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, Avi-



lus 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.

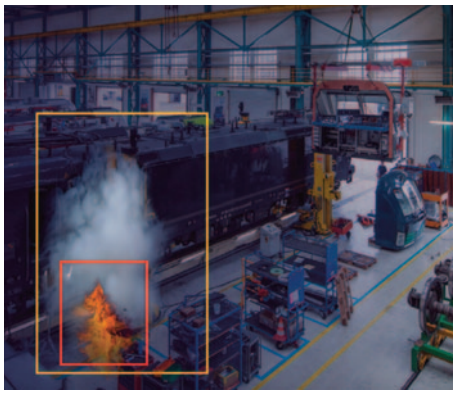
Goaco und Thales demokratisieren Identitätsprüfung

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

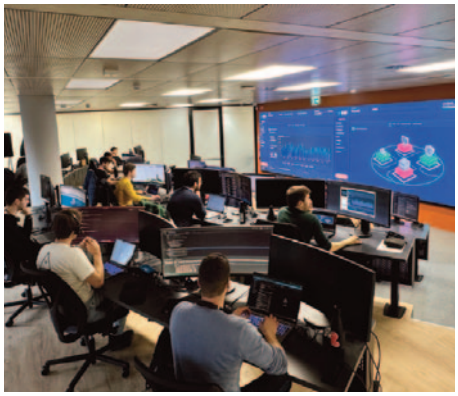
Mit der CorvoX-Drohne stellt SYPAQ ein KI-gestütztes System für Aufklärung und Lagebilderstellung vor. Wärmebildsensorik und autonome Funktionen ermöglichen Einsätze bei schlechter Sicht oder in gefährlichen Umgebungen. Das Projekt steht exemplarisch für den Übergang von experimentellen UAVs zu regulären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