröffentlichte die EU-Kommission Leitlinien, die verbotene KI-Systeme präzisieren.

Dies schafft erstmals klare rote Linien, z.B. gegen intransparentes Emotion-Trakking am Arbeitsplatz. Forschungsseitig sorgt die Regulierung für Orientierung und setzt zugleich Impulse zur Entwicklung vertrauenswürdiger KI. Die Botschaft: Innovation in KI ja – aber bitte sicher und ethisch.

Techniktrends

Auf internationaler Bühne rückte KI-Politik ins Rampenlicht. Beim AI Action Summit in Paris am 7. Februar mahnte Bitkom-Geschäftsleiterin Susanne Dehmel, Deutschland solle bei KI „vom Reden ins Handeln" kommen. Während USA und China mit enormem Tempo KI-Innovationen vorantrieben, konzentriere sich Europa bislang „zu sehr auf Regulierung, was Unternehmen verunsichert und Innovation bremst".

Der Pariser Gipfel setzte daher bewusst auf einen Perspektivwechsel: Chancen von KI für Wirtschaft und Gesellschaft sollten in den Vordergrund rücken. Bitkom forderte die künftige Bundesregierung auf, mehr Mut für KI-Innovationen und weniger Blockade durch bürokratische Hürden aufzubringen. Die Tech-Trends im Februar standen damit ganz im Zeichen der Balance zwischen Fortschritt und Regulierung.

Verbände

Tarifpolitisch gab es im Februar einen Durchbruch: In Nordrhein-Westfalen einigte sich die private Sicherheitswirtschaft auf einen neuen Lohntarif.

BDSW und Gewerkschaft ver.di verkündeten am 12. Februar einen Abschluss bis Ende 2026 mit Gehaltssteigerungen von insgesamt bis zu 9,5 %. Bereits zum 1. April 2025 steigen die Stundenlöhne um gut 5 % (in manchen Lohngruppen sogar knapp 6 %).

Eine zweite Erhöhung um 3,5 % folgt zum Februar 2026. Außerdem steigen die Ausbildungsvergütungen jeweils zum April 2025 und Februar 2026 deutlich an. Branchenvertreter wie Gunnar Vielhaack begrüßten den zügigen Abschluss „ohne Leermonate".

Der Tariffrieden in NRW sendet ein positives Signal – und zeigt, dass auch die Sicherheitsbranche attraktive Arbeitsbedingungen aktiv gestaltet.

03/2025 Plattformen, Verantwortung und die neue Ernsthaftigkeit der Sicherheit

Nach dem operativen Fokus des Februars rückt die Sicherheitsbranche im März 2025 in eine Phase der strategischen Konsolidierung. Übernahmen, personelle Weichenstellungen und staatliche Aufträge zeigen: Sicherheit wird zunehmend als Systemaufgabe verstanden. Parallel verschärfen sich die Debatten um öffentliche Sicherheit, Datenschutz und Verteidigungsfähigkeit. Technik allein reicht nicht mehr – gefragt sind integrierte Konzepte, klare Zuständigkeiten und gesellschaftliche Akzeptanz.

Motorola Solutions schließt Theatro-Übernahme ab

Mit dem Abschluss der Theatro-Übernahme stärkt Motorola Solutions gezielt sein Portfolio für KI-gestützte Kommunikations- und Sicherheitslösungen im Enterprise-Umfeld. Besonders im Einzelhandel und bei Organisationen mit dezentralem Personal soll die Verbindung aus Funk, Sprache und Echtzeit-Analyse operative Abläufe beschleunigen. Die Akquisition ist Teil einer klaren Strategie: physische Sicherheit, Kommunikation und Software werden zu einer gemeinsamen Plattform verschmolzen. Motorola positioniert sich damit als Orchestrator sicherheitsrelevanter Echtzeitprozesse.

ASSA ABLOY erweitert architektonische Kompetenz

Mit der Übernahme von Senior Architectural Systems baut ASSA ABLOY seine Präsenz im Bereich architektonischer Sicherheitslösungen weiter aus. Der Fokus liegt auf komplexen Gebäudeprojekten im Objekt- und Fassadenbau, bei denen Design, Funktion und Sicherheit ineinandergreifen. Strategisch stärkt der Konzern seine Rolle als Komplettanbieter – von mechanischem Zutritt über elektronische Systeme bis hin zu integrierter Gebäudesicherheit.

Verkada setzt auf internationales Wachstum

Verkada meldet im März eine personelle Verstärkung auf globaler Ebene: Ein neuer Head of Global soll die internationale Skalierung der cloudbasierten Plattform vorantreiben. Der Schwerpunkt liegt auf Europa sowie auf der engeren Verzahnung von Video, Zutritt und Sensorik in einer einheitlichen Cloud-Architektur. Verkada unterstreicht damit seinen Anspruch, fragmentierte Insellösungen durch zentral gemanagte Sicherheitsplattformen zu ersetzen.

Konica Minolta trennt sich von Mehrheitsbeteiligung an MOBOTIX

Der Verkauf der Mehrheitsbeteiligung an MOBOTIX markiert eine strategische Neuausrichtung. Konica Minolta fokussiert sich stärker auf sein Kerngeschäft, während MOBOTIX neue Spielräume für industrielle und sicherheitsfokussierte Partnerschaften erhält. In der Branche wird der Schritt als möglicher Wendepunkt für die zukünftige Positionierung des Kameraherstellers gewertet.

Securitas und Essence Security: Sicherheit „on demand"

Mit MyShield / ShieldPro bringen Securitas und Essence Security eine mobile Sicherheitslösung auf den Markt, die speziell für temporäre Objekte, kleinere Standorte und mobile Anwendungen konzipiert ist. Sensorik, Konnektivität und Service werden in einem schnell einsetzbaren Gesamtpaket gebündelt. Die Lösung adressiert einen wachsenden Markt für flexible Sicherheitskonzepte jenseits dauerhaft installierter Systeme.

Monatsfazit für März

Der März 2025 steht für eine neue Ernsthaftigkeit in der Sicherheitsbranche. Plattformstrategien, staatliche Projekte und wissenschaftliche Impulse greifen ineinander. Sicherheit wird nicht mehr als isolierte Technik verstanden, sondern als Zusammenspiel aus Technologie, Organisation und gesellschaftlicher Verantwortung. Der Monat markiert damit einen weiteren Schritt hin zu integrierten Sicherheitsökosystemen – mit klaren Erwartungen an Verlässlichkeit, Transparenz und Resilienz.

Wichtige Projekte des Monats



Bodycams und öffentliche Sicherheit – Berlin als Warnsignal

Die Bodycam-Debatte bei der Berliner Feuerwehr macht ein strukturelles Defizit sichtbar: Einsatzkräfte agieren zunehmend ohne ausreichenden technischen Eigenschutz. Das Projektfeld umfasst nicht nur die Einführung von Bodycams zur Dokumentation, Deeskalation und Beweissiche-

rung, sondern auch klare Einsatzregeln, Datenschutzkonzepte und organisatorische Zuständigkeiten. Der Diskurs zeigt exemplarisch, wie eng Technik, Recht und politische Prioritätensetzung in der öffentlichen Sicherheit miteinander verknüpft sind.

Dallmeier – Datenschutzkonforme Videoüberwachung mit KI-Verpixelung

Dallmeier präsentiert im März konkrete Anwendungen seiner KI-gestützten Verpixelungstechnologie. Ziel ist es, Videoüberwachung in öffentlichen und halböffentlichen Räumen DSGVO-konform zu betreiben, ohne auf Analysefähigkeit verzichten zu müssen. Das Projekt richtet sich an



Betreiber sensibler Bereiche, die Sicherheit, Transparenz und Akzeptanz in Einklang bringen müssen – ein entscheidender Faktor für den breiten Einsatz moderner Videoanalyse.

Teledyne FLIR – Drohnenabwehr für militärische Auftraggeber

Mit einem Auftrag der Bundeswehr unterstreicht Teledyne FLIR den steigenden Bedarf an spezialisierter Sensor- und Aufklärungstechnologie. Im Fokus stehen Systeme zur Erkennung und Abwehr feindlicher Drohnen.

Das Projekt verdeutlicht die zunehmende Verschmelzung von militärischer und ziviler Sicherheitstechnologie – und den wachsenden Stellenwert hochpräziser Sensorik im sicherheitsbehördlichen Kontext.

MÄRZ IM ÜBERBLICK

Wissenschaft & Forschung

Die Bundesforschungsministerium (BMBF) richtete vom 17. bis 19. März in Berlin die Nationale Konferenz IT-Sicherheitsforschung 2025 aus, Motto: „IT-Sicherheit und Demokratie". Rund 400 Expertinnen und Experten aus Wissenschaft, Wirtschaft, Politik und Behörden diskutierten aktuelle Forschungsschwerpunkte.

Im Fokus standen etwa die Auswirkungen von Künstlicher Intelligenz auf die IT-Sicherheit und die Zunahme KI-basierter Desinformation, aber auch menschzentrierte Sicherheitskonzepte und Quanten-Kryptografie.

Die Konferenz betonte die Bedeutung interdisziplinärer Vernetzung und förderte den Austausch über neue Schutzansätze. Fazit: Ob KI, Fake News oder Quantencomputer – Sicherheitsforschung liefert entscheidende Impulse, um die digitale Demokratie resilient zu halten.

Techniktrends

Deutschlands Industrie setzt zunehmend auf KI in der Produktion. Pünktlich zur Hannover Messe (April) präsentierte Bitkom Ende März Zahlen: 42 % der Industrieunternehmen nutzen bereits KI im Produktionsprozess, weitere 35 % planen dies.

Über 80 % sind überzeugt, dass KI entscheidend für die künftige Wettbewerbsfähigkeit ist. Gleichzeitig befürchten 46 % der Firmen, die deutsche Industrie könne die KI-Revolution verschlafen. Bitkom-Vizepräsidentin Christina Raab mahnte deshalb, die Industrie brauche mehr Tempo bei digitalen Schlüsseltechnologien, um geopolitischen und konjunkturellen Herausforderungen zu begegnen. Industrie 4.0 bleibt ein riesiges Chancenfeld: Bereits 71 % der Betriebe nutzen vernetzte Technologien in der Fertigung. Engpässe sehen viele bei fehlendem KI-Know-how und unklaren Erfahrungswerten. Die Zahlen machen Mut und Druck zugleich: Deutschlands Maschinenraum digitalisiert sich – darf aber den Anschluss in Sachen KI nicht verlieren.

Verbände

In der Sicherheitsbranche standen virtuelle Branchenevents hoch im Kurs. Der BHE Bundesverband Sicherheitstechnik veranstaltete am 18. März seinen ersten digitalen Thementag „Sicherheit in KRITIS", gemeinsam mit dem BSKI (Schutz Kritischer Infrastrukturen). Die Online-Konferenz versammelte Sicherheitsverantwortliche, Planer, Anbieter und Behörden, um neueste Entwicklungen und Lösungen zum Schutz kritischer Infrastrukturen zu erörtern.

Geboten wurde ein umfangreiches Vortragsprogramm per Videostream – inklusive interaktiver Fragerunden. Themen- schwerpunkte waren u.a. aktuelle Gesetzeslagen (eingeleitet von BSKI-Vorstand Holger Berens) sowie intelligente physische und Cyber-Sicherheitslösungen für z.B. Umspannwerke.

Zeitgleich lud am 25. März der ASW-Bundesverband gemeinsam mit dem Verfassungsschutz zur 18. Sicherheitstagung nach Berlin, um Wirtschaft, Behörden und Wissenschaft zum Austausch über Bedrohungslagen zusammenzubringen.

Beide Veranstaltungen zeigen: Die Verbände treiben den Wissenstransfer voran – ob digital oder vor Ort – und bündeln Kräfte für besseren Schutz kritischer Infrastruktur.

04/2025 Souveränität, Compliance und Hochsicherheit als neue Leitplanken

Der April 2025 markiert einen strategischen Verdichtungspunkt im Sicherheitsjahr. Während die Vormonate Integration und Plattformdenken geprägt haben, rücken nun Souveränität, Regulierung und Hochsicherheitsarchitekturen ins Zentrum. Rechenzentren werden zu KRITIS-Objekten, physische Sicherheit zum Compliance-Faktor und KI-Infrastruktur zur geopolitischen Frage. Technik, Politik und Betrieb wachsen weiter zusammen.

iGenius nimmt „Colosseum" in Betrieb– souveräne KI für sensible Anwendungen

Mit dem Start des Colosseum-Rechenzentrums setzt iGenius ein starkes Signal für souveräne KI-Infrastrukturen in Europa. Die Kombination aus Vertiv-Technologie und NVIDIA-Hardware adressiert gezielt hochsensible Anwendungen in Verwaltung, Industrie und kritischer Infrastruktur. Der Schritt steht für eine bewusste Abkehr von rein public-cloud-basierten Modellen hin zu kontrollierten, nationalen KI-Umgebungen. Für Betreiber bedeutet das: mehr Kontrolle über Daten, geringere Abhängigkeiten – und neue Maßstäbe für Sicherheits- und Resilienzkonzepte.

ASSA ABLOY: KRITIS-Dachgesetz macht Zutritt zur Pflichtdisziplin

ASSA ABLOY positioniert sich im April klar zum KRITIS-Dachgesetz. Der Konzern unterstreicht, dass physische Sicherheitskomponenten – von Zutrittskontrolle bis Notöffnung – künftig nicht nur Best Practice, sondern regulatorische Pflicht sind. Zutritt entwickelt sich damit vom Facility-Thema zur Compliance-Komponente. Für Betreiber kritischer Infrastrukturen wird physische Sicherheit messbar, prüfbar und auditfähig.

Frequentis modernisiert Leitstellen der Polizei Thüringen

Mit der Umsetzung einer neuen Einsatz- und Leitstellenlösung für die Landespolizei Thüringen zeigt Frequentis, wie softwarezentrierte Sicherheitsarchitekturen den Behördenbetrieb verändern. Ziel ist eine bessere Verzahnung von Notrufannahme, Einsatzkoordination und Lagebildern. Das Projekt steht exemplarisch für den Umbau klassischer Leitstellen hin zu integrierten, datengetriebenen Plattformen – mit direktem Einfluss auf Reaktionszeiten und Einsatzqualität.

Verkada und SimonsVoss: Cloud und Zutritt wachsen zusammen

Auf dem VerkadaOne-Event kündigen Verkada und SimonsVoss eine vertiefte Zusammenarbeit an. Cloudbasierte Video- und Zutrittslösungen sollen enger integriert werden, um skalierbare Sicherheitskonzepte für Unternehmen und öffentliche Einrichtungen zu ermöglichen. Der Fokus liegt auf vereinfachtem Betrieb, zentralem Management und schnellerem Rollout – ein weiteres Beispiel dafür, wie Cloud-Ansätze die physische Sicherheit transformieren.

Giesecke+Devrient setzt Standard bei IoT-Konnektivität

Giesecke+Devrient (G+D) wird als erster Anbieter GSMA-zertifiziert für IoT-eUICC. Damit etabliert das Unternehmen einen neuen Standard für sichere, global einsetzbare Konnektivität in IoT- und Sicherheitsanwendungen. Besonders für KRITIS, Logistik und Smart Infrastructure entsteht eine verlässliche Basis für skalierbare Sicherheitslösungen – von vernetzten Sensoren bis zu mobilen Sicherheitsdiensten.

Monatsfazit für April

Der April 2025 zeigt eine Branche im Souveränitätsmodus. Ob KI-Rechenzentren, KRITIS-Regulierung oder Hochsicherheits-Rechenzentren – Sicherheit wird national, strategisch und regulatorisch gedacht. Physische und digitale Schutzkonzepte verschmelzen weiter, während Forschung und Verbände den langfristigen Rahmen setzen. Der Monat macht klar: Sicherheit ist kein isoliertes Technikthema mehr, sondern Teil von Infrastruktur-, Industrie- und Standortpolitik.

Wichtige Projekte des Monats



Bargeldsicherheit – Schließsysteme als kritische Infrastruktur

Mehrere Beiträge zur Bargeldlogistik machen deutlich: Bargeld bleibt ein sicherheitsrelevanter Faktor. Projekte unter anderem von STUV setzen auf hochsichere, flexible Schließsysteme für Transport, Lagerung und Verarbeitung. Ziel ist es, Bargeldprozesse auch im digitalen Zeitalter resilient, nachvollziehbar und manipulationssicher zu gestalten – insbesondere für Banken und Cash-Handling-Dienstleister.

Datenschutzkonforme Kennzeichenerkennung – Genetec AutoVu ANPR

Genetec demonstriert im April konkrete Anwendungen seiner AutoVu-ANPR-Technologie zur Kriminalitätserkennung. Das Projekt kombiniert automatisierte Kennzeichenerfassung mit klaren Datenschutz-, Zweckbindungs- und Löschkonzepten. Einsatzfelder sind Verkehrsüberwachung, kommunale Sicherheit und kritische Zufahrtskontrollen.
Der Fokus liegt auf rechtskonformer Umsetzung statt maximaler Datensammlung – ein entscheidender Faktor für Akzeptanz im öffentlichen Raum.



Rechenzentren als Hochsicherheitsobjekte

Beiträge zu iGenius, ASSA ABLOY und weiteren Akteuren zeigen: Rechenzentren entwickeln sich zu Hochsicherheitszonen. Projekte kombinieren physische Zutrittskontrolle, Videoüberwachung, Umgebungsmonitoring und IT-Security zu ganzheitlichen Schutzkonzepten.

Ziel ist es, Ausfallrisiken zu minimieren und gleichzeitig steigende regulatorische Anforderungen zu erfüllen. Das Rechenzentrum wird damit zum Paradebeispiel integrierter Sicherheit.

APRIL IM ÜBERBLICK

Wissenschaft & Forschung

Deutsche Forschende präsentierten einen Durchbruch in der KI-Hardware. Am 20. März stellten Jülicher Wissenschaftler neuartige Memristoren vor, elektronische Bauteile, die sich ähnlich wie Gehirnzellen verhalten. Diese winzigen „Gedächtnis-Widerstände" sind robuster als frühere Versionen und können analog wie digital betrieben werden.

Damit könnten sie das Problem des „katastrophalen Vergessens" lösen, bei dem neuronale Netze bereits Gelerntes plötzlich verlieren. Die Memristoren passen ihre Leitfähigkeit dynamisch an – analog zur Metaplastizität biologischer Synapsen – und bewahren so altes Wissen trotz neuem Training.

KI-Experten feiern diese Entwicklung als wichtigen Schritt zu lernfähigerer, „hirnähnlicher" KI-Hardware. Die Grundlagenforschung an solchen neuro-inspirierten Bauteilen soll nun helfen, KI-Systeme dauerhaft lernfähig und ausfallsicher zu machen.

Techniktrends

Zur Hannover Messe im April zeigte sich, wie Digitalisierung und KI die Industrie beflügeln. Bitkom-Berechnungen prognostizieren, dass der deutsche Smartphone-Markt inklusive Apps, Dienste und Infrastruktur 2025 erstmals über 40 Milliarden € umsetzen wird.

Wachstumstreiber sind Datendienste (23,5 Mrd. €) und Geräteverkäufe (12,1 Mrd. €), aber auch der Boom mobiler KI-Anwendungen: Bereits 72 % der Smartphone-Nutzer verwenden KI-Funktionen – am häufigsten Sprachassistenten (58 %) und Chatbots à la ChatGPT (48 %).

Bitkom-Vizepräsident Markus Haas betont, dass „ohne KI künftig kein Smartphone mehr auskommt".

Parallel zeigte eine Bitkom-Umfrage, dass die Bundesbürger bewusster mit Elektronik umgehen:

Der Berg an alten Handys schrumpft erstmals leicht – aktuell horten die Deutschen rund 195 Millionen Alt-Handys (nach 210 Mio. Ende 2022).

Bitkom ruft dazu auf, ungenutzte Geräte zu recyceln, um wertvolle Rohstoffe zurückzugewinnen. Ob in der Industrie 4.0 oder im Alltag: Die Techniktrends im April zeigen Fortschritt – und mahnen zu nachhaltigem Umgang mit digitalen Ressourcen.

Verbände

Die Verbände nutzten den Frühling für Branchentreffs. Am 2. und 3. April feierte der BHE-Fachkongress „Brandschutz" sein 10. Jubiläum in Fulda. Facherrichter, Planer und Behördenvertreter nutzten die Gelegenheit zum Austausch über neueste Brandschutztechnik und Normen. Im Mittelpunkt standen praxisnahe Vorträge und der Netzwerkgedanke – Fulda wurde zum Mekka der Brandschutz-Community.

Auch personell gab es frischen Wind: Auf der ASW-Bundesversammlung am 2. Juni (bereits in Ausblick) wurden die Weichen neu gestellt: Johannes Strümpfel (Siemens AG/BVSW) wurde einstimmig zum neuen Vorstandsvorsitzenden der Allianz für Sicherheit in der Wirtschaft gewählt. Gleichzeitig gab der Verband sich einen neuen Namen und Markenauftritt: Aus ASW Bundesverband wird fortan der Verband für Sicherheit in der Wirtschaft (VSW). Diese strategische Neuausrichtung im Verbandswesen – modernisiertes Image und erfahrene Führung – spiegelt die gestiegene Bedeutung der Sicherheitswirtschaft wider und soll die Stimme der Branche gegenüber Politik und Öffentlichkeit weiter stärken.

05/2025 Sicherheit als Infrastruktur: Von Logistik bis Identität

Im Mai 2025 wird sichtbar, wie stark sich Sicherheit als integraler Bestandteil moderner Infrastruktur etabliert hat. Die Diskussion verlagert sich weiter weg von Einzeltechnologien hin zu ganzheitlichen Systemen, die Effizienz, Nachhaltigkeit und Resilienz verbinden. Ob Logistik, Campus, Stadt oder digitale Identität – Sicherheit wird zum Ermöglicher neuer Betriebsmodelle und politischer Handlungsfähigkeit.

Dallmeier electronic: KI- und Multifocal-Sensortechnologie für anspruchsvolle Umgebungen

Dallmeier stellt im Mai neue Videolösungen vor, die KI-gestützte Analyse mit Multifocal-Sensorik kombinieren. Die Systeme sind für komplexe Einsatzszenarien ausgelegt – etwa Selbstbedienungsbereiche, Tankstellen oder urbane Räume –, in denen gleichzeitig Überblick und Detailtiefe erforderlich sind. Der Fokus liegt auf stabiler Analyse bei wechselnden Licht- und Wetterbedingungen sowie auf der nahtlosen Integration in bestehende Leitstellen. Videoüberwachung wird damit robuster, präziser und besser skalierbar.

ASSA ABLOY treibt biometrischen und cloudbasierten Zutritt voran

ASSA ABLOY erweitert sein Portfolio um Komponenten für Zutritt, Fluchtwegsicherung und biometrische Identifikation. Die Lösungen sind konsequent auf Smart-Building-Umgebungen ausgerichtet und verbinden lokale Hardware mit cloudbasiertem Management. Der Konzern positioniert sich damit klar als Anbieter ganzheitlicher Zutrittsinfrastrukturen – mit Fokus auf Skalierbarkeit, zentrale Administration und regulatorische Anschlussfähigkeit.

Stölting Gruppe meldet Rekordumsatz

Die Stölting Gruppe verzeichnet für 2024 den höchsten Umsatz ihrer Unternehmensgeschichte. Wachstumstreiber sind integrierte Sicherheitsdienstleistungen für Industrie, Handel und öffentliche Auftraggeber. Der Erfolg unterstreicht einen klaren Markttrend: Gefragt sind kombinierte Konzepte aus Technik, Personal und Prozessen, die Sicherheit als Dienstleistung begreifen – nicht als isoliertes Produkt.

Giesecke+Devrient und Daon bündeln Kräfte bei digitalen Identitäten

Mit einer strategischen Partnerschaft bündeln Giesecke+Devrient (G+D) und Daon ihre Kompetenzen im Bereich digitaler Identitäten. Ziel ist es, Identitätsprozesse von der Registrierung bis zur Authentifizierung sicher abzubilden. Die Kooperation adressiert insbesondere regulierte Märkte und hochsensible Anwendungen – von Behörden über Finanzdienstleister bis hin zu kritischen Infrastrukturen.

Axis Communications integriert Video, Audio und Analyse

Axis Communications erweitert im Mai sein Portfolio, um Videoüberwachung, Zwei-Wege-Audio und Analysefunktionen enger zu verzahnen. Die Lösungen richten sich an Betreiber, die Sicherheitsereignisse nicht nur erkennen, sondern unmittelbar darauf reagieren wollen – etwa im Einzelhandel, in Verkehrsanlagen oder auf Campussen. Sicherheit wird damit zunehmend interaktiv und handlungsorientiert.

Monatsfazit für Mai

Der Mai 2025 verdeutlicht, dass Sicherheit längst Infrastruktur ist: in Logistik, Städten, Gebäuden und digitalen Identitäten. Unternehmen setzen auf integrierte Systeme, Forschung und Politik rücken Resilienz in den Mittelpunkt, und Verbände stellen sich personell neu auf. Sicherheit wird damit nicht nur technischer Schutz, sondern strategischer Standortfaktor – und Voraussetzung für nachhaltige, digitale Geschäftsmodelle.

Wichtige Projekte des Monats



Smarte Sicherheit für grüne Logistik – videobasierte Lösungen

Die Titelstory des Monats stellt eine videobasierte Sicherheitslösung von Dallmeier electronic für nachhaltige Logistikstandorte vor. KI-gestützte Videoanalyse und Multifocal-Sensortechnologie ermöglichen die zuverlässige Überwachung weitläufiger, personalfreier Areale. Das Projekt richtet sich an Logistik- und Tankstellenstandorte im 24/7-Betrieb, bei denen klas-

sische Bewachung weder wirtschaftlich noch ökologisch sinnvoll ist. Über angebundene Leitstellen lassen sich Ereignisse erkennen, verifizieren und Maßnahmen einleiten. Sicherheit wird so zum integralen Bestandteil effizienter und ressourcenschonender Logistikprozesse.

Campus- und Stadtsicherheit – integrierte Plattformen im Einsatz

Mehrere Praxisberichte zeigen konkrete Umsetzungen integrierter Sicherheitskonzepte. Die Binghamton University modernisiert ihre Campus-Sicherheit mit Genetec, während die italienische Stadt Imperia auf Videotechnologie von Dallmeier setzt. Beide Projekte kombinieren Video, Zutritt und zentrale Leitstellenprozesse, um Transparenz, Prävention und Reaktionsfähigkeit zu erhöhen. Campus- und Stadtsicherheit werden damit als vernetzte Systeme gedacht – nicht mehr als Ansammlung einzelner Maßnahmen.

Biometrische Zutrittskontrolle – Salto XS4 Face im Realbetrieb

Mit Salto XS4 Face wird eine biometrische Zutrittslösung vorgestellt, die Gesichtserkennung direkt in die Türhardware integriert. Das Projekt adressiert Büro-, Bildungs- und Gesundheitsbauten, in denen kontaktloser Zugang und klare Nachvollziehbarkeit gefragt sind. Im Mittelpunkt stehen eine DSGVO-konforme Implementierung, transparente Nutzerinfor- mation und die einfache Verwaltung über zentrale Software. Biometrie wird damit praxistauglich – jenseits von Pilotprojekten.



MAI IM ÜBERBLICK

Wissenschaft & Forschung

Im Mai richtete sich der Blick auf den europäischen Regulierungsrahmen und die IT-Sicherheitslage. Die EU bereitete weitere Maßnahmen zur Cyber-Resilienz vor, und Experten betonten die Bedeutung von Innovation: Beim ITS-Fachkongress der Gesellschaft für Informatik wurden etwa neueste Erkenntnisse zu KI in sicherheitskritischen Systemen vorgestellt (u.a. Abwehr von Deepfakes und KI-gestützte Cyberangriffe).

Gleichzeitig stand der jährliche BSI-Lagebericht in den Startlöchern, dessen Entwurf eine weiter „angespannte" IT-Sicherheitslage für Deutschland diagnostizierte – mit anhaltend hoher Bedrohung durch Ransomware und staatliche Cyber-Spionage.

Die Forschungs- und Behörden-Community war sich einig: Nur durch verstärkte Zusammenarbeit von Wissenschaft, Wirtschaft und Staat lässt sich das hohe digitale Risiko nachhaltig senken. Entsprechend flossen im Mai zusätzliche Fördermittel des BMBF in neue Projekte der zivilen Sicherheitsforschung, etwa zu KI-gestützter Detektion von Cyberbedrohungen.

Techniktrends

Nach der Bundestagswahl im Frühjahr wirkte die digitale Agenda im Mai deutlich nach. Bitkom begrüßte die digitalpolitischen Vorhaben der entstehenden Regierungskoalition und pochte auf rasche Umsetzung.

Besonders das Signal zur Schaffung eines eigenständigen Digitalministeriums erhielt breite Zustimmung: 71 % der Deutschen fordern laut Bitkom-Befragung ein solches Ministerium, um die Zuständigkeiten zu bündeln.

Bitkom-Präsident Ralf Wintergerst legte der neuen Regierung ein „Digitales 100-Tage-Programm" vor. Darin enthalten: eine Generalklausel zur Abschaffung zeitraubender Papierpflichten, ein Moratorium für neue Auflagen und gezielte Investitionsanreize (Superabschreibungen) für digitale Innovation. Außerdem betonte Bitkom die Bedeutung digitaler Bildung, um Desinformation entgegenzuwirken.

Kurz gesagt: Der Mai stand im Zeichen des Aufbruchs. Die Botschaft der Digitalbranche an die Politik lautete – „Liefern statt Zaudern" –, damit Deutschland digital souverän und wirtschaftlich stark bleibt.

Verbände

Die Mitglieder des BDSW haben am 22. Mai einen neuen Präsidenten gewählt: Werner Landstorfer, Geschäftsführer von Securitas Deutschland, erhielt 86 % der Stimmen und steht nun dem Präsidium vor. Ihm zur Seite stehen bewährte und neue Vizepräsidenten, darunter Gerhard Ameis, Rainer Ehrhardt, Friedrich P. Kötter sowie Cornelius Toussaint, Rasmus Wackerhagen und Nora Rauch als erste Vizepräsidentin. Mit diesem personellen Umbruch läutet der Bundesverband eine neue Ära ein – Landstorfer folgt auf den langjährigen Präsidenten Gregor Lehnert und will frischen Wind in die Verbandsarbeit bringen.

Zeitgleich würdigte der BDSW im Mai die Basis der Branche: Auf der Jahresversammlung wurde zum achten Mal der „Mitarbeiterpreis" verliehen. Ausgezeichnet wurden Sicherheitsmitarbeitende, die durch couragiertes Handeln den Wert der Branche für die Gesellschaft demonstriert haben.

Diese Mischung aus neuer Führung und Anerkennung der Leistungsträger vor Ort zeigt, wie die Sicherheitsverbände 2025 Modernisierung mit Tradition verbinden.

06/2025 Regulierung, Ökosysteme und kritische Infrastrukturen im Fokus

Der Juni 2025 steht im Zeichen der Verbindlichkeit. Während die Vormonate Integration und Wachstum geprägt haben, rücken nun Regulierung, belastbare Partnerschaften und der Schutz kritischer Infrastrukturen in den Vordergrund. Sicherheit wird nicht nur strategisch geplant, sondern politisch eingefordert, organisatorisch verankert und technisch überprüfbar gemacht. Der Monat zeigt, wie eng Unternehmensstrategien, staatliche Rahmenwerke und Verbandsarbeit inzwischen ineinandergreifen.

ASSA ABLOY: 20 Jahre PARTNERSHIP-Programm als Stabilitätsanker

ASSA ABLOY nutzt den Juni, um das PARTNERSHIP-Programm als langfristiges Ökosystem für Facherrichter und Integratoren zu positionieren. Ergänzt durch personelle Anpassungen und Produktneuheiten im Bereich Zutritts- und Schließsysteme, unterstreicht der Konzern seine Strategie: Weg vom Einzelprodukt, hin zu belastbaren Partnerstrukturen. Gerade für KRITIS-nahe Anwendungen und Großprojekte wird Kontinuität zum entscheidenden Wettbewerbsfaktor.

Frequentis: Führungswechsel im Segment Public Safety

Bei Frequentis wird ein Führungswechsel im Bereich Public Safety bekanntgegeben. Hintergrund sind steigende Anforderungen an Leitstellen, Notrufsysteme und integrierte Einsatzplattformen. Der strategische Fokus liegt auf Skalierbarkeit, Interoperabilität und der engeren Verzahnung von Sprache, Daten und Lagebildern. Frequentis reagiert damit auf den wachsenden Druck, behördliche Sicherheitsarchitekturen zukunftsfähig aufzustellen.

Nedap setzt auf neue Führung im Sicherheitsgeschäft

Nedap bestellt im Juni eine neue Geschäftsführerin für den Bereich Security. Ziel ist es, das Wachstum in den Segmenten Zutrittskontrolle, Identtechnologien und datenbasierte Sicherheitslösungen zu beschleunigen. Besonders im Fokus stehen Anwendungen in Bildungseinrichtungen, im Gesundheitswesen und in kritischen Infrastrukturen – Märkte, in denen regulatorische Anforderungen und Effizienzbedarf gleichermaßen steigen.

Verkada und SimonsVoss v ertiefen strategische Allianz

Ein Interview beleuchtet die Zusammenarbeit von Verkada und SimonsVoss, die im Juni weiter konkretisiert wird. Cloudbasierte Videoüberwachung und digitale Schließsysteme sollen funktional enger zusammengeführt werden. Ziel ist es, Betrieb, Wartung und Skalierung insbesondere in der DACH-Region zu vereinfachen. Zutritt und Video wachsen damit nicht nur technisch, sondern auch organisatorisch zusammen.

Thales warnt vor neuen Cloud-Risiken

Mit der Global Cloud Security Study 2025 lenkt Thales den Blick auf wachsende Risiken in KI-gestützten Cloud-Umgebungen. Kritisiert werden insbesondere mangelnde Transparenz und unklare Verantwortlichkeiten in hybriden und Multi-Cloud-Architekturen. Für Betreiber sicherheitskritischer Systeme ist das ein klares Signal: Cloud-Nutzung erfordert neue Governance-Modelle und klare Zuständigkeiten.

Monatsfazit für Juni

Der Juni 2025 macht deutlich: Sicherheit wird verbindlich. Regulierung, Partnerschaften und Hochsicherheitsprojekte prägen das Bild. Unternehmen reagieren mit stabilen Ökosystemen, Politik schafft klare Rahmenbedingungen, und Verbände stellen sich organisatorisch neu auf. Sicherheit wird damit zur prüfbaren Infrastrukturleistung – und zur Voraussetzung für Vertrauen in eine zunehmend digitale Gesellschaft.

Wichtige Projekte des Monats



Digitales Schließsystem für den Wohncampus Halle – dormakaba in der Praxis

Im Projekt Wohngroup Bauträger / dormakaba wird ein digitales Schließsystem für einen smarten Wohncampus in Halle umgesetzt. Ziel ist eine flexibel steuerbare, zentral verwaltete Zutrittsstruktur für Bewohner, Dienstleister und Verwaltung. Das Projekt zeigt, wie elektronische Schließtechnik den Betrieb großer Wohnanlagen effizienter, transparenter und sicherer macht – bei gleichzeitig reduziertem Verwaltungsaufwand.

Cloud-Security im Gesundheitswesen – Genetec als Plattform

Genetec stellt im Juni konkrete Anwendungsfälle für cloudbasierte Sicherheits-



lösungen im Gesundheitswesen vor. Krankenhäuser bündeln Video, Zutritt und Alarme über zentrale Plattformen. Der Fokus liegt auf Ausfallsicherheit, Datenschutz und vereinfachtem Betrieb – bei gleichzeitig steigenden regulatorischen Anforderungen. Das Projekt verdeutlicht, wie Plattformansätze die Komplexität im Klinikbetrieb reduzieren können.

Flughafen- und KRITIS-Sicherheit – Kassel Airport und SITA

Mehrere Beiträge beleuchten Sicherheitsprojekte im Flughafen-Umfeld. Am Kassel Airport kommt 3D-LiDAR-Technologie zur Überwachung von Rollfeldern zum Einsatz, während SITA smarte Zeit- und Prozesssteuerung entlang der gesamten Passagierkette thematisiert. Beide Projekte



zeigen, wie physische Sicherheit, Sensorik und IT-Systeme in kritischer Infrastruktur zusammengeführt werden – mit dem Ziel höherer Effizienz und Resilienz.

JUNI IM ÜBERBLICK

Wissenschaft & Forschung

Im Juni schlug die Stunde der europäischen Cybersicherheitspolitik. Die EU verabschiedete den „Cyber Resilience Act", der Herstellern verbindliche IT-Sicherheitsstandards für digitale Produkte auferlegt – ein Novum, das als Gamechanger für „Security by Design" gilt.

Zugleich stimmte der Bundesrat dem deutschen Umsetzungsplan der NIS2-Richtlinie zu, um bis Jahresende tausende Unternehmen kritischer Sektoren zu höheren Cyber-Mindeststandards zu verpflichten.

Die Forschungs-Community begrüßte diese Weichenstellungen: Sie schaffen einheitliche Rahmenbedingungen, in denen innovative Security-Lösungen greifen können. In der KI-Forschung rückte unterdessen die Verifizierbarkeit von KI-Modellen in den Fokus. So präsentierte eine Fraunhofer-Arbeitsgruppe in Berlin einen Ansatz, wie maschinelles Lernen transparent und prüfbar gestaltet werden kann – wichtig u.a. für vertrauenswürdige KI in der Sicherheits- und Rüstungsindustrie. Juni-Fazit: Regulierung und Forschung ziehen an einem Strang, um Technologie innovativ und sicher zu gestalten.

Techniktrends

Die neue Bundesregierung nahm ihre Arbeit auf – und Digitales steht so prominent auf der Agenda wie nie. In den Koalitionsvereinbarungen wurde erstmals ein eigenständiges Bundesdigitalministerium verankert, ganz im Sinne der Bitkom-Forderungen. Bitkom lobte außerdem den geplanten „Digitalcheck" für neue Gesetze, der verhindern soll, dass regulatorische Stolpersteine die Digitalisierung bremsen.

Unterdessen zeigte eine Bitkom-Studie zum Digitalverhalten im Alltag, dass Kontaktlos- und Mobile-Payment endgültig in der Mitte der Gesellschaft angekommen sind: Drei Viertel der Deutschen wollen überall bargeldlos zahlen können, was Handel und Banken zum Ausbau sicherer digitaler Zahlungssysteme treibt.

Im Techniktrend „KI für alle" startete im Juni die öffentliche Betaphase mehrerer deutschsprachiger Chatbot-Alternativen, gefördert vom Bund. Insgesamt wehte im Juni ein frischer digitaler Wind: Politik und Wirtschaft setzen vermehrt auf Tempo – von der Verwaltung bis zum Zahlungsvorgang.

Verbände

Der ASW-Bundesverband firmiert seit Juli mit neuem Namen und neuer Führung: Aus „Allianz für Sicherheit in der Wirtschaft" wurde der Verband für Sicherheit in der Wirtschaft (VSW). Bereits auf der Mitgliederversammlung am 2. Juni wurde Johannes Strümpfel (Siemens AG, BVSW) einstimmig zum neuen Vorstandsvorsitzenden gewählt. Er folgt auf Volker Wagner und bringt über 25 Jahre Erfahrung mit. Strümpfel betonte in seiner Antrittsrede die wachsende Bedrohungslage für die Wirtschaft und rief zu noch engerer Kooperation mit Regierung und Sicherheitsbehörden auf.

Zeitgleich unterstreicht die Umbenennung zum VSW den Anspruch, als moderne, schlagkräftige Interessenvertretung der gesamten deutschen Wirtschaftssicherheitsbranche aufzutreten. Auch in Landesverbänden gab es Veränderungen: So wählten etwa die bayerischen Sicherheitsunternehmen am 30. Juni Markus Klaedtke (Siemens) zu ihrem neuen BVSW-Vorstandsvorsitzenden.

Insgesamt markieren diese Personalwechsel im Frühsommer einen Generations- und Strategieumbruch: Die Sicherheitsverbände rüsten sich organisatorisch für neue Herausforderungen – mit frischen Gesichtern an der Spitze und geschärftem Profil.

07-08/25 Sommermodus, Dauerbetrieb: Resilienz wird zur Grundfunktion

Die Sommerausgabe 7/8-2025 zeigt eine Branche, die auch in der „ruhigen" Jahreszeit nicht runterfährt. Im Gegenteil: DORA, Cloud-Ökosysteme, Verbraucherschutz und kritische Infrastruktur laufen im Dauerbetrieb – und der Sicherheitsmarkt verschiebt sich weiter in Richtung Plattformen, Daten und vernetzte Einsatzkonzepte. Während Hersteller ihr Portfolio zusammenziehen, zeigen Projekte im Katastrophenschutz und an Flughäfen, wie sehr Sicherheit 2025 von Sensorfusion, Prozessintegration und klaren Verantwortlichkeiten abhängt.

Matrix42: DORA-Umsetzung wird operativ – und messbar

Matrix42 setzt im Sommer einen klaren Akzent in Richtung Finanzbranche: DORA wird nicht als Compliance-Text verstanden, sondern als Betriebsauftrag. Transparenz über IT-Assets, strukturierte Risikobewertungen und nachvollziehbare Abläufe für Vorfälle und Resilienztests rücken in den Mittelpunkt. Die Botschaft an Banken und Versicherer ist deutlich: DORA lässt sich nicht „nebenbei" erfüllen – nötig sind integrierte IT- und Security-Management-Plattformen, die Auditfähigkeit in tägliche Routinen übersetzen.

SentinelOne x AWS: Security wandert dorthin, wo Cloud beschafft wird

Mit der Bereitstellung von SentinelOne-Lösungen im AWS Marketplace wird ein Trend sichtbar, der sich 2025 beschleunigt: Security-Software wird dort konsumiert, wo IT heute gemanagt, skaliert und bezahlt wird. Für Cloud-native Kunden bedeutet das schnellere Beschaffung, direktere Integration und klarere Betriebsmodelle. Für den Markt ist es ein Signal: Sicherheitsanbieter müssen nicht nur schützen, sondern sich in Cloud-Ökosysteme nahtlos einfügen.

Vodafone: Spam-Schutzschild macht Verbraucherschutz zur Sicherheitsleistung

Vodafone zieht nach drei Monaten eine Bilanz und meldet 15 Millionen Warnmeldungen vor potenziell betrügerischen Anrufen. Damit rückt ein neues Rollenbild in den Vordergrund: Telekommunikationsanbieter werden zu Akteuren der öffentlichen Sicherheit – mit datenbasierter Erkennung, automatisierten Warnmechanismen und einem direkten Impact im Alltag. Security wird hier nicht als Produkt verkauft, sondern als Schutzfunktion im Kommunikationsnetz.

Axis Communications: AXIS C17 – Video, Audio und Information in einem System

Mit der AXIS C17 Network Display Speaker Series stärkt Axis die Verbindung von Video, Audio und visueller Information. Ziel sind Anwendungen in Verkehr, Industrie und öffentlichen Räumen, in denen es nicht nur um Erkennung, sondern um situative Kommunikation geht: informieren, warnen, steuern – aus einem System heraus. Damit verschiebt sich Sicherheitskommunikation weiter weg von Einzelgeräten hin zu integrierten, netzwerkfähigen Bausteinen.

Genetec: Plattformlogik als Marktstandard in der Videoüberwachungssoftware

Genetec unterstreicht im Sommer seine Marktposition und setzt inhaltlich auf das, was 2025 besonders zählt: offene Plattformen, Integration heterogener Sensorik und die Verbindung von physischer Sicherheit mit IT-Security-Prozessen. Für große, verteilte Infrastrukturen ist das entscheidend: Nicht „die beste Kamera" gewinnt, sondern die Plattform, die Daten, Ereignisse und Workflows zusammenführt – ohne Lock-in und ohne Insellösungen.

Monatsfazit für Juli und August

Juli und August 2025 zeigen Sicherheit als Dauerfunktion: DORA wird operativ, Cloud-Security wird Einkaufs- und Betriebsmodell, Telekommunikation wird Verbraucherschutz, und KRITIS-Projekte – von Drohnen bis Flughafen – setzen auf Sensorfusion und Prozesse statt Einzeltechnik. Der Sommer ist damit kein Leerlauf, sondern die Phase, in der die Branche ihre Systeme, Verbände und Strategien so aufstellt, dass der Herbst nicht nur laut, sondern auch lieferfähig wird.

Wichtige Projekte des Monats



KI-Drohnen im operativen Einsatz – von der Plattform zur Einsatzroutine

Euro Security zeigt, wie AIR6 SYSTEMS, Aerial UAS, Avilus und Alpha Unmanned Systems KI-gestützte Drohnen als Sicher-

heitswerkzeug positionieren – nicht als Demo. Entscheidend sind definierte Betriebskonzepte: BVLOS-Fähigkeit, sichere Datenübertragung, Sensorintegration (optisch/thermisch/LiDAR) und die Anbindung an Leitstellen und Einsatzorganisationen.

Die Drohne wird damit zur wiederkehrend einsetzbaren Komponente in Industrie, Behörden und KRITIS – eingebettet in Prozesse statt im Schaukasten.

Katastrophenschutz & Bevölkerungswarnung – Sirenen und Apps als Duo

Mehrere Beiträge widmen sich der Stärkung des Katastrophenschutzes: neue Sirenenförderung, digitale Warnsysteme, Notruf- und App-Lösungen.

Auffällig ist das Zusammenspiel aus „alter" und „neuer" Infrastruktur: Sirenen als robuste Basis, digitale Kanäle als präzise Verstärkung. Ziel ist Reichweite, Geschwindigkeit und Verlässlichkeit – und



damit eine Resilienzlogik, die nicht auf eine einzelne Technologie setzt, sondern auf Redundanz.

Flughafenlösungen 2025 – Sensorfusion für KRITIS-Dauerbetrieb

Die Ausgabe zeichnet ein klares Bild moderner Flughafensicherheit: Axis adressiert Situationskommunikation in Terminals und Sicherheitszonen mit vernetzten Video-, Audio- und Display-Komponenten. FLIR



liefert Wärmebild- und Perimeterfähigkeiten für schlechte Sichtbedingungen und sensible Areale. Ergänzend zeigen physische Schutzmaßnahmen die Breite der Architektur: Delta Scientific mit temporären Fahrzeugsperren, DEHN mit Schutzsystemen für kritische Infrastrukturelemente. Das Muster ist eindeutig: Flughafensicherheit ist 2025 Sensorfusion plus physischer Schutz plus Leitstellenanbindung – ausgelegt auf Dauerbetrieb.





JULI IM ÜBERBLICK

Wissenschaft & Forschung

Im Juli stand insbesondere der Schutz vor neuen Cyber-Gefahren im Mittelpunkt. Die halbjährliche Auswertung des BSI zeigte, dass besonders KI-gestützte Phishing-Angriffe und Deepfakes rasant zunehmen.

Sicherheitsforscher stellten daraufhin verbesserte Erkennungsmethoden vor: So können KI-Systeme inzwischen Täuschungsmuster in synthetischen Videos und Audio erkennen, indem sie minimale Pixel-Unregelmäßigkeiten oder unnatürliche Atempausen auswerten.
Auch im Bereich Kritische Infrastrukturen gab es Neues: Ein Konsortium deutscher Fraunhofer-Institute startete ein Forschungsprojekt, um Smart Grids gegen KI-basierte Hackerangriffe zu wappnen – beispielsweise durch Anomalieerkennung im Stromnetz.
Diese Entwicklungen untermauern: Die Sicherheitsforschung reagiert agil auf neuartige Risiken, um Wirtschaft und Staat resilienter zu machen.

Chronik 2025

Techniktrends

Der Sommer brachte Zahlen zur Digitalwirtschaft und Verbraucherelektronik. Die ITK-Branche erweist sich weiter als Jobmotor: Laut Bitkom-Prognose entstehen 2025 net- to rund 20.000 neue Stellen in IT und Telekommunikation. Gleichzeitig kühlt der klassische Unterhaltungselektronikmarkt weiter ab (–7,5 % Umsatz erwartet), während Software (+9,8 %) und Cloud-Services (+17 %) zweistellig wachsen. Bitkom-Präsident Wintergerst fordert daher politische Unterstützung, um das digitale Wachstumstempo hochzuhalten.

Im Verbrauchersektor zeigt eine Bitkom-Umfrage: Die Zahl gehorteter Alt-Handys ist mit 195 Millionen Geräten erstmals rückläufig. Immer mehr Menschen trennen sich von alten Smartphones – 21 % haben in den letzten 12 Monaten mindestens ein Gerät verkauft, verschenkt oder recycelt.

Bitkom wertet dies als Fortschritt in Richtung Kreislaufwirtschaft und gibt Tipps zur fachgerechten Entsorgung. Unterm Strich signalisieren die Juli-Trends: Der digitale Wandel schreitet voran – ökonomisch, ökologisch und im Arbeits- markt.

Verbände

Zur Jahresmitte stellt sich die Sicherheitsverbandslandschaft neu auf. Ende Juli gab der bisherige ASW-Bundesverband nicht nur seinen Namenswechsel zu VSW bekannt, sondern feierte auch die Umsetzung des internen Reformprozesses. Die Modernisierung reicht von neuer Corporate Identity bis zu erweiterten Serviceangeboten für Mitglieder. Unter Führung von Johannes Strümpfel (Vorsitz) und Geschäftsführerin Caroline Eder will der VSW bundesweit präsenter sein und aktiv an der Sicherheitsgesetzgebung mitwirken.

Parallel blickte der BDSW auf erfolgreiche erste 100 Tage unter Präsident Landstorfer zurück: In einem Sommerinterview betonte dieser, der Verband werde sich verstärkt in politische Debatten – etwa zum geplanten Sicherheitsgewerbegesetz – einbringen. Zudem laufen beim BDSW die Vorbereitungen für den 11. Bayerischen Sicherheitstag im November auf Hochtouren, der aktuelle Herausforderungen der Unternehmenssicherheit beleuchten wird. Die Sommermonate zeigen: Die Verbände nutzen die ruhigere Zeit, um intern zu konsolidieren und strategisch auszurichten, bevor im Herbst wieder wichtige Branchentermine anstehen.

AUGUST IM ÜBERBLICK

Wissenschaft & Forschung: Im August richtete sich die Aufmerksamkeit der Security-Community auf die internationalen Hacker- und Cyber-Sicherheitskonferenzen. Bei der traditionsreichen Black Hat USA in Las Vegas wurden neue Verwundbarkeiten und Abwehrmethoden diskutiert. Besonders im Fokus: KI-gehärtete Malware, die signifikant schwerer zu entdecken ist. Forschungsteams präsentierten konternd KI-gestützte Intrusion-Detection-Systeme, die ungewöhnliches Verhalten auch von KI-Malware erkennen können.

Zeitgleich berichtete das Europäische Forschungsprojekt "DEEP-Shield" erste Erfolge: Ein neuer Algorithmus kann Deepfakes mit 99 % Trefferquote als solche identifizieren, indem er auf mikroskopische Artefakte in Bild und Ton achtet. Diese Fortschritte im August verdeutlichen: Forschungseinrichtungen weltweit arbeiten mit Hochdruck daran, den „Wettlauf" zwischen Angreifern und Verteidigern im Cyberspace zu gestalten – mit KI als Schlüsselelement auf beiden Seiten.

Techniktrends

Die Urlaubszeit tat der Digitalpolitik keinen Abbruch. Bundesdigitalminister (erstmals im Amt) skizzierte im August eine Digitalstrategie, die vom flächendeckenden 5G/Glasfaserausbau bis zur KI-Förderung reicht. Bitkom lobte insbesondere die geplante Bürokratie-Entlastung für digitale Geschäftsmodelle und das Vorhaben, Genehmigungsprozesse via Online-Verfahren zu beschleunigen. Im Marktblick offenbarte eine Bitkom-Studie spannende Zahlen zum E-Commerce: Mehr als 50 % der Bundesbürger haben 2025 schon per Sprachassistent eingekauft, was zeigt, wie sehr smarte Lautsprecher & Co. das Konsumverhalten verändern.

Zudem trendet "Social Commerce" – der Verkauf über soziale Netzwerke – stark aufwärts, insbesondere bei jüngeren Käuferschichten. Technik-Trend des Monats war jedoch eindeutig das Thema Cybersicherheit bei KMU: Eine Bitkom-Befragung ergab, dass zwei Drittel der Mittelständler in den letzten zwölf Monaten Opfer von Cyberattacken wurden. Bitkom forderte deswegen einen einfacheren Zugang zu Sicherheitsberatung und warnte vor Sorglosigkeit: Auch im Sommerloch gilt – Cyberkriminelle machen keinen Urlaub.

Verbände

Im August hielten viele Sicherheitsunternehmen ihre interne „Sommerklausur". Die großen Verbände hingegen starteten bereits die Planung für anstehende Herbstveranstaltungen.

Der BHE etwa kündigte seinen 9. Fachkongress Videosicherheit/Zutrittssteuerung für Anfang September an – nach pandemiebedingter Pause ein wichtiges Branchentreffen, das in Mainz stattfinden wird. Personell gab es im August vor allem Kontinuität: Wichtige Gremienposten waren bereits im Frühjahr neu besetzt worden, sodass nun die Umsetzung der gesteckten Ziele im Vordergrund steht.

Eine personelle Überraschung lieferte lediglich der Rückzug von Securitas-Deutschlandchef Jörg H. Zürn, der nach zwei Jahrzehnten zum Jahresende 2025 in den Ruhestand geht (das gab das Unternehmen im August bekannt). Branchenbeobachter erwarten, dass sein Nachfolger auch im BDSW-Vorstand eine aktive Rolle einnehmen wird. Insgesamt war der August im Verbandswesen von ruhiger Sacharbeit und Vorbereitung geprägt – die Basis für einen arbeitsreichen Herbst ist gelegt.

09/2025 Transparenz, Leitstellen und die Rückkehr der Ernsthaftigkeit

Der September 2025 markiert den Übergang vom Sommer in den arbeitsintensiven Sicherheitsherbst. Messen, Studien und neue Plattform-Updates zeigen: Sicherheit wird technischer, transparenter – und zugleich politischer. IT- und OT-Welten wachsen weiter zusammen, Leitstellen entwickeln sich zu digitalen Nervenzentren, und Identität rückt als Schlüsselthema für Unternehmen jeder Größe in den Fokus. Der Monat steht für eine Rückkehr zur Ernsthaftigkeit nach der Sommerphase.

Kentix: KentixONE 8.6 verbindet IT- und OT-Sicherheit

Mit KentixONE 8.6 treibt Kentix die Integration von IT- und OT-Überwachung voran. Visualisierung, Alarmierung und Reaktion werden in einer Plattform gebündelt. Betreiber von Rechenzentren und kritischen Infrastrukturen können physische Sensorik, Netzwerkzustände und Umgebungsdaten gemeinsam auswerten. Der Schritt verdeutlicht einen zentralen Markttrend: Sicherheit entsteht nicht mehr in getrennten Silos, sondern durch konvergente Lagebilder.

Google Cloud adressiert KI-Security ganzheitlich

Auf dem Google Cloud Security Summit stellt Google neue Sicherheitsfunktionen für KI-gestützte Workloads vor. Im Fokus stehen Angriffserkennung, der Schutz von Trainingsdaten und sichere Innovationspfade für KI-Anwendungen. Für Unternehmen wird klar: Cloud-Security und KI-Security lassen sich nicht mehr getrennt betrachten. Wer KI produktiv nutzt, muss Sicherheit von Anfang an mitdenken – technisch wie organisatorisch.

GIGAMON zeigt Lücke zwischen Anspruch und Realität

Eine Analyse von GIGAMON zeichnet ein ernüchterndes Bild der Cyber-Resilienz. Viele Unternehmen überschätzen ihren Sicherheitsgrad, während es an Transparenz in Netzwerken und OT-Umgebungen mangelt. Besonders Industrie- und KRITIS-Betreiber stehen vor dem Problem, dass Angriffsflächen nicht vollständig sichtbar sind. Die Studie fungiert als Weckruf: Resilienz beginnt mit Sichtbarkeit.

8com: Malware-Analyse enttarnt Hackergruppe

8com berichtet über die Enttarnung einer Hackergruppe, die sich durch Fehler in der eigenen Malware identifizierbar machte. Der Fall zeigt exemplarisch, wie wichtig Analysekompetenz, Threat Intelligence und schnelle Reaktionsfähigkeit geworden sind. Cyberabwehr ist 2025 weniger Tool-Frage als Know-how-Disziplin.

Goaco und Thales demokratisieren Identitätsprüfung

Mit gemeinsamen Lösungen adressieren Goaco und Thales gezielt kleine und mittlere Unternehmen. Sichere Identitätsprüfung, bislang oft Großunternehmen vorbehalten, wird damit auch für KMU zugänglich. Identität etabliert sich als zentraler Sicherheitsbaustein – unabhängig von Unternehmensgröße.

Monatsfazit für den September

Der September 2025 bringt Klarheit und Fokus zurück in die Sicherheitsdebatte. Transparenz in IT- und OT-Systemen, leistungsfähige Leitstellen und verlässliche Identitätslösungen prägen den Monat. Unternehmen, Forschung und Verbände stellen sich auf einen intensiven Herbst ein – mit der gemeinsamen Erkenntnis, dass Sicherheit nur dort wirkt, wo Technik, Organisation und Vertrauen zusammenkom men.

Wichtige Projekte des Monats



Branddetektion mit Video und Thermografie

Die Titelstory widmet sich video- und thermografiebasierten Branddetektionssystemen. Anbieter wie FLIR zeigen, wie Brände in Industrieanlagen, Hochregallagern und Außenbereichen bereits im Entstehungsstadium erkannt werden können. Ziel ist Prävention statt Reaktion: Brände sollen identifiziert werden, bevor Rauchmelder oder Sprinkler überhaupt auslösen. Für Betreiber bedeutet das höhere Sicherheit und geringere Folgeschäden.

it-sa Expo & Congress 2025 – IT und OT rücken zusammen

Die it-sa Expo & Congress 2025 startet mit Rekordzahlen: 950 Aussteller in fünf Messehallen. Thematisch dominieren KRITIS, industrielle IT-Sicherheit sowie Regulatorik wie NIS2 und Cyber Resilience Act. Besonders sichtbar ist die Annäherung von IT- und OT-Security – von Leitständen bis zu

Chronik 2025



Produktionsnetzen. Die Messe bestätigt: Security ist Querschnittstechnologie für Industrie, Verwaltung und Infrastruktur.

Leitstellenmanagement – NXGEN und Stadtwerke Schwerin

NXGEN demonstriert, wie mobile Video- und Alarmintegration moderne Leitstellen flexibler macht. Parallel investieren die Stadtwerke Schwerin in eine neue Leitwarte, um Steuerung und Überwachung kritischer Versorgungsprozesse zu optimieren. Beide Projekte verdeutlichen den Wandel der Leitstelle zum digitalen Nervenzentrum von Energie-, Verkehrs- und Sicherheitsinfrastruktur.



SEPTEMBER IM ÜBERBLICK

Wissenschaft & Forschung

Im September beschäftigten neue Studien die Sicherheitswelt. Das Hasso-Plattner-Institut veröffentlichte seinen jährlichen Report zu Cybergefahren: Darin wird vor einer starken Zunahme von „API-Angriffen" gewarnt – also Attacken auf die Datenschnittstellen moderner Anwendun- gen.

Diese Angriffe hätten sich 2025 im Vergleich zum Vorjahr nahezu verdoppelt, da immer mehr Dienste über Cloud- und Web-APIs vernetzt sind. Die Forschung reagiert mit speziellen Sicherheitstools für Entwickler, um verwundbare Schnittstellen frühzeitig abzusichern.

Parallel erschien die Polizei-Studie „Sicherheit 2025" in der Schweiz, die aufzeigt, dass das subjektive Sicherheitsgefühl der Bevölkerung trotz technologischer Hilfsmittel (wie Gesichtserkennung im ÖV) leicht gesunken ist. Experten führen dies auf mediale Berichterstattung über Hacker und Terror zurück.

Die Ergebnisse regen zu weiterführender Forschung an, wie Technik Vertrauen schaffen kann, ohne Freiheitsrechte zu beschneiden – eine zentrale Herausforderung der Sicherheitsforschung.

Techniktrends

Im politischen Berlin brachten der nahende Regierungswechsel und die anstehende Digitalbudget-Verhandlung Bewegung in die Diskussion. Bitkom mahnte im September, dass die geplanten Investitionen in digitale Bildung, Verwaltung und Infrastruktur dringend verstetigt werden müssten – andernfalls drohe ein „Digitalisierungsstillstand".

Parallel veröffentlichte Bitkom eine repräsentative Umfrage zum Thema Social Media & Wahlen: 88 % der Deutschen befürchten ausländische Einflussnahme via Fake News auf die kommende Bundestagswahl.
Bitkom-Präsident Wintergerst forderte daher stärkere Anstren- gungen gegen Desinformation in sozialen Netzwerken. Technikseitig stand alles im Zeichen der IAA Mobility in München: Vernetzte Fahrzeuge, intelligente Verkehrssysteme und Datensicherheit im Auto wurden breit diskutiert. Die Branche betonte, dass Cybersicherheit bei Autos so wichtig ist wie Airbags – ein Motto, das nach dem Subaru-Hack vom Jahresanfang (siehe Januar) umso einprägsamer wirkt.

Verbände

Der September war ein echter Wahlmonat in der Sicherheitsbranche. Mehrere BDSW-Landesgruppen wählten turnusgemäß ihre Vorstände neu. In Berlin/Brandenburg etwa bestätigte man den langjährigen Landeschef Rainer Ehrhardt im Amt, während in Brandenburg Mathias Fiedler (Securitas) neu an die Spitze gewählt wurde.

Im hohen Norden verabschiedete die Landesgruppe Hamburg ihren langjährigen Vorsitzenden Jens Müller in den Verbandsruhestand und wählte Andreas Segler einstimmig zu seinem Nachfolger. Auch in Mecklenburg-Vorpommern, Sachsen, Hessen und anderen Ländern gab es Vorstandswahlen, meist mit Wiederwahlen bewährter Kräfte.

Diese regionalen Führungswechsel zeigen die Vitalität der Verbandsstruktur: Vor Ort werden neue Köpfe eingebunden und altgediente Experten geehrt.

Der Austausch bei den Landesversammlungen diente zugleich der Vorbereitung auf den BDSW-Bundeskongress im Oktober, wo die Branche ihre politischen Forderungen – etwa nach einem modernen Sicherheitsgewerbegesetz – geschlossen vertreten will.

10/2025 Hochverfügbarkeit, Identität und der Ernst der Skalierung

Der Oktober 2025 markiert den Höhepunkt des sicherheitspolitischen und technologischen Herbstes. Großprojekte, Messen, Gerichtsurteile und politische Verhandlungen verdichten sich – und zeigen, wie sehr Sicherheit inzwischen von Skalierung, Hochverfügbarkeit und rechtlicher Belastbarkeit geprägt ist. Ob Casino, Stadion, Rechenzentrum oder Cloud: Sicherheit muss funktionieren, jederzeit, unter Last und unter Beobachtung.

Dallmeier: Modulare VMS-Architektur fdas Grand Sapphire Casino

Mit dem Projekt im Grand Sapphire Casino realisiert Dallmeier eine umfassende Videoüberwachung für 42 Live-Game-Tische und mehr als 300 Slot-Maschinen. Zum Einsatz kommt eine modulare VMS-Architektur mit KI-Potenzial, ausgelegt auf 24/7-Betrieb, hohe Bildqualität und Ausfallsicherheit. Das Projekt unterstreicht Dallmeiers Stärke in hochregulierten Umgebungen mit strengen Compliance- und Dokumentationspflichten – ein klassischer Härtetest für Sicherheitsarchitekturen.

AMD und OpenAI: 6 Gigawatt KI-Rechenleistung als neue Dimension

Die angekündigte Partnerschaft von AMD und OpenAI zum Ausbau von KI-Rechenkapazitäten auf bis zu 6 Gigawatt setzt Maßstäbe. Für die Sicherheitsbranche bedeutet das: KI-gestützte Videoanalyse, Cyberabwehr und Entscheidungsunterstützung skalieren weiter. Gleichzeitig wachsen die Anforderungen an Energieeffizienz, Standortwahl, physische Sicherheit und digitale Souveränität der Rechenzentren – Sicherheit wird zur Voraussetzung von KI-Skalierung.

HID übernimmt Idmelon und stärkt passwortlose Identität

Mit der Übernahme von Idmelon erweitert HID sein Identitätsportfolio um passwortlose Authentifizierung. Die Integration in den Microsoft-Entra-Marktplatz adressiert Unternehmen, die Identität, Zutritt und IT-Sicherheit enger verzahnen wollen. Identitätsmanagement etabliert sich damit als Brückentechnologie zwischen physischer und digitaler Sicherheit.

KÖTTER Aviation Security erhält OSPA

KÖTTER Aviation Security wird mit dem OSPA (Outstanding Security Performance Award) für eine herausragende Sicherheitspartnerschaft ausgezeichnet. Gewürdigt wird das Zusammenspiel aus Technik, Personal und Prozessen im sensiblen Flughafenbetrieb. Das Modell zeigt, wie integrierte Sicherheitsdienstleistungen Effizienz und Schutz zugleich erhöhen können – besonders relevant angesichts steigender Bedrohungslagen.

TeleTrusT wächst und stärkt europäische IT-Security

Der IT-Sicherheitsverband TeleTrusT begrüßt zwölf neue Mitgliedsunternehmen. Der Zuwachs spiegelt den steigenden Stellenwert europäischer Sicherheitslösungen wider – insbesondere vor dem Hintergrund von NIS2, Cyber Resilience Act und dem Wunsch nach digitaler Souveränität. Verbandsarbeit wird damit zunehmend zum Standortfaktor.

Monatsfazit für den Oktober

Der Oktober 2025 zeigt Sicherheit im Stresstest der Skalierung. Großprojekte, KI-Rechenleistung, Identitätsmanagement und rechtliche Vorgaben treffen aufeinander. Sicherheit muss hochverfügbar, rechtssicher und integrierbar sein – in Casinos ebenso wie in Stadien, Rechenzentren oder Cloud-Ökosystemen. Der Monat macht klar: Wer Sicherheit nicht von Anfang an mitdenkt, verliert im Betrieb.

Wichtige Projekte des Monats



Casino-Sicherheit im Dauerbetrieb – Dallmeier als Systemarchitekt

Das Casino-Projekt in Kambodscha zeigt Videoüberwachung als Hochverfügbarkeitsinfrastruktur. Dallmeier kombiniert zentrale Aufzeichnung, intelligente Analyse und modulare Erweiterbarkeit, um Spielbetrieb, Betrugsprävention und Personensicherheit gleichzeitig abzudecken. Entscheidend ist die langfristige Betriebssicherheit unter Dauerlast – bei klaren regulatorischen Vorgaben und internationa- lem Umfeld.

Smart Arena – Salto Systems im Estadio Santiago Bernabéu

Im modernisierten Estadio Santiago Bernabéu implementiert Salto Systems integrierte Zutrittslösungen für Stadionbetrieb, Hospitality und Back-of-House-Bereiche. Digitale Schlüssel, zentrale Verwaltung und hohe Ausfallsicherheit ermöglichen die flexible Steuerung von Besucherströmen und Sicherheitszonen. Das Projekt zeigt, wie Event-Sicherheit 2025 auf skalierbare, softwaregestützte Infrastruktur setzt.

Chronik 2025



Drohnenabwehr und Grenzsicherheit

Beiträge zur Drohnenabwehr in Hessen und zur Sicherung europäischer Grenzen verdeutlichen den Reifegrad entsprechender Systeme.
Detektionssensorik, Lagebildfusion und Leitstellenanbindung stehen im Vordergrund. Drohnenabwehr wird damit Teil regulärer Sicherheitsarchitekturen für Behörden und KRITIS-Betreiber – nicht mehr Sonderfall, sondern Standard.



OKTOBER IM ÜBERBLICK

Wissenschaft & Forschung

Im Oktober waren es oft juristisch-tech- nische Themen, die von sich reden machten. So bestätigte der Europäische Gerichtshof in einem viel beachteten Urteil den strengen Kurs der EU-Datenschutz-Grundverordnung: Das „Recht auf Vergessenwerden" gilt auch für Suchmaschinen-KI – entsprechende Lösch-Algorithmen müssen nachweislich diskriminierungsfrei arbeiten, ansonsten drohen Sanktionen.

Diese Entscheidung zwingt Tech-Konzerne, ihre KI-gestützten Systeme zur Datenverarbeitung transparenter und überprüfbarer zu gestalten, was Datenschützer als wissenschaftlichen Erfolg verbuchen.

Gleichzeitig lief Ende Oktober die heiße Phase der europäischen Cybersicherheitsübung „Blue Octopus 2025": Über 400 Organisationen probten länderübergreifend den Ernstfall koordinierter Cyberangriffe auf Energie- und Finanzsektor. Die Auswertung durch Forschungsinstitute wird wertvolle Erkenntnisse zur Resilienz kritischer Infrastrukturen liefern.

Schon jetzt zeigt sich: Internationales Üben und Forschen Hand in Hand ist unverzichtbar, um komplexe Bedrohungsszenarien zu bewältigen.

Techniktrends

Im Vorfeld der Regierungsbildung legte Bitkom Ende Oktober ein detailliertes Schatten-Digitalbudget vor. Darin werden jährlich 3 Milliarden € zusätzlich für digitale Bildung, Cybersicherheit und KI-Förderung gefordert. Bitkom argumentiert, diese Summe sei gut investiert, um langfristig Wirtschaftswachstum und Innovationsführerschaft zu sichern.

Technologisch rückte das Thema Smart City ins Rampenlicht: Eine Bitkom-Studie zum Smart City Index 2025 zeigte, dass deutsche Städte bei digitaler Verwaltung, Mobilität und Sicherheitsinfrastruktur aufholen – Hamburg, München und Köln führen das Ranking an, u.a. dank vernetzter Sensorik bei Verkehr und Kriminalitätsprävention. Allerdings mahnt Bitkom, gerade beim Ausbau städtischer Datennetze müsse noch mehr Tempo her.

Ein weiteres Trendthema war Generative KI im Unternehmenseinsatz: Laut Bitkom nutzen inzwischen 31 % der Firmen Tools wie ChatGPT zur Text- oder Code-Generierung. Hier fordert Bitkom Leitlinien der neuen Regierung, um Rechtssicherheit beim KI-Einsatz zu schaffen. Der Oktober machte deutlich: Ohne politische Flankierung keine digitale Transformation – diese Botschaft trägt Bitkom in die Koalitionsverhandlungen.

Verbände

Die Sicherheitsverbände reagierten im Oktober empfindlich auf politische Signale. Für Unmut sorgte eine Entscheidung der Bundesregierung, private Sicherheitsdienste erneut nicht als „gemeinwohldienlich" im Sinne des Arbeitsrechts einzustufen – eine seit Jahren erhobene Branchenforderung blieb unerfüllt. Der VSW-Bundesverband (ehem. ASW) kritisierte diese Haltung scharf und warf der Politik „fehlende Wertschätzung gegenüber einer unverzichtbaren Branche der Inneren Sicherheit" vor. Parallel starteten in mehreren Bundesländern die Tarifrunden für 2026: ver.di kündigte bspw. in Hessen die Wach- und Sicherheits-Tarifverträge, um ab November neu zu verhandeln.Verbände wie der BDSW bereiteten sich auf harte Gespräche vor, signalisierten aber Kompromissbereitschaft, um faire Löhne und Planungssicherheit zu erreichen.

Personell gab es im Oktober einen Abgang bei der BHE-Geschäftsführung: Langzeitgeschäftsführer Stephan Schütte verabschiedete sich in den Ruhestand, seine Nachfolge tritt zum Jahreswechsel die bisherige stellv. Geschäftsführerin Maren Rauh an.

Damit einher geht ein Generationenwechsel, den der BHE mit Dank für Schüttes Verdienste und frischem Elan ins neue Jahr gestalten will.

11/2025 Sicherheit unter Druck: Souveränität, Infrastruktur und Umsetzung

Der November 2025 ist der Monat der Bilanz und Zuspitzung. Während sich das Jahr dem Ende nähert, verdichten sich operative Großprojekte, regulatorische Umsetzungen und politische Grundsatzdebatten. Luftsicherheit, Grenzmanagement, Verkehrsinfrastruktur und Cyberabwehr zeigen exemplarisch, wo Sicherheit heute stehen muss: hochautomatisiert, interoperabel und souverän. Gleichzeitig wird klar, dass gerade Mittelstand und öffentliche Hand vor erheblichen Umsetzungsherausforderungen stehen.

Smiths Detection: iCMORE setzt Maßstab an deutschen Flughäfen

Mit der Zertifizierung des iCMORE-CT-Systems durch die Bundespolizei erreicht Smiths Detection einen zentralen Meilenstein in der Luftsicherheit. Die Technologie ermöglicht hochauflösende, automatisierte Gepäckkontrollen und erfüllt neue europäische Vorgaben. Für Flughäfen bedeutet das schnellere Abläufe bei gleichzeitig höherem Sicherheitsniveau – ein entscheidender Faktor angesichts wachsender Passagierzahlen und steigenden Effizienzdrucks.

secunet: Flughafen Zürich startet EU-Ein-/Ausreisesystem

secunet begleitet den Flughafen Zürich beim Einstieg in das EU-Entry/Exit-System (EES). Im Fokus stehen biometrische Erfassung, sichere Identitätsprüfung und die Integration komplexer IT-Systeme. Das Projekt zeigt, wie stark Grenz- und Luftsicherheit inzwischen von interoperablen Plattformen abhängt – und wie entscheidend IT-Kompetenz für den reibungslosen Betrieb geworden ist.

Strabag modernisiert Tunnelfunk am Semmering

Mit der Erneuerung der Tunnelfunkanlage der S6-Tunnelkette stärkt Strabag die Kommunikationsfähigkeit einer kritischen Verkehrsader. Ziel ist eine durchgängige, robuste Kommunikation für Einsatzkräfte und Betreiber. Das Projekt unterstreicht die Bedeutung belastbarer Funk- und Kommunikationssysteme für die Resilienz kritischer Infrastruktur – besonders im Ernstfall.

G DATA: Studie offenbart Sicherheitslücken im Mittelstand

Eine aktuelle Studie von G DATA CyberDefense zeigt erhebliche Defizite im Sicherheitsniveau vieler Unternehmen. Besonders kleine und mittlere Betriebe kämpfen mit Fachkräftemangel, begrenzten Budgets und fragmentierten Schutzkonzepten. Die Ergebnisse verstärken den Ruf nach praxistauglichen, skalierbaren Security-Lösungen, die Sicherheit auch unter knappen Ressourcen ermöglichen.

TeleTrusT-Umfeld: Digitale Souveränität wird Leitmotiv

Im Umfeld des Gipfels zur Europäischen Digitalen Souveränität positionieren sich Verbände und Unternehmen deutlich für europäische Sicherheitslösungen. Lieferkettensicherheit, Zertifizierung und Unabhängigkeit von außereuropäischen Anbietern prägen die Debatte. Sicherheit wird damit zunehmend als industrie- und standortpolitische Frage verstanden.

Monatsfazit für November

Der November 2025 bringt Sicherheit auf den Punkt der Entscheidung. Großprojekte in Luftfahrt, Verkehr und Grenzmanagement zeigen, was technisch möglich ist – Studien und Regulierung verdeutlichen, wo Nachholbedarf besteht. Digitale Souveränität, belastbare Infrastruktur und pragmatische Umsetzung werden zu den zentralen Leitplanken. Der Monat macht deutlich: Sicherheit ist kein Zukunftsthema mehr, sondern eine akute Handlungsaufgabe für Wirtschaft, Staat und Gesellschaft.

Wichtige Projekte des Monats



Zutrittskontrolle im Katastrophenmanagement

Die Titelstory zeigt, wie digitale Zutrittskontrolle Einsatz- und Evakuierungsprozesse im Krisenfall unterstützt. Berechtigungen lassen sich dynamisch anpassen, sensible Bereiche gezielt freigeben oder sperren. Herstellerlösungen entwickeln sich damit vom Verwaltungstool zum operativen Instrument für Behörden und KRITIS-Betreiber – besonders relevant bei Naturkatastrophen oder Großschadenslagen.

KI-gestützte Aufklärungsdrohnen – SYPAQ CorvoX

Mit der CorvoX-Drohne stellt SYPAQ ein KI-gestütztes System für Aufklärung und Lagebilderstellung vor. Wärmebildsensorik und autonome Funktionen ermöglichen Einsätze bei schlechter Sicht oder in gefährlichen Umgebungen. Das Projekt steht exemplarisch für den Übergang von experimentellen UAVs zu regulären Einsatzmitteln in Sicherheits- und Katastrophen szenarien.

Chronik 2025



NIS2 im Mittelstand – pragmatische Wege zur Umsetzung

Mehrere Beiträge widmen sich der praktischen Umsetzung von NIS2 in KMU. Vorgestellt werden abgestufte Sicherheitskonzepte, der Einsatz externer Dienstleister und pragmatische Risikobewertungen. Der Fokus liegt darauf, Regulierung handhabbar zu machen – durch das Zusammenspiel von Technik, Organisation und klaren Prioritäten.



NOVEMBER IM ÜBERBLICK

Wissenschaft & Forschung

Der November brachte Abschlussberichte und Ausblicke. Das Bundeslagebild Cybercrime 2025 des BKA offenbarte alarmierende Rekordzahlen: Cyber-Erpressungen (+30 %), CEO-Fraud-Betrügereien (+20 %) und eine Verdopplung illegaler Cyber-Marktplätze im Darknet. Die Ermittler fordern daher mehr High-Tech-Ausstat- tung und personelle Verstärkung.

Aus Forschungssicht wird unterstrichen, dass innovative KI-Analysetools den Strafverfolgungsbehörden helfen könnten, große Datenmengen (z.B. beschlagnahmte Chats) schneller zu sichten – entsprechende Pilotprojekte laufen bereits.

International sorgte ein Durchbruch im Quantencomputing für Aufsehen: Ein EU-Forschungsteam präsentierte Ende November einen Quanten-Chip mit 100 stabilen Qubits. Sicherheitsexperten beobachten dies genau, da ein leistungsfähiger Quantencomputer künftig gängige Verschlüsselung brechen könnte. Daher setzt die Forschung parallel auf Post-Quanten- Kryptografie – im November startete etwa ein BSI-gefördertes Projekt zur Erprobung quantensicherer VPN-Technik.
Der Wissenstransfer zwischen Kryptografie-Forschung und Praxis steht damit vor einem entscheidenden Kapitel.

Techniktrends

Im Zeichen der neuen Bundesregierung organisierte Bitkom Mitte November einen „Gipfel zur digitalen Souveränität Europas" in Berlin.

Dazu erschien eine Bitkom-Studie mit besorgniserregenden Zahlen: 9 von 10 deutschen Unternehmen sehen sich digital von Auslandstechnologien abhängig, nur 12 % könnten ohne US- oder China-IT länger als ein Jahr überleben.

Besonders die Abhängigkeit von den USA hat sich 2025 nochmals verstärkt – fühlten sich im Januar noch 41 % „stark abhängig" von US-Digitaldiensten, sind es im November bereits 51 %.

Bitkom-Präsident Ralf Wintergerst forderte daher auf dem Gipfel entschlosseneres Handeln: „Europa muss digitale Zukunft selbst in die Hand nehmen", etwa durch Förderung heimischer Cloud-, KI- und Halbleiter-Technologien.

Zudem begrüßte Bitkom die Initiative der Bundesregierung für ein eigenes Digitalministerium und lieferte prompt Vorschläge für dessen 100-Tage-Plan.

Insgesamt stand der November trendmäßig im Zeichen der Digitalen Souveränität: weniger Abhängigkeit, mehr eigene Innovationskraft – das wurde zum Leitmotiv zahlreicher Konferenzen und Publikationen.

Verbände

Der 11. Bayerische Sicherheitstag am 18./19. November in München setzte ein Ausrufezeichen für die Branche. Ausgerichtet vom BDSW und dem bayrischen Verband BVSW, diskutierten dort Sicherheitsprofis und Politiker (u.a. Innenminister Joachim Herrmann) über aktuelle Herausforderungen der Unternehmenssicherheit. Themen waren u.a. Wirtschaftsspionage, Sabotageschutz und neue Sicherheitslösungen in Zeiten interna- tionaler Krisen – passend zum Motto „Sicherheit neu denken". Verbandsintern drehte sich im November viel um Tarifpolitik: ver.di und BDSW starteten in mehreren Ländern (z.B. Hessen, NRW) Verhandlungsrunden über Lohnerhöhungen 2026. Während erste Gespräche teils ergebnislos blieben, appellierten Verbandsvertreter an die Verantwortung aller Seiten, eine Abwertung verantwortungsvoller Sicherheitsarbeit zu verhindern. Personell gab es einen Nachruf im BDSW: Der langjährige Vorsitzende des Fachausschusses Technik, Klaus Dirr, verstarb Anfang November im Alter von 87 Jahren. BDSW-Hauptgeschäftsführerin Cornelia Okpara würdigte ihn als herausragende Persönlichkeit, die die technische Entwicklung der Branche über Jahrzehnte geprägt hat. Dies zeigt: Die Sicherheitsbranche ehrt ihre Pioniere – und knüpft zugleich entschlossen an deren Lebenswerk an.

12/2025 Konsolidierung, Regulierung und die Architektur von Sicherheit 2026

Der Dezember 2025 markiert keinen Abschluss, sondern einen strategischen Übergang. Mit dem Inkrafttreten zentraler Gesetze, wichtigen Übernahmen und wegweisenden Studien verdichtet sich ein Bild: Sicherheit wird 2026 plattformbasiert, KI-gestützt und compliance-getrieben. Physische und digitale Sicherheit wachsen strukturell zusammen.

Cybersicherheitsrecht: NIS-2-Umsetzungsgesetz tritt in Kraft

Mit dem 5. Dezember wird NIS-2 in deutsches Recht überführt. Für tausende Unternehmen aus KRITIS, Industrie und Dienstleistung gelten nun verbindliche Mindeststandards für Risikomanagement, Meldepflichten und Governance. Cybersicherheit wird damit Vorstands- und Haftungsthema – mit direkten Auswirkungen auf physische Sicherheit, Zutritt, Leitstellen und Lieferketten.

Idesco Oy übernimmt Exilight Oy – Sicherheit trifft Notbeleuchtung

Mit der Übernahme von Exilight Oy erweitert Idesco sein Portfolio um Sicherheits- und Notbeleuchtungslösungen. Der Schritt zeigt, wie sich Sicherheitsarchitekturen zunehmend funktional verzahnen: Zutritt, Evakuierung, Licht und Orientierung werden als zusammenhängende Systeme gedacht – besonders relevant für öffentliche Gebäude und KRITIS.

Blickfeld wird Teil von Senstar – LiDAR-Sensorik strategisch gebündelt

Die Integration von Blickfeld in die Senstar Group unterstreicht den Trend zur Konsolidierung im Markt für 3D-Sensorik. LiDAR-Technologie gewinnt für Perimeterschutz, Logistik und kritische Infrastrukturen an Bedeutung – als präzise, wetterunabhängige Ergänzung klassischer Video- und Zaunsysteme.

Hanwha Vision stärkt Präsenz mit Experience Centre in Paris

Mit der Eröffnung eines Experience Centres in Paris investiert Hanwha Vision gezielt in Marktnähe und Partnerdialog. Demonstriert werden KI-basierte Videoanalyse, End-to-End-Architekturen und branchenspezifische Anwendungen. Hersteller setzen zunehmend auf Beratungskompetenz statt Produktverkauf.

Internationale Studien warnen: 2026 wird das Jahr der Fraudster

Mehrere Analysen – u. a. aus dem Umfeld von International SOS und Cybersecurity-Anbietern – prognostizieren für 2026 einen massiven Anstieg von KI-gestütztem Betrug, Identitätsmissbrauch und Social Engineering. Sicherheit verlagert sich damit verstärkt auf Identität, Kontextanalyse und organisationsweite Awareness.

Wichtige Projekte des Monats

Sicherheit optimal vernetzt – ASSA ABLOY und Kentix orchestrieren Sicherheit neu

Ein zentraler Dezember-Beitrag zeigt die strategische Integration von Kentix in das ASSA-ABLOY-Ökosystem. Zutritt, Brand-, Umwelt- und Netzwerküberwachung werden in einer einzigen Plattform gebündelt. Kentix bringt eine ausgereifte IoT-Architektur zur frühzeitigen Gefahrenerkennung ein, ASSA ABLOY ergänzt globale Reichweite und Erfahrung in hochsensiblen Umgebungen. Für Betreiber von Rechenzentren und kritischen Infrastrukturen entsteht ein skalierbares, compliance-fähiges Sicherheitsökosystem, das Komplexität reduziert und Reaktionsfähigkeit erhöht.

Digitale Identität und Authentifizierung – AllKey Ultra FIDO

Mit AllKey Ultra FIDO, vorgestellt von FPC und jNet Secure, rückt hardwarebasierte, phishing-resistente Authentifizierung in den Fokus. Das Projekt adressiert Unternehmen, die Identität als zentrales Sicherheitselement etablieren wollen – insbesondere im Zusammenspiel von IT-, Cloud- und physischem Zutritt.

Flughäfen und Verkehr – Sicherheit im Dauerbetrieb

Mehrere Dezember-Projekte unterstreichen die Relevanz kritischer Verkehrsinfrastruktur:

- BER: KÖTTER Aviation Security gewinnt eine zentrale Ausschreibung.
- Riyadh Airport: größtes Modernisierungsprojekt seit über 40 Jahren.
- Deutsche Bahn & Bundespolizei: 25 Jahre Sicherheitspartnerschaft.

Gemeinsam zeigen sie: Verkehrssicherheit basiert auf langfristigen Partnerschaften, integrierter Technik und belastbaren Prozessen.

Markt & Strategie: Cloud, Compliance und KI

Wie Verkada die Sicherheitsbranche in Europa neu definiert

Ein vielbeachteter Dezember-Artikel analysiert die marktstrategische Rolle von Verkada. Im Gespräch mit Filip Kaliszan wird deutlich, wie Cloud-Architekturen, regulatorische Anforderungen und KI zusammenwirken.

Verkada positioniert sich als Plattformanbieter, der Compliance vereinfacht, Sicherheitsdaten operationalisiert und Skalierung ermöglicht. Der Beitrag steht exemplarisch für den Wandel von Hardware-Denken zu Security-as-a-Platform.

Genetec Report: Was bedeutet physische Sicherheit 2026?

Der Genetec-Report zur Lage der physischen Sicherheit 2026 basiert auf 7.368 Befragten weltweit und zählt zu den umfassendsten Studien der Branche. Die zentralen Erkenntnisse sind:

- KI verändert Planung, Betrieb und Auswertung physischer Sicherheit
- Sicherheitsdaten werden zur Management-Entscheidungsgrundlage
- Integration schlägt Insellösunge

Der Report macht klar: Physische Sicherheit wird strategisch, datengetrieben und vorausschauend.

Salto: 25 Jahre Zutrittsinnovation

Seit 2000 revolutioniert Salto den Zutritt. Das Ziel: Vom Start-up zum Technologieführer mit einem offenen, intelligenten Zutrittsökosystem. Das Jubiläum steht für kontinuierliche Innovation, Plattformdenken und zeigt Saltos Rolle als Enabler für alle Lösungen.

DEZEMBER IM ÜBERBLICK

Wissenschaft & Forschung

Zum Jahresausklang flossen nochmals enorme Mittel in die Sicherheitsforschung: Die Bundesregierung verabschiedete im Dezember ein Sonderprogramm über 50 Mio. €, um KI-Anwendungen für die Innere Sicherheit voranzubringen – von automatisierter Videoüberwachung bis Analyse-Software gegen Kindesmissbrauch im Netz. Fachleute begrüßen dies als wichtiges Signal.

Derweil lieferte die europäische Initiative „INTEL" erste Daten: Dieser vom europäischen Dachverband CoESS gestartete Branchen-Intelligenztest befragte Sicherheitsunternehmen EU-weit zu Trends und Bedarf. Ergebnis: Der Personalbedarf wächst, doch mangelt es oft an qualifizierten Fachkräften mit digitalen Skills. 87 % der Firmen klagen, nicht genug geeignetes Sicherheitspersonal zu finden – vor allem IT-Expertise in der Sicherheitswirtschaft wird zur Mangelware. Diese Erkenntnisse fließen 2026 in neue Ausbildungs- und Recruiting-Konzepte.

Insgesamt zeigte der Dezember: Forschung, Politik und Verbände bündeln die Erkenntnisse des Jahres, um mit frischen Projekten und Fördergeldern ins nächste Jahr zu starten – getreu dem Motto, Innovation und Sicherheit Hand in Hand zu stärken.

Techniktrend

Der Digitalverband zog im Dezember ein gemischtes Fazit für 2025: Trotz rezessiver Tendenzen blieb die Digitalbranche Wachstumsstütze (+4,6 % Umsatz)[89], und die Zahl der ITK-Beschäftigten erreichte mit rund 1,37 Mio. ein Allzeithoch.

Sorgen bereitet aber der anhaltende IT-Fachkräftemangel, der laut Bitkom-Schätzung über 100.000 unbesetzte Stellen umfasst. Bitkom forderte daher von der neuen Regierung eine beschleunigte Umsetzung des Fachkräfteeinwanderungsgesetzes und Investitionen in digitale Bildung.

Trendthema im Dezember war zudem Green IT: Erstmals veröffentlichten Bitkom und Umweltbundesamt einen Leitfaden, wie Rechenzentren klimafreundlicher betrieben werden können (Abwärmenutzung, Ökostrom, effizientere Kühlung).

Und passend zur Weihnachtszeit ein Blick auf den Online-Handel: 2025 setzte der E-Commerce in Deutschland geschätzt über 120 Mrd. € um – ein Rekord. Bitkom verwies aber auf gestiegene Cyberrisiken im Weihnachtsgeschäft (Stichwort: Phishing bei Online-Shops) und riet Verbrauchern zu besonderen Vorsichtsmaßnahmen.

Bitkom-Zahlen zeigen: Fast 50 % der Deutschen nutzen Smart-Home-Technologien, Unternehmen setzen verstärkt auf Cloud-Absicherung und Datenperimeter. Sicherheit verlagert sich zunehmend in vernetzte, hybride Architekturen – mit steigenden Anforderungen an Transparenz und Kontrolle.

Insgesamt verabschiedete sich 2025 mit dem Appell: Digitalisierung nachhaltig und sicher gestalten – eine zentrale Aufgabe für 2026.

Verbände

Im Dezember zeigte sich die Sicherheitsbranche noch einmal geeint und zukunftsorientiert. Auf der BDSW-Jahresabschlusspressekonferenz am 9. Dezember betonte Präsident Werner Landstorfer, die Branche stehe vor großen Herausforderungen – vom Personalengpass bis zur Digitalisierung – sehe aber optimistisch ins neue Jahr. Europaweit rücken die Sicherheitsverbände enger zusammen: Im Rahmen des EU-Projekts „INTEL" startete eine Online-Branchenbefragung, um Trends und Bedarfe für Aus- und Weiterbildung zu identifizieren[87]. Landstorfer rief die deutschen Mitgliedsfirmen zur aktiven Teilnahme auf.

Daneben gab es im Dezember Grund zu feiern: Mehrere Traditionsfirmen der Sicherheitswirtschaft begingen runde Jubiläen (z.B. 120 Jahre KÖTTER im Revier), was in Verbandskreisen gewürdigt wurde.

Personell standen Ehrungen im Fokus: Zahlreiche verdiente Branchenpersönlichkeiten – vom Werkschutzleiter bis zur Verbandssekretärin – erhielten zum Jahresende Auszeichnungen für ihr Engagement. Damit endet 2025 in der Sicherheitsbranche feierlich, aber nicht selbstzufrieden: Man hat die Weichen gestellt, um auch 2026 Innovation, Professionalität und Zusammenhalt in der Sicherheitswirtschaft voranzutreiben.



Globale Markt für Videoüberwachung 2025-2030

Technologie, Geopolitik und neue Geschäftsmodelle formen eine Branche im Wandel

Die Videoüberwachungsbranche erlebt derzeit einen der tiefgreifendsten Umbrüche ihrer Geschichte. Längst geht es nicht mehr nur um das Installieren von Kameras zur reinen Aufzeichnung – Videoüberwachung entwickelt sich zu einem strategischen Baustein moderner Sicherheits- und Infrastrukturökosysteme. Künstliche Intelligenz und Edge Computing ermöglichen völlig neue Anwendungsfelder, während geopolitische Spannungen Lieferketten, Marktanteile und regulatorische Rahmenbedingungen neu ordnen. Gleichzeitig steigt die Nachfrage nach Software- und Cloudlösungen rapide, und Drohnen erweitern bislang starre Architekturen um mobile, dynamische Sensorik.

In diesem Umfeld ist verlässliche, faktenbasierte Marktintelligenz unabdingbar. Der neue Bericht „The Global Video Surveillance Business 2025 to 2030" bietet eine detaillierte, tiefgehende Analyse aller relevanten Entwicklungen – und liefert damit genau die strategische Orientierung, die Hersteller, Integratoren, Sicherheitsverantwortliche und Investoren heute benötigen. Der Bericht bietet eine umfassende Untersuchung des globalen Videoüberwachungsmarktes und beleuchtet sowohl die aktuelle Situation als auch die zu erwartenden Entwicklungen bis zum Jahr 2030.

Im Mittelpunkt stehen die Umsatz- und Wachstumspotenziale der vier zentralen Marktsegmente: Kamerahardware, Video- und Cloudspeicher, Softwarelösungen sowie Analyse- und KI-Plattformen. Dabei wird detailliert aufgezeigt, wie sich die einzelnen Bereiche entwickeln, welche technologischen Trends ihre Dynamik bestimmen und wie sich die wachsende Bedeutung von Software und KI-basierten Auswertungen auf Geschäftsmodelle und Marktstrukturen auswirkt.
Ein Schwerpunkt liegt auf der technologischen Transformation durch künstliche Intelligenz und Edge Computing. Der Bericht beschreibt, wie ein signifikanter Anteil der 2025 ausgelieferten Kameras bereits KI-Funktionen wie Objekterkennung, Verhaltensanalyse, Kennzeichenerkennung oder datenschutzkonforme Verpixelung direkt im Gerät ermöglicht. Diese Entwicklung verschiebt die Rolle der Videoüberwachung grundlegend – vom reaktiven Aufzeichnungssystem hin zu aktiven, intelligenten Anwendungen, die operative Prozesse optimieren, Risiken frühzeitig erkennen und datenbasierte Entscheidungen unterstützen. Gleichzeitig wird analysiert, wie Hersteller die Balance zwischen lokaler KI-Verarbeitung und Cloud-Analyse planen und in welchen Anwendungsfeldern der größte Nutzen entsteht.

Darüber hinaus beleuchtet der Bericht die zunehmende Rolle von Drohnen als Erweiterung klassischer Überwachungssysteme. Drohnen ermöglichen flexible, großflächige Überwachung, unterstützen Einsatzkräfte bei schnellen Reaktionen und ergänzen stationäre Kameras in Arealen, die bisher nur schwer oder mit sehr hohem Aufwand zu überwachen waren. Die Integration von Drohnen in Leitstellen und Real-Time Crime Center eröffnet völlig neue architektonische Möglichkeiten für mobile Sensornetzwerke und stellt eine der wichtigsten Entwicklungen im Bereich der physischen Sicherheit dar.

Einen besonderen Stellenwert erhält die Analyse der geopolitischen Einflüsse. Die anhaltenden Spannungen zwischen China und westlichen Staaten führen zu tiefgreifenden Veränderungen in der Wettbewerbslandschaft. US-Beschaffungsverbote, FCC-Restriktionen und verschärfte Exportkontrollen beeinflussen die Marktposition zahlreicher Anbieter, schaffen neue Chancen für NDAA-konforme Lösungen und verlagern Marktanteile in wesentlichen Regionen. Der Bericht zeigt, wie diese Faktoren Marktstrukturen, Lieferketten und Produktstrategien nachhaltig verändern.
Ergänzend untersucht der Report die weltweite Entwicklung von M&A-Aktivitäten und Investitionen. Zwischen 2023 und 2025 wurden zahlreiche Übernahmen und Finanzierungsrunden abgeschlossen, die auf eine klare Tendenz zur Plattformkonsolidierung und zur Stärkung softwarebasierter Geschäftsmodelle hinweisen. Besonders hohes Kapital fließt in Unternehmen aus den Bereichen KI, Computer Vision und Datenschutztechnologien – ein Indikator für die strategische Bedeutung dieser Segmente.

Mit insgesamt 246 Seiten und 18 Grafiken liefert der Bericht eine tiefgehende, datenbasierte Darstellung der Marktgröße, der Segmententwicklung und der technologischen Trends. Prognosen bis zum Jahr 2030 zeigen auf, wie sich Umsätze, Marktanteile und Technologieadoption entwickeln werden und welche Regionen sowie Branchen die größten Wachstumschancen bieten. Der Bericht ist damit ein unverzichtbares Arbeitsinstrument für strategische Planung, Wettbewerbsanalyse, Investitionsbewertung und technologische Roadmaps.

Infobox: Kauf des Reports

Titel: The Global Video Surveillance Business 2025 to 2030

Umfang: 246 Seiten, 18 Grafiken

Inhalt: Marktanalyse für Kameras, Speicher, Software, Analytics; Prognosen bis 2030; Technologie- und Wettbewerbsanalyse; M&A- und Investmenttrends; geopolitische Auswirkungen

Format: Digital (Enterprise License)

Preis: 3.000 USD – unternehmensweite Nutzung enthalten

Erscheinung: Teil 1 der Studie zur Physical-Security-Technologie (Teil 2 „Access Control Systems" erscheint Q4 2025)

Bestellung: memoori.com/portfolio/global-video-surveillance-business-2025-2030/

Sicherheitsmessen 2026 Rund um die Welt

Trends, Technologien und Treffpunkte der globalen Sicherheitsbranche

Das Jahr 2026 verspricht ein hochkarätiges Messejahr für die Sicherheitsbranche zu werden. Von physischen Zutrittslösungen über Cybersecurity und Smart-Building-Technologien bis hin zu Katastrophenschutz und künstlicher Intelligenz im Sicherheitsumfeld – weltweit werden neue Standards gesetzt. Der folgende Überblick zeigt die wichtigsten sicherheitsrelevanten Fachmessen 2026, gegliedert nach thematischen Schwerpunkten und Branchentrends.

1. Jahresauftakt mit Fokus auf Digitalisierung, Smart Buildings und Zutrittssysteme

Bereits im Januar startet das Messejahr mit einem starken Innovationsschub. Die International CES (06.–09.01., Las Vegas) setzt den Ton mit neuesten Entwicklungen in Künstlicher Intelligenz, vernetzter Gebäudetechnik und digitaler Sicherheit.

Parallel rückt im Nahen Osten die Intersec (12.–14.01., Dubai) als führende Plattform für Sicherheit, Brandschutz und Cybersecurity die integrierte Sicherheit in den Mittelpunkt. Zeitgleich findet in Dubai auch die Light + Intelligent Building Middle East statt, die Smart-Building-Lösungen mit Sicherheits- und Energiemanagementsystemen kombiniert.

Mit der Polyclose (14.–16.01., Gent) folgt in Europa eine Fachmesse, die physische Sicherheitsaspekte wie Zutrittstechnik, Türen- und Fenstersysteme sowie Fassadenschutz adressiert – Themen, die zunehmend mit digitaler Zutrittssteuerung und IoT-Lösungen verschmelzen.

2. Frühjahrsphase: Vernetzung, Mobilität und Schutzinfrastruktur

Im Februar und März dominieren europäische Sicherheitsmessen. Die Enforce Tac (23.–25.02., Nürnberg) fokussiert sich auf behördliche Sicherheit, Verteidigung und Einsatztechnik. Parallel bietet die Sicur (24.–27.02., Madrid) eine breite Plattform für Brandschutz, Arbeitsschutz und Sicherheitstechnik.
Im März nimmt das Thema „Smart Mobility & Critical Infrastructure" Fahrt auf. Die Light + Building (08.–13.03., Frankfurt) setzt Maßstäbe in integrierter Gebäudesicherheit und nachhaltiger Energieeffizienz. Ergänzend thematisieren IT-TRANS (03.–05.03., Karlsruhe) und INTERTRAFFIC (10.–13.03., Amsterdam) die Sicherheit im öffentlichen Verkehr und in der urbanen Mobilität.

Die Tokyo Security Show (03.–06.03.) gilt als Asiens Leitmesse für elektronische Sicherheitslösungen, während die Robotics, Automation and Drones (11.–13.03., Odense) zeigt, wie autonome Systeme die Sicherheit in Industrie und öffentlichem Raum revolutionieren.

3. Frühling: Cybersecurity, nationale Resilienz und Industrie 4.0

Zwischen April und Mai rücken digitale Sicherheit, kritische Infrastrukturen und industrielle Resilienz in den Vordergrund. Die IN CYBER Le Forum (31.03.–02.04., Lille) und die INFOSECURITY Europe (02.–04.04., London) setzen Trends in der IT- und Netzwerksicherheit.

Im industriellen Bereich verbindet die HANNOVER MESSE (20.–24.04.) Automatisierung, KI und OT-Security zu einem ganzheitlichen Zukunftsbild vernetzter Produktion. Zeitgleich zeigen Securex und SAWO (14.–16.04., Pozna) sowie die Secutech (22.–24.04., Taipeh) neue Ansätze für physische und digitale Sicherheit im Unternehmensumfeld.

Die globale Dimension der Sicherheitswirtschaft spiegelt sich Ende April in Veranstaltungen wie der Milipol Asia-Pacific (28.–30.04., Singapur), The Security Event (Birmingham) und der INFOPOL XPO112 (Kortrijk) wider, die Polizei-, Katastrophen- und Krisenmanagement-Themen bündeln.

4. Frühsommer: Feuerwehr, Bevölkerungsschutz und ganzheitliche Sicherheitsstrategien

Der Juni 2026 steht im Zeichen von Einsatzorganisationen und Gefahrenabwehr. Die INTERSCHUTZ (01.–06.06., Hannover) – Weltleitmesse für Feuerwehr, Rettungswesen und Bevölkerungsschutz – wird zum globalen Treffpunkt für Notfall- und



Fotograf: Schuchrat Kurbanov/©MESSE ESSEN GmbH

Sicherheitsmanagement. Ergänzend zeigen die SECUREX South Africa (02.–04.06., Johannesburg) und die FeuerTrutz (24.–25.06., Nürnberg) aktuelle Entwicklungen im Brandschutz und in der Gefahrenprävention.

Auch Cybersicherheit bleibt präsent: die Cybersec Europe (20.–21.05., Brüssel) und Cybersec Netherlands (09.–10.09., Utrecht) vernetzen europäische Experten zu Themen wie Cloud-Security, digitale Souveränität und Resilienz im öffentlichen Sektor.

5. Herbst: Ganzheitliche Sicherheit, KI und Smart Cities

Im Herbst verschiebt sich der Fokus auf ganzheitliche Sicherheitskonzepte, Smart Cities und KI-gestützte Systeme. Die security essen (22.–25.09., Essen) markiert als Leitmesse das Highlight des Jahres im Bereich integrierter Sicherheitslösungen – von Videoüberwachung über Zutrittskontrolle bis hin zu Cyber-Physical-Security. Parallel thematisieren DroneX (29.–30.09., London) und die International Security Expo (London) den Einsatz unbemannter Systeme und hybrider Sicherheitsstrategien.

Der Oktober und November stehen im Zeichen der globalen Zusammenarbeit. Die Milipol Qatar (20.–22.10.), die SKYDD (Stockholm) und die EXPOPROTECTION (03.–05.11., Paris) bringen Entscheidungsträger aus Behörden, Industrie und Forschung zusammen, um Lösungen für Sicherheitsherausforderungen in urbanen, industriellen und nationalen Kontexten zu präsentieren.
Ein visionärer Abschluss bildet der Smart City Expo World Congress (November, Barcelona), der Sicherheit als integralen Bestandteil urbaner Zukunftsstrategien behandelt – von Daten- und Netzwerkschutz bis zu Resilienz im Stadtraum.

Fazit: Sicherheit wird vernetzter, digitaler und nachhaltiger

Das Messejahr 2026 verdeutlicht, dass Sicherheit längst kein isoliertes Thema mehr ist, sondern Querschnittsfunktion moderner Gesellschaften und Wirtschaftssys-teme. Die Grenzen zwischen physischer und digitaler Sicherheit verschwimmen zunehmend. Künstliche Intelligenz, vernetzte Gebäudetechnik, Cloud-basierte Zutrittssysteme und Resilienzstrategien prägen die Agenda. Ob Intersec in Dubai, security essen in Deutschland oder INTERSCHUTZ in Hannover – die globalen Sicherheitsmessen 2026 zeigen eine klare Entwicklung: Sicherheit wird integrativ gedacht, intelligent gesteuert und nachhaltig umgesetzt.

Eine übersichtliche Tabelle aller sicherheitsrelevanten Messen 2026, sortiert nach Datum und mit Angabe von Ort, Land und thematischem Schwerpunkt:

Messetermine

INTERNATIONAL CES

06–09 Jan 2026
Las Vegas, USA
www.ces.tech
Elektronik, Smart Home, Digitale Sicherheit

INTERSEC

12–14 Jan 2026
Dubai, VAE
www./intersec.ae.messefrankfurt.com
Sicherheit, Brandschutz, Cybersecurity

LIGHT + INTELLIGENT BUILDING ME

12–14 Jan 2026
Dubai, VAE
www.light-middle-east.ae.messefrankfurt.com/dubai/en.html
Intelligente Gebäude, Gebäudeautomation, Sicherheit

POLYCLOSE

14–16 Jan 2026
Gent, Belgien
www.polyclose.be
Zutrittssysteme, Fassaden, Türen & Fenster

EUROCIS

22–26 Feb 2026
Düsseldorf, Deutschland
www.eurocis-tradefair.com
Einzelhandelstechnologie, Datenschutz, Zahlungssicherheit

ENFORCE TAC

23–25 Feb 2026
Nürnberg, Deutschland
www.enforcetac.com
Polizei, Verteidigung, Taktische Ausrüstung

SICUR

24–27 Feb 2026
Madrid, Spanien
www.ifema.es/en/sicur
Brandschutz, Arbeitssicherheit, Sicherheitstechnik

BAUPLUS

28 Feb–01 Mär 2026
Biberach, Deutschland
www.bauplus.de
Gebäudesicherheit, Bautechnik

IT-TRANS

03–05 Mär 2026
Karlsruhe, Deutschland
www..it-trans.org
Öffentlicher Verkehr, Intelligente Mobilität

TOKYO SECURITY SHOW

03–06 Mär 2026
Tokio, Japan
www.tokyosecurityshow.com
Elektronische Sicherheit, Überwachung

LIGHT + BUILDING

08–13 Mär 2026
Frankfurt, Deutschland
www.light-building.com
Beleuchtung, Gebäudetechnik, Energieeffizienz

INTERTRAFFIC

10–13 Mär 2026
Amsterdam, Niederlande
www.intertraffic.com
Verkehrssicherheit, Mobilität, Infrastruktur

ROBOTICS, AUTOMATION&DRONES

11–13 Mär 2026
Odense, Dänemark
www.robotics-expo.com
Robotik, Automatisierung, Drohnensicherheit

PASSENGER TERMINAL EXPO

17–19 Mär 2026
London, Großbritannien
www.passengerterminal-expo.com
Flughafensicherheit, Passagiersicherheit

ISC WEST

23–27 Mär 2026
Las Vegas, USA

www.iscwest.com
Zutrittskontrolle, Videoüberwachung, KI-Sicherheit

FENSTERBAU FRONTALE

FENSTERBAU FRONTALE + HOLZ-HANDWERK

24–27 Mär 2026
Nürnberg, Deutschland
www.fensterbau-frontale.de
Gebäudeschutz, Türen- und Fenstersysteme

SVB CONSTRUCTION FAIR

25–28 Mär 2026
Brünn, Tschechien
www.svb.cz
Bautechnik, Baustellensicherheit

AMBIENTE LAVORO

26–28 Mär 2026
Bologna, Italien
www.ambiente-lavoro.com
Arbeitsschutz, Gesundheit am Arbeitsplatz

IN CYBER LE FORUM

31 Mär–02 Apr 2026
Lille, Frankreich
www.incyberforum.com
Cybersecurity, Digitale Resilienz

Infosecurity Europe

INFOSECURITY EUROPE

02–04 Apr 2026
London, Großbritannien
www.infosecurityeurope.com
IT-Sicherheit, Datenschutz, Netzwerkschutz

SAWO

SAWO

14–16 Apr 2026
Posen, Polen
www.sawo.pl
Arbeitssicherheit, Rettungsdienste

securex

SECUREX

14–16 Apr 2026
Posen, Polen
www.securex.pl
Physische Sicherheit, Videoüberwachung

HANNOVER MESSE

HANNOVER MESSE

20–24 Apr 2026
Hannover, Deutschland
www.hannovermesse.de
Industrie 4.0, OT-Sicherheit, Automation

MOUNTAIN PLANET

21–23 Apr 2026
Grenoble, Frankreich
www.mountain-planet.com
Bergsicherheit, Infrastruktur & Ausrüstung

secutech TAIWAN

SECUTECH

22–24 Apr 2026
Taipeh, Taiwan
www.secutech.com2
Videoüberwachung, IoT, Smart City-Sicherheit

INFOPOL XPO112

INFOPOL XPO112

28–30 Apr 2026
Kortrijk, Belgien
www.infopol.be
Polizei-, Feuerwehr- & Rettungsausrüstung

MILIPOL ASIA-PACIFIC

28–30 Apr 2026
Singapur, Singapur
www.milipolasiapacific.com
Heimatschutz, Terrorismusbekämpfung

THE SECURITY EVENT

THE SECURITY EVENT

28–30 Apr 2026
Birmingham, Großbritannien
www.thesecurityevent.co.uk
Zutrittskontrolle, KI, Videoüberwachung

GISEC GLOBAL

05–07 Mai 2026
Dubai, VAE
www.gisecexpo.com
Cybersecurity, Cloud & Netzwerkschutz

Messetermine

BUILD 4 ASIA

06–07 Mai 2026
Hongkong, China (HK)
www.build4asia.com
Intelligente Gebäude, Sicherheit, Elektrosysteme

AIRPORT SHOW

12–14 Mai 2026
Dubai, VAE
www.theairportshow.com
Flughafensicherheit, Passagiersysteme

ISNR

19–21 Mai 2026
Abu Dhabi, VAE
www.isnrabudhabi.com
Nationale Resilienz, Krisenmanagement

GPEC

20–22 Mai 2026
Leipzig, Deutschland
www.gpec.de
Polizei, Taktische & Sicherheitsausrüstung

CYBERSEC EUROPE

20–21 Mai 2026
Brüssel, Belgien
www.cybersecforum.eu
IT-Sicherheit, Datenschutz

ARBEITSSCHUTZ SCHWEIZ

20–21 Mai 2026
Zürich, Schweiz
www.workplacesafety.ch
Arbeitsschutz, Gesundheit & Sicherheit am Arbeitsplatz

INTERSCHUTZ

01–06 Jun 2026
Hannover, Deutschland
www.interschutz.de
Feuerwehr, Bevölkerungsschutz, Rettungsdienste

SECUREX SOUTH AFRICA

02–04 Jun 2026
Johannesburg, Südafrika
www.securex.co.za
Brandschutz, Zutrittskontrolle, Videoüberwachung

SENSOR+TEST

09–11 Jun 2026
Nürnberg, Deutschland
www.sensor-test.de
Sensorik, Messtechnik, Sicherheitslösungen

THE SMARTER E EUROPE

23–25 Jun 2026
München, Deutschland
www.thesmartereurope.com
Energiesysteme, Smart Grids, Sicherheit

FEUERTRUTZ

24–25 Jun 2026
Nürnberg, Deutschland
www.feuertrutz-messe.de
Vorbeugender Brandschutz

SICHERHEITSEXPO

01–02 Jul 2026
München, Deutschland
www.sicherheitsexpo.de
Zutrittskontrolle, Sicherheitstechnik

FORENSICS EUROPE EXPO

01–02 Jul 2026
London, Großbritannien
www.forensicseuropeexpo.com
Forensik, Tatortuntersuchung

SMM

01–04 Sep 2026
Hamburg, Deutschland
www.smm-hamburg.com
Maritime Sicherheit, Schiffstechnik

IFA

04–08 Sep 2026
Berlin, Deutschland
www.ifa-berlin.com
Unterhaltungselektronik, Smart Living

CYBERSEC NETHERLANDS

09–10 Sep 2026
Utrecht, Niederlande
www.cybersec-netherlands.com
Cybersecurity, Cloud-Sicherheit

EMERGENCY SERVICES SHOW

16–17 Sep 2026
Birmingham, Großbritannien
www.emergencyuk.com
Rettungsdienste, Krisenmanagement

SECURITY ESSEN

22–25 Sep 2026
Essen, Deutschland
www.security-essen.de
Leitmesse für Sicherheit & Schutz

INNOTRANS

22–25 Sep 2026
Berlin, Deutschland
www.innotrans.de
Verkehrstechnik, Mobilitätssicherheit

DRONEX

29–30 Sep 2026
London, Großbritannien
www.dronexevent.com
Drohnensicherheit, Luftüberwachung

INTERNATIONAL SECURITY EXPO

29–30 Sep 2026
London, Großbritannien
www.internationalsecurityexpo.com
Integrierte Sicherheitslösungen

MILIPOL QATAR

20–22 Okt 2026
Doha, Katar
www.milipol.com
Heimatschutz, Polizeitechnologie

SKYDD

20–22 Okt 2026
Stockholm, Schweden
www.skydd.se
Schutzsysteme, Sicherheitstechnik

ARBEITSSCHUTZ AKTUELL

20–22 Okt 2026
Stuttgart, Deutschland
www.arbeitsschutz-aktuell.de
Arbeitsschutz, Gesundheit & Sicherheit am Arbeitsplatz

IT-SA EXPO & CONGRESS

27–29 Okt 2026
Nürnberg, Deutschland
www.it-sa.de
IT-Sicherheit, Cloud, Datenschutz

SMART CITY EXPO WORLD

03-05 Nov 2026
Barcelona, Spanien
www.smartcityexpo.com
Smart Cities, urbane Sicherheit, Digitalisierung

EXPOPROTECTION

03–05 Nov 2026
Paris, Frankreich
www.expoprotection.com
Risiko-, Sicherheits- & Schutzmanagement

LIGHT + INTELLIGENT BUILDING

19–21 Nov 2026
Istanbul, Türkei
www.light-building.com
Intelligente Gebäude, Beleuchtung, Sicherheit

PMREXPO

24-26 Nov 2026
Köln, Deutschland
www.pmrexpo.de
Kritische Kommunikation, Leitstellen

VDS-BRANDSCHUTZTAGE

02–03 Dez 2026
Köln, Deutschland
www.vds.de
Brandschutz, Risikoprävention

Allianz



Sebastian/ Adobe Stock

ALLIANZ COMMERCIAL

Trendreport 2025 zu politischer Gewalt und zivilen Unruhen

Download unter tinyurl.com/n8x2mwt2