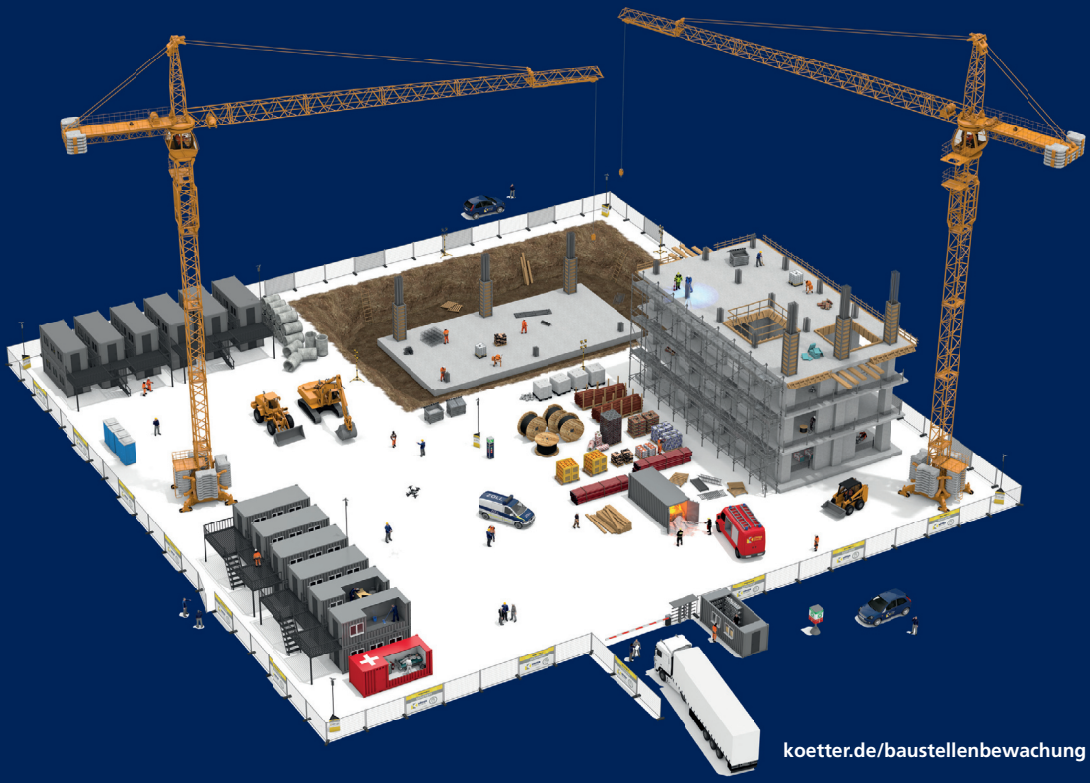
# EURO SECURITY

Das deutsche Fachmagazin für Sicherheit und Management in der DACH Region

## Security und Service für Baustellen



koetter.de/baustellenbewachung

- **Perimeter Protection**
  Ausblicke für das Jahr 2023 - Technologien und Schwerpunkte
- **PMRExpo 2022**
  Neue Lösungen für Kommunikationslösungen im KRITIS-Bereich
- **Einzelhandel**
  EuroShop Düsseldorf - EHI Retail Institute: Metaverse im Handel

ISSN 09481249 • 12-2022 • ZKZ 16724 Postvertriebsstück bezahlt • 80383 BAY Germany ©SEC Global • euro-security.de

# Inhalt


**Inhaltsangabe** 2
**Impressum** 3
**Editorial** 4

## COVERSTORY

**Alles aus einer Hand** 6

## INFOPAGES

**ASSA ABLOY: Video & eBook** 54
Wie die Wohnungswirtschaft von moderner Sicherheitstechnik profitiert
**Termine** 54
VdS Fachtagungen (1. Halbjahr 2023) und BHE (1. Ql 2023)
**BVSW** 55
Eventankündigung: Audi Driving Experience in Seefeld

## INTERNET-SICHERHEIT

**Bitdefender** 48
10 Beiträge für sichereres Internet der Dinge

## INTERVIEW

**Standards als Trendsetter für die Sicherheitsbranche** 21
Standards by OSS im Gespräch mit Herstellern und Anwendern

## GEBÄUDETECHNIK

**ASSA ABLOY Opening Solutions** 70

Openings Studio-Software rationalisiert den Spezifikationsprozess für ein Luxusprojekt in Dubai
**dormakaba** 71
VAMED vertraut bei der Wartung ihrer Tür- und Toranlagen auf dormakaba: Zugangslösungen für einen reibungslosen Betriebsablauf
**ASSA ABLOY** 80
Segelclub in Finnland vertraut auf PULSE

## MARKTBERICHTE

**G Data** 51
Deutschland: IT-Sicherheitsgefühl hat abgenommen: Studie „Cybersicherheit in Zahlen" offenbart großen Mangel an IT-Sicherheitsfachleuten
**Genetec** 74
Umfrage zur Lage der physischen Sicherheit 2022

## MARTKTTRENDS

**Nach Wachstum 2022 wird es im Jahr 2023 ein wenig ruckelig** 16
**Retarus** 18
Business-Kommunikation: Fünf Trends für 2023
**Thales** 25
Cybersecurity Trends 2023
**Sharp Europe** 27
Was sind die Vorhersagen und Trends für den IT-Dienstleistungssektor im Jahr 2023?
**BSI: Die Laage der IT-Sicherheit in Deutschland 2022** 29

## IT-TRENDS

**Cisco** 30
Security, Netzwerk, Nachhaltigkeit Tech-Trends 2023 - Sieben Trends für das neue Jahr
**Bauindustrie** 32
Wie Digitalisierung und Nachhaltigkeit die Bauwirtschaft der Zukunft prägen: Sieben Trends
**Sieben Experten** 36
2023 mit neuen Cyber-Bedrohungen und -Herausforderungen

## MESSEN/EVENTS

**EuroShop 2023** 20

## PERIMETER PROTECTION

**Videosysteme** 10
Messefeature: So bleibt der Perimeterschutz im Blick
**Drohnen** 11

Messefeature: Gefahr aus der Luft

**Perimeter Protection im Jahr 2022** 13
**Welche Technologien prägen die Perimetersicherheit?** 14
**Faktoren für eine effiziente Videotechnik im Rahmen der Perimeter Sicherheit** 15



euro-security.tv EURO SECURITY euro-security.de

# Inhalt


## PMR EXPO

**Mehr Funktionalität für BWV-Lösung** 50

Qognify VMS 7.2 unterstützt den Ermittlungsprozess und fügt Cloud-Funktionen hinzu

**Frequentis** 52

Integrierte Leitstelle Saarland

**Sepura** 53

500.000stes TETRA-Funkgerät in Deutschland in Betrieb genommen

**Johnson Controls** 60

Brandschutz- und Sicherheitslösungen für Gebäude

**Motorola Solutions** 62

Einsatzkräfte erhalten neue sicherheitskritische Applikationen

**Airbus** 64

Was ist Tactilon Agnet?

Download Datenblatt für Tactilon Agnet 900

**securelandcommunications** 65

Samsung arbeitet mit Airbus an einem Smartphone mit integrierter Tactilon Agnet-Lösung

**Hexagon unterstützt Smart-City-Umbau in Brasilien** 66

**Was ist HxGN OnCall Dispatch?** 67

Die Einsatzleitsoftware für Notfall- und Katastrophenmanagement

## SICHERHEIT IM EINZELHANDEL

**Checkpoint RF** 40

EAS im Einzelhandel

**Autonome Geschäfte der Zukunft im Einzelhandel** 44

Kassenlose Geschäfte: Der Wandel ist eingeläutet

## VIDEOTECHNIK

**Axis Communications** 68

Gebäudeplanung mit modernen IP-Video-Systemen

**IDIS** 76

Videoüberwachung in Hotels - für Sicherheit und Gästemanagement. Ein eBook zeigt Vorteile der Videoüberwachung im Beherbergungsgewerbe

**Hanwha Techwin** 78

Museum und Denkmal aus dem 13. Jahrhundert: Videotechnik im Schloss Ujazdowsk

**Wissenschaft** 82



## KÖTTER

### Security und Service für Baustellen, Werften und ISPS-Anlagen

Architekten, Projektleiter und Planer stehen bereits bei der Konzeption von Bauvorhaben vor immer komplexeren Sicherheitsaufgaben. Zur Verbesserung der Performance während aller Bauphasen bietet KÖTTER Services den Sicherheitsverantwortlichen umfassende Schutz- und Servicekonzepte, die mit Bausteinen zur Arbeitssicherheit, zum Brandschutz und dem zollkonformen Zutrittsmanagement weit über den bekannten Wachdienst hinausgehen.

**https://www.koetter.com**

## Impressum *ISSN 09481249*

**Redaktion** *Euro Security Fachmedien; Dr Claudia Mrozek; 83083 Riedering, Tel: +49 (0)8036 3025071; Email: redaktion@euro-security.de*
**Redaktionsteam** *Dr. Claudia Mrozek (presserechtlich verantwortlich), Caroline Best, Angela Kloose, Dirk Lehmanski, Maria Lehmen, Anne Schneider, Heiko Scholz, Patricia Ova, Markus Steben, Cathy Thomens, Sophie Mrozek, Alexander Mrozek, Mariam Nassreddin;*
**Aboverkauf** *DCMN Marketing Agentur, Email: abo@sec-global.org*
**Anzeigenverwaltung/-vertretung** *DCMN Marketing Agentur Oberbayern; Bestellungen und Druckvorlagen: anzeigen@euro-security.de*


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

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

# Editorial

## Können Messen wieder zur alten Stärke zurückkehren?

Im Jahr 2022 - nach den beiden Corona-Jahren – zeigte sich, dass unsere Gesellschaft und die Wirtschaft unter den Auswirkungen der Pandemie gelitten haben. Und diese Entwicklung ging auch nicht einfach an der Sicherheitsbranche vorüber. Im Frühjahr öffneten Unternehmen wieder zaghaft Ihre Pforten und nahmen die normale Geschäftstätigkeit auf. Schnell wurde klar, dass auch in unserer Branche der Fachkräfte- und Arbeitskräftemangel entscheidende Auswirkungen hatte. Trotzdem hat die weltweite Seuche auch bei den Sicherheitsunternehmen einen entscheidenden Einfluss gehabt: Der Grad der Digitalisierung ist immerhin in der Unternehmenskommunikation – in der Außenkommunikation und im internen Dialog – gestiegen. Videokonferenzen via Zoom und anderen Lösungen sind heute in die tägliche Routine im Unternehmen integriert, sparen Kosten und ermöglichen einen intensiveren Meinungsaustausch. Und trotzdem waren alle Marktakteure froh, als auch mit der Öffnung die Veranstaltungen wie Messe und Konferenzen auf der Agenda standen. Alle waren glücklich wieder im persönlichen Austausch Geschäftsbeziehungen zu pflegen und Projekte zu entwickeln. Die bisher so erfolgreichen Messen, auf denen in der Vergangenheit die Unternehmen der Sicherheitsbranche ausstellten, fanden bisher nicht zur alten Stärke zurück und auch der globale Kontext, in dem sich bisher die deutschen Sicherheitsunternehmen bewegten, litt erheblich. Die Messe-Events spiegelten nicht mehr die internationale Sicherheitsindustrie wider und waren fragmentiert. Bleibt zu hoffen, dass das kommende Jahr mehr Erfolg bringt. Aber die Chancen stehen gut.

So startet das neue Jahr mit der Perimeter Protection 2023. Die Messe Nürnberg als Organisator vermeldet eine Rekordanzahl von Ausstellern und hofft nun natürlich auch auf entsprechende Besucherzahlen. Schließlich berücksichtigt das Angebot auf dem Nürnberger Messegelände die Topthemen der Sicherheitsverantwortlichen in Deutschland. So stehen nicht nur mechanische und elektronische Grundstückssicherungen im Fokus. Auch intelligente, KI-basierte Videotechnik oder Sicherheitsdienstleitungen wie Drohnenschutz stehen auf dem Programm. Damit kann auf die Nachfrage nach einem besseren Schutz von kritischen Infrastrukturen (KRITIS), aber auch nach Sicherheitslösungen für privatwirtschaftliche gedeckt werden. Auch andere wichtige Messe finden in Nürnberg statt. Was wäre die deutsche Sicherheitsindustrie ohne die Feuertrutz oder die it-sa, die Schlüsselveranstaltungen für die Branche darstellen?

Andere Messen, wie z.B. die SicherheitsExpo in München muss sich dieses Jahr erneut beweisen. Nach einem Eigentümerwechsel und einer leichten Marktermüdung, müssen dieses Jahr neue Akzente gesetzt werden, um an die erfolgreiche Vor-Corona-Zeit anzuknüpfen.

Auch in diesem Jahr vor einem Neuanfang steht die PMRExpo. Die Messe, die bisher nur auf dem Messegelände in Köln unter anderer Organisation stattfand, wird in Zukunft auch vom Management der KölnMesse geplant und durchgeführt. Auch bei dieser Spezialmesse ist ein Blick in die Zukunft interessant. Diese auf Leitstellen und Kommunikation beschränkte Messe könnte auf Grundlage der hier präsentierten Technologien einen Wachstumsimpuls durch eine Ausweitung der Themen erhalten. Leitstellen sind die Basis für eine Vielzahl von Projektlösungen in der modernen digitalen Welt. So wäre das Thema Smart Cities für die im November stattfindende Messe sicher eine Bereicherung. Bleibt abzuwarten, wie der bisher maßgebende Verband zu solch einer thematischen Ausweitung stehen würde. Überlegenswert wäre es alle Mal.

Hoffentlich wird das Jahr 2023 mit all den unterschiedlichen Veranstaltungen für die Sicherheitsbranche zielführend. Denn das Jahr 2024 sollte mindestens wieder eine Leitmesse bereithalten, auf der Innovationen der deutschen und internationalen Sicherheitsbranche gezeigt werden und ihre Heimat finden. Das braucht die Branche ohne Frage.

**Dr Claudia Mrozek**

17.–19.1.2023 // Nürnberg, Germany

PERIMETER PROTECTION

Internationale Fachmesse für Perimeter-Schutz, Zauntechnik und Gebäudesicherheit

# WENN SICHERHEIT DOCH NUR SO EINFACH WÄRE...

... Lösungen finden Sie auf der Perimeter Protection, Europas führende Fachmesse mit Fokus auf Gebäudesicherheit und Freigeländeschutz.

**Jetzt Ticket sichern!**
perimeter-protection.de/besucher-werden

NÜRNBERG MESSE

# Alles aus einer Hand

## Der Praxisevent SITE SAFETY 2022 von KÖTTER SERVICES in Bremen als Erstveranstaltung im Rahmen von Sicherheitskonzepten für Baustellen, Werften und KRITIS-Bereichen mit namhaften Partnerunternehmen.

**KÖTTER Security hat in Bremen am 6. Oktober 2022 einen ‚Tag der offenen Tür' für Security & Services für Baustellen, Werften und ISPS-Anlagen veranstaltet. Mit über zehn Partnern* wurde eine Vielzahl von unterschiedlichen Themen** vorgestellt. Der Praxisevent für Architekten, Planer und Sicherheitsverantwortliche in der Baubranche eröffnete interessante Perspektiven für die Bereiche Baubewachung. Besonders durch eine Gesamtlösung für sichere ‚Sites' ergeben sich für Kunden größere Freiräume in Geschäftsabläufen.**

Kriminelle haben Baustellen in der Vergangenheit als Selbstbedienungsläden für ihre Raubzüge in allen Regionen der Bundesrepublik gesehen. Dabei wurden nicht nur Baumaschinen und -Fahrzeuge von Baustellen in Deutschland entwendet und verschwinden auf Nimmerwiedersehen. Auch wertvolle Baustoffe (Holz, Dämmstoffe), Gegenstände aus Metall oder mit hohem Metallanteil (z.B. Buntmetall und Kupfer, Kabel jeglicher Art und Werkzeuge stehen bei Kriminellen hoch im Kurs. Nach Angaben der Polizei werden das Diebesgut

ES_DACH_A5-12-2022_01012023.qxp_EuroSecurity A5 20 13.01.23 12:50 Seite 7



auf ‚Bestellung' ausgewählt, schnell weiterverkauft oder sogar selbst genutzt. Baumaschinen, die nicht ins Ausland geschafft werden, werden auch durch Hehler weiterveräußert.
Die wirtschaftlichen und organisatorischen Folgen sind erheblich: Immense Kosten für Ersatzbeschaffungen, Terminverzögerungen bei der Baufertigstellung, Diskussionen mit Kunden und Versicherungen behindern den Baufortschritt und verzögern die Fertigstellung der Objekte.

Die Zahl der gemeldeten Diebstähle auf Baustellen lag laut Bundeskriminalamt bei 22.773 (2021). Und rund zehn Prozent werden nur aufgeklärt. Versicherungstechnisch bedeutet, dass Bauunternehmen und Handwerker auf Baustellen grundsätzlich bis zur Abnahme halten. Also auch für jegliche beweglichen Güter (Baumaschinen, Fahr- und Werkzeuge) auf einem Baustellengrundstück sind sie verantwortlich und müssen bei Diebstahl diese ersetzen. Auf Grund der gegenwärtigen Rechtsprechung bleibt es für einen Handwerksbetrieb damit ein erhebliches Risiko, wenn er Werkzeuge und Materialien bis zur vollständigen Abnahme auf der Baustelle lagert.
Neben Diebstahl erhöhten sich auch die Vandalismusvorfälle in den vergangenen Jahren. Brandstiftung und mutwilliges Zerstören von Teilen von Rohbauten und anderen Gebäudeteilen sind leider keine Seltenheit.
Meistens kommen die Bösen im Schutz der Dunkelheit und so sind Beleuchtungskonzepte und Videokameras, die in der Nacht Geschehnisse aufzeichnen bzw. melden können besonders wichtig. Im Zusammenspiel mit anderen Sicherheitslösungen kann eine Täteransprache oder Alarmverfolgung durch einen Sicherheitsdienst erfolgen und so selbst Personen, die schon unbefugt auf Grundstücke gelangt sind, vertreiben. Präventions- und Sicherheitskonzepte für ‚Sites' und speziell Baustellen stehen angesichts der Kriminalitätsraten nun schon seit einiger Zeit hoch im Kurs. Auch KÖTTER Security bietet Baustellenbetreibern und Grundstückseigentümern umfassende Sicherheitslösungen mit personellen und technischen Lösungen. Charakteristisch für die KÖTTER Dienstleistungen ist der sog. Revierwachdienst, der Baustellenareale mehrmals in der Nacht (am Wochenende oder feiertags auch tagsüber) auf ihren Zustand überprüft. Diese Sicherheitsdienstleistung dient vor allem der Prävention und Intervention. Darüber hinaus bietet das Essener Unternehmen mit ausgesuchten Partnern technische Sicherheitskonzepte für den gesamten Baustellenzyklus an: Der Kunde schließt dabei einen Vertrag aus einer Hand ab: Alle Gewerke auch von Partnerunternehmen werden während der gesamten Bauphase von KÖTTER koordiniert. Bauzaun-Banner, rund um die Baustelle, zeigen an, dass das Grundstück über- wacht und geschützt ist. Einheitliche Sicherheitsstandards machen eine effiziente Lösung vor Ort bundesweit möglich, die je nach Baufortschritt angepasst werden.

## Sicherheit und Arbeitsschutz

KÖTTER ist sich der Wichtigkeit eines effektiven Betreibermodells für die Planung, die Einrichtung oder den Betrieb von Baustellen bewusst. Eine Erstellung von Gefährdungsbeurteilungen und die Definition der benötigten Fachkraft für Arbeitssicherheit vor Ort gehört zum Dienstleistungskonzept. Dabei müssen nicht nur die zahlreichen Gewerke aufeinander abgestimmt werden, auch die Aspekte der Arbeitssicherheit in Deutschland und des Gesundheitsschutzes müssen gewährleistet sein. Die gesetzlichen Vorgaben des Zolls und der Berufsgenossenschaften sind wichtige Rahmenbedingungen, die ebenfalls in Sicherheitskonzepten Beachtung finden müssen.
Die richtige Arbeitsbekleidung, z.B. die Pflicht zum Tragen des Helms auf der Baustelle (zwingend vorgeschriebene persönliche Schutzausrüstung), oder der Zutritt zur Baustelle muss rechtskonform geregelt werden.

## Zutrittsmanagement

Mit dem Partner IQ-Pass sorgt eine integrierte Zutrittskontrollsoftware für Dokumentation verschiedener Daten und Unterlagen, die heute für Baustellenbetreiber essenziell sind. Dabei werden die Firmen- und Personenanmeldungen, die das Betreten der Baustelle legitimieren, genauso überprüft, wie auch die Registrierung der Arbeitenden bei den relevanten Sozialsystemen (Baugenossenschaft, Kranken- und Rentenversicherung). Natürlich können auch allgemeine Legitimationsprüfungen (Ausweis- & A1 Prüfungen)

ES_DACH_A5-12-2022_01012023.qxp_EuroSecurity A5 20 13.01.23 12:50 Seite 8

abgefragt werden und eine Mindestlohnprüfung (mtl. Mindestlohnabfrage) ist inkludiert. Damit wird ein Beitrag gegen Schwarzarbeit auf Baustellen geleistet.

Mittels einer einheitlichen Auswertungsplattform können Anwesenheiten (Ein- und Ausgang, Ein- und Ausfahrt) dokumentiert werden. Diese Daten können mittels cloudbasierten Zugriffs von überall auf der Welt abgefragt werden, was für global tätige Unternehmen wichtig ist. In Bezug auf das Asset-Management auf dem Baustellenareal kann eine entsprechende Ausgangskontrolle stattfinden, die gewährleistet, dass auch wirklich alle Maschinen und Werkzeuge auf dem Baustellengelände verbleiben.

### Videomanagement

Weil jede Baustelle individuelle Besonderheiten aufweist, werden natürlich auch unterschiedliche Sicher-

# „Wir bieten den Kunden eine Lösung"

**Daniel von Grumbkow, Regionalleiter und Prokurist und ab dem 1. Januar 2023 Geschäftsführender Direktor der KÖTTER SE & Co. KG Security Hamburg, stellt in einem Statement das Leistungsportfolio des Branchenriesen dar.**

„Die SITE SAFETY 2022 wurde im jetzt Oktober das erste Mal dem Fachpublikum vorgestellt. Wegen des Erfolgs der Veranstaltung planen wir dieses Event im kommenden Jahr an anderen Orten in der Bundesrepublik. Für die Erstveranstaltung haben wir wegen der geographischen Lage Bremen ausgewählt. Baustellensicherheit ist nicht nur klassischer Hoch-, Tief- und Neu- bzw. Umbau. Auch viele Werften und Hafengebiete befinden sich in der Region. Dabei stellt jeder Schiffsbau eine Baustelle dar und untersteht auch ähnlichen oder gleichen gesetzlichen Anforderungen wie eine herkömmliche Baustelle. Und diese Konzepte, die wir hier anbieten, sind ebenso interessant für den Bereich kritische Infastrukturen (KTRITIS). Insbesondere für Hafenanlagen im Bereich des International Ship and Port Facility Security Codes (ISPS-Code). Darum haben wir Bremen als Ort für unseren ersten Praxistag mit unseren Partnern ausgewählt."

### Services rund um Sicherheit für Baustellen

"KÖTTER SERVICE bietet Services für Baustellen über den klassischen Service hinaus. Normalerweise sucht ein

ES_DACH_A5-12-2022_01012023.qxp_EuroSecurity A5 20 13.01.23 12:50 Seite 9

Mike Jürgens, Geschäftsführer von KOOI Security Deutschland, stellte in Bremen die Videolösungen, die bei KÖTTER Security - Lösungen zum Einsatz kommen, vor. Besonders wies er darauf hin, dass aufgrund fehlenden Personals und knappen Budgets eine Videoüberwachung trotzdem den notwendigen Sicherheitsgrade auf bewachten Grundstücken gewährleistet. Auch er bewertete die Veranstaltung sehr positiv und freut sich auf die Veranstaltungen im Jahr 2023. [Foto ©DCM2022]

Bauträger einen Sicherheitsdienstleister, der Bewachungspersonal benötigt, im zweiten Schritt benötigt er einen Dienstleister, der Videotechnik stellt und im dritten Schritt noch jemanden, der zollkonforme Besuchermanagementsysteme anbietet. Dieses Paket bietet KÖTTER Services aus einer Hand. Damit hat der Kunde schon mal drei Themen abgehakt. Aber dies ist ja noch nicht alles. Darüber gibt es weitere Dienstleistungen, die die Kunden heutzutage benötigen. Von der Planung, zur Umsetzung bis hin zur Nachhaltigkeitsüberprüfung bietet KÖTTER alles an."

- "In der Planung – der Phase 1 - unterstützen wir den Kunden z.B. bei der Erstellung von Sicherheitskonzepten sowie Gefährdungsanalysen, bei der Arbeitssicherheit und Brandschutzkonzepten."
- "In der Phase 2, in der Bauunterstützung sind wir mir den ersten Bewachungstätigkeiten vor Ort, implementieren das zollkonforme Sicherheitsmanagement und Ausweiswesen und installieren die erste Sicherheitstechnik, z.B. Videomanagementsysteme."
- "In der dritten Phase, in der Bauphase selber, sind wir zusätzlich für Ort. Das skaliert von Stepp zu Stepp: Mit Brandwachen, Rettungs- bzw. Betriebssanitätern – auch anderen Einheiten des betrieblichen Rettungswesens und Feuerwehren. Die Hardware, der Perimeterschutz und auch die Zutrittskontrollen werden je nach Baufortschritt weiter ausgebaut oder entwickelt."

"Damit sind Sicherheitskonzepte und -lösungen an die Baufortschritte angepasst und skalierbar und damit individuell für jeden Kunden ausgearbeitet.Der Kunde hat einen Ansprechpartner, der alles aus einer Hand als ‚Rund-um-Sorglosplaket' anbietet, realisiert und Gewerke managed. Ein operativer Ansprechpartner spart viel Planungszeit ein und last-but-not-least: der Kunde bekommt von uns eine Rechnung, auf der alles abgerechnet wird."

heitsmaßnahmen benötigt. Die Videoüberwachung hat sich in den vergangenen Jahren bei Projekten als obligatorische Lösung erwiesen: Mit dem KÖTTER Security Video Tower bietet das Essener Unternehmen einen bis auf acht Meter ausfahrbaren Video Tower an.

Damit ist der Schutz vor Diebstahl, Vandalismus, Sabotage und Manipulation in einem hohen Maße gewährleistet. Unbefugte Personen (oder Fahrzeuge) werden vollautomatisch erfasst, aufgezeichnet und können über eine Live-Ansprache von eventuellen, kriminellen Vorhaben abgehalten werden. Mit dem Video Tower kann ebenfalls der Baufortschritt dokumentiert werden und durch diese mobile Lösung kann der Standort des Video Towers je nach Baufortschritt variabel angepasst werden. Aber auch fest installierte Videokameras zum Einsatz kommen, z.B. auf Großbaustellen, können zum Einsatz.

**[www.koetter.de]**

*Themen & Live-Demos vor Ort: Baustellenbewachung, Alarmaufschaltung und Intervention; Schrankensysteme, Perimeterschutz und Videosysteme; Baucontainer, Drehkreuze und Zutrittskontrollsysteme; Zollkonformes Zutrittsmanagement; Vorbeugender und abwehrender Brandschutz; Arbeitssicherheit und Sicherheitsunterweisungen; Betriebliches Sanitätswesen; Digitale Baudokumentation; Planung, Errichtung, Wartung und Service; Baureinigung und Bauschlussreinigung

** Unternehmen vor Ort: KÖTTER Security; KÖTTER Cleaning; German Business Protection; TERAPON Consulting; CSS Computer Security Service; BAU.CAMERA; KOOI; IQ-Pass; Comp-Pro; ESB Solutions

PERIMETER PROTECTION

# Videosysteme: So bleibt der Perimeterschutz im Blick

**Kameras sind die Augen moderner Sicherheitssysteme. Das macht sie zu einem unverzichtbaren Bestandteil des Geländeschutzes. Gerade dann, wenn große Flächen oder mehrere Standorte zentral überwacht werden müssen, kann die Videotechnologie ihre Vorteile ausspielen.**

Videosysteme eignen sich perfekt dazu, um bei der Zugangskontrolle, im Rahmen des Einbruchschutzes oder zur Bewegungsdetektion Aufnahmen zu machen, aus denen sich weitere Maßnahmen ableiten lassen. Sie sind im Idealfall individuell auf die jeweilige Anwendung und die zu schützenden Objekte zugeschnitten. Oft machen sich Kameras aber schon durch ihre abschreckende Wirkung bezahlt: Sichtbar angebracht können sie unbefugtem Eindringen oder kriminellen Handlungen vorbeugen.

Je nach Bedarf reicht die Auswahl von Kameras, die nur das reine Videobild liefern, bis hin zu Hightech-Lösungen mit komplexen Analysemöglichkeiten. Dabei können die Geräte selbst mit intelligenten Features aufwarten und mit ihren Sensoren Informationen für den Perimeterschutz bereitstellen. Geht es nur um die Detektion von Bewegungen reichen abgespeckte Videosysteme oder intelligente Videokameras. Sie lösen nur im Alarmfall aus – also wenn eine Bewegung detektiert wird.

## Videoüberwachung als Teil des IoT

Sind wirkungsvollere Lösungen gefragt, empfiehlt es sich, die Videosysteme mit der Sicherheits-IT und anderen Komponenten des Geländeschutzes zu vernetzen. Sie sind über das Internet of Things mit Servern verbunden und kombinieren die elektronische Verarbeitung in der Kamera mit weiteren Softwareanwendungen. Meldet das System zum Beispiel eine Kartennutzung an einer Zufahrt, löst die Kamera aus und die Bilderkennungssoftware kann die Fahrzeugnummer identifizieren. Software- und Schnittstellenstandards sowie Normen wie DIN EN 62676 „Videoüberwachungsanlagen für Sicherungsanwendungen – Anwendungsregeln" erleichtern dabei die Integration.

Der sicherheitsrelevante Einsatz von Kameras kann aber weit über das Erkennen von unbefugten Personen oder Fahrzeugen auf dem Gelände hinausgehen. Ausgestattet mit Wärmebildsensoren können sie nicht nur bei allen Lichtverhältnissen Menschen erkennen, sondern zum Beispiel auch Brände und Rauchentwicklung frühzeitig erfassen.

Video-Codecs und digitale Aufzeichnungsgeräte bieten durch ihre Rechenkapazität und ihren Speicherplatz weitergehende Möglichkeiten. Dazu zählt beispielsweise die Künstliche Intelligenz. Algorithmen ermöglichen es dabei, vorgegebene Daten oder Erkenntnisse aus der Vergangenheit zu nutzen, Ereignisse besser zu erkennen und Gefahren abzuwenden. Nur ein geschütztes Videosystem erhöht die Sicherhei

Die Verwendung von Videotechnik auf dem Gelände hat allerdings auch ihre Tücken. Datenschutz und Datensicherheit müssen bei der Planung unbedingt von Anfang an mitberücksichtigt werden, damit der rechtssichere Einsatz gewährleistet ist. Was den Datenschutz angeht, reicht oft schon eine Kennzeichnung des überwachten Bereichs. Hinzu kommen Betriebsvereinbarungen und der Schutz der Privatsphäre von Mitarbeitern oder Besuchern, z. B. in Umkleideräumen.

Wie bei allen vernetzten Systemen gilt es auch bei Videoanlagen das Sicherheitssystem nicht zum Einfallstor für Angreifer zu machen. Videobilder, Tonaufnahmen oder Bewegungsmuster können Kriminelle ausnutzen. Schon alleine deshalb ist es ratsam, das Videoüberwachungssystem mit in die Infrastruktur der IT-Sicherheit einzubinden.

## Planung von Video-Sicherheitstechnik

Bei der Planung von Videoanlagen

spielt die erforderliche Bildqualität eine Hauptrolle. Aspekte wie Kontrast, Auflösung, Bilder pro Sekunde und Beständigkeit gegen Wettereinflüsse müssen miteinander in Einklang gebracht werden. Sind die Bilder im schlimmsten Fall nicht verwertbar oder von der Software nicht zufriedenstellend analysiert, sparen Unternehmen an der falschen Stelle. Ein zu mächtiges Videosystem wiederum lässt im schlimmsten Fall die Investitionskosten in die Höhe schießen. Kosten und erforderliche Bildqualität sollten also immer Basis der Investitionsentscheidung sein. Bei der Planung leisten erfahrene Berater wertvolle Dienste – auf der Perimeter Protection in Nürnberg sind die Experten für Videoüberwachung beispielsweise anzutreffen.

Auch nach der Installation eines Systems, ist es erforderlich, die Hardware weiterhin zu warten und die Software dauerhaft auf dem neuesten Stand zu halten. Nur so bleibt die Funktionalität erhalten und die Cybersicherheit gewährleistet. Mangelnde Wartung führt beispielsweise zu gehäuften Fehlalarmen und stellt damit die Akzeptanz und den Sinn des Systems infrage. Deshalb sind eine sorgfältige Einweisung und Schulung des Sicherheitspersonals und die Festlegung von Zuständigkeiten sowie von Prüf- und Wartungsplänen wichtig. Sind die Ressourcen im eigenen Unternehmen nicht vorhanden, gibt es qualifizierte Sicherheitsanbieter, die die Anlagen kontinuierlich auf dem Stand der Technik halten.

Bei der Investition in eine Videoüberwachungsanlage müssen Unternehmen also verschiedene Abwägungen beachten, die von Objekt zu Objekt variieren. Hat man einmal die richtige Anwendung ausgewählt, ergeben sich daraus häufig weitere Vorteile für die Sicherheit von Menschen und Vermögenswerten.

---

**Messe für Perimeterschutz, Zauntechnik und Gebäudesicherheit • Messezentrum • 90471 Nürnberg • Datum & Öffnungszeiten • 17. - 19. 01.2023 • 09:00 - 17:00 Uhr (17. und 18. Januar), 09:00 - 16:00 Uhr (19. 01) > Kostenlose Eintrittskarte mit dem CodePPEUROS23LIT: 👉 https://lnkd.in/e7tTagfk**

## PERIMETER PROTECTION

# Drohnen - Gefahr aus der Luft

**Flugdrohnen für den privaten und gewerblichen Gebrauch kann man inzwischen in jedem Baumarkt bekommen. Mit der breiten Zugänglichkeit und ihren immer leistungsfähigeren Kameras und Sensoren, stellen die unbemannten Fluggeräte eine zunehmende Gefahr für den Perimeterschutz dar.**

Drohne - Gefahr aus der Luft // © unsplash

Drohnen haben sich in den letzten Jahren zur elektronischen Massenware für jedermann entwickelt. Die technologische Entwicklung der Geräte geht dabei mit ungeahnter Geschwindigkeit voran und lässt sich mit den Entwicklungssprüngen bei Mobiltelefonen vergleichen. Unternehmen und Behörden in der Sicherheitsbranche machen sich die fliegenden Augen schon länger zunutze, um den Überblick bei der Sicherung von Geländen oder Veranstaltungen zu behalten. Bei der Überwachung von Freigeländen, Industriegebieten und kritischen Infrastrukturanlagen leisten sie unverzichtbare Dienste. Im Alarmfall liefern Drohnen binnen Minuten Videoaufnahmen und damit Informationen für den Geländeschutz.

Doch mit Preisen von 50 Euro aufwärts kann sich inzwischen jeder eine Drohne leisten – und damit auch Kriminelle. Sie erkennen Sicherheitslücken im Luftraum, spionieren mit den Kameras Firmengeheimnisse aus,

schmuggeln Drogen über Grenzzäune oder Waffen und Werkzeuge in Gefängnisse. Auch das Abgreifen von Daten aus Firmennetzen ist mit ihnen möglich. Unternehmen und Organisationen sollten deshalb ihr individuelles Drohnenrisiko ermitteln, Schwachstellen im Sicherheitssystem identifizieren und Vorkehrungen treffen.

## EU erkennt Sicherheitsrisiken

Zwischenfälle mit Drohnen häufen sich – darunter sind auch immer mehr kritische Situationen. So berichtete die Polizei Brandenburg im Mai 2022 davon, dass eine Drohne einem Passagierflugzeug gefährlich nahegekommen ist und den Anflug auf den Hauptstadtflughafen BER behindert hat. Wenige Monate zuvor verfehlte ein Quadrocopter eine Boeing 737 mit 189 Passagieren an Bord nur um wenige Meter. Abgesehen von der Gefährdung des Flugverkehrs sind Vorfälle, bei denen sich Bewohner von den fliegenden Kameras ausspioniert fühlen, inzwischen alltäglich.

Die EU hat das wachsende Sicherheitsrisiko erkannt und 2021 eine Regelung eingeführt, die das Betreiben von Drohnen auf ein rechtliches Fundament stellt. So müssen Drohnen über 250 Gramm registriert werden und die Betreiber müssen bestimmte Vorgaben einhalten. Eine Remote-ID fungiert dabei als digitaler Ausweis und erkennbare Registrierung. Die Wahrscheinlichkeit, dass Kriminelle eine registrierte Drohne verwenden, ist allerdings eher gering.

Bei einer Drohne handelt es sich im Wesentlichen um einen fliegenden Computer. Und genau wie diese können sie auch für Cyberattacken eingesetzt werden, um beispielsweise Daten abzugreifen. Wer Drohnen zum Perimeterschutz verwendet, sollte sich auch darüber im Klaren sein, dass mit ihnen ein angreifbares Ziel durch die Lüfte schwebt. Auch das einschmuggeln von Malware über die oft schlecht geschützte Drohnensoftware ist denkbar. Drohnen im Dienste der eigenen Sicherheitsabteilung sollten deshalb unbedingt von der IT-Abteilung geprüft und mit entsprechenden Schutzmaßnahmen ausgestattet werden.

## Passive Abwehr als einzige Wahl?

Abwehrmaßnahmen begrenzen sich meist auf bauliche oder technische Möglichkeiten, die das Überfliegen erschweren oder unbefugte Drohen erkennen sollen. Dazu gehören Installationen, aber auch Detektionsgeräte. In der Umgebung von Gefängnissen verhindern beispielsweise Netze das Eindringen in den Luftraum des Geländes. Sichtschutze wiederum verbergen sensible Bereiche auf dem Unternehmensgelände. Sogar Raubvögel wurden schon als Drohnenabwehr in Betracht gezogen: Die Polizei in den Niederlanden testete den Einsatz von Adlern, um Drohnen einzufangen. Nach einer Testphase mussten die Behörden aber feststellen, dass die Ausbildung und Effizienz der Vögel doch komplizierter und teurer war als erwartet. Das Programm wurde deshalb eingestellt.

Inzwischen stehen ausgereifte Systeme zur Verfügung, mit denen sich Drohnen detektieren und abwehren lassen. Viele der angebotenen Lösungen zur aktiven Drohnenabwehr sind in Deutschland aber nicht zugelassen. So ist die Verwendung von Störsendern, das sogenannte Jamming oder Spoofing, hierzulande behördlichen und militärischen Sicherheitseinrichtungen vorbehalten.

Passive Abwehrmaßnahmen, mit denen sich Unternehmen schützen können, reichen von der Radar- und Kameradetektion bis hin zur RF-3D-Detektion mit Hochfrequenzdetektoren. Diese und weitere Lösungen zur Drohnenabwehr präsentiert die Branche 2023 auf der Perimeter Protection in Nürnberg. Die Messe legt den Fokus auf die Sicherheit von Freigeländen und Außenanlagen und integriert die Plattform U.T.SEC, die sich auf die technischen, rechtlichen und praxisnahen Möglichkeiten zum Einsatz und zur Abwehr von Drohnen und anderen unbemannten Technologien konzentriert.

PERIMETER PROTECTION

**Messe für Perimeterschutz, Zauntechnik und Gebäudesicherheit • Messezentrum • 90471 Nürnberg • Datum & Öffnungszeiten • 17. - 19. 01.2023 • 09:00 - 17:00 Uhr (17. und 18. Januar), 09:00 - 16:00 Uhr (19. 01) > Kostenlose Eintrittskarte mit dem CodePPEUROS23LIT: 👉 https://lnkd.in/e7tTagfk**

# Perimeter Protection im Jahr 2022

Bei der Perimetersicherheit sind derzeit mehrere Trends zu beobachten: So hat zum einen der Einsatz der Videotechnik erheblich zugenommen und zum anderen wird die Integration von zusätzlichen, technischen Lösungen verstärkt. So setzen die Anwender vermehrt auf den Einsatz von Sensoren und kombinierbaren Technologien. So versucht man präventiv ausgerichtete Lösungen wie Wärmekameras oder Radaranwendungen in Lösungskonzepte einzubeziehen. In Kombination mit Beleuchtungskonzepten und Audioanwendungen ist eine Abschreckung gegenüber Kriminellen effizient möglich.

Dabei ist besonders wichtig, dass angewendete Technologien in der Standardisierung offen gestaltet sind. Durch die vorhandenen IP-Strukturen ergeben sich wieder neue Risikostrukturen. Angesichts der Tatsache, dass jeder Endpunkt des Netzwerks eine potenzielle Schwachstelle für die Cybersicherheit darstellt, und wegen der allgemeinen Bedrohungspotentiale durch Cyberangriffe müssen sowohl die physische als auch die IT-Sicherheit ganzheitlich betrachtet werden.

## Sicherheitslösungen für spezifische Anwendungen

Eine besondere Rolle spielt die Sicherheit in der Umgebung kritischer Infrastrukturen (KRITIS) im Alltag, um die wirtschaftliche und soziale Stabilität zu untermauern. Besonders Versorgungsdienstleistungen stehen im Mittelpunkt von Schutzkonzepten und das Ziel ist, diese sicher und effizient bereitzustellen. Damit. Stellt die Perimeter Sicherheit eine geeignete Technologie zum Schutz von Bürgern, Passagieren, Daten und Vermögenswer- ten dar und verhindert Betriebsunterbrechungen von entsprechenden Anlagen. Auch Verkehrsstrukturen, wie beispielsweise See- und Flughäfen, gehören zu den zu schützenden Anlagen. Risiken von Terrorismus und anderen Bedrohungen und Schwachstellen sind viele exponierte Einrichtungen ausgesetzt.

## KI-gesteuerte Sicherheitssysteme

KI hat die Geräte intelligenter gemacht. Aufgrund von Daten und Systemintelligenz können schnellere und effektivere Entscheidungen als je zuvor. Auf einer Plattform laufen nun die Überwachungsergebnisse von verschiedenen Sicherheitssystemen und Tausenden von Kameras und Sensoren zusammen. Durch die Unterstützung der Integration beliebiger Geräte, Dienste oder Lösungen und die Zusammenführung von Daten in einem einzigen Bereich können Unternehmen ein anderes Sicherheitslevel erreichen.

## Videotechnologie ist wichtiger denn je

Die Videoüberwachungstechnologie ist Teil einer mehrschichtigen Sicherheitsstrategie. Kameras ergänzen das Sicherheitspersonal und ermöglichen den Betreibern eine effektive Echtzeitüberwachung und Alarmmanagement, während gleichzeitig ermittlungstechnische und forensische Daten gesammelt werden können. Außerdem sind koordinierte Notfallreaktionen möglich.

Die Kombination aus wertvollen Video- und Sicherheitstools ermöglicht es Anwendern, durch intelligente Datenerfassung vitalere Sicherheitsprogramme aufzubauen. Die funktionsreiche Videobetrachtung und die richtlinienbasierte Verteilung verbessern das Notfallmanagement, während containerisierte Videomanagement-Plattformen als intuitive Plattform dienen, die ein neues Maß an Situationsbewusstsein fördert und eine schnelle Reaktion ermöglicht.

Da viele unternehmenskritische Einrichtungen Personal abbauen mussten und auch nicht auf neues Sicherheitspersonal zurückgreifen können, ist die Nachfrage nach Videotechnologien sprunghaft angestiegen."

## Die Zukunft

Wie in vielen anderen Bereichen der physischen Sicherheit gibt es auch bei Perimetersystemen immer mehr intelligente Geräte, integrierte Lösungen und datengesteuerte Prozesse. Die Gewährleistung der Cybersicherheit ist unumgänglich geworden, und Systemintegratoren beginnen, dies als Teil ihrer Dienstleistungen anzubieten.
KI und Videotechnologie sind wichtiger denn je, da sie den Betreibern verwertbare Erkenntnisse liefern und es ihnen ermöglichen, schneller und effizienter zu reagieren.

# Welche Technologien prägen die Perimetersicherheit?

**Nach Aussagen des Marktforschungsinstituts ‚Markets and Markets' s wird der Markt für Perimetersicherheitskomponenten von 62 Mrd. Euro im Jahr 2020 auf 98 Mrd. Euro im Jahr 2026 anwachsen. Dir durchschnittliche Wachstumsrate beträgt laut Prognose 7,9 Prozent.**

**Die Grundstückssicherheit gehört in der Sicherheitsbranche zu den Wachstumsbereichen. Da die Bedeutung von Sicherheitslösungen, die schon an der Grenze zu Arealen greifen, wächst, ist der Bedarf nach solchen Lösungen sehr groß. Dabei geht es jedoch nicht nur um die Absicherung von Freigeländen und Grundstücks- bzw. Geländegrenzen von kritischen Infrastrukturen (KRITIS), wie z.B. bei Justizvollzugsanstalten, Flughäfen oder Rechenzentren, sondern auch zunehmend um Anwendungen im privatwirtschaftlichen Bereich, wie Logistikbetrieben, Industriegeländen oder Baustellen.**

Perimetersicherheit soll Personen oder Geräte direkt an der Außengrenze eines Grundstücks abhalten in dieses einzudringen bzw. bei einem Versuch des Eindringens Alarm auslösen.
Diese Art von Sicherheitslösungen ist für eine Vielzahl von Unternehmen und Institutionen wichtig. Sicherheitskonzepte rund um die Perimetersicherheit umfassen die Erkennung von Bedrohungen durch Sensoren, die jeweils über eine eigene Erkennungsmethode verfügen. Einige Technologien haben in den vergangenen Jahren an Bedeutung gewonnen bzw. gehören zur Basisausstattung einer Lösung. Wir möchten diese im Folgenden vorstellen.

1. Lidar-Sensoren senden Laserimpulse in die Umgebung und berechnen die Entfernung eines Objekts anhand der Zeit, die die Impulse für den Rückweg benötigen. Zu den Vorteilen dieser Technologie gegenüber der Videotechnik besteht darin, dass es unabhängig von Licht- und Wetterverhältnissen ist. Da Lidar nicht nur in der Sicherheitsindustrie Anwendung finden, sondern besonders im Automobilsektor Einsatz finden, sind die Preise für Lidar-Lösungen in den letzten Jahres erheblich gesunken. Damit wurde Lidar für den Betrieb im Freien interessant und ist bei vielen Anwendungen inzwischen eingesetzt.
2. Faseroptische Sensoren übertragen Laserlichtimpulse über Fiberoptik und messen die Lichtreflexionen, die entlang der Faser auftreten. Eine Störung der Faser, die z. B. durch die Berührung des Zauns verursacht wird, verändert die Menge des von diesem Punkt zurückgeworfenen Lichts. Aus Expertensicht ist Fiberoptik eine kostengünstige Lösunge für kleinere Standorte mit überdurchschnittlicher Lebensdauer.
3. Drahtlose Lösungen und eine drahtlose Kommunikation zwischen dem Sensor und dem Hauptsystem wird besonders bei Wohngebäuden und kleinen bis mittelgroßen Gewerbebetrieben immer wichtiger.
4. Auch Remote- und Überwachungsfunktionen werden besonders stark nachgefragt. Die Steuerung per Smartphone für die Fernsteuerung und Überwachung ist heute State-of-the-Art, besonders aus dem Privatbereich. Auch im Bereich der Hausautomatisierung ist diese Technologie besonders wichtig.
5. Besonders wichtig ist gegenwärtig die Videoüberwachung. Sie hat sich mittlerweile als obligatorische Technologie für die Perimetersicherheit entwickelt. Nicht zuletzt wegen des anhaltenden Mitarbeitermangels ist eine zunehmende Fernüberwachung wichtig. Im Perimeterbereich er-

gibt sich automatisch ein größerer Bedarf an visueller Verifizierung, um die Kosten und die Menge an Fehlalarmen zu senken.

Andere Sensoren sind wertvoll, wenn es darum geht, festzustellen, wer auf ein Grundstück gelangt oder es versucht. Mit Hilfe von Video können Dienstleister oder Betreiber aus der Ferne eindeutiger feststellen, um welche Situation es sich handelt.

Um die Effektivität der Videoüberwachung und -bewertung zu maximieren, muss das Videoverwaltungssystem in der Lage sein, den Ort des Alarms mit einer Kamera oder PTZ-Voreinstellung zu verknüpfen. Damit kann das Bedienpersonal schneller reagieren, braucht weniger Schulungsbedarf, und die Vorprogrammierung ermöglicht eine optimierte Videoqualität sowie Speichereinstellungen. Standortspezifische Maßnahmen zur Abschreckung sind so auch schneller umzusetzen.

### Sensoren in Kombination

Natürlich hat jede Erkennungstechnologie ihre Vor- und Nachteile. Die Verwendung einer Kombination dieser Technologien (Sensorfusion) macht die Erkennung von Sicherheitslücken effektiver. Intelligente, integrierte Lösungen benötigen ein Zusammenspiel der hier vorgestellten Technologien, um deren Stärke zu maximieren. Eine Sensorfusion kann z.B. durch die Nutzung von Echtzeitdaten zusammen mit historischen, ortsbezogenen, umweltbezogenen und klassifizierten Informationen analysieren, bevor ein Alarm ausgelöst wird. So werden Fehlalarme vermieden.

## Faktoren für eine effiziente Videotechnik im Rahmen der Perimeter Sicherheit

Die Grundstücksgrenze ist die erste Detektionslinie bei Sicherheitssystemen für Gebäude und Areale. Wie effizient Sicherheitslösungen sind, entscheidet über die Wirksamkeit der gesamten Sicherheitsinfrastruktur und auch darüber, ob ein unerwünschter Zwischenfall verhindert werden kann, bevor er eintritt. Moderne Lösungen bieten verschiedene Optionen zum Schutz eines Geländes. Diese reichen von verschiedenen Arten von Videoüberwachungskameras bis hin zu Bewegungssensoren, Analysegeräten, Wärmekameras oder auch Radar bzw. LiDAR.
Die Basis aller Lösungen unter all diesen Möglichkeiten sind nach wie vor die Überwachungskameras, um Beweise in Bild und Ton zu liefern.
Die Installation von Überwachungskameras im Freien bringt jedoch einige Herausforderungen mit sich.
Die Temperatur ist beim Betreiben von Kamerasein wichtiger Faktor. Extrem niedrige Temperaturen können sich negativ auf jede Überwachungskamera auswirken. Die Kameras können einfrieren, erodieren und Eisablagerungen auf dem Objektiv bilden, die die Sicht trüben können. In schlimmeren Fällen lässt sich das Gerät möglicherweise gar nicht mehr einschalten.
Kondenswasser ist ein großes Problem, das die Sicht einschränkt und der Elektronik schadet. Bei Überwachungskameras kann Kondenswasser die Linsen trüben und dazu führen, dass die elektronischen Bauteile mit der Zeit erodieren. Wenn Kameras an einem Ort installiert sind, an dem sie ständig Luftdruckschwankungen und Regen ausgesetzt sind, besteht die Gefahr, dass Dichtungen und Bauteile Risse bekommen, was dazu führt, dass sich im Inneren Feuchtigkeit ansammelt.

Die Witterungsbedingungen sind nicht der einzige Feind der Überwachungskameras. Wenn sich die Kameras im maritimen Umfeld befinden, kann durch den Salzgehalt in der Luft das Gerät mit der Zeit korrodieren. Eine ähnliche Problemstellung ergibt sich, wenn die Kamera in medizinischen oder industriellen Bereichen eingesetzt wird, in denen starke Chemikalien verwendet werden.

Durch die Beachtung der IP-Einstufung (IP = Ingression Protection) ist ein Schutz vor Außenbedingungen möglich. Die Schutzart IP 66 schützt vor festen Stoffen wie Staub und Flüssigkeiten wie Regenwasser und bietet damit einen großen Schutzgrad. Auch ist wichtig auf die Korrelation der Betriebstemperatur mit der Temperatur des Installationsortes zu achten. Generell hat der Montageortes einen großen Einfluss darauf haben, wie gut eine Kamera funktioniert. Wichtig ist auch die Qualität der Oberflächen, auf denen Kameras montiert sind. Denn sie können Temperaturen leicht übertragen und damit die Betriebstemperatur mit beeinflussen.

# Nach Wachstum 2022 wird es im Jahr 2023 ein wenig ruckelig

Im Jahr 2022 konnte die Mehrheit der 50 größten internationalen Sicherheitsunternehmen im Bereich Videoüberwachung und Zugangskontrolle ein deutliches Marktwachstum verbuchen. Trotz dieser positiven Gesamtergebnisse gehen Experten davon aus, dass im kommenden Jahr die Branche mit Problemen kämpfen wird.

Dem Marktbericht ‚Security 50' folgend, werden die Top-10-Unternehmen die Umsatzzahlen halten können. So werden die zehn größten Hersteller im Bereich Videoüberwachung und Zugangskontrolle (Umsatzvergleich zum Jahr 2021: Hikvision Digital Technology, Dahua Technology, ASSA ABLOY, Axis Communications, Motorola Solutions, Uniview Technologies, Tiandy Technologies, Allegion, Hanwha Techwin und Aiphone keine Einbußen verbuchen. Die Marktführerschaft von Hikvision wird besonders deutlich, wenn man sich bewusst wird, dass im Jahr 2021 die 10-Milliarden-Euro-Umsatzmarke überschritten wurde. Dies entspricht einer Wachstumsrate von 16,9 Prozent gegenüber 8,7 Milliarden Euro Umsatz im Jahr 2020.

Hikvision sieht sich in dieser Toplage durch die Forcierung technologischer Innovationen, die die Schlüsselelemente für den unternehmerischen Erfolg darstellen. Nach Aussagen von Frank Zhang, VP von Hikvision, unterstützt die kontinuierliche Weiterentwicklung von Produkten und Marktposition das Kundenverhältnis und baut langfristiges Vertrauen auf.

Sechs Unternehmen wurden 2022 neu in die Security 50 aufgenommen: Die chinesischen Unternehmen Dnake (Intercom), Jovision (Video) und EVETAR (Objektiv), das US-amerikanische Unternehmen Evolv, Anbieter von Screening, die australische Ava Group mit Risikomanagement-Lösungen, und der koreanische Videoüberwachungsanboeter Webgate gehören nun zu den Topunternehmen. Alleine 15 Unternehmen der Top 50 kommen aus China. Und alleine vier unter den Top 10: Hikvision, Dahua, Uniview und Tiandy.
Durch die COVID-Situation in China

mussten die chinesischen Unternehmen im ersten Halbjahr 2022 Umsatzrückgänge im Vergleich zu 2021 verschmerzen. Die Handelssanktionen der USA gegenüber chinesischen Firmen und Produkten haben weniger Auswirkungen. Taiwanesische Hersteller wie Dynacolor, Hi Sharp und GeoVision stehen gut da und durch die Konzentration auf Nischen-Lösungen konnte die Marktposition stabilisiert werden. Der wirtschaftliche Ausblick ist stark von der Situation der OEM-Aufträge an Taiwan abhängig, die noch nicht abschließend bewertet werden können.
Rückblick 2021-2022: Bei der Biometrie, Zugangskontrolle, Videoanalyse und digitale Intelligenz verzeichneten Unternehmen in diesem Jahr alle ein deutliches Wachstum. Grund dafür ist die erhöhte Nachfrage an Sicherheits- und Netzwerkvideolösungen und die dynamische technologische Entwicklung. So werden neue und innovativere Produkte und Lösungen nachgefragt, die alte Technologien ersetzen.

Prognose 2023: Die Sicherheitsbranche sieht sich Rezessionsgefahren gegenüber. Die Nach-COVID-Zeit hält eine Vielzahl von Problemen bereit:

1. So verursachen Bauteil- und Rohstoffmangel Probleme in der Lieferkette. Und auch die Pandemiebedingten Schließungen führten zu Verlusten. Die Lieferkettenkrise verlangsamten Wachstum in den Jahren 2020 und 2021. Marktführer wie Axis sehen aber nun eine Rückkehr zu zweistelligen Wachstumsraten. Die Diversifizierung der Lieferketten durch einige Hersteller führte zu Verschiebungen im Markt.

2. Die starke Inflation beeinflusst die Preise von Dienstleistungen, Arbeitskosten und Rohmaterial. So kann man auch für die Jahre 2022 und 2023 von Preissteigerungen für Sicherheitsprodukte ausgehen. Dabei haben sich die Beziehungen zu den Kunden geändert und sowohl Zahlungs- als auch Servicemodelle haben sich verändert. Kunden werden so nicht überfordert, sondern können ihren Geschäften planvoll weiter nachgehen.

3. Natürlich beeinflusst auch der Konflikt zwischen Russland und Ukraine die Wirtschaftslage. In beiden Ländern ruht augenblicklich die Wirtschaftsaktivität von globaltätigen Sicherheitsherstellern und -anbietern.

4. Interessant sind die Auswirkungen der Datenschutzbestimmungen für die Videoüberwachung und KI-unterstützte Technologien. So ist die Branche gefordert, auf die Bestimmungen zu reagieren und bei den Softwareentwicklungen diese zu berücksichtigen.

Nach dem Top 50-Bericht könnte das Jahr 2023 trübe Wachstumsaussichten für die physische Sicherheit bereithalten. im Jahr 2022 konnte die Sicherheitsbranche wieder Wachstum verzeichnen. Nach Aussagen des Branchenzweiten Dahua Technology wird die Lage im asiatisch-pazifischen Raum, in Afrika, Lateinamerika und im Nahen Osten ‚relativ' optimistisch sein, allerdings wird ein relativ schwaches Wachstum nach Prognose des chinesischen Herstellers eintreten.

Der Weltmarkt für Videoüberwachungshardware und -software wird im Jahr 2022 voraussichtlich um 11,7 Prozent wachsen. Im Jahr 2023 um 6,4 Prozent. Auf längere Sicht wird es zu einem nachhaltigen und signifikanten Wachstum im hohen einstelligen Prozentbereich geben.

Durch die schon angesprochenen Wirtschaftsprobleme werden weniger Investitionen in Sicherheitstechnik realisiert werden. Umso wichtiger sind die Beziehungen zu Bestandskunden, da hier Ersatzinvestitionen u.a. zur Kostenreduktion des vorhandenen (Sicherheits-)Managements umgesetzt werden können.

Trends bleiben weiterhin Künstliche Intelligenz (KI), Edge Computing, Cloudlösungen und Cybersicherheit weiterhin dominieren. Aus Sicht des Marktführers werden Visualisierungslösungen verstärkt Einsatz finden. Besonders multidimensionale Technologien wie Radar, Wärmebildtechnik, Röntgendurchleuchtung, Temperaturmessung, Feuchtigkeitsmessung und Gasleckerkennung erhalten mehr Raum. Damit werden Sicherheitslösungen effizienter. Generell wird die Rolle der Sensoren bei Sicherheitsanwendungen immer wichtiger.

[Grundlage des Artikels sind Informationen in englischer Sprache auf der Website www.asmag.com]

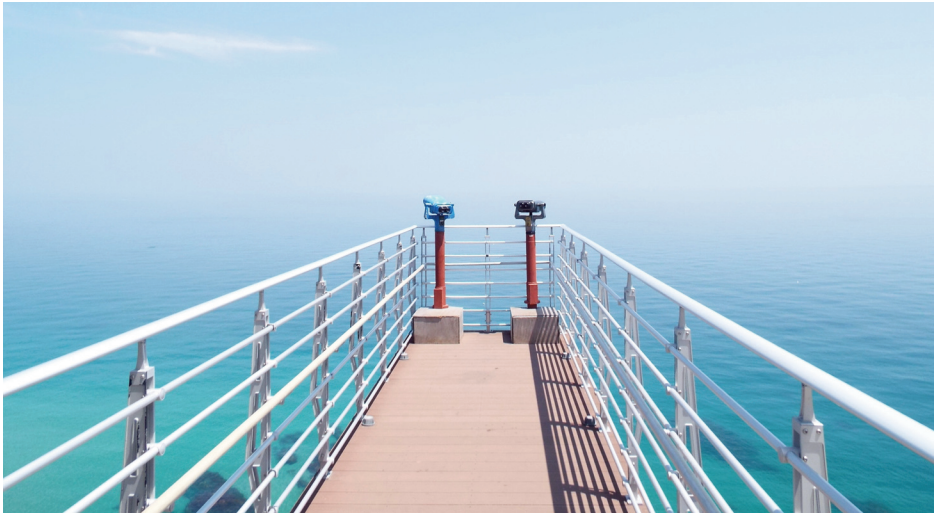
# Business-Kommunikation: Fünf Trends für 2023

## Mit Digitalisierung, Automatisierung und Cloudifizierung Resilienz stärken

**Vom russischen Angriffskrieg gegen die Ukraine über die Lieferkettenkrise bis hin zur Deglobalisierung: Wirtschaftssysteme stehen derzeit unter großem Druck. Die zunehmende Inflation und der vorherrschende Fachkräftemangel spannen die Situation zusätzlich an. Damit ihr Geschäft auch vor diesem Hintergrund am Laufen bleibt, müssen Unternehmen ihre Kommunikationsprozesse entsprechend überdenken. Der Münchner Enterprise-Cloud-Dienstleister Retarus hat fünf Trends identifiziert, die Unternehmen bei ihrer Business-Kommunikation 2023 im Blick behalten sollten.**

### 1. Cyber-Resilienz als Teil der Business-Strategie

In unsicheren Zeiten müssen Unternehmen mit immer perfideren Angriffen auf ihre Kommunikationsinfrastruktur rechnen. Ransomware gilt dabei nach wie vor als Hauptbedrohung, E-Mail als häufigstes Einfallstor. Da sich Cyberangriffe unmittelbar auf den Geschäftserfolg auswirken, muss Cyber-Resilienz ein Thema auf Vorstandsebene sein. Damit zentrale Prozesse und Infrastrukturen selbst unter außergewöhnlichen Umständen funktionieren, sollten Business-Continuity-Konzepte neben umfassenden Mechanismen zur Advanced Threat Protection auch Strategien für den Ernstfall enthalten. So ermöglicht beispielsweise eine E-Mail-Conti-



nuity-Lösung außerhalb der eigenen Infrastruktur auch in Notfallsituationen eine nahtlose Kommunikation per E-Mail.
Geopolitische Konflikte erhöhen das Risiko für Cyberattacken aus bestimmten Regionen zusätzlich. Mit Services wie der Retarus Predelivery Logic https://tinyurl.com/3tyydk78 lassen sich Nachrichten anhand ihrer GeoIP vorsorglich isolieren - sei es aus reinen Sicherheitserwägungen oder aufgrund interner Compliance-Vor- gaben.

## 2. Nachhaltige Cloudifizierung von Geschäftsmodellen

Digitale Geschäftsmodelle setzen sich durch. Die Cloud bildet hierfür die Basis. Spätestens seit der COVID-19-Pandemie und den damit verbundenen Homeoffice-Regelungen haben sich digitale Angebote und virtuelle Zusammenarbeit durchgesetzt. Cloud Computing ist mittlerweile fest in den IT-Abteilungen etabliert. Andererseits sehen sich Unternehmen mit einem erheblichen Kostendruck konfrontiert. Budgetverantwortliche sind angehalten, möglichst kosteneffizient und nachhaltig zu planen. Auch hier schaffen Cloud Services Abhilfe. Sie sind flexibel und skalierbar, sodass die Services sich exakt an den aktuellen Bedarf anpassen und Über- oder Unterkapazitäten vermeiden lassen. Folglich lassen sich innovative Angebote schneller auf dem Markt einführen und Kosten besser regulieren.
Unternehmen profitieren dabei besonders von Cloud-Dienstleistern, die mit Plattform-Angeboten, Managed Services und innovativen Lösungen die eigene IT-Infrastruktur entlasten. Unternehmen werden zudem optimal dabei unterstützt, neue Geschäftsmodelle einzuführen, da ein Cloud Service agiles Handeln und eine direkte, schnelle Kommunikation in den Markt ermöglicht.
So liefert etwa die Retarus Enterprise Cloud https://tinyurl.com/5hahp2z3 eine Vielfalt an Services, die Unternehmen für diverse Anwendungsszenarien in unterschiedlichen Industrien nutzen können. Dabei erfüllen die Services alle gängigen Branchenstandards. Standardschnittstellen ermöglichen die nahtlose Einbindung in On-Premises-, Cloud- und hybride Infrastrukturen.

## 3. Verstärkte Automatisierung in der Supply Chain

Das vergangene Jahr hat gezeigt, wie störanfällig Lieferketten sind. Zudem bekommen Firmen den Fachkräftemangel derzeit so stark zu spüren wie noch nie zuvor. 2023 wird es für Unternehmen folglich darauf ankommen, ihre Lieferketten resilienter zu gestalten und verstärkt auf Automatisierungstechnologien zu setzen. Dadurch wirken sie dem wachsenden Qualifikationsdefizit entgegen und steigern ihre Produktivität in der Supply Chain.
Werden beispielsweise eingehende Geschäftsdokumente automatisiert erfasst und verarbeitet, entfällt die zeitraubende manuelle Datenerfassung von Warenbestellungen und Aufträgen. Unternehmen profitieren von einer effizienteren Prozesskommunikation, einem reibungslosen Cashflow und Kostensenkungen von rund 60 Prozent im Vergleich zur manuellen Auftragsabwicklung. Fachkräfte können sich wieder auf Innovationen konzentrieren und dadurch dem Unternehmen idealerweise Wettbewerbsvorteile verschaffen.

## 4. Optimierte Customer Journey

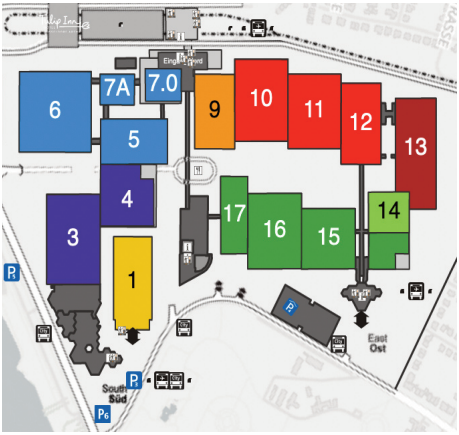
Kunden haben nicht zuletzt aufgrund der Pandemie gestiegene Ansprüche an digital Angebote. Sie sind mittlerweile an digitale Interaktionen und Touchpoints gewöhnt. Eine positive Customer Experience ist Grundvoraussetzung für den Geschäftserfolg. Erst eine zuverlässige, sichere und individuell gestaltete Business-Kommunikation ermöglicht das Angebot vielfältiger Touchpoints mit den Kunden und schafft dadurch Kundenzufriedenheit und -bindung. Unternehmen, die nicht in ihre Kundenkommunikation investieren, verlieren Kunden an ihre Wettbewerber. Mit digitalen Kommunikationsplattformen bedienen Unternehmen digitale Touchpoints wie Multi-Faktor-Authentifizierung, E-Mail-Bestellbestätigungen, transaktionale E-Mails wie Newsletter, Wetter-Warnungen per SMS oder Statusmeldungen. Die Services lassen sich idealerweise über standardisierte APIs nahtlos in Business-Applikationen oder digitale Plattformen integrieren und jederzeit schnell und flexibel an neue Anforderungen anpassen.

## 5. Komplexere Datenschutz-Vorgaben

Laut dem Analystenhaus Gartner werden 75 Prozent der Weltbevölkerung bis 2024 ihre persönlichen Daten durch Datenschutzbestimmungen abgesichert haben. Gesetzliche Vorgaben spielen eine immer größere Rolle, denn die regulatorischen Anforderungen entwickeln sich international ständig weiter und werden zunehmend komplexer.
Unternehmen drohen bei Verstößen hohe Geldbußen. Umso wichtiger ist es, bei der Auswahl eines externen Dienstleisters darauf zu achten, dass dieser alle aktuellen Datenschutz-Richtlinien befolgt.
Idealerweise erfüllt der Service Provider nicht nur die DSGVO-Vorgaben, sondern auch branchenspezifische Standards und individuelle Compliance-Anforderungen. Alle Daten sollten in lokalen, auditierbaren Rechenzentren verarbeitet werden. Einige Anbieter sichern dies ihren Kunden bereits heute per Service Level Agreements vertraglich zu.

## Retail Technology Stage in Halle 6 / I61

Auf der Retail Technology Stage werden Entwicklungen und Trends im Bereich Retail Technology anhand aktueller Use-Cases präsentiert. Die Themen umfassen u. a. Mobile Solutions, die neuesten Entwicklungen bei Self-Checkout und Self-Scanning, Trends im Bereich Analytics, RFID, IoT, Smart Stores und Payment sowie aktuelle Sicherheitstechnik. Erfahren Sie die Dimension Retail Technology nicht nur im Austausch mit den Ausstellenden, die ihre neuesten Lösungen für Seamless Stores, Customer Centricity oder den Einsatz von KI präsentieren, sondern nehmen Sie Anreize und Inspirationen aus den Vorträgen der Retail Technology Stage mit. Besucher der EuroShop können kostenfrei und ohne Voranmeldung die Vorträge der Retail Technology Stage besuchen und sich in kompakten Vorträgen über aktuelle Entwicklungen informieren.




**Veranstaltungsdatum & Öffnungszeiten**
Veranstaltungsdatum
26. Februar - 02. März 2023
Öffnungszeiten für Besucher
täglich: 10:00 - 18:00 Uhr
Öffnungszeiten für Aussteller

**Messe Düsseldorf GmbH**
**Messeplatz**
**40474 Düsseldorf**
**Tel: +49 211 4560-01**
**Fax: +49 211 4560-668**
**Web: www.messe-duesseldorf.de**

EuroShop
THE WORLD'S NO. 1 RETAIL
TRADE FAIR 26 FEB – 2 MAR 2023
DÜSSELDORF, GERMANY

PRIME TIME.
FÜR IHR BUSINESS.

Messe Düsseldorf

# Standards als Trendsetter für die Sicherheitsbranche

## Standards by OSS im Gespräch mit Herstellern und Anwendern

**Die non-profit Organisation OSS-Association Open Security Association) etabliert standardisierte Protokolle für die internationale Sicherheitsindustrie. Die Mitglieder und angeschlossenen Unternehmen entwickeln Komponenten und Codierungen sicherheitsrelevanter Hard- und Software. Im Rahmen des ersten Media-Talks fragten wir Frederik Hamburg, Vorsitzender der OSS-Association und Geschäftsführer der ZUGANG GmbH, nach seiner Motivation und seinen Erfahrungen mit dem Einzug der Standards in der Sicherheitsindustrie. Wir sprachen zudem mit Matthias Schmid, Manager im Business Development bei ASSA ABLOY, über die Vorteile des Einsatzes von Standards aus Herstellersicht. Einen weiteren Blick aus Herstellersicht gab Harmut Beckmann, Sales Manager bei Uhlmann & Zacher, und schließlich zeigte uns Patrick Senneka, Senior Product Developer in der IT-Abteilung der Fraport AG, interessante Sichtweisen zum Einsatz von Standard-Zugangskontrolle aus Sicht des Anwenders auf.**

**Frederik Hamburg ist Vorsitzender der OSS-Association. Wie ordnen Sie Standards in der Sicherheits-Industrie ein?**

Eigentlich stammt die Grundidee von den Anwendern und damit auch meine Motivation vor allem von denjenigen, die viele Schlösser im Einsatz haben. Ihr Anliegen war und ist es, sich von den proprietären Systemen der Hersteller zu lösen. Denn mittlerweile sind die Anforderungen an komplexe Sicherheitssysteme gestiegen. Der Markt ist oft unübersichtlich und da entstand der Wunsch der Kunden, dass die unterschiedlichen Systeme miteinander kommunizieren können, ganz unabhängig von den Herstellern.

**Wann wurde denn die OSS-Association gegründet?**

Schon im Jahr 2015 wurde die OSS-Association gegründet. Die Idee war von Anfang an, „aus der Industrie für die Industrie" Standards zu entwickeln. Außerdem wollten wir immer dann, wenn es neue Anforderungen gibt, in die Weiterentwicklung gehen. Die Mitglieder der OSS-Association umfassen decken das gesamte Spektrum der Sicherheitsbranche ab.
Gemeinsam können sie so an der Fortentwicklung der Standards mitwirken. Ziel ist, die einzelnen Komponenten zu verbinden, sodass zum Beispiel die Schlüsselkarte mit der Software der Datenbank kommuniziert, um Berechtigungen für Türschlösser sowie Zutrittskontroll- und Zeiterfassungssystemen auslesen zu können. Diese Kommunikation basiert auf Standards by OSS, damit die Kompatibilität mit und die Unabhängigkeit von Herstellern unterschiedlicher Marken gewährleistet ist.

**Haben die Anwender Einfluss auf die Weiterentwicklung?**

Auf jeden Fall, die Anwender sind unsere erste Quelle, wenn es um die Identifikation von notwendigen Weiterentwicklungen geht. Die Hersteller und ihre Kunden gehen da in den Dialog. Vor der Pandemie haben wir Anwendertreffen durchgeführt, um in direktem Kontakt Kundenwünsche in Erfahrung zu bringen. Wir planen das nächste Anwendertreffen im Jahr 2023. Solche Anwendertreffen die-

nen dazu, das „Ohr am Kunden zu haben" und zu verstehen, welche Komponenten weiterentwickelt, welche hinzukommen sollten. Aber wir stellen auch immer mehr fest, dass der Bedarf an dem Einsatz von Standards steigt – auch wenn es manche Hersteller gibt, die die Vorteile der Standards noch nicht wahrhaben wollen. Der Einsatz von Standards bedeutet auch, sich anderen Systemen gegenüber zu öffnen und das – zugegebenermaßen geringe – Risiko einzugehen, dass sich die Kunden für andere Produkte entscheiden (können), da die Proprietät aufgegeben wird. Doch de facto ist das Gegenteil der Fall. Mit dem Einsatz von Standards by OSS werden Hersteller wettbewerbsfähig und sind durch die stetige Weiterentwicklung der Standards auch in dieser Hinsicht immer auf dem aktuellen Stand. Einzelne Komponenten von unterschiedlichen Herstellern können nun miteinander kommunizieren. Der Endkunde schätzt diese Flexibilität, die auch eine Kostensenkung nach sich ziehen kann, da die Auswahl größer wird und die Abhängigkeit von einem Hersteller aufgehoben ist.

## ASSA ABLOY

**Als Hersteller von Sicherheitstechnik ist ASSA ABLOY der große Player auf dem internationalen Markt. In über 70 Ländern mit mehr als 50.000 Mitarbeitern und einem Jahresumsatz von über 9 Milliarden Euro zählt das Unternehmen zu den führenden in der Sicherheitsbranche. Allein in der DACH-Region wurden im Jahr 2021, 275 Millionen Euro durch die ASSA ABLOY Einheit „Opening Solutions" umgesetzt und das vor allem in dem Bereich der elektronischen Zugangskontrolle, Schutzeinrichtungen und Schließanlagen. Mathias Schmid ist seit 2019 als Business Development Manager Access Control bei der ASSA ABLOY Sicherheitstechnik GmbH tätig und verantwortet dort die Weiterentwicklung des Lösungsportfolios im Bereich der elektronischen Zutrittssteuerungssysteme. Wir fragten ihn nach der Entwicklung von Standards aus Herstellersicht.**

**Welche Motivation hatte ASSA ABLOY als Hersteller, den Einsatz von Standards voranzubringen?**

ASSA ABLOY setzt seit 2015 Standard Offline ein und ist eines der Gründungsmitglieder der OSS- Association e.V. Für unsere Kunden, Endkunden wie Systemintegratoren, haben die Erwartung bzw. Anforderung an uns als System- und Komponentenanbieter gestellt, dass die elektronischen Beschläge und Zylinder auch mit Produkten anderer Anbieter interagieren können. Das war für uns der Startschuss, das Thema Entwicklung von Standards gemeinsam mit der OSS-Association voranzubringen. Das Produktportfolio Aperio, das seit mehr als 15 Jahren sowohl die Online-Integration via Funk als auch die Offline-Integration via „Data on Card" beinhaltet, unterstützt OSS Standard Offline ab Werk. Das ermöglicht unseren Kunden und Partnern, die Aperio Komponenten einfach in ihr System zu integrieren und bei Bedarf mit anderen Komponenten kommunizieren zu lassen. Die Kunden entscheiden sich also für ein Produkt, das sie überzeugt. Das scheint zuerst einmal nicht günstig für die Hersteller. Denn die Zeiten von proprietären Systemen gehören damit der Vergangenheit an und die Lieferantenbindung ist ein Stück weit aufgelöst.

**Welche Vorteile gibt es dann aus Herstellersicht für den Einsatz von Standards?**

Die Lieferantenunabhängigkeit scheint auf den ersten Blick nachteilig für die Hersteller. Doch das Gegenteil ist der Fall. Denn mit den wachsenden Marktanforderungen kann alles das, was der Kunde sucht und erwartet, tatsächlich geliefert werden. Denn die durch die Standards by OSS möglich gewordene Integration unterschiedlicher Komponenten und Produkte verschiedener Hersteller bietet oft bessere Lösungen als ein einzelner Anbieter mit potenziell begrenztem Portfolio bieten kann. Deshalb eröffnen die Standards auch für uns als Hersteller einen größeren Spielraum in der Integration anderer Systeme und wir können das Optimum für den Kunden entstehen lassen.
Wir sehen dabei immer wieder, wie wichtig es ist, dass die Hersteller bei neuen Anforderungen an einer gemeinsamen Entwicklung arbeiten, so wie es die OSS-Association praktiziert. Und nicht nur das: Bei Ausschreibungen können Systemintegratoren Teilkomponenten unterschiedlicher Hersteller anbieten, denn diese sind dank der herstellerunabhängigen Standards mit anderen kompatibel geworden. Der Vorteil für den Ausschreibenden ist die „perfekte Lösung", die seinen

Anforderungen entspricht und die er im weiteren Verlauf um standardkonforme Komponenten einfach erweitern kann. Das fördert die Akzeptanz der Zutrittssteuerungs- und Schließsysteme und fördert damit das Marktwachstum für die gesamte Branche.

**Wohin geht denn die Reise in den nächsten Jahren?**

Ein wichtiges Thema wird sicherlich in den nächsten Jahren der Mobile Access sein, d.h. die Zugangskontrolle über mobile Endgeräte. Von der Branche wird das gefordert, aber die Akzeptanz und Verbreitung in Deutschland ist noch nicht flächendeckend vorhanden. Auch hier wird man sehen, ob ein Standard der Treiber für den Mobile Access sein kann.

## Fraport

**Aus Kundensicht bietet der Einsatz von Standards viele Vorteile. Wir befragten Patrick Senneka, seit 2012 bei der Fraport AG, der für den Einsatz und für die Weiterentwicklung des Produktes ESA (Elektronische Schließanlage) zuständig ist, nach seinen Erfahrungen.**

**Was ist die Motivation für Sie, Standards einzusetzen?**

Die OSS-SO Standardisierung ermöglicht es, Software- und Hardware-Komponenten unterschiedlicher Anbieter in die Gesamtlösung zu integrieren. Somit gewährleisten wir Investitionsschutz und verzichten gleichzeitig auf proprietäre Systeme. Insgesamt setzen wir ca. 75.000 Flughafenausweise und ca. 7500 Offlineleser am Flughafen Frankfurt am Main ein. Wir können mit dem Einsatz von Standard Offline große Installationen realisieren und beispielsweise bei Lieferschwierigkeiten oder besonderen Anforderungen auf alternative OSS-Komponenten zurückgreifen. Das ist ein großer Vorteil für uns. Der Einsatz von Standards ermöglicht eine hohe Interoperabilität der Produkte und Flexibilität bei der Implementierung.

**Ein Flughafen hat besondere Anforderungen an die Sicherheit. Wie ist dies durch den Einsatz von Standards gesichert?**

Stellen Sie sich vor, jeder der Mitarbeitenden bei Fraport hätte einen eigenen Schlüssel für die unterschiedlichen Zugangsberechtigungen. Der Mitarbeitende scheidet aus, verliert den Schlüssel, wechselt die Position und damit auch die Zugangsberechtigungen. Was für ein Aufwand, dies über mechanische Schlüssel abzuwickeln und dabei noch die Sicherheit zu gewährleisten! Die elektronischen

Schließanlagen und damit auch das Protokoll von Standard Offline ermöglicht es zeitlich begrenzte Schlüssel / Berechtigungen auszustellen, die im zentralen System mit einem Klick geändert werden können. Damit ist sowohl die Sicherheit gewährleistet als auch ein optimierter Einsatz an Ressourcen.

**Mobile Access, so die Prognose, wird in den nächsten Jahren eine zunehmend wichtige Rolle für die Zugangskontrolle spielen. Wie sieht es denn mit dem Mobile Access am Flughafen aus?**

Das ist ein Thema, das für uns aktuell zwar interessant, aber weniger relevant ist. Die für die Sicherheitsbereiche geltenden Gesetze fordern das dauerhafte Tragen eines Sichtmerkmals, was mit mobilen Geräten momentan nicht zu realisieren ist.

**Was ist Ihr Wunsch für 2023?**

Ein Anwendertreffen, um über neue Entwicklungen zu diskutieren und in den Austausch mit anderen Anwendern zu kommen, wäre wichtig für die Fortentwicklung der Standards by OSS.

## Uhlmann & Zacher

**Ein weiterer Hersteller, bzw. OEM, (Original Equipment Manufacturer), ist das familiengeführte Unternehmen Uhlmann & Zacher. Insgesamt mehr als 1.000.000 elektronische Schließeinheiten produzierte das Unternehmen bislang. Wir fragten Hartmut Beckmann, Prokurist und Sales Manager bei Uhlmann & Zacher, nach seinen Erfahrungen zum Einsatz von Standards in Deutschland und auch weltweit.**

**Herr Beckmann, wie schätzen Sie die Situation in Deutschland zum Einsatz von Standards ein?**

In Deutschland existieren noch einige Hersteller, die es bevorzugen, ihre eigenen, proprietären Systeme einzusetzen. Diese sehen im Einsatz von Standards eigentlich einen Verlust ihrer Marktmacht. Es gibt jedoch auf Hersteller- wie auf Anwenderseite Unternehmen, die die Vorteile der Standards für sich entdeckt haben. Wenn viele Schließanlagen für eine große Anzahl von Menschen sehr hohe Sicherheitsstandards aufweisen müssen, eröffnen die Standards neue Möglichkeiten. Es wäre ja auch erstrebenswert, dass die Standards by OSS länderübergreifend, also im internationalen Zusammenhang eingesetzt werden könnten. Hier haben wir z.B. in Frankreich einige Partner, die OSS-SO verwenden.

**Was ist aus Ihrer Sicht der Vorteil von Standards by OSS?**

Uhlmann & Zacher verkauft nicht an Endkunden, das ist die Strategie unseres Unternehmens. Durch OSS-SO haben wir die Möglichkeit neue Integrationspartner zu gewinnen, ohne dass diese Partner eine proprietäre Lösung entwickeln müssen.

**Wie sehen Sie die Zukunft von Mobile Standard?**

Mobile Endgeräte sind zum Beispiel mit Bluetooth ausgestattet. Hier sorgt ein Standard für die Kommunikationsfähigkeit unterschiedlicher Endgeräte. In dem Mobile Sektor tummeln sich verschiedene Hersteller, zum Teil neu am Start und im Wachstum, zum Teil etabliert. In diesem Bereich sorgt der Standard dafür, dass die Technologie zukunftsfähig bleibt, auch wenn ein Unternehmen wieder vom Markt verschwindet.

**Und der Gesamtblick auf Deutschland? Wie sieht es mit der mobilen Nutzung, d.h. Mobile Access in Deutschland aus?**

In Deutschland ist die Akzeptanz von der Steuerung der mobilen Zugangskontrolle – ganz im Gegensatz zu anderen Ländern - noch etwas zögerlich. Aktuell allerdings arbeiten wir an einem Projekt um eine eigene Mobile Access Plattform zu etablieren. Auf die nächsten Schritte und die Weiterentwicklung freuen wir uns.

**Ihr Blick in die Zukunft, was würden Sie sich wünschen?**

Wir würden uns freuen, wenn große Firmen – unabhängig vom Wettbewerbsdenken – kooperieren und an der Weiterentwicklung der Standards mitwirken würden. Aus unserer Sicht wird der Vertrieb wesentlich vereinfacht, wenn möglichst viele größere Projekte (und Unternehmen) auf den Standard by OSS setzen würden.

**Die Gespräche führte Martina Müller, pr-ide GbR, im Auftrag der OSS-Asscociation**
**[www.oss-association.com]**

©pixabay.com

# Cybersecurity Trends 2023

Autor: Todd Moore, VP Encryption Products bei Thales

**Das Security-Jahr 2022 neigt sich dem Ende zu und es ist Zeit, einen Ausblick auf das zu wagen, was die Branche 2023 erwarten wird. Hierbei lassen sich aus Sicht von Thales die folgenden sechs Trends beobachten.**

# IT-Trends 2023

**1. Massenentlassungen in der Tech-Branche werden eine große Sicherheitslücke auslösen**

Massenentlassungen bei Tech Firmen – von denen viele virtuell stattfinden – werden zweifellos zu großen Sicherheitslücken führen, sei es durch verärgerte Mitarbeiterinnen und Mitarbeiter oder durch verkleinerte IT-Teams, die nicht die richtigen Schritte zur Aufhebung der Zugriffsrechte unternehmen.

Auf die eine oder andere Weise werden wir im Jahr 2023 einen größeren Sicherheitsverstoß erleben, der auf schlecht verwaltete Benutzerkonten zurückzuführen ist.

**2. Datensouveränität in Multi-Cloud-Umgebungen**

Vor einem Jahr bedeutete Souveränität, dass die Daten die Grenzen des Unternehmens nicht verlassen. Heute verstehen einige Unternehmen unter Souveränität die Möglichkeit, den Speicherort ihrer Daten zu kontrollieren. Sie verlagern den Standort ihrer Daten in regelmäßigen Abständen an einen anderen Ort, um sie vor fremden Zugriffen zu schützen.

Dieser Trend wird anhalten und der Datentransfer für globale Unternehmen zur obersten Priorität werden. Um dies zu erreichen, müssen Unternehmen sicherstellen, dass sie über Cloud-agnostische Technologien verfügen, damit sie eine Workload in der Cloud problemlos an einen anderen Standort verlagern können.

DevOps-Ansätze können auch helfen, indem sie Cloud-neutralen Code schreiben, so dass Workloads überall gestartet werden können.

**3. Die Rezession wird die Konsolidierungsstrategien von Unternehmen beschleunigen**

Unternehmen werden sich von Einzellösungen verabschieden und zur Datenkonsolidierung zurückkehren. Angesichts der Rezession, der enorm steigenden Lebenshaltungskosten und des sich abzeichnenden Fachkräftemangels, werden Vereinfachung und Effizienz im Jahr 2023 zu den wichtigsten Prioritäten gehören. Die Automatisierung wird einen gewissen Beitrag zur Vereinfachung leisten, aber Unternehmen müssen mit den richtigen Partnern zusammenarbeiten, um sicherzustellen, dass die Assets und Daten angemessen abgesichert sind.

Durch die Kombination von robuster Verschlüsselung, richtlinienbasierten Zugriffskontrollen, zentraler Verwaltung und unternehmensweitem Schlüsselmanagement können Unternehmen konsolidieren und gleichzeitig sicherstellen, dass ihre wertvollen Ressourcen geschützt sind sowie die gesetzlichen Vorschriften eingehalten werden.

**4. Vernetzte Autos werden das nächste große Ziel für Hacker sein**

Der Markt für vernetzte Autos wächst weiter und wird zu einem immer größeren Ziel für Ransomware-Gruppen. Vernetzte Autos arbeiten mit Millionen von Computercodes, die, wenn sie nicht richtig gesichert sind, leicht gehackt werden können. Die Installation von Schadsoftware im Betriebssystem eines Fahrzeugs könnte schwerwiegende Folgen haben – sei es, dass die Bremsen auf einer viel befahrenen Straße deaktiviert werden, dass Benutzer ausgesperrt werden, bis ein Lösegeld gezahlt wird oder Unternehmensdaten gestohlen werden.

Zusätzliche Aufmerksamkeit muss auch den Elektrofahrzeugen gewidmet werden. Deren Entwicklungstempo könnte zusätzliche Sicherheitsrisiken mit sich bringen. Security by Design ist entscheidend und es ist unerlässlich, dass Automobilhersteller von Anfang an robuste Cybersicherheitsstandards einbauen.

**5. Das Metaverse wird eine neue Grenze für Hacker und Erpresser eröffnen**

Mit der zunehmenden Beliebtheit des Metaverse und anderer virtueller Plattformen, wird virtuellen Diensten und Ressourcen eine immer größere Bedeutung beigemessen – die Nutzer beginnen, diese Güter genauso zu schätzen wie physische. Vor allem Kinder sind frühe Nutzer dieser Plattformen und verwenden oft die Bankdaten ihrer Eltern, um virtuelle Währungen zu kaufen, was sie zu einem verwundbaren Ziel und einem potenziellen Einfallstor für Angriffe macht.

Diese Plattformen sind sehr schnell im Mainstream angekommen, so dass das Eigentum an diesen virtuellen Vermögenswerten einer strengen Kontrolle unterworfen werden muss sowie mit dem gleichen Maß an Sicherheit und Kontrolle wie bei anderen Plattformen begegnet werden sollte.

**6. Das Geschäft mit der Computerkriminalität: Erpresserische Ransomware wird zunehmen**

Angriffe auf kritische Infrastrukturen

werden auch im Jahr 2023 weiterhin stattfinden. Die Taktiken dieser Bedrohungsakteure werden wahrscheinlich unverändert bleiben. Die Realität ist, dass Cyberkriminelle wie ein Unternehmen agieren.
Wenn sie mit ihren Angriffen weiterhin erfolgreich sind, werden sie keine Notwendigkeit sehen, damit aufzuhören.

Die Art und Weise, wie sich Cyberkriminelle Zugang verschaffen, verändert sich zwar nicht, jedoch die Vorgehensweise bei der Lösegelderpressung. Angriffe mit doppelter und sogar dreifacher Erpressung gegen kritische Infrastrukturen werden sich zügig ausbreiten, da sie den Angreifern größere Lösegeldsummen und mehrere Zahlungsmöglichkeiten in Aussicht stellen. Die so erzielten Einnahmen werden dann wieder in ihre eigene Infrastruktur investiert.

# Trends 2023

## Was sind die Vorhersagen und Trends für den IT-Dienstleistungssektor im Jahr 2023?

**Expertenmeinung von Colin Blumenthal, Vizepräsident für IT-Dienstleistungen bei Sharp Europe.**

**Die heutige Organisation stützt sich zunehmend auf IT-Dienstleistungen und die Auslagerung bestimmter Verantwortlichkeiten, um ihr Wachstum zu unterstützen und zu fördern. Die letzten zwölf Monate waren für Unternehmen aller Größenordnungen und insbesondere für KMU nicht einfach. Externe Faktoren haben ihre Finanzen unter Druck gesetzt und ihre Ressourcen bis zum Äußersten beansprucht.**

**Dadurch rückten Fragen nach Effizienz, Sicherheit und Wertschöpfung in den Vordergrund. Im digitalen Zeitalter müssen wir uns noch stärker auf Strategie und Zusammenarbeit konzentrieren, um die begrenzten Ressourcen und das knappe Personal voll ausschöpfen zu können. In diesem Zusammenhang werden wir versuchen, einen Ausblick auf die neuen Trends zu geben, die 2023 sowie die kommenden Monate und Jahre für die IT-Dienstleistungsbranche bereithalten.**

1 Migration in die Cloud: Die Migration von Geschäften, Dienstleistungen und Prozessen von KMU in die öffentliche Cloud, ein Trend, den wir in den letzten Jahren zunehmend beobachten konnten, zeigt keine Anzeichen einer Verlangsamung. Laut einer aktuellen Studie[1] wird die Nutzung der öffentlichen Cloud durch europäische KMU zwischen 2020 und 2021 um 5 % zunehmen. Darüber hinaus verlassen sich 41 % der Organisationen in der EU auf die eine oder andere Weise auf solche Dienste, insbesondere um ihre E-Mail-Systeme zu hosten und Dateien in elektronischem Format zu speichern.Dieser Trend dürfte sich fortsetzen und stabil wachsen. Viele unserer Kunden sind beispielsweise zur öffentlichen Cloud Microsoft 365 gewechselt - dem derzeit mit Abstand dominantesten Akteur auf dem Markt für kleine und mittlere Unternehmen.

# IT-Trends 2023

2 Zunahme der Telearbeit: Die stetige Verlagerung von Arbeitslasten, Prozessen und Daten in die Cloud und auf interne Infrastrukturen hat es den Unternehmen ermöglicht, ihren Mitarbeitern eine stärker hybride Umgebung zu bieten. Dieses Modell wird beliebt bleiben, da es den Mitarbeitern mehr Flexibilität und Kontrolle bietet - nicht nur am Arbeitsplatz, sondern auch auf die Art und Weise. Kleine und mittlere Unternehmen brauchen erstklassige IT-Umgebungen, um eine neue Generation zu unterstützen, die geschickter mit neuen Technologien umgeht und anspruchsvoller ist als früher. Dieser Faktor wird entscheidend sein, wenn es darum geht, die besten Talente zu rekrutieren und zu halten. Durch den Aufbau der richtigen Infrastruktur schaffen Organisationen ein echtes Wertangebot, insbesondere für die Generation der jungen Menschen, die in den Markt eintreten.

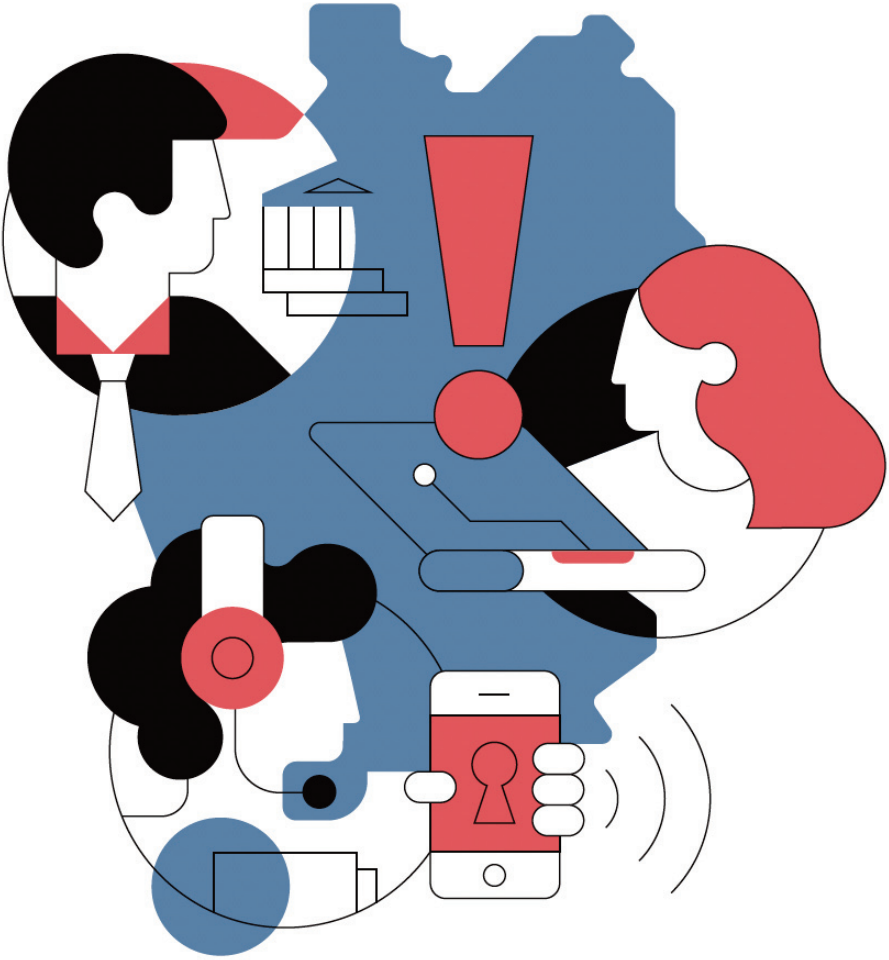
3 Sicherheit um jeden Preis: Da die Menge an Informationen, die in der öffentlichen Cloud gehostet werden, nie dagewesene Ausmaße annimmt, müssen Unternehmen über die Frage des Datenschutzes nachdenken. Dies reicht von der offensichtlichsten Software (gegen Viren, Malware oder ähnliches) bis hin zur Einführung strenger Backup-Richtlinien, da die Anbieter öffentlicher Clouds diese nicht immer selbst durchführen (diese Verantwortung liegt bei den Unternehmen). Das Bewusstsein für die Datensicherheit und der Bedarf an ständiger Unterstützung werden daher im nächsten Jahr entscheidende Trends sein. Da die Kosten immer stärker in den Fokus rücken, werden die Unternehmen in allen Bereichen nach Einsparmöglichkeiten suchen. Und die Sicherheit gehört zu diesen Bereichen, in denen Ausgabenkürzungen in Betracht gezogen werden könnten.

Allerdings wäre eine solche Entscheidung in jeder Organisation schlecht beraten. Ein ernsthaftes Datenleck oder ein Hackerangriff reicht aus, um ein Unternehmen aus dem Verkehr zu ziehen und in den Bankrott zu treiben. Einige Statistiken zeigen, dass 60 % der Unternehmen innerhalb von sechs Monaten nach einem schweren Cyberangriff schließen würden. Wie bei den Vorteilen der Sicherheit müssen die Anbieter von IT-Dienstleistungen den Wert ihrer Produkte, die ihren Kunden gewidmet sind, besser hervorheben. Nur wenn sie einen ausgefeilteren Ansatz verfolgen, können diese ihre Bedeutung voll und ganz unter Beweis stellen. Diese Vorgehensweise dürfte sich in Zukunft zu einem wichtigen Trend entwickeln.

4 Datenautomatisierung: Im Jahr 2023 dürfte die Datenverwaltung, ähnlich wie die von Microsoft Power BI bereitgestellten Fähigkeiten, weiter an Bedeutung gewinnen. Diese Business-Intelligence-Plattform bietet Geschäftsanwendern mit nicht-technischen Profilen die Werkzeuge, die sie benötigen, um Daten zu aggregieren, zu analysieren, zu visualisieren und weiterzugeben. Bis vor kurzem war diese Technologie mittleren und großen Unternehmen vorbehalten, aber wir beginnen zu sehen, dass auch kleine Unternehmen die Vorteile dieser Technologie voll ausschöpfen. Ob sie nun mit IT-Dienstleistungspartnern zusammenarbeiten oder auf sich allein gestellt sind, auch kleine Unternehmen produzieren mittlerweile wertvolle Informationen. Die Automatisierung von Prozessen wird auch 2023 ein starker Trend bleiben. Wir erleben derzeit einen Schub in Richtung Prozessautomatisierung - nicht nur, um mühsame Aufgaben zu rationalisieren, sondern auch, um Workflows effizienter zu gestalten. Angesichts des finanziellen Drucks, dem Organisationen aller Größen ausgesetzt sind, kann die Automatisierung nämlich dabei helfen, die laufenden Kosten zu senken.

5 Voice over IP: Es wird erwartet, dass die IP-Telefonie im Jahr 2023 einen großen Hype erleben wird. Denn das Integrated Services Digital Network (ISDN) und das Public Switched Telephone Network (PTSN) entsprechen nicht mehr den Bedürfnissen der Nutzer in einer immer stärker digital ausgerichteten Welt. So wird ISDN 2025 abgeschaltet, was IT-Dienstleistern die Möglichkeit gibt, ihren Kunden Unified Communications und IP-basierte Lösungen anzubieten. Organisationen, die ihre Überlegungen zur Umstellung auf IP-Telefonie aufschieben, könnten sich mit einem Mangel an Ressourcen konfrontiert sehen, aber auch mit einem Mangel an qualifiziertem Personal, das diese Aufgabe bewältigen kann. Wir sind bereits in Gesprächen mit vielen Organisationen, die einen solchen Übergang anstreben, sehr engagiert. Für viele andere bleibt jedoch noch viel zu tun, um das Bewusstsein für die Vorteile und die Notwendigkeit einer möglichst raschen Umstellung zu schärfen.

# Die Lage der IT-Sicherheit in Deutschland 2022



Bundesamt
für Sicherheit in der
Informationstechnik

**Download**
https://tinyurl.com/2s6daxjp

Deutschland
Digital•Sicher•BSI•

**Auch 2023 wird das wirtschaftliche Klima weiter davon geprägt sein, Kosten zu senken und die Effizienz zu steigern. Der Zukunftsblick vieler Unternehmen richtet sich daher auf innovative Technologien, die hier helfen können. Liz Centoni, Chief Strategy Officer und GM of Applications bei Cisco, skizziert darum die sieben Technologietrends für 2023 aus den Bereichen Security, Effizientsteigerung im Netzwerk, Nachhaltigkeit und KI.**

Im Zentrum der IT-Aufgaben stehen 2023 IT-Securtiy und Effizienzsteigerung: Laut Gartner werden bis 2025 60% der Unternehmen weltweit Zero Trust als Grundlage ihrer Security-Architektur definieren – und 80% der Unternehmen weltweit werden eine Strategie implementieren, die Web-Anwendungen, Cloud-Services und private Apps über eine einheitliche Plattform laufen lassen. Dazu werden auch KI und Nachhaltigkeit immer wichtiger.

# Trends: Security, Netzwerk, Nachhaltigkeit

## Tech-Trends 2023 - 7 Trends für das neue Jahr

**Security: Cloud Native Application Protection Platform (CNAPP) und Quantenkryptographie auf dem Vormarsch • Network: Full-Stack Observability (FSO) und Internet of Things (IoT) steigern Unternehmenseffizienz und -resilienz • Nachhaltigkeit & Künstliche Intelligenz mit konkretem Einfluss**

# IT-Security

### 1 Anwendungs- und API-Sicherheit

Da moderne Cloud-Native-Umgebungen immer mehr zum Geschäftsmotor werden, ist deren Schutz entscheidend. Im Jahr 2023 werden Entwickler weitere Tools an die Hand bekommen, um verteilte Anwendungsarchitekturen zu verwalten und zu sichern. Außerdem wird es eine weitere Entwicklung hin zu Tools geben, die es Entwicklern, SREs und Sicherheitsexperten ermöglichen, nahtlos zusammenzuarbeiten. Das Ganze trägt dann das klangvolle Akronym CNAPP - Cloud Native Application Protection Platform.

### 2 Vormarsch der Quantenkryptographie

Die Übermittlung von Schlüsseldaten stellt ein grundsätzliches Sicherheitsrisiko dar. Die Technologie der Quantenschlüsselverteilung (Quantum Key Distribution, QKD) wird sich als besonders wirkungsvoll erweisen, da sie eine Verteilung der Schlüssel über einen unsicheren Kanal vermeidet. Im Jahr 2023 steht mit der Einführung von QKD in Rechenzentren, IoT, autonomen Systemen und 6G ein neuer Makrotrend bevor.

# Effizienz

### 3 Full-Stack Observability (FSO) steigert Unternehmenseffizienz

Zu viele Daten mit zu wenig Kontext – vor dieser Herausforderung stehen viele Unternehmen derzeit bei ihrem Monitoring. Viele der erhobenen Datenmengen bringen der Unternehmensführung keinen echten Mehrwert. Das wird sich ändern. Der Ansatz des Full-Stack Observability optimiert Geschäftsprozesse und wird sich im Jahr 2023 zunehmend durchsetzen.

### 4 Internet der Dinge (IoT) macht Lieferketten resilienter

Unternehmen und Logistikdienstleister werden das Internet der Dinge zunehmend nutzen, um 2023 vollständige Transparenz in ihre Lieferketten zu bringen. IoT und andere Technologien werden nicht nur eine größere Rolle bei der Verbesserung der Widerstandsfähigkeit, Effizienz und Nachhaltigkeit von Lieferketten spielen, sondern auch die Cybersicherheit und das IT/OT-Netzwerkmanagement verbessern. Unternehmen und Logistikanbieter werden ihre Lieferketten auf der Grundlage prädiktiver und präskriptiver Modelle, einschließlich intelligenter Verträge und verteilter Ledger, neu konfigurieren.

### 5 Optimierung von Multi-Cloud-Ressourcen

2023 ist das Jahr, in dem sich Unternehmen den Herausforderungen des Cloud-Managements stellen werden. Sie werden zahlreich ihre Cloud-Ressourcen optimieren – auch um größere Leistungsprobleme ihrer Multi-Cloud-Infrastruktur zu beheben oder ihnen vorzubeugen. Maschinelles Lernen und Deep Analytics kommen dabei verstärkt zum Einsatz.

Außerdem werden wir Innovationen erleben, die eine integrativere und nachhaltige Zukunft für alle schaffen.

# Nachhaltigkeit & KI

### 6 Nachhaltige Rechenzentren in der Zukunft

Net Zero bleibt 2023 weiter das Handlungsziel, um Rechenzentren in eine nachhaltigere Zukunft zu führen. Dazu tragen große Fortschritte beim Power over Ethernet (PoE) bei. Netzwerke und APIs werden in der Verwaltung von Rechenzentrumsplattfor- men weiterentwickelt, um den Energieverbrauch zu überwachen, zu verfolgen und zu ändern. IT-Anbieter und Ausrüstungspartner werden transparent sein bei der Wiederverwendung von Hardware (Kreislaufwirtschaft).

### 7 Verantwortungsvolle Künstliche Intelligenz (KI)

Auch im Jahr 2023 werden Einzelpersonen und Organisationen künstliche Intelligenz einsetzen, um unethische und gesellschaftlich zerstörerische Ziele zu erreichen. Industrie, Regierungen, Hochschulen und NGOs werden darum gemeinsam einen Rahmen für einen ethischen und verantwortungsvollen Umgang mit künstlicher Intelligenz ausarbeiten, um den möglichen Schaden zu begrenzen. Dieser Rahmen wird auf Grundsätzen wie Transparenz, Fairness, Rechenschaftspflicht, Datenschutz, Sicherheit und Zuverlässigkeit beruhen und erste Landmarken auf dem Weg zur „Verantwortungsvollen KI“ setzen.

**Autor: Liz Centoni, CSO / GM of Applications bei Cisco**

Wie Digitalisierung und Nachhaltigkeit die Bauwirtschaft der Zukunft prägen

# Sieben Trends

**Nachhaltiger und digitaler: Die Bau- und Immobilienwirtschaft steht vor einschneidenden Veränderungen. Doch wie wird die Zukunft des Bauens und des Gebäudebetriebs aussehen? Siemens Smart Infrastructure hat sieben Trends ausgemacht, die zeigen, wohin die Reise geht.**

## 1 Digitale Gebäudeplanung mit BIM zukunftfähig

Moderne Gebäude werden schon heute oft zweimal gebaut – einmal am Computer, und erst dann in der physischen Welt. Das Zauberwort, das die Tür in die Zukunft der Gebäudeplanung aufgestoßen hat, heißt BIM – Building Information Modeling (BIM). Das ist eine Art Computer Aided Design (CAD) für Gebäude.

Die digitale Planung mit BIM gibt der Bauherrschaft wesentlich mehr Kontrolle über ihr Projekt. Tatsächlich kann sie dank BIM ihr Gebäude nämlich schon während der Planung virtuell «begehen». Möglich macht das ein detailliertes virtuelles Modell des Gebäudes, ein sogenannter digitaler Zwilling. Dieser basiert auf den BIM-Daten.

Das virtuelle Modell erlaubt es der Bauherrschaft, Realisierungsvarianten in 3D zu begutachten und Feedback zu geben. Dabei kann sie auch finanzielle Faktoren berücksichtigen: Im digitalen Zwilling sind die Kosten jeder Planungsmaßnahme hinterlegt. Daher ist immer ersichtlich, wie sich eine bestimmte Änderung auf den Preis auswirkt.

Auf Grundlage der Rückmeldungen der Bauherrschaft und anderer Stakeholder nehmen die Planenden Anpassungen am Projekt vor, die dann erneut begutachtet werden können. Diese Iterationszyklen sind kurz und kostengünstig, weil Algorithmen den Planenden viel Arbeit abnehmen. Wird etwa bei der Planung eines Krankenhauses die Raumgröße reduziert, passt ein Algorithmus die Wände im virtuellen Modell aufgrund vordefinierter Kriterien automatisch an. Dasselbe gilt für andere Details, etwa die Anzahl und Position der Brandmelder. Dadurch steigt die Planungssicherheit und -effizienz. Denn am digitalen Zwilling kann gewerkeübergreifend transparent geplant werden. Damit lassen sich Fehler vermeiden, Gewerke optimal aufeinander abstimmen und Kosten jederzeit aktuell ausweisen. Dieser Trend wird sich verstärken und die Gebäudeplanung nicht nur transparenter, sondern auch effizienter und kostengünstiger machen.

## 2 Kooperation am digitalen Zwilling

Damit die digitale Planung ihre Vorteile ausspielen kann, müssen die verschiedenen am Bau beteiligten Akteure ihre Daten teilen und gemeinsam nutzen – nur dann kann Transparenz über den gesamten Planungs- und Bauprozess hergestellt werden.

Vorbild für diese Prozesse sind Software-Entwicklungsplattformen wie Github oder Gitlab. Diese ermöglichen, dass mehrere Programmierer gemeinsam an einem Projekt arbeiten. Die Software verwaltet alle Eingaben, und alle Änderungen sind für alle nachvollziehbar.

So weit ist die Baubranche noch nicht. Viele Beteiligte arbeiten noch mit zweidimensionalen Plänen oder verschieben die BIM-Daten mit großen Anpassungsverlusten in andere Systeme. Die angestrebte Transparenz über den gesamten Planungsprozess ist derzeit noch Zukunftsmusik.

Offen ist zudem, wie sich bei diesem neuen Ansatz Aufwände verrechnen lassen, wenn die Beteiligten ihre Gewerke gemeinsam mit anderen planen. Gefragt sind neue Ansätze. So könnte beispielsweise der Gebäudebesitzer, der bei der Betriebsoptimierung vom digitalen Zwilling profitiert, die Planer, die ihn erstellt haben, für diesen Mehrwert entschädigen.

## 3 Digitales Projektmanagement als Basis

Wenn der digitale Gebäudezwilling steht, geht es um die Frage, in welchen Schritten das physische Gebäude gebaut wird. Heute wird die Ablaufplanung vom Projektplanenden festgelegt. Sie basiert auf Erfahrung, ist meist ungenau und lässt sich nur schwer anpassen, wenn es in einem Teilschritt zu Verzögerungen kommt.

Die Digitalisierung verspricht für das Projektmanagement einschneidende Verbesserungen. So arbeitet beispielsweise das US-amerikanische Unternehmen Alice Technologies daran, diesen Prozess komplett zu automatisieren. Dabei erlernt der Computer die ideale Abfolge der Projektschritte – und erstellt anhand der BIM-Daten selbstständig Projektpläne. Diese können blitzschnell aktualisiert werden, falls irgendwo Verzögerungen auftreten. Damit ist sichergestellt, dass die bestmögliche Abfolge gewählt wird. Bereits heute können laut Firmenangaben mit dieser Lösung bei der Gebäuderealisierung durchschnittlich 11 Prozent der Kosten und 17 Prozent der Zeit eingespart werden.

In Zukunft dürfte das computergestützte Projektmanagement noch weiter verfeinert werden. Das wiederum könnte die Art und Weise verändern, wie Aufträge in Bauprojekten vergeben werden: So ließen sich auch kleine Projektschritte wie etwa die «Installation der Raumbediengeräte wie Thermostate» als Arbeitspakete über eine App zu einem vorgegebenen Preis ausschreiben – ähnlich wie die Firma Uber ihren Fahrern Aufträge anbietet. Damit hätten auch kleine, lokale Installateure die Chance, sich am Bau zu beteiligen. Auch die Qualitätskontrolle könnte durch «Reviews und Feedback» über eine solche App sichergestellt werden.

## 4 Ressourcenschonend bauen - Baumaterialien sparen

Der Bau von Gebäuden ist ressourcenintensiv und alles andere als klimafreundlich: Jährlich werden rund 4,4 Milliarden Tonnen Zement produziert – dabei wird in etwa so viel CO2 freigesetzt wie in 700 Kohlekraftwerken.

Um den ökologischen Fußabdruck von Gebäuden und Infrastrukturen zu verringern, ist ein nachhaltiger Umgang mit Baustoffen entscheidend. Zum einen muss mehr Baumaterial wiederverwertet werden. Ansatzweise ist das bereits heute der Fall.

So wird eine bestehende Betonhülle nicht mehr gesprengt und neu gebaut, sondern in die Planung des neuen Gebäudes einbezogen oder als Füllmaterial wiederverwendet. Zum anderen müssen vermehrt alternative Baustoffe wie Holz zum Einsatz kommen, die klimafreundlicher sind.

Auch neue Technologien können zu ressourcenschonenderem Bauen beitragen. So verspricht der 3D-Druck nicht nur effizientere Prozesse, sondern auch eine massive Reduktion des ökologischen Fußabdrucks, weil sich in additiver Fertigung neue Formen drucken lassen, die mit weniger Baumaterial auskommen, ohne Kompromisse bei der Stabilität zu machen.

## 5 Roboter auf der Baustelle - Automatisierung schreitet voran

Als weiteren Trend lässt sich schon heute der Einsatz von Robotern erkennen: Bereits im Einsatz sind beispielsweise Bohrroboter von Schindler oder Hilti, die nach Datenvorgaben selbstständig Löcher in den Beton bohren. Roboter werden auch bereits genutzt, um aus alternativen Baustoffen komplexe Strukturen zu fertigen.

Erhöhter Kostendruck wird zu mehr industriellem Bauen führen. Mit neuen digitalen Fertigungsmethoden können Bauteile individuell und «on demand» hergestellt werden. Weil in Zukunft mehr Elemente in die Vorfabrikate integriert werden können – beispielsweise elektrische Komponenten –, wird es auf der Baustelle der Zukunft vermehrt darum gehen, vorgefertigte Elemente zusammenzufügen.

## 6 Der datenbasierte Gebäudebetrieb dank Algorithmen

In der Nutzungsphase des Gebäudes wird für Heizen, Kühlen und Warmwasseraufbereitung am meisten Energie benötigt. Ein intelligentes Gebäude der Zukunft verfügt über Sensoren und intelligente Steuerungen, um den Betrieb der gebäudetechnischen Anlagen so effizient wie möglich zu machen. Dabei berücksichtigt es auch das Verhalten und die Bedürfnisse der Gebäudenutzenden: Wo sich beispielsweise niemand aufhält, muss auch nicht geheizt werden. Dabei bezieht das intelligente Gebäude Wetterprognosen und die Verfügbarkeit erneuerbarer Energie – etwa von der PV-Anlage auf dem Dach – in sein Verhalten mit ein.

Die Daten, die im intelligenten Gebäude erfasst werden, lassen sich durch Algorithmen auswerten, um das Gebäudemanagement zu optimieren: Wenn Abweichungen auftreten, wird der Facility Manager informiert, so dass er entscheiden kann, was zu tun ist. Die Daten werden standardisiert verfügbar sein und es wird Applikationen geben, welche die Daten verarbeiten und Mehrwerte anbieten, wie etwa Energie-Einsparungen. Diese Applikationen können in einem virtuellen Marktplatz zur Verfügung stehen, und die Kunden können diejenigen auswählen, die ihren Zwecken am besten dienen.

## 6 Das Auto als Stromspeicher für Energiemanagement

Im intelligenten Gebäude werden Energiespeicher eine größere Rolle spielen, als sie es heute tun. Das Elektroauto wird dabei eine wichtige Rolle übernehmen: Wenn es tagsüber auf dem Parkplatz am Arbeitsplatz steht, erhält es beispielsweise Solarstrom und wird geladen. Der gespeicherte Strom kann dann abends zu Hause genutzt werden. Intelligente Systeme stellen sicher, dass die Batterie noch genügend geladen ist, um am nächsten Tag wieder zur Arbeit

fahren zu können. Ist im Kalender ein Termin weiter auswärts vermerkt, wird die Entladung früher gestoppt, damit der Ort gut erreicht werden kann.

Solche Vernetzungen von Daten der Verbraucher und der Energieerzeugung ermöglichen die optimale Ausnutzung der erneuerbaren Energien und werden für eine nachhaltige Energieversorgung eine wichtige Rolle spielen. Durch solche Energieoptimierungen werden sich auch neue Geschäftsmodelle ergeben. So könnte man überschüssigen Strom gegen eine Vergütung dem Nachbarn abtreten. Allerdings bestehen für solche Lösungen derzeit noch hohe bürokratische und politische Hürden.

## Ausblick

Obwohl Technologien und Materialien für eine nachhaltigere und intelligentere Bau- und Immobilienwirtschaft bereits existieren: Der Weg in die Zukunft des Bauens ist reich an Hindernissen. Viele Unternehmen sehen heute noch keinen Anreiz, aktiv Veränderungen voranzutreiben. Regulative Vorgaben und historisch gewachsene Strukturen behindern teilweise den Fortschritt. Und solange der Kostendruck nicht hoch genug ist, wird die Automatisierung des Bausektors nicht vorangehen. Auf Dauer wird das Festhalten am Status Quo jedoch kein taugliches Konzept sein. Der Fortschritt und Digitalisierung setzten sich bekanntlich durch, wie Beispiele aus dem Druckbereich, der Fotografie oder auch der Musikindustrie deutlich gezeigt haben.

**Die gute Nachricht ist:** Es gibt zahlreiche Möglichkeiten, um die Baubranche zu modernisieren. Software-Entwickler, Start-ups und moderne Technologien können und werden noch vieles revolutionieren – wir stehen heute erst am Anfang.

**Über den Autor**
Von Michael Kiy, Director Innovation Management, Siemens Smart Infrastructure.
Michael Kiy hat Physik studiert und an der ETH Zürich promoviert. Danach arbeitete er als Senior Engineer am Centre Suisse d'Electronique et de Microtechnique (CSEM), als Projektleiter bei Alcan Packaging, Associate Director of Engineering bei Vistaprint / Cimpress sowie als Director of Engineering bei Heptagon OY / AMS AG. Seit 2018 ist er Director of Innovation bei Siemens Smart Infrastructure. Seit 2019 ist Michael Kiy zudem Mitglied des Expert Board von Electrosuisse und Mitglied im Organisationskomitee des schweizerischen Gebäude- technik-Kongresses und des Forum Smart Home.

# 2023 mit neuen Cyber-Bedrohungen und -Herausforderungen

## Sieben Security-Experten haben für uns erläutert, worauf Unternehmen sich in puncto IT-Sicherheit im kommenden Jahr einstellen müssen.

**So könnte der Einsatz von Wiperware-Schadsoftware nächstes Jahr verstärkt länderübergreifend stattfinden, während hybride Mensch-Maschine-Angriffeautomatisiert Schwachstellen identifizieren, die anschließend von einem menschlichen Experten ausgewertet werden. Zunehmen wird auch Ransomware-as-a-Service im Darknet, um beispielsweise gezielt die Konkurrenz zu sabotieren oder Cyberattacken politisch auszunutzen. Im nächsten Jahr wird auch Mobiles Edge-Computing über 5G erstmals in den Produktivbetrieb gehen, was den Einsatz moderner Sicherheitskonzepte wie ZTNA (Zero-Trust-Network-Access-Konzept) erfordern wird.**

**Fleming Shi, CTO bei Barracuda Networks**

**„Wiperware wird verstärkt länderübergreifend stattfinden und Ransomware-Banden werden kleiner und geschickter."**

„Der Angriff Russlands auf die Ukraine hat uns noch einmal deutlich vor Augen geführt, dass der moderne, digitale Krieg quasi auch vor der eigenen Haustür stattfindet. Dabei fiel insbesondere der verstärkte Einsatz von sogenannter Wiperware auf. Ein Wiper ist eine destruktive Schadsoftware, die auf Dateien, Backups oder die Bootsektoren des Betriebssystems abzielt. Wir sahen Angriffe gegen ukrainische Organisationen und kritische Infrastrukturen. Die Häufigkeit hat drastisch zugenommen, wie etwa WhisperGate, Caddy Wiper oder HermeticWiper zeigen, die seit Ausbruch des Krieges Schlagzeilen machten. Im Gegensatz zu den monetären Motiven und dem Entschlüsselungspotenzial von Ransomware wird Wiperware in der Regel von nationalstaatlichen Angreifern mit dem Ziel eingesetzt, die Systeme eines Gegners so zu beschädigen und zu zerstören, dass eine Wiederherstellung unmöglich ist. Zudem wird die von Russland ausgehende Wiperware, künftig wahrscheinlich auf andere Länder übergreifen, da die geopolitischen Spannungen keineswegs abnehmen, ebenso Hacktivismus nichtstaatlicher Angreifer, die nach weiteren Maßnahmen zur Ausbeutung ihrer Opfer suchen. Um die Geschäftskontinuität trotz eines Angriffs zu gewährleisten, müssen sich Unternehmen auf die Wiederherstellung des gesamten Systems konzentrieren, damit nicht nur die Daten, sondern die gesamte IT-Infrastruktur wieder funktionsfähig ist. Eine schnelle Wiederherstellung der virtuellen Version eines angegriffenen physischen Systems kann beispielsweise die Widerstandsfähigkeit eines Unternehmens gegen Wiperware oder andere destruktive Malware-Angriffe erheblich verbessern

2022 standen die großen Ransomware-Banden - LockBit, Conti und Lapus$ - hinter Aufmerksamkeit heischenden Angriffen, die sie regelmäßig in die Schlagzeilen brachten. 2023 mit dem boomenden Geschäftsmodell Ransomware-as-a-Service und dem jüngsten Build-Leak von LockBit 3.0 wird eine neue Ge-

neration kleinerer und intelligenterer Banden ihnen die Schau stehlen. Und Unternehmen werden sich öfter Ransomware-Angriffen mit neuen Taktiken gegenübersehen. Wer darauf nicht vorbereitet ist, wird sich in den Schlagzeilen wiederfinden und riskieren, Geschäft und Ruf zu beschädigen."

**Jörg von der Heydt, Regional Director DACH bei Bitdefender.**

## „Hybride Mensch-Maschine-Angriffe zielen auf Unternehmen aller Größen."

„Der Wettlauf zwischen Hackern und IT-Sicherheitsteams geht 2023 weiter. Neue Tools und schnellere Hardware bei wachsendem oft staatlich unterstütztem Budget bringen die Angreifer in eine immer stärkere Position. Eine kontinuierlich steigende Anzahl von Schwachstellen und die fehlenden Ressourcen oder unzureichende Tools, diese zeitnah zu patchen, unterstützen diese Tendenz.
Eine besondere Gefahr ist die zeitnahe Verfügbarkeit von Quanten-Computing, welches Verschlüsselung und Passwort-Sicherheit disruptiv verändern wird. Bereits jetzt ist ein Umdenken nötig. Ebenso wichtig sind hybride Mensch-Maschine Angriffe: Automatisierte Tools identifizieren Schwachstellen in der anzugreifenden Infrastruktur – Experten werten diese dann hinsichtlich des Angriffspotenzials aus. Eigentlich sollte auch die Cyberabwehr so vorgehen. Ihr fehlen jedoch häufig Budget, Zeit, Skills und das kompetente Personal. Wollen Unternehmen – gleich welcher Größe und Branche – nicht Opfer eines solchen intelligenten Angriffs werden, müssen sie ebenfalls auf hybride Abwehr setzen. „Fight Fire with Fire" gilt also auch hier: Firmen müssen entweder selbst Teams (aus-)bilden – oder sie durch externe Managed Detection and Response (MDR) ergänzen. Wichtig ist dabei, die möglichen Schäden zu verstehen. Viele Gespräche der jüngsten Vergangenheit zeigen, dass dieses Bewusstsein häufig fehlt und IT-Sicherheit zu oft noch lediglich als Kostenfaktor mit unsichtbarem Nutzen betrachtet wird."

**Lothar Hänsler, COO bei Radar Cyber Security**

## „Bedrohungslage bleibt im Jahr 2023 angespannt, KRITIS-Betreiber nach wie vor gefordert"

„So lange Russland Krieg fuhrt, ist die Bedrohungslage besonders ernst zu nehmen. Hier sind v.a. KRITIS-Betreiber gefordert, bspw. im Energie- und Finanzsektor. In der öffentlichen Verwaltung ist kunftig vermehrt mit DDoS-Angriffen zu rechnen (wie etwa kurzlich bei der Attacke gegen den Website-Zugang des EU-Parlaments). Eine der größten Bedrohungen fur Unternehmen und Behörden ist nach wie vor die sich ständig verändernde Bedrohungslage um Ransomware und E-Mails, die gefährliche Schadsoftware enthalten bzw. sogar die Kombination aus beiden Formen. Neuere Arten der Erpressungssoftware setzen gar nicht mehr unbedingt auf die Verschlusselung von Daten, sondern auf die Exfiltration. Die Angreifer uben dann Druck aus, indem sie mit der Veröffentlichung der Daten drohen. Sie wenden immer ausgefeiltere Methoden an, um zu erreichen, dass E-Mail-Anhänge geöffnet werden oder bestimmte Websites angesteuert werden. Im schlimmsten Fall erreichen sie es, dass Anmeldedaten und Login-Informationen abgefangen werden, die zur weiteren Kompromittierung genutzt werden.
Eines der zentralen Themen fur Unternehmen und Behörden bleibt daher E-Mail-Security. Um die wesentlichen „offenen Flanken" abzudecken, braucht man ein dreiteiliges Maßnahmenpaket: Technik (Reputationsprüfung von Webseiten, Sandboxing, Malware-Schutz, kontinuierliche Überwachung, Analyse von Ereignissen), Personal (Sensibilisierungsmaßnahmen, Schulungen) und Prozesse (regelmäßige zeitnahe Behebung von Schwachstellen, Notfallpläne und -ubungen). Als Konsequenz daraus ergibt sich, dass wir Systeme konsequent cyber-widerstandsfähiger machen mussen. Zero-Trust-Netzwerke mussen ebenso ins Auge gefasst werden wie die Absicherung von Remote-Zugängen. Der Einsatz von Endpoint Detection and Response (EDR) ist dringend anzuraten – und

auch die OT-Sicherheit darf nicht vergessen werden. Die ganzheitliche und konsolidierte Sicherheitsbetrachtung wird im Kontext von Risikomanagement zunehmend wichtiger."

**Robert Rudolph, Product Marketing Consultant bei ForeNova**

## „Heterogene Angriffe diktieren eine verhaltensba- sierte und proaktive Abwehr."

„Das Jahr 2023 wird die Welt der Cybergefahren weiter umwälzen. Trends, die zuletzt schon sichtbar waren, werden sich weiter verschärfen. Insbesondere der Mittelstand, wie etwa das produzierende Gewerbe, steht dabei im Blickpunkt. Zum einem wegen seines wertvollen sensiblen Knowhows und potenziell zur Genüge vorhandenen Kapitals, um hohe Lösegeldforderungen zu bedienen, zum anderen wegen einer zu traditionellen IT-Security aus Firewall und AV. Die aktuellen Krisenlagen finden ihren Niederschlag in gezielten Angriffen auf Verbündete in Konflikten und deren kritische Infrastruktur.

Zugleich professionalisieren sich die Cyberkriminellen weiter. Ransomware-as-a-Service im Darknet führt zu mehr Begehrlichkeiten bei allen, die die Konkurrenz sabotieren wollen oder Cyberattacken politisch ausnutzen möchten. Die Angreifer gehen immer gezielter vor. Sie durchleuchten die Opfer im Vorfeld umfangreich und nutzen erkannte Lücken zielsicher aus. Sie finden über Sicherheitslücken und Social Engineering nur allzu oft einen Weg in die Unternehmensnetzwerke. Zumal nahezu die gesamte Unternehmenskommunikation etwa zwischen Menschen, Geräten und Schaltern mittlerweile im Netzwerk stattfindet. Zunehmend viele „Clients" – wie etwa IoT-Geräte im Gesundheitswesen sind dann Angriffsfläche für Cyberattacken. IT-Verantwortliche müssen daher klassische signaturbasierte Abwehransätze mit Sicherheitstechnologien ergänzen, die anomale Aktivitäten im Netzwerk und auf Endpunkten effektiv aufspüren.

Neben der Verhaltensanalyse ist der nächste Trend der proaktive Schutz: Funktionen wie Ransomware-Honeypots können Aktionen der Angreifer gezielt triggern und aktiv bekämpfen, bevor der Cyberkriminelle seinen Gesamtplan durchführt. Wer sich dagegen wehren will, sollte auf die Hilfe externer Cybersecurity-Experten zurückgreifen."

---

**Ari Albertini, Co-CEO bei FTAPI**

## „Nachhaltigkeit mit den Chancen der Digitalisierung verknüpfen."

„Die Digitalisierung und Automatisierung von Prozessen sowie der Weg von On-Premise betriebenen Systemen hin zu einer sicheren, europäischen Cloud wird Unternehmen, Behörden und Organisationen im Jahr 2023 ebenso beschäftigen wie das Thema Nachhaltigkeit.

Diese drei Themen sind eng miteinander verknüpft: Idealerweise ist ein digitaler, automatisierter Prozess papierlos und führt - richtig umgesetzt - bei den Mitarbeitenden zu einer erheblichen Zeitersparnis. Allerdings geht es beim Thema Nachhaltigkeit um mehr als um den Weg zum papierlosen Büro. Unternehmen müssen lernen, die Ressourcen, die ihnen zur Verfügung stehen, besser und effizienter zu nutzen. Automatisierte bestehende Prozesse räumen Mitarbeitenden wertvolle Zeit ein, die sie kreativ nutzen können, beispielsweise um zukunftsfähige Strategien anzugehen oder innovative Arbeitsweisen umzusetzen.

Unternehmen werden außerdem ihre Kompetenzen stärker zentralisieren, aber zugleich immer mehr darauf ver-

zichten, Rechenzentren im eigenen Unternehmen zu betreiben. Die meisten Verantwortlichen wissen mittlerweile ganz genau, dass es effektiver ist, Daten in einer sicheren, europäischen Cloud speichern.
Nachhaltigkeit ist mehr als ein Trend - sie ist für die gesamte Gesellschaft zum elementaren Thema geworden. Sie mit den Chancen der Digitalisierung zu verknüpfen, wird eine der zentralen Herausforderungen im nächsten Jahr sein."

**Arne Jacobsen, Director of Sales EMEA, Aqua Security**

## „Absicherung von Software 2023 auf der Prioritätenliste der CISOs ganz oben."

„Es gibt immer mehr Angriffe auf die Software-Supply-Chain, allein von 2020 auf 2021 nahmen sie um 300 Prozent zu. Inzwischen beschäftigt die verschärfte Bedrohungslage auch die Politik: Das Weiße Haus veröffentlichte kürzlich eine entsprechende „Durchführungsverordnung", und in einer aktuellen Richtlinie des EU-Parlaments ist die Absicherung der Supply-Chain sogar eine der vier zentralen Anforderungen.
Diese Bestrebungen sind meiner Meinung nach ein großer Schritt in die richtige Richtung, um Software sicherer zu machen. Auch wenn es wie damals bei der DS-GVO noch eine Übergangsphase gibt, bis die Richtlinie in allen EU-Ländern ratifiziert wird, sollte man sich bereits jetzt vorbereiten. Die Absicherung von Software wird daher 2023 ganz oben auf der Prioritätenliste der CISOs stehen. Konkret müssen sie vor allem in Lösungen zur Analyse der Software-Zusammensetzung, zur Absicherung der Tool-Chain sowie in „Software Bills of Materials" (kurz SBOM) investieren. Im Zuge dessen wird auch die Verbreitung von DevSecOps – nach jahrelangen Diskussionen – stark zunehmen.
Im Zentrum der branchenweiten Anstrengungen wird Stand jetzt SBOM stehen – beschleunigt durch die angesprochenen Anordnungen der Politik. Das heißt: Unternehmen, die Software nutzen – was heutzutage für fast alle gilt –, sollten ab sofort darauf achten, dass ihre Software-Lieferanten die Richtlinien umsetzen, Tools zur Absicherung ihres gesamten Entwicklungsprozesses einsetzen sowie Herkunft und Sicherheit aller Software-Bestandteile über eine komplette SBOM garantieren können. Software-Hersteller wiederum müssen jetzt in Lösungen investieren, die den kompletten Prozess absichern, um Fehler in ihren Lösungen so früh wie möglich zu erkennen und zu beheben."

---

**Jan Willeke, Area Director Central Europe bei Cradlepoint**

## „Mobiles Edge-Computing über 5G-Netze geht 2023 in den Produktivbetrieb und erfordert moderne Sicherheitskonzepte wie ZTNA."

„5G-Netze – ob privat, öffentlich oder hybrid – im Zusammenspiel mit Mobile-Edge-Computing: Dies wird 2023 eines der marktbestimmenden Themen sein. In den vergangenen zwei, drei Jahren haben Technologieunternehmen, Hersteller von Edge-Devices, Applikationsprovider, Forschungsinstitute sowie Endkunden viele Ressourcen in die Entwicklung von Anwendungsszenarien und funktionierenden Eco Systems investiert. Jetzt kommen wir an den Punkt, wo diese Entwicklungen in die produktive Umsetzung gehen und Mehrwerte schaffen.

Eine wichtige Rolle im produktiven Betrieb spielt der sichere Zugriff vom Netzwerk-Edge auf Anwendungen und andere Ressourcen. Mit dem Zero-Trust-Network-Access-Konzept, kurz ZTNA, steht hier ein intelligenter, einfach anzuwendender und zuverlässiger Ansatz zur Verfügung. Unternehmen können damit das Risiko sogenannter Seitwärtsbewegungen von Schad-Software im Netzwerk verringern, weil die Benutzer direkt mit Anwendungen statt mit dem Netzwerk verbunden sind.
Zero Trust Network Access entwickelt sich immer mehr zu einem Standard im Networking-Bereich, den es auch bei Wireless-WANs einzuhalten gilt."

Bildnachweis:Checkpoint Systems GmbH

# EAS im Einzelhandel

**Wieso Diebstahlprävention die beste Strategie für Einzelhändler ist. Warum eine Elektronische Artikelsicherung immer wichtiger und zeitgemäßer wird. Und wie die Implementierung eines EAS-Systems am wirtschaftlichsten gelingt.**

Der gesamte deutsche Einzelhandel verlor im Jahr 2021 laut EHI Retail Institute etwa 4,1 Milliarden Euro durch Inventurdifferenzen. Der Anteil der Verluste durch Diebstähle von Kunden, Beschäftigen, Lieferanten und Servicekräften betrug dabei rund 79 Prozent, das entspricht circa 3,23 Milliarden Euro. Diese Zahl allein ist bereits ausreichend Grund zum Handeln, was die Situation aber noch drängender macht, ist die große Dunkelziffer: Weniger als zwei Prozent der Diebstähle werden angezeigt. Rein rechnerisch kann man also davon ausgehen, dass jährlich über 19,8 Millionen Ladendiebstähle mit je einem Warenwert von 106 Euro unentdeckt bleiben.

## Prävention ist besser als Reaktion

Was kann man aus diesen Zahlen ableiten? Eine mögliche Erkenntnis daraus könnte sein, dass es für Einzelhändler vor allem wichtig ist, präventive Maßnahmen zu ergreifen und weniger auf Strafverfolgung und Verbrechensaufklärung zu setzen. Aber aufgepasst: Eine Maßnahme, die früher äußerst populär war und auch heute noch häufig eingesetzt wird, sollte überdacht werden – das Wegschließen bzw. Wegräumen von teuren Waren und Waren mit hohem Diebstahlrisiko. „Wenn Kunden Ware nicht sehen und erleben können, werden Spontankäufe ausgeschlossen und viele Cross-Selling-Möglichkeiten vergeben. Die Berechnung dieser entgangenen Einnahmen ist schwierig, aber wir konnten ermitteln, dass im umgekehrten Fall – also bei offener Warenpräsentation – die Umsätze steigen", erklärt Hans-Jürgen Nausch von Checkpoint Systems, einem vertikal integrierten Anbieter von RF/RFID-Lösungen für den Einzelhandel. „Außerdem verspielt der stationäre Handel so einen seiner größten Vorteile gegenüber dem Online-Handel – das haptische Erlebnis." Das heißt, die ideale Lösung zur Diebstahlprävention muss nicht nur Diebstähle verhindern, sondern auch eine offene Präsentation der Waren begünstigen – sonst schaden sich Einzelhändler quasi selbst.

## Die sicheren drei

Hinsichtlich dieser Anforderungen an die Artikelsicherung haben sich vor allem drei Lösungen bewährt: EAS, Kameraüberwachung und Sicherheitspersonal. Das Sicherheitspersonal hat einige Vorteile, unter anderem eine sehr hohe Abschreckungswirkung, aber auch einige Schwachpunkte. Zum einen ist da der Kostenfaktor. Laut den Studien des Global Retail Theft Barometers macht das Wachpersonal weltweit den größten Teil der Budgets vieler Einzelhändler für die Verlustprävention aus. Zum anderen ist die Qualität der Überwachung schwer zu überprüfen, denn während in der Vergangenheit viele Unternehmen Sicherheitspersonal auf ihrer eigenen Gehaltsliste hatten, wird dies immer seltener. Und bei der Vertragsbewachung ist es schwierig, den Standard des Wachpersonals zu garantieren und seine Wirksamkeit zu messen.

Die Videoüberwachung kann zwar auch als präventive Maßnahme gewertet werden, wenn die Kameras sehr auffällig platziert sind und dadurch eine abschreckende Wirkung entfalten, allerdings besteht ihr Hauptbeitrag darin, im Nachhinein visuell zu klären, was, wie und wann passiert ist. Außerdem liefert sie den Einzelhändlern Hinweise auf die Identität der Beteiligten. Sie also in erster Linie eher eine Maßnahme zur Strafverfolgung nach erfolgter Tat.

Die dritte Lösung ist EAS – die Elektronische Artikelsicherung. Das Grundprinzip der EAS hat sich seit den 1960er Jahren nicht allzu sehr verändert. Es basiert auf der Prämisse, dass die Waren mit einem elektronischen Etikett versehen sind, das mit einer Antenne im Geschäft kommuniziert, die sich in der Regel in der Nähe des Eingangs/Ausgangs eines Geschäfts befindet. Wenn das Etikett in Reichweite der Antenne kommt, ertönt ein Alarm, der das Personal und die Geschäftsleitung darauf aufmerksam macht, dass ein Artikel das Geschäft illegal verlässt. Einzelhändler haben bei EAS grundsätzlich die Wahl zwischen einer diskreten versteckten Kennzeichnung, bei der sich das RF-Etikett im Inneren der Verpackung befindet, und einer offenen Kennzeichnung, bei der ein deutlich sichtbares Etikett, manchmal sogar mit dem RF-Schaltkreis selbst, und eine Sicherheitsnachricht auf dem Etikett angebracht sind. "Im Sinne der Diebstahlprävention sollte man auf jeden Fall auf die sichtbare Kennzeichnung setzen", erläutert Hans-Jürgen Nausch von Checkpoint Systems. „So erhöhen die EAS-Etiketten nicht nur den Aufwand und das Risiko, erwischt zu werden, für professionellere Diebe, sondern schrecken auch wirksam Gelegenheitsdiebe ab. Das belegen auch Untersuchungen."

EAS – zeitgemäße Artikelsicherung

Es gibt EAS seit über 40 Jahren in verschiedenen Technologieformaten.

Durchgesetzt haben sich aber die akustisch-magnetische (AM) und die Hochfrequenztechnologie (RF). Diese Technologien unterscheiden sich in einem wesentlichen Punkt: der Frequenz, mit der sie arbeiten, gemessen in Hertz. Während AM ursprünglich die bevorzugte Frequenz für EAS war, hat sich in letzter Zeit ein Trend hin zu RF entwickelt – und das hat verschiedene Gründe: „Unter anderem sind RF-Systeme im Betrieb energiesparender als AM-Systeme, was natürlich in Zeiten der Energieknappheit und steigenden Energiekosten besonders attraktiv ist. Ihr Gesamtenergiebedarf liegt um etwa 70 Prozent niedriger pro Geschäft, zusätzlich kann der Verbrauch durch die Koppelung mit einer intelligenten Stromschaltsoftware noch weiter reduziert werden", führt Hans-Jürgen Nausch von Checkpoint Systems aus.
„Auch bei der Erfüllung einiger in Deutschland geltender Richtlinien haben RF-Systeme die Nase vorn. Beispielsweise sind Einzelhändler beim Einsatz von EAS-Systemen dazu verpflichtet, eine Gefährdungsbeurteilung hinsichtlich der Exposition gegenüber elektromagnetischen Feldern (EMF-Exposition) durchzuführen. Unsere auf RF-basierenden Systeme der Serien EVOLVE und NEO erfüllen alle diesbezüglich in Deutschland geltenden Anforderungen. Das bestätigt uns auch die BGHW, die Berufsgenossenschaft Handel und Warenlogistik."

Auch wenn sich die generelle Wirkweise der EAS seit den Anfängen nicht verändert hat, gab es zahlreiche Fortschritte seit der Einführung digitaler, softwaregesteuerter Lösungen – insbesondere im RF-Bereich. Verbesserungen bei der CPU-Kapazität haben die technischen Betriebsmöglichkeiten von RF-Systemen auf ein viel höheres Niveau gebracht. Die neueste Technologie verwendet beispielsweise sichere drahtlose Kommunikation anstelle von festverdrahteter Verkabelung. Größere Erfassungsbereiche ermöglichen breitere Gänge von bis zu 2,70 Metern zwischen den Antennen. Die Softwarefilterung reduziert Fehlalarme und ermöglicht eine bessere Alarmintegrität als je zuvor, und die Fernkonnektivität reduziert die Ausfallzeiten der Systeme im Fall der Fälle.

„Aber bei den Verbesserungen der modernen EAS-Systeme geht es nicht nur um Leistung, sondern auch um eine Verbesserung des Kundenerlebnisses. Es gibt eine große Auswahl an Designoptionen und zusätzlichen Funktionen, wodurch sich heute kein Einzelhändler mehr zwischen Warensicherung und Ladenoptik entscheiden muss. Der klassische „GateLook" ist passé", berichtet Hans-Jürgen Nausch von Checkpoint Systems. „Auch die Einschränkungen auf Produktseite, die frühere Systeme hatten, gibt es nicht mehr. Mittlerweile sind EAS-Etiketten für alle Produkttypen erhältlich, einschließlich lebensmittelechter und mikrowellengeeigneter Etiketten, die sogar auf Metallbehältern wie Dosen angebracht werden können."
Ein weiterer Pluspunkt, den EAS-Systeme und besonders RF-basierte EAS-Systeme mit sich bringen: Sie unterstützen den Self-Checkout der Kunden, denn die Deaktivierung eines RF-Etiketts kann sowohl beim Scan-Vorgang des Barcodes durch den Kassierer als auch durch den Kunden selbst an einem Self-Checkout-Gerät (SCO) erfolgen. Durch diese Möglichkeit können RF-basierte EAS-Systeme in jede beliebige Selbstbedienungsanwendung integriert werden und lassen sich durch die Option, die gekennzeichneten Produkte erst nach Abschluss der Zahlung zu deaktivieren, weiter verbessern.

## Zwei Schritte zum EAS-Einstieg

Im Idealfall würde ein Einzelhändler, der eine EAS-Lösung einsetzen möchte, jeden einzelnen Artikel in seinen Geschäften mit Sicherheitsetiketten ausstatten. Die Realität sieht aber oft anders aus: Das Anbringen der Sicherheitsetiketten im Ladenalltag ist kein leichtes Unterfangen, da die meisten Einzelhändler in Bezug auf verfügbares Personal knapp bemessen sind. Es gibt oftmals schlichtweg nicht genug Mitarbeitende, um sich der umfassenden Etikettenausstattung und gleichzeitig den eigentlichen Aufgaben wie dem Verkauf und der Kundenberatung innerhalb der regulären Arbeitszeiten zu widmen. Und die Zuweisung zusätzlicher Arbeitsstunden für die Anbringung von Sicherheitsetiketten erzeugt erhebliche Kosten. „Um die Einführung von

EAS möglichst gewinnbringend zu gestalten, empfehlen wir Einzelhändlern zwei Punkte, die am besten kombiniert werden. Erstens sollte man sich beim Artikelschutz zunächst nur etwa auf die 20 am häufigsten gestohlenen Artikel konzentrieren. Zum einen reduziert das den Einführungsaufwand und zum anderen machen diese Waren einen unverhältnismäßig großen Anteil am Gesamtverlust aus. Konzentriert man sich auf sie, kann man die Verluste in kürzerer Zeit verringern, als wenn man versucht, ganze Warengruppen oder Warensortimente pauschal zu schützen. Es ist keine Seltenheit, dass dabei die Verluste bei diesen Hochrisikoartikeln um bis zu 50 Prozent gesenkt werden konnten", erläutert Hans-Jürgen Nausch von Checkpoint Systems. „Zweitens sollten Einzelhändler ihr gewähltes EAS-Programm erstmal in einem Pilotprojekt testen, bevor sie es groß ausrollen. Dadurch können Sie den Return on Investment (ROI) vorhersagen und nachweisen, auch wenn jede Filiale einen leicht unterschiedlichen ROI hat, bevor eine große Investition getätigt wurde. Außerdem zeigt sich dabei auch, ob der Einzelhändler wirklich die für ihn passende EAS-Lösung ausgewählt hat, und das Team lernt überdies die Lösung effektiv und effizient zu nutzen, bevor dauerhaft „flächendeckend" damit gearbeitet wird." Vereinfacht zusammengefasst müssen für ein solches Pilotprojekt die richtigen Geschäfte gewählt werden – möglichst repräsentativ für das gesamte Risikoprofil -, die passenden Produkte einbezogen werden - zu Beginn am besten die Hochrisikoartikel, die einfach zu kennzeichnen sind – und der richtige Zeitraum festgelegt werden – zwischen drei und sechs Monate. Und nicht zu vergessen: Das jeweilige Filialteam muss mit im Boot sein, um das Pilotprojekt erfolgreich zu gestalten.

## Quellensicherung als Lösung

Eine besondere Lösung für EAS im Einzelhandel ist die Quellensicherung, eine Art Kooperation von Einzelhändlern und Herstellern. Dabei werden Produkte bereits an der Quelle gekennzeichnet, bevor sie in den Laden gelangen. Diese Lösung wird immer populärer, denn sie bietet diverse Pluspunkte. Das Ladenpersonal muss die Produkte nicht mehr selbst kennzeichnen und kann sich auf das Kerngeschäft konzentrieren. Die Etiketten können systematisch auf jedem einzelnen Artikel an der exakt gleichen Stelle angebracht werden – wo sie keine Informationen verdecken oder die Markenwirkung schmälern. Und der Artikelschutz ist umfassender: Quellensicherung bedeutet, dass die Produkte von der Quelle bis zum Geschäft geschützt sind und nicht erst am Verkaufsstandort. Wenn die Quellensicherung mit RFID erfolgt, kann dies eine Produktverfolgung über die gesamte Lieferkette hinweg ermöglichen, was die Anzahl der verlorenen Artikel reduziert, Prozesse rationalisiert und eine bessere Verfügbarkeit im Regal am Ende der Kette ermöglicht. Auch die Abzweigung von Produkten in den sogenannten Grauen Markt, der für große wirtschaftliche Verluste verantwortlich ist, und die Verbreitung von Fälschungen werden auf diese Weise erschwert.

## Resümee

EAS-Lösungen, speziell auf RF-Basis, sind eine wirkungsvolle Maßnahme zur Diebstahlprävention und gleichzeitig eine Gelegenheit, Waren offen zu präsentieren und den Abverkauf zu fördern. Sie entwickeln sich mit dem technischen Fortschritt weiter und erlauben Einzelhändlern Schritt zu halten und Sicherheitsmaßnahmen immer mehr und leichter in den Arbeitsalltag zu integrieren. Aber sie sind nicht der einzig gangbare Weg.

„Eine Komplettlösung zur Diebstahlprävention sollte nach unserer Erfahrung immer alle drei Methoden – EAS, Kameraüberwachung und Sicherheitspersonal – beinhalten", rät Hans-Jürgen Nausch von Checkpoint Systems. „Wenn diese drei Schutzmethoden parallel eingesetzt werden, können sie Einzelhändlern in Summe bedeutende Vorteile bieten. Aber auch die beste Kombination wird nicht alle Kriminelle abschrekken. Ziel ist es, ein Schutzniveau zu etablieren, dass die meisten Diebe abschreckt und die Diebstahlrate senkt – abgestimmt auf das individuelle Risikoprofil des betreffenden Geschäfts oder Standorts."

EUROSHOP 2023

## Sind autonome Geschäfte die Zukunft des Einzelhandels?

# Kassenlose Geschäfte: Der Wandel ist eingeläutet

**Die in den letzten Jahren mit hoher Geschwindigkeit voranschreitende Digitalisierung der Handelsbranche hat auch dazu geführt, dass stationäre Geschäfte mit immer mehr technologischer Intelligenz ausgestattet werden. So haben sich vielfältige automatisierte Store-Konzepte entwickelt, bei denen der Einkaufsvorgang weitestgehend digitalisiert abläuft. Deshalb ist das Thema Smart Stores Stores eines der Hot-Topics der EuroShop 2023, The No.1 Retail Trade Fair, vom 26. Februar bis 02. März in Düsseldorf.**

Es ist fast 40 Jahre her, dass der Erfinder David R. Humble auf die Idee der Selbstbedienungskasse kam, nachdem er angeblich in einer langen Schlange in einem Lebensmittelgeschäft in Südflorida gestanden hatte. Seitdem hat sich die Technologie massiv weiterentwickelt und ist in immer mehr Einzelhandelsgeschäften zu finden. Laut dem Bericht Global EPOS and Self-Checkout 2022 des Strategieforschungs- und Beratungsunternehmens RBR wuchs der Weltmarkt im vergangenen Jahr um 11 Prozent, wobei im Jahr 2021 weltweit 200.000 Selbstbedienungsgeräte ausgeliefert wurden. Die Technologie verspricht enorme Vorteile, wie kürzere Wartezeiten für die Kunden und Kundinnen und eine verbesserte Effizienz der Geschäfte für die Einzelhändler, aber wie bei den meisten Dingen ist sie nicht ohne Makel.

Ist der Einzelhandel auf dem Weg in eine reibungslosere Zukunft, wenn Unternehmen wie Amazon vollautomatische Läden einrichten, in denen die Kundschaft den Kassiervorgang ganz überspringen kann? „Die Zeiten des 20. Jahrhunderts, in denen jeder einzelne Artikel langsam über einen Barcode-Scanner gescannt wurde, sind vorbei", erklärt Will Glaser, CEO des US-Unternehmens Grabandgo. „Der Käufer ist in der Lage, das Geschäft zu wählen, das er aufgrund von Preis und Komfort bevorzugt."

2018 sorgte der Online-Handelsriese Amazon für Schlagzeilen, als er in sei-

ner Heimatstadt Seattle seinen ersten kassenlosen Laden eröffnete, der mit der „Just Walk Out"-Technologie des Unternehmens ausgestattet ist. Heute gibt es mehr als 40 Amazon Go- und Amazon Fresh-Standorte in den USA und Großbritannien, und weitere sollen weltweit eröffnet werden. Das so genannte "Just Walk Out"-Einkaufserlebnis nutzt die gleichen Technologien wie selbstfahrende Autos, einschließlich Computer Vision, Deep Learning-Algorithmen und Sensorfusion, und ermöglicht es den Kunden und Kundinnen, den Laden zu betreten, das Gewünschte zu nehmen und zu verlassen. Während Amazon laut RBR derzeit weltweit die meisten kassenlosen Läden betreibt, experimentieren auch andere Supermarktketten wie Tesco, ALDI und REWE mit Technologien, die das Einkaufserlebnis im Laden erleichtern sollen. RBR prognostiziert, dass es bis Ende 2027 weltweit mehr als 12.000 Geschäfte mit kassenloser Technologie geben könnte.

„Der physische Einzelhandel befindet sich in einem beispiellosen Wandel. Einzelhändler investieren in großem Umfang in Technologien, um ihre Läden umzugestalten, den Shoppern einen reibungsloseren Einkauf zu ermöglichen und die steigenden Arbeitskosten und den Arbeitskräftemangel in einigen Märkten auszugleichen", sagt Alex Maple, der die RBR-Studie Mobile Self-Scanning and Check-Out Free 2022 geleitet hat. „Im Allgemeinen sind Einzelhändler immer bestrebt, das Kundenerlebnis zu verbessern und gleichzeitig die Kosten zu senken", so Maple weiter. „Der zunehmende Einsatz von Self-Checkout-Terminals zum Beispiel zeigt, dass Einzelhändler gerne Technologie einsetzen, wenn sie dadurch die Personalkosten senken und die Zahl der Verkaufsstellen erhöhen können, indem sie den Kunden und Kundinnen neue, bequeme Möglichkeiten bieten, den Kassiervorgang abzuschließen. Eine erfolgreiche Implementierung der kassenlosen Technologie würde die

# EuroShop 2023

Geschäfte von der Konkurrenz abheben, die Personalkosten (möglicherweise erheblich) senken, den Warenschwund reduzieren (was ein potenzielles Problem bei Self-Checkout/Mobile Self-Scanning ist) und der Kundschaft ein reibungsloses Erlebnis" bieten. „Die Bequemlichkeit ist einer der Hauptgründe, warum die Technologie in kleinen Geschäften an stark frequentierten Orten gut funktioniert", so Maple. "Auch die Pandemie hat die kassenlose Technologie für einige attraktiver gemacht, da sie den menschlichen Kontakt minimiert und als hygienischere Art des Einkaufens angesehen werden könnte."

Vor einem Jahr (Oktober 2021) eröffnete die größte britische Supermarktkette Tesco ihren ersten kassenlosen Laden im Zentrum Londons, nachdem sie zuvor einen Versuch am Hauptsitz des Unternehmens in Welwyn Garden City durchgeführt hatte. Tesco hat sich mit dem israelischen Computer-Vision-Start-up-Unternehmen Trigo zusammengetan, um die EasyOut-Technologie in seiner „GetGo"-Filiale in High Holborn zu installieren, so dass die Kundschaft mit der Tesco.com-App in der Filiale einchekken, die benötigten Lebensmittel abholen und direkt wieder gehen können, ohne eine Kasse zu besuchen. Durch die Kombination von Kameras und Gewichtssensoren wird festgestellt, was die Kunden und Kundinnen eingekauft haben, und dann direkt über die mobile App abgerechnet, wenn sie das Geschäft verlassen.Kürzlich arbeitete Trigo mit der deutschen Supermarktkette REWE Group zusammen, um seinen zweiten autonomen Hybrid-Lebensmittelmarkt in Berlin zu eröffnen. Außerdem hat Trigo mit ALDI Nord an einem KI-gesteuerten kassenlosen Discounter in Utrecht (Niederlande) gearbeitet. „Die Lösung von Trigo hat einen zweiseitigen Nutzen", erklärt Shay Ziv, VP Marketing des Unternehmens. „Für die Shopper sparen wir Zeit und verbessern das Einkaufserlebnis, indem wir die Kassenschlangen abschaffen und ein nahtloses Einkaufserlebnis schaffen. Für Einzelhändler modernisieren wir die Arbeitsabläufe, indem wir Kosten für den Ladenbetrieb einsparen und die Effizienz steigern. Unsere Lösung wirkt sich auch direkt auf das Endergebnis aus, da sie den Warenschwund reduziert und dazu beiträgt, dass der durchschnittliche Einkaufskorb größer wird."

Anfang des Jahres eröffnete ALDI auch eine kassenlose Filiale in Großbritannien, die eine KI-gestützte Lösung des Technologieanbieters AiFi nutzt. Wie bei den anderen Filialen können die Kunden und Kundinnen auch bei ALDI Shop&Go ihren Einkauf abschließen, ohne ein einziges Produkt zu scannen oder eine Kasse passieren zu müssen. Die Filiale nutzt sogar die Gesichtserkennungstechnologie von Yoti, um den Kauf von Alkohol zu genehmigen (wer das System nicht nutzen möchte, dem stehen Mitarbeiter der Filiale bereit, um das Alter zu überprüfen). In den USA hat der Buch- und Schreibwarenhändler WH Smith seinen ersten kassenlosen Laden am LaGuardia Airport in New York eröffnet, der die Just Walk Out-Technologie von Amazon nutzt.

Laut Rebecca Hobbs von der Trendforschungsagentur Stylus gibt es mehrere treibende Kräfte, die das Wachstum der autonomen Geschäfte

anführen, abgesehen von der schieren Geschwindigkeit und dem Komfort, die normalerweise als Hauptvorteile angesehen werden. „Der größte Vorteil für die Verbraucher besteht darin, dass die Marken in der Lage sind, Online- und Offline-Verbraucherdaten leichter zusammenzuführen", sagt sie. „Sie können ein System einrichten, bei dem sich die Verbraucher in einem Kundenkonto anmelden müssen, um ein Geschäft zu betreten, so dass jeder im Geschäft dasselbe Profil hat wie online. Dies hilft ihnen, das Kaufverhalten zu ermitteln und Entscheidungen über den Warenbestand und das Merchandising zu treffen.

„Diese Geschäfte können sogar feststellen, was ein Kunde mitnimmt und was er wieder wegwirft", fügt Hobbs hinzu. „Wenn viele Kunden und Kundinnen einen Artikel in die Hand nehmen, ihn wegwerfen und sich dann dafür entscheiden, das Produkt online zu kaufen, wäre das eine Bestätigung für die Entscheidung, das Produkt im Geschäft zu haben, um es zu entdecken. Dieses Maß an Konnektivität wird den Aufstieg des Omnichannel-Einzelhandels vorantreiben - ein Wort, das schon seit Jahren in aller Munde ist, aber mit dieser Art von Technologie erst richtig zur Geltung kommen wird."

Johnston ist der Ansicht, dass diese Formate nicht nur die wirtschaftliche Ausgrenzung, sondern auch die Bedürfnisse eines breiteren Spektrums von Verbrauchern und Einkaufszielen berücksichtigen müssen, einschließlich der Bedürfnisse der Verbraucher nach Barrierefreiheit und Inklusion. „Gegenwärtig scheinen diese Formate an die Überzeugung der Einzelhändler gebunden zu sein, dass die Verbraucher reibungslose Erfahrungen wünschen", sagt er. Ich befürchte, dass Einzelhandelsmarken und -unternehmen, die sich ausschließlich darauf konzentrieren, ihrer Kundschaft diese Art von reibungslosen Einkaufserlebnissen zu bieten, vergessen, dass viele Verbraucher persönliche Erlebnisse wollen oder brauchen, die ein hohes Maß an menschlichen und sozialen Interaktionen beinhalten, die einen Mehrwert schaffen und ein hohes Maß an Vertrauen und Loyalität aufbauen. „Darüber hinaus wird es Menschen geben (entweder aus demografischen Gründen oder aufgrund ihrer Einstellung), die sich einfach nicht in jedem Geschäft, das sie betreten, digital anmelden wollen", argumentiert Hobbs. „Ich sehe keine nahe Zukunft (innerhalb von fünf Jahren) voraus, in der jedes Geschäft automatisiert sein wird", schließt Hobbs, „aber wenn diese Technologie billiger wird, die Verbraucher sich darauf einstellen und die Verwendung von Bargeld weiter zurückgeht, wird sich die Entwicklung sicherlich beschleunigen."

Den State-of the-Art und Innovationen rund um Smart Stores und Autonome Stores sind auf der EuroShop in der Dimension Retail Technology in den Hallen 4, 5, 6 und 7a zu finden.

Die EuroShop 2023 ist für Fachbesucherinnen und -besucher von Sonntag 26. Februar bis Donnerstag 02. März 2023, täglich von 10.00 bis 18.00 Uhr geöffnet. Messetickets gibt es nur online unter www.euroshop.de/1130 ab November 2022. Die Tageskarte kostet 70,- Euro, die 2-Tageskarte 120,-- Euro und die Dauerkarte 165,-- Euro.

# 10 Beiträge für sichereres Internet der Dinge

## Wie Hersteller und Anwender die Risiken der Konnektivität einschränken können

**Fachartikel von Jörg von der Heydt, Regional Director DACH bei Bitdefender**

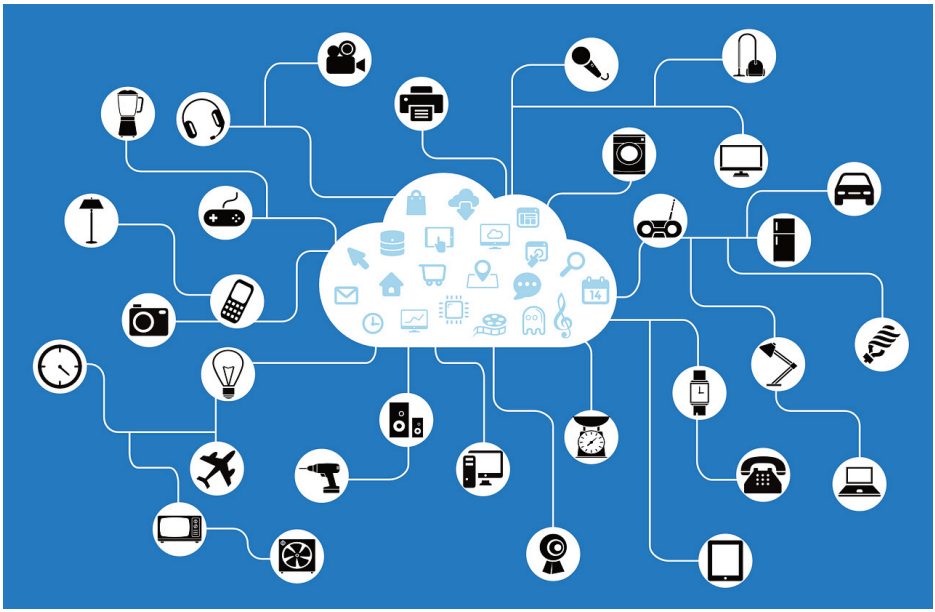
**Die Anbindung der lokalen IT an das Internet wird immer dichter. Smarte Hardware und Sensoren werden zunehmend Teil von Unternehmensnetzen, was die Angriffsfläche unübersichtlicher und damit fehleranfälliger macht. Hersteller und Anwender stehen zunächst in der Pflicht, für Sicherheit zu sorgen. IT-Administratoren dürfen die Kontrolle über die neuen Anschlüsse an das Internet der Dinge nicht verlieren oder müssen sie erst erlangen.**

Neben Videokameras oder anderer konnektiver Hardware öffnet auch das Remote-Office neue Risiken. Mitarbeiter, die von zu Hause aus arbeiten, eröffnen unter Umständen neue Schwachstellen, in dem sie ihre Internet-of-Things (IoT)-Hardware über ihr PC-System unbewusst und damit unkontrolliert an ein Unternehmensnetzwerk anbinden. Geräte mit Internetanschluss in den verschiedensten Branchen – etwa in den Bereichen Industrie oder im Gesundheitswesen – sorgen für mehr Berührungspunkte an das Internet und damit für neue potenzielle Hintertüren ins Netz. Auch wenn IoT und IT noch nicht völlig verschmelzen, steigt das Risiko für den Anwender.
Selbst wenn der Trend sich etwas abschwächt – die Zeichen stehen weiter auf Expansion: 2021 wuchs laut den Experten von IOT Analytics Index die Zahl der IoT-Geräte um acht Prozent auf 12,2 Milliarden weltweit. Laut dem 2022 Mobile Security Index von Verizon gaben 31 % der befragten Verantwortlichen für den Einkauf, das Management und das Sichern von IoT-Geräten zu, dass Hacker ihre IoT kompromittiert hatten. Bei zwei Dritteln davon kam es zu größeren Folgen („major impact"): 59 % beklagten einen Ausfall der Systeme, 56 % einen Datenverlust und 29% mussten Compliance-Bußgelder bezahlen. 41 % der Befragten gaben zu, IoT-Sicherheitsbelange zu opfern, um ihre Aufgaben erledigen zu können.

Für die Sicherheit der IoT-Geräte sind verschiedene Beteiligte zuständig, wie etwa Fachverbände, Behörden und nationale Regierungen. Eine Hauptverantwortung liegt jedoch bei Herstellern und Anwendern. IT-Administratoren müssen sich darüber im Klaren sein, dass „Verantwortungslosigkeit" für sie zum Sicherheitsrisiko werden kann.

### Was können Hersteller tun? – Sicherheitsstandards durchsetzen

- **Sicherheit mit entwickeln:** Um IoT-Funktionalitäten sicherer zu gestalten, bedarf es oftmals nur weniger Vorkehrungen, denn viele Risiken sind auf Nachlässigkeit und Intransparenz in der Entwicklung zurückzuführen. Wenn Hersteller undokumentierte User mit Default-Passwörtern anlegen, sind diese dem Anwender nicht bekannt. Mit der Zeit vergessen, sind



sie dennoch voll funktionsfähig und verfügen oft über umfangreiche Rechte. Hacker machen sich dies zu Nutze und suchen mit automatisierten Tools nach Schwachstellen. Deshalb müssen Hersteller diese Konten offenlegen, damit die Anwender sie deaktivieren oder mit eigenen Zugangsdaten versehen können. IT-Administratoren müssen damit rechnen, dass Cyberkriminelle die Rechte unbekannter Nutzer eskalieren.

- **Risikobewusstsein schärfen:** Hersteller sollten das Ändern des Passwortes beim Einrichten standardmäßig vorschreiben, um die Anwender zu einem besseren und bewussteren Umgang mit den eigenen Passwörtern zu erziehen. Dies schafft einfach und sehr effektiv mehr Sicherheit. Zudem schützt es auch IoT-Identitäten, die dann von einer Identitäts-Management-Lösung überwacht werden können.
- **Updates automatisieren:** Da der Anwender meist zu bequem dazu ist, Aktualisierungen vorzunehmen, oder dies ganz einfach vergisst, sollten Hersteller diese Aufgabe selbst übernehmen und automatisierte Updates anbieten. Denn es ist wichtig, die Software bei IoT-Produkten immer auf dem neuesten Stand zu halten. Anwender erwarten das Einhalten des Plug-and-Play-Versprechens oder haben schlicht keine Zeit für den IoT-Administrationsaufwand. Die Verantwortung, aktuelle Software anzubieten, liegt im Internet der Dinge in noch höherem Maße beim Hersteller als in der klassischen IT.
- **Standardbetriebssysteme benutzen:** Laut Bitdefender-Angaben verursachen proprietäre Betriebssysteme 96 Prozent aller entdeckten Sicherheitslücken. Und das obwohl ihr Anteil an den beobachteten Geräten lediglich 34 Prozent ausmacht. Daher sollten Standardbetriebssysteme ein Einkaufskriterium bei der Wahl für eine IoT-Hardware sein.
- **Sicherheit durch Zusammenarbeit:** Genauso wichtig ist die Zusammenarbeit der Hersteller mit IT-Sicherheitsexperten, welche oft auch gut funktioniert. Es gibt jedoch immer noch Hersteller von

IoT-Hardware, die keinen Sicherheitsansprechpartner nennen. Dies verzögert das gemeinsame Beheben von Verwundbarkeiten zum Schaden der Anwender. IT-Administratoren sollten die Kommunikation des IoT-Hardware-Herstellers ihrer Wahl verfolgen, um sich über eventuell entdeckte Zero-Day-Lücken zu informieren.

### Was können Anwender tun? – Den Wert von Sicherheit erkennen

- **Sich nicht in falscher Sicherheit wiegen:** IoT-Hardware ist schnell vom einzelnen Mitarbeiter oder auch von Gebäudetechnikern, die nicht immer die IT-Sicherheitskompetenz einer IT-Abteilung haben, installiert. Diese ignorieren oft das dadurch entstehende Risiko. Dieses besteht zum Beispiel darin, eine gekaperte IP-Videokamera für eine Distributed-Denial-of-Service-Attacke zu nutzen. Andere Angreifer versuchen, darüber ins Unternehmensnetz zu gelangen. Diese Gefahr merkt der Privatanwender unter Umständen nicht, weil sie ihn und das Verhalten seines Rechners nicht unmittelbar betrifft. Der Anwender sollte dies immer im Kopf haben und vorsichtig den Weg in das Internet der Dinge suchen. IT-Administratoren sollten ihre Mitarbeiter über diese Risiken aufklären. Eine Beschaffungsabteilung, die eigene IoT-Hardware bereitstellt, hilft Wildwuchs zu verhindern und kann Kontrolle gewinnen.
- **Qualität hat ihren Preis:** Sicherheit ist in der Regel kein leeres Markenversprechen, und deshalb sollten Anwender lieber nicht am falschen Ende sparen. Wer wenig Geld ausgeben will, kauft sich eher ein Risiko ein. Im Vergleich zu No-Brands, welche oft in Sachen Sicherheit zu wünschen übriglassen und keinen oder zumindest keinen realistisch erreichbaren Support haben, bieten teure Geräte hier einen Mehrwert in Sachen Sicherheit, Dokumentation und Support. Davon profitiert jedes Sicherheitsteam in einem Unternehmen.
- **Kurze Lebensdauer = Sicherheit mit Verfallsdatum:** Viele Geräte sind nur für eine kurze Einsatzzeit entwickelt worden und sind nicht dafür vorgesehen, diese zu überschreiten. Unternehmen verwenden etwa ihre Videokamera oder ihr Türsicherungssystem oft so lange, wie sie funktionieren. In der Zwischenzeit haben Hersteller ihren Support möglicherweise eingestellt und die Systeme veralten sicherheitstechnisch im Hintergrund. Ohne Updates entstehen so Sicherheitslücken durch Gefahren, die in der Zwischenzeit den Hakkern bekannt werden. IT-Sicherheitsverantwortliche sollten veraltete Hardware entfernen.
- **Passwortdisziplin:** Voreingestellte Passwörter sollten sofort geändert werden. Im weiteren Betrieb empfiehlt sich ein kontinuierlicher Wechsel oder ein geeigneter Passwortmanager. Für die meisten Hacker sind voreingestellte Kennworte leicht zu knacken, wenn sie mit Tools gezielt nach IoT-Geräten suchen.
- **Last but not least – Nicht den eigenen Datenschutz vergessen:** Alle IoT-Geräte geben Daten weiter – das ist ihre Aufgabe, dafür wurden sie entwickelt. Ein Server für diese Informationen außerhalb der EU hat sicher andere und oft schwächere Vorgaben für den Datenschutz. Wer über die zunehmende Menge an Daten, die auch über das Internet der Dinge in Zukunft transportiert werden, die Kontrolle bewahren will, sollte von Anfang an darauf achten.

### Last Line of Defense

IT-Sicherheitsverantwortliche müssen angesichts solcher von außen angetragener Probleme vor allem die Sichtbarkeit über die Konnektivität an das Internet erlangen und aufrechterhalten. Die Unübersichtlichkeit und Dynamik dieses Bereiches der IT, der als Schatten-IT sich oft ihrer Kontrolle entzieht, macht diese Aufgabe nicht einfach. Wichtig ist vor allem, spätestens den Zugriff auf das Unternehmensnetz über IoT zu kontrollieren. Eine IT-Sicherheit, die ganzheitlich die IT-beobachtet, kann auch die IoT-Endpunkte und ihre Auswirkung auf das Verhalten von PCs, Systemen und Applikationen im Blick haben.

Autor: Jörg von der Heydt, Regional Director DACH bei Bitdefender

UMFRAGE VON G DATA UND STATISTA:

# Deutschland: IT-Sicherheitsgefühl hat abgenommen

## Studie „Cybersicherheit in Zahlen“ offenbart großen Mangel an IT-Sicherheitsfachleuten in Deutschland

**Wie steht es um die IT-Sicherheit in Deutschland? Die kurze Antwort lautet: schlecht. Die Corona-Pandemie und der Ukraine-Krieg beeinflussen die Stimmung. Ein ausführliches Lagebild enthält das neue Magazin „Cybersicherheit in Zahlen“ von G DATA CyberDefense und Statista. Die darin enthaltene Arbeitnehmerumfrage zeigt die größten Problemfelder der Digitalisierung in Deutschland auf: Fachkräftemangel, Angst vor Cyberattacken und fehlendes Wissen, was im IT-Notfall zu tun ist.**

Die aktuelle Studie „Cybersicherheit in Zahlen“ von G DATA CyberDefense und Statista belegt: Die Corona-Pandemie und der Ukraine-Konflikt haben auch bei der IT-Sicherheit Spuren hinterlassen. Der G DATA Index Cybersicherheit ist innerhalb eines Jahres um zwei Prozent zurückgegangen. Das heißt: Die gefühlte IT-Sicherheit in Deutschland hat abgenommen. Insbesondere beim Fachwissen und dem Sicherheitsgefühl sind die Indexwerte gesunken. Gleichzeitig ist das Risikoempfinden zurückgegangen.

Im beruflichen Umfeld schätzt ein Drittel der Befragten das Risiko als hoch oder sehr hoch ein, Cyberkriminalität zum Opfer zu fallen. Im privaten Umfeld liegt der Anteil sogar noch höher – bei 38 Prozent. Ein möglicher Grund: Es fehlt vielen Menschen an den Kompetenzen, um sich und ihre digitalen Geräte entsprechend zu schützen.

„Über viele Jahre war Cybersicherheit vor allem ein Thema für die IT-Abteilung, mit dem das Management sich höchstens punktuell beschäftigen wollte. Das war und ist eine Fehleinschätzung“, sagt Andreas Lüning, Mitgründer und Vorstand von G DATA CyberDefense. „IT-Sicherheit mag mit der Technik beginnen.
Aber dort ist lange noch nicht Schluss. Gerade Führungskräfte müssen eine gute Fehlerkultur vorleben und Mitarbeitende ermutigen auch Fehler, welche die Sicherheit gefährden können, zu melden.“

### Große Personalnot bei IT-Sicherheit

Bereits zum zweiten Mal hat Statista im Auftrag von G DATA eine repräsentative Studie zum Stand der IT-Sicherheit in Deutschland geführt. Mehr als 5.000 Arbeitnehmer*innen wurden im beruflichen und privaten Kontext befragt.

Die Umfrage zeigt, wie groß der Personalmangel in der IT ist: Insgesamt klagen 36 Prozent der Befragten über fehlende Mitarbeitende im IT-Bereich. Weitaus dramatischer ist die Lage bei kleinen Firmen. In Unternehmen mit weniger als 50 Angestellten sprechen mehr als zwei Drittel der Umfrageteilnehmer*innen von fehlendem Personal. Daher überrascht es auch nicht, dass Mitarbeitende für IT generell händeringend gesucht werden – gerade für den Bereich der IT-Sicherheit. Mehr als 44 Prozent der Befragten aus großen Unternehmen haben hier den größten Handlungsbedarf.
„Die Studie von G DATA und Statista zeigt, dass es keine hundertprozen-

tige IT-Sicherheit gibt. Wir sollten den Angreifern nicht mehr Angriffsflächen bieten als unbedingt nötig", sagt Robin Rehfeldt, Senior Analyst bei Statista.

„In der zweiten Ausgabe von 'Cybersicherheit in Zahlen' nehmen wir Unternehmen und Organisationen in den Fokus, schauen auf Systeme, Strukturen oder auf Prozesse. Und fragen: Wie können und müssen sich Firmen in einer gefährlicher werdenden Welt aufstellen? Wie funktioniert Sicherheit – für die Institution, die Führung, die Mitarbeitenden?"

### Umfassendes Nachschlagewerk der IT-Sicherheit

Diese exklusiven Zahlen sind nur ein kleiner Einblick in das Magazin „Cybersicherheit in Zahlen" von G DATA, brand eins und Statista. Neben einer groß angelegten Arbeitnehmerumfrage enthält das Magazin spannende Zahlen rund um IT-Sicherheit und dient als breit aufgestelltes Nachschlagewerk zu dem Thema Cybersicherheit:

- Die Zahl der gemeldeten Phishing-Fälle hat sich innerhalb von fünf Jahren um mehr als 1.560 Prozent erhöht (Quelle: FBI).
- Der jährliche Schaden durch Ransomware ist in Deutschland von 2019 auf 2021 um 358,5 Prozent gestiegen.
- Ein Drittel der deutschen Unternehmen ist 2021 laut der Initiative „Deutschland sicher im Netz" einem Phishing-Versuch zum Opfer gefallen.

„Cybersicherheit in Zahlen" zeichnet sich durch eine hohe Informationsdichte und besondere methodische Tiefe aus.

Das Magazin „Cybersicherheit in Zahlen" steht hier kostenlos unter Angabe der Kontaktdaten zum Download bereit: www.gdata.de/cybersicherheit-in-zahlen

G DATA IT-Security-Trends 2023

## Professionelle Cyberkriminelle erhöhen Risiko für Unternehmen weiter

### Social Engineering und Missbrauch von Standard-Anwendungen gefährden die IT-Sicherheit in Deutschland massiv

Um ihren Profit zu vergrößern, bedienen sich die Cyberkriminellen immer ausgefeilterer und effizienterer Vorgehensweisen. Dafür verfeinern und ändern sie einerseits ihre Methoden, um Netzwerke zu infiltrieren, andererseits nutzen sie neue Tools für ihre Attacken. Daher sind insbesondere Schwachstellen in Systemen, die flächendeckend zum Einsatz kommen, ein großes Risiko. Dazu zählt beispielsweise die Java-Schwachstelle Log4Shell, mit der sich Kriminelle Zugriff auf Unternehmensserver verschafft haben und die immer noch ausgenutzt wird. Das zeigt: eine einzige Lücke reicht und Angreifer*innen kompromittieren mehrere hundert oder gar tausend Unternehmen gleichzeitig. Deshalb gilt für Administratoren, Server und Endgeräte immer mit aktuellster Software auf neuestem Stand zu halten.

„Ein zentrales Problem für die IT-Sicherheit in Deutschland ist und bleibt, dass Unternehmen die Warnungen zu Schwachstellen oder Sicherheitsrisiken nicht ernst nehmen", sagt Andreas Lüning, Mitgründer und Vorstand von G DATA CyberDefense. „Sie unterschätzen weiterhin das reale Risiko eines Cyberangriffs für sich und setzen auf das Prinzip Hoffnung. Dabei müssen Verantwortliche jetzt handeln, denn angesichts der wirtschaftlichen angespannten Lage kann sich kein Unternehmen Umsatzeinbußen oder Betriebsausfälle leisten, die ihren Ursprung in einem IT-Sicherheitsvorfall haben."

### Rootkit-Renaissance

Ein weiterer Angriffsweg: Rootkits kommen wieder vermehrt bei Angriffen zum Einsatz, bei dem Cyberkriminelle verschiedene Schadprogramme

miteinander kombinieren. Denn mit Rootkits lassen sich Schadprogramme vor Sicherheitslösungen verstecken. So werden Anmeldungen von Kriminellen auf dem Computer verschleiert, ebenso wie die mit diesem Vorgang verbundenen Dateien und Prozesse. Researcher haben in einer Machbarkeitsstudie nachgewiesen, dass Angreifer Rootkits von GitHub, einer Plattform zur Verwaltung quelloffener Software, kopieren und diese Programme in ihre Angriffsketten einbauen, um Unternehmen zu infiltrieren.

„Das Problem liegt darin, dass Rootkits im ursprünglichen Sinne nicht als Malware gelten und deswegen legal auf GitHub bereitgestellt werden", kommentiert Karsten Hahn, Lead Engineer Prevention, Detection and Response bei G DATA CyberDefense. „Gerade für Kriminelle mit geringen IT-Kenntnissen sind solche Angebote interessant, denn das Programmieren von Rootkits ist alles andere als trivial."

## Ohne Fachkräfte fehlt es an IT-Sicherheit

Eine große Herausforderung betrifft insbesondere kleine und mittelständische Unternehmen: Der Mangel an ausgebildeten IT-Sicherheitsfachleuten. Das fehlende Know-how wirkt sich nachhaltig auf das IT-Sicherheitsniveau aus. Aus eigener Kraft können mittelständische Firmen diese Lücke nicht schließen. Ein Weg aus diesem Dilemma bieten Managed Security Services sowie in Cybergefahren geschulte Mitarbeitende. Wichtig ist dabei, dass Unternehmen jetzt handeln. Denn ein Angriff auf die IT mit womöglich unkontrollierbaren Folgen kann jederzeit passieren.

## Endverbraucher im Visier: Angriffsziel iPhone

Ein attraktives Ziel bleiben private Smartphones, nicht nur, weil Nutzer es für Mobile-Banking, -Payment oder als digitalen Schlüssel nutzen. Dabei nehmen die Cyberkriminellen künftig vermehrt iPhones ins Visier. Der Grund: iPhone-Anwender gelten als kaufkräftiger und sind damit auch für Angreifer lukrativer.

„Die Kriminellen nutzen insbesondere Schwachstellen des iOS-Betriebssystems aus, weil sie auf diesem Weg Root-Rechte und damit vollständige Kontrolle über das Gerät erhalten", warnt Stefan Dekker, Mobile Security Experte bei G DATA CyberDefense. „Wie ernst die Lage ist, hat das aktuelle Jahr gezeigt, denn Apple musste mehrfach Patches für kritische Lücken bereitstellen." Anwender müssen deshalb bereitgestellte Patches und Updates für ihr Smartphone schnellstmöglich installieren.

## Social Engineering: Der Mensch im Fadenkreuz

Da sich der technologische Schutz gegen Schadsoftware deutlich verbessert hat, passen Cyberkriminelle ihre Angriffsmethoden immer wieder an.
Social-Engineering-Attacken können jeden treffen und haben das Ziel, persönliche Daten oder Informationen von Opfern abzugreifen. Smartphones spielen hierbei eine entscheidende Rolle: Angreifer nehmen vermehrt via Messenger-Dienst, wie etwa per Whatsapp oder Telegram, Kontakt zu ihren potenziellen Opfern auf.
Wie real die Gefahr ist, zeigen aktuelle Betrugsversuche. Dabei haben Täter den Enkeltrick in den digitalen Raum verlagert, sozusagen als "Enkeltrick 2.0". Täter geben sich als ein Familienmitglied in Not aus und versuchen, ihr Opfer zur Überweisung eines größeren Geldbetrags zu überreden.

Wer einen Notfall-Anruf erhält, sollte– so schwer es auch fallen wird – kühlen Kopf bewahren und das Szenario analysieren. Und auf einem anderen Kanal (E-Mail oder Telefonat) prüfen, ob der beschriebene Notfall tatsächlich eingetreten ist.

# Videos

**Video & eBook**

## Wie die Wohnungswirtschaft von moderner Sicherheitstechnik profitiert

Während Mieter und Gebäudetechniker längst mit ihren Smartphones vieles online erledigen, schließen genau diese Menschen noch mehrere Millionen Türen mit einer rein mechanischen Schließanlage auf und zu, die 30 Jahre oder sogar noch viel älter ist. Warum ist das so?
Schließanlagen sind langlebig und ein Wechsel oft aufwändig. Daher freuen sich Nutzer älterer Schließzylinder zwar über deren nach wie vor reibungslose Funktion, sollten aber auch wissen, dass deren technischer Stand nicht Up-to-date ist und man damit auf sehr viele konkrete Vorteile im Alltag verzichtet.
Das fällt bei einer kleinen Wohneinheit noch nicht so ins Gewicht, verspielt aber bei größeren Gebäuden mit unterschiedlichen Nutzern geradezu entscheidende Effizienzvorteile beim Anlagenmanagement im Alltag. Die Sicherheitstechnik hat sich in den letzten Jahrzehnten enorm weiterentwickelt.

So bieten zum Beispiel elektronische Lösungen gerade in der Wohnungswirtschaft sehr viele Vorteile. Diese sind:

- Geringerer Verwaltungsaufwand und geringerer administrativer Aufwand;
- Keine Gefahr durch existierende Nachschlüssel;
- Keine Gefahr mehr bei Schlüsselverlust durch einfaches Ausprogrammieren;
- Erheblich geringere Kosten bei Schlüsselverlust;
- Kontrolliertes Betreten der Gebäude durch Dienstleister: Räume und Uhrzeiten können exakt zugewiesen werden;
- Umsetzung aller gesetzlichen und versicherungstechnischen Anforderungen in Bezug auf Rettungswegtechnik und Zutrittskontrolle;
- Auf- und Nachrüstung auch in historischen Türen ohne Lärm und Dreck möglich.

### Video zeigt 8 konkrete Situationen aus dem Alltag

Was sich zunächst theoretisch anhört, zeigt das Video „eCLIQ Schließanlagen in der Wohnungswirtschaft" ganz anschaulich anhand acht Szenarien, wie sie Abteilungsleiter der Gebäudetechnik jeden Tag erleben. Hier werden die häufigsten Situationen durchleuchtet, die durch den Wechsel auf oder den Einsatz von elektronischen Schließlösungen mit Eigentümern, Mietern und Hausmeistern entstehen.

**https://youtu.be/ELZeuuKjeGQ**

**VdS**

## Fachtagungen 1. Halbjahr 2023

Auf den ein- bis zweitägigen Fachtagungen berichtenReferenten mit Praxiserfahrung aktuell zu bestimmten Themenbereichen. Sie informieren zum Beispiel über neue technische Entwicklungen, geänderte Regelwerke sowie spannende Fallbeispiele. VdS-Fachtagungen bieten einen Überblick über ein Thema, die Gelegenheit, das Wissen auf den neuesten Stand zu bringen und sich intensiv mit anderen Teilnehmern auszutauschen.

**17.04.2023 Köln: VdS-Fachtagung**
Kontrolle und Wartung von Brandschutzanlagen
**18.04.2023 Köln: VdS-Fachtagung**
Brandschutz in Krankenhäusern
**19.04.2023 Köln: VdS-Fachtagung**
Schadenverhütung bei Biogasanlagen
**20.04.2023 Köln: VdS-Fachtagung**
Evakuierung und Räumung von Gebäuden
**21.04.2023 Köln: VdS-Fachtagung**
Sicherheit von Veranstaltungen
**27.04.2023 Köln: VdS-Fachtagung**
53. Fortbildungsseminar für Brandschutzbeauftragte
**28.04.2023 Köln VdS-Fachtagung**
Sicherheit in Kreditinstituten
**02.05.2023 - 03.05.2023 Köln: VdS-Fachtagung**
Brandschutz in Bus-Betriebshöfen
**12.06.2023 Köln: VdS-Fachtagung**
Meinungs- und Erfahrungsaustausch nach § 29a BImSchG
**13.06.2023 Köln: VdS-Fachtagung**
Gewässerschutz/Löschwasser-Rückhaltung
**14.06.2023 Köln: VdS-Fachtagung**
Die Ermittlung von Brand- und Explosionsursachen
**21.06.2023 - 22.06.2023 Köln VdS-Fachtagung**
Sicherheitsfachtagung

**VdS-Bildungszentrum:**
**Telefon +49 (0)221-7766-555**
**mailbildungszentrum@vds.de**

BVSW

## Audi Driving Experience in Seefeld

**BVSW bietet exklusives Winterfahrtraining in Österreich an**

Reagiert ein Elektroauto anders, wenn es die Traktion bei glatter Fahrbahn verliert, als ein Fahrzeug mit Verbrennungsmotor? Und wenn ja – wie? Erleben und vergleichen Sie bei diesem Training die Besonderheiten zweier Antriebskonzepte mit dem Audi RS e-tron GT und mit einem sportlichen RS-Verbrenner. Und erfahren Sie die besten Basis-Tipps für eine kontrolliertere und souveränere Fahrweise. Denn wer weiß, wie sein Fahrzeug reagiert, fühlt sich im Alltag sicherer – ganz gleich mit welcher Antriebsform. Performance ist das Ziel, höchstmögliche Sicherheit die Devise. Dieses Training bringt Sie an Ihre Grenzen, damit Sie in Zukunft bei winterlichen Bedingungen noch souveräner unterwegs sind. Ob Fahrdynamik auf glattem Untergrund, den spektakulären Drift oder eine kontrolliertere Fahrzeugbeherrschung unter widrigsten Bedingungen – erleben Sie puren Fahrspaß mit zwei verschiedenen Antrieben: der rein elektrische Audi RS e-tron GT sowie der Audi RS 5 Sportback stehen für Sie bereit.

Sie erlernen wechselweise in zwei Gruppen eine souveränere Fahrweise unter winterlichen Bedingungen sowie die kontrolliertere Fahrzeugbeherrschung auf Eis und Schnee. Um Ihnen die Grundlagen der Fahrdynamik auf glatter Fahrbahn näherzubringen, steht Ihnen der Audi RS e-tron GT zur Verfügung. Sie werden erstaunt sein, wieviel puren Fahrspaß ein rein elektrisch angetriebenes Fahrzeug bietet. Mit dem Audi RS 5 Sportback erlernen Sie unter Anleitung unseres erfahrenen Instruktoren-Teams die Grundlagen des perfekten Drifts – zum Beispiel im eleganten Powerslide oder im schwungvollen Dynamikparcours. Dieses Trainingsangebot richtet sich vor allem an Fahrerinnen und Fahrer, die in komprimierter Form maximalen Fahrspaß und die Zukunft der Mobilität erleben möchten. Abgerundet wird das Erlebnis auf der Eisstrecke in Seefeld mit einem gemütlichen gemeinsamen Get-Together am Vorabend im alpinen 4* Grandhotel "Krumers Alpin".

**Trainingsinhalte:**

- Warm-up Session, • Drifttraining
- Dynamikslalom, • Powerslide
- Parcours

**Teilnahmegebühr:** 1.980,00 € für BVSW-Mitglieder (2.300,00 € für Nichtmitglieder): Dieser Betrag ist gemäß §4 Nr. 22a UStG von der Umsatzsteuer befreit. **Enthaltene Leistungen:** Audi Driving Experinence Winterfahrtraining (wir belegen jedes Fahrzeug mit 2 Personen), Einführungsvortrag am Vorabend, 1 Hotelübernachtungen im Krumers Alpin Resort in Seefeld (EZ inkl. Halbpension, Mittagessen und ausgewählten Getränken), Trainingsfahrzeuge werden gestellt Audi RS 5 Sportback & Audi RS e-tron GT, Vollkaskoversicherung mit € 1.000 Selbstbeteiligung), Kraftstoff-/Ladestromkosten
**Termin:** 23. Februar 2023 , (mit individueller Anreise am 22.02.2023 & individueller Abreise am 23.02.2023)
**Anmeldung bitte per**
**E-Mail an caroline.eder@bvsw.de**

BHE

## Präsenz-Seminare im 1. Quartal 2023

24.01.23 Hünfeld: Brandmeldeanlagen - Auffrischungsseminar
25.01.23 Hünfeld: Brandmeldeanlagen – Grundlagen
01.02.23 Hünfeld: BMA: DIN VDE 0833-2, MVV-TB und MLAR
02.02.23 Hünfeld: Brandwarnanlagen nach DIN VDE V 0826-2
06.02.23 Hünfeld: Videosicherheitssysteme nach DIN EN 62676
09.02.23 Dortmund: Identifikationsmanagement
14.02.23 Fulda: Vorbereitung zur Prüfung VdS-Fachkraft Video
16.02.23 Fulda: Feststellanlagen inkl. Berechtigung zur Erstinbetriebnahme mit herstellergebundener Autorisierung
22.02.23 Fulda-Künzell: Einbruchmeldeanlagen - Grundlagen
01.03.23 Webinar: Cyber-Security-Beauftragter Zertifizierung
01.03.23 Hünfeld: Perimetersicherung
07.03.23 Fulda: Grundlagen der Netzwerktechnik für die Sicherheitsbranche
07.03.23: Mettmann: DIN 14675/Sprachalarmierung: Vorbereitungsseminar für hauptverantwortliche Fachkräfte (Prüfung)
09.03.23 Hünfeld: Workshop „Instandhaltung RWA-Anlagen"
14.03.23 Wetzlar: Rauch- und Wärmeabzugsanlagen
14.03.23 Gießen: EMA – Auffrischung (VDE 0833, VdS 2311)
16.03.23 Gießen: Technik im IP-Netzwerk – Aufbauseminar
16.03.23 Gießen: Q-Trainerausbildung für die geprüfte Fachkraft Rauchwarnmelder (Erstausbildung/Auffrischung)
21.03.23 Hünfeld: Fachkundiger für Notausgänge und Fluchtwegsicherungen
22.03.23 Hünfeld: Fachkundiger für Feststellanlagen an Feuerschutzabschlüssen
23.03.23 Hünfeld: Fachkundiger für die Instandhaltung von Rauch- und Feuerschutztüren
28.03.23 Hünfeld: So verkaufen Profis auch in Zukunft erfolgreich!
29.03.23 Hünfeld: Professionelles Verhalten als Servicetechniker
29.03.23 Ratingen: Zugangs- und Zutrittssteuerung: Grundlagen und Systeme zur Personenidentifikation
29.03.23 Ense: Fachkundiger für Sicherheitsbeleuchtung und dynamische Sicherheitsleitsysteme
30.03.23 Ense: Planung und Projektierung von Sicherheitsbeleuchtungsanlagen

**Weitere Informationen: https://tinyurl.com/4fxmjnuc**

# Mehr Funktionalität für BWV-Lösung

## Qognify VMS 7.2 unterstützt den Ermittlungsprozess und fügt Cloud-Funktionen hinzu

**Qognify, Anbieter von Video- und Enterprise Incident Management-Lösungen, hat die zweite Version seiner Videomanagement-Software Qognify VMS auf den Markt gebracht. Die neueste Softwareversion - Qognify VMS 7.2 - bietet erweiterte Unterstützung für Body-Worn-Kameras, zusätzliche Funktionen zur Unterstützung von Ermittlungen und eine neue Web-Client-Architektur.**

Qognify VMS 7.2 adressiert den zunehmenden Einsatz von am Körper getragenem Video (BWV = Body Worn Video) in vielen Bereichen, von der Polizei über Sicherheitsanwendungen bis hin zu Kundenservice und Qualitätskontrolle. Da BWV zu einer wichtigen Komponente im Sicherheits-Ökosystem vieler Qognify VMS-Kunden geworden ist, wird die Notwendigkeit, BWV-Material zu Ermittlungszwecken in eine voll ausgestattete VMS-Umgebung zu integrieren, immer deutlicher. In diesem Zusammenhang ist es von entscheidender Bedeutung, dass das BWV-Integrationsframework in der Lage ist, die Beweiskette des aufgenommenen Bildmaterials für Strafverfolgungsanwendungen aufrecht- zuerhalten. Daher hat Qognify eng mit den Herstellern von BWV-Systemen zusammengearbeitet, um sicherzustellen, dass die Protokolle zur Beweiskette eingehalten werden - vor allem, wenn die Geräte in mehreren Schichten von verschiedenen Benutzern verwendet werden. Mit Qognify VMS 7.2 sind diese erweiterten Funktionen nun auch für Organisationen verfügbar, die BWV von Axis einsetzen. Die Integration anderer Hersteller wird in zukünftigen Versionen folgen.

Zusätzlich zur Unterstützung weiterer Videoquellen bietet Qognify VMS 7.2 neue Funktionen der Unternehmensklasse zur Vereinfachung von Ermittlungen und zur Verbesserung des Datenschutzes. Kameras, Lagepläne und Layouts können nun mit logischen Bezeichnungen versehen und so entsprechend gruppiert werden. Wenn Bediener beispielsweise die Videoübertragungen aller Kameras in einem bestimmten Treppenhaus sehen möchten, wählen sie einfach die entsprechende Entitätsbezeichnung aus, und alle entsprechenden Kameras werden automatisch angezeigt - unabhängig davon, wo diese in der logischen Struktur der Installation liegen mögen. Dadurch können sich die Bediener schneller ein umfassendes Bild von der Situation machen und Effizienzgewinne realisieren. Da der Ermittlungsprozess häufig mit Datenschutzaspekten verbunden ist, ist es mit Qognify VMS 7.2 nun auch möglich, den Zugriff auf bestimmte Kameras auf bestimmte Arbeitsplätze zu beschränken. Darüber hinaus ermöglicht eine neue statische Scramble-Funktion die Unschärfe eines bestimmten Bereichs innerhalb des Kamerabildes mit Hilfe einer einstellbaren Privatsphärenmaske, wodurch sich die Videomaskierung für eine ganze Reihe neuer Anwendungen öffnet.

Qognify VMS 7.2 setzt auch die strategische Initiative des Unternehmens fort, Cloud-Funktionen der Unternehmensklasse zu entwickeln. Als Teil des Releases bietet Qognify nun Cloud-Speicherangebote, die auf die speziellen Anforderungen des Videomana- gements zugeschnitten sind. Die Nutzung herkömmlicher Cloud-Speicherlösungen ist oft mit unvorherseh- baren Kosten verbunden, da der Cloud-Speicheranbieter in der Regel Gebühren für den Abruf von Videomaterial von seinen Servern erhebt. Viele IT-Abteilungen können dies in ihrer Budgetstruktur nicht berücksichtigen, was sie oft davon abhält, diese Technologie zu nutzen. Im Gegensatz dazu berechnet Qognify nur das Volumen des genutzten Cloud-Speichers auf einer Terabyte-Basis,

unabhängig davon, wie oft der Kunde Videos abrufen muss - was zu konsistenten "Pay as you go"-Kosten führt, die leicht zu budgetieren sind.

Die neue Software-Version bietet auch einen ersten Blick auf die neue Web-Client-Architektur von Qognify, die sich durch eine leistungsstarke Videodarstellung auszeichnet.
Yaniv Toplian, VP R&D bei Qognify, erklärt den Ansatz von Qognify: "Viele VMS-Webclients erfordern entweder die Installation zusätzlicher Softwarekomponenten, was sie unflexibel macht und Risiken für die Cybersicherheit mit sich bringt, oder sie gehen Kompromisse bei der Anzeigeleistung und Latenz ein. Um dies zu überwinden, haben wir eine neue, revolutionäre Streaming- und Wiedergabetechnologie entwickelt, die die Anzeige von Videoströmen mit sehr geringer Latenz in einer Standard-Browserumgebung ohne zusätzliche Softwarekomponenten ermöglicht. Dies ist umso wichtiger, als der Web-Client ein wesentlicher Bestandteil der umfassenden Cloud-Strategie von Qognify ist, die darauf abzielt, Unternehmen ein Höchstmaß an Flexibilität für ihre Implementierungen zu bieten."
Der neue Qognify Web Client schafft ein Framework, das es Unternehmen ermöglicht, ihre Ermittlungs- und Reaktionsprozesse durch adaptive Workflows und verbesserte Kommunikations- und Koordinationsmöglichkeiten zu verbessern. Für Qognify VMS 7.2 wird eine begrenzte Funktionalität zur Verfügung stehen, die mit jeder

neuen Version weiter ausgebaut wird.

Jeremy Howard, Vice President of Sales, Physical Security - Americas bei Qognify, hebt einen weiteren wichtigen Aspekt der neuen Version 7.2 hervor: "Nach der Markteinführung von Qognify VMS im April dieses Jahres haben wir ein massives Interesse von Kunden erfahren, die derzeit andere VMS-Produkte von Qognify nutzen, auf unsere neue Flaggschifflösung umzusteigen, da sie die spezifischen Anforderungen und Anwendungsfälle vieler Branchen auf einzigartige Weise erfüllt. Wir freuen uns, unseren Kunden dieses Maß an Flexibilität bieten zu können und wollen ihnen die Übergänge innerhalb unseres Lösungsportfolios so einfach wie möglich machen. Mit dem neuen Release haben wir Qognify VMS daher um einige echte Enterprise-Funktionalitäten erweitert, die Kunden in anderen VMS-Lösungen von uns sehr schätzen. Darüber hinaus stellen wir leistungsstarke praktische Tools zur Verfügung, um eine reibungslose Umstellung zu unterstützen."

Für Kunden, die ein Upgrade von Ocularis auf Qognify VMS durchführen möchten, steht daher ein leistungsfähiges Upgrade-Tool zur Verfügung, das große Teile des Umstellungsprozesses automatisiert und eine effiziente Umstellung selbst großer Systeme mit mehreren hundert Kameras in weniger als einem Tag ermöglicht. Während die Aufzeichnungen unangetastet bleiben, da beide Systeme dieselbe Aufzeichnungsplattform nutzen, überträgt das Upgrade-Tool Benutzer, Gruppen, Berechtigungen und Ansichten von Ocularis zu Qognify VMS.

Qognify VMS 7.2 ist ab sofort weltweit verfügbar.

Frequentis

# Integrierte Leitstelle Saarland

**Beauftragung des Notrufabfrage- und Funkvermittlungssystems durch ZRF Saar • Zuschlag für die Neubeschaffung des Notruf- und Funkabfragesystems der Leitstellen der ILS Saarlandstärkt Marktposition im BOS-Bereich • Vollständig redundantes, auf Voice over IP (VoIP) basierendes Kommunikationssystem**

**Die Frequentis Deutschland GmbH erhielt vom Zweckverband für Rettungsdienst und Feuerwehralarmierung Saar (ZRF Saar) den Zuschlag für das Projekt im Zuge einer EU-weiten Ausschreibung für die Lieferung und Integration der Kommunikationssysteme am Hauptstandort Winterberg sowie an den Redundanzstan- dorten Merzig und Bexbach.**

Das Saarland hat fast 1 Mio. Einwohner und rund 2.570 km² Fläche. Die ILS Saarland ist die einzige Leitstelle der nicht-polizeilichen Gefahrenabwehr im Saarland. Die Aufgaben sind im Wesentlichen die Notrufannahme, die Alarmierung der Einsatzkräfte, die Koordination der Rettungseinsätze oder auch die Disposition der Krankentransporte.
Vor dem Hintergrund einer langfristigen Wirtschaftlichkeit bei Nutzung und Betrieb und von erforderlichen Weiterentwicklungen der Systemtechnik, ergaben sich folgende Ziele der Beschaffungsmaßnahme:

- sehr hohe Verfügbarkeit der Kommunikationstechnik
- übergreifende Systemvernetzung der neuen Kommunikationstechnik zur flexiblen Besetzung von verfügbaren Arbeitsplätzen und Nutzung von Ressourcen an den Standorten
- Erweiterbarkeit des Systems mit Blick auf weitere zukünftige Dienste und veränderte Umgebung
- Wirtschaftlichkeit durch Einbindung der neuen Kommunikationstechnik in die vorhandenen modernen IT-Infrastruktur des ZRF's
- Favorisierte Nutzung von Standard-Applikationen und Open Source, d.h. grundsätzlicher Verzicht auf leitstellenspezifische Spezialentwicklungen

Um diesen Anforderungen gerecht zu werden, wird nun das Kommunikationssystem ASGARD zum Einsatz kommen. ASGARD integriert alle Kommunikationsmittel einer Leitstelle in eine Anwendung und ermöglicht dadurch eine einheitliche, für die Bedürfnisse moderner Sicherheitszentralen optimierte, schnelle und vor allem sichere Bedienung.

Die bewährte Frequentis Software-Lösung – das Kommunikationssystem ASGARD ist bereits in ca. 50 Leitstellen in Deutschland im Einsatz – sichert dank hoher Flexibilität und Ausfallsicherheit sowie der vielfältigen Integrationsmöglichkeiten in Infrastrukturen ein Kommunikationsmanagement für diese Aufgaben.

Dazu Rainer Buchmann, Fachbereichsleiter der ILS Saarland: "Wir freuen uns auf die Zusammenarbeit mit der Firma Frequentis. Mit Frequentis wurde ein Unternehmen gefunden, das uns ein modernes IT- und Kommunikationssystem "aus einem Guss" und basierend auf moderner IP-Technik liefert.

Mit dem System wird die nicht-polizeiliche Gefahrenabwehr des Saarlandes optimal auf zukünftige Anforderungen und kommende Großschadenslagen vorbereitet sein."

Reinhard Grimm, Geschäftsführer von Frequentis Deutschland, betont: "Mit ASGARD können wir BOS-Leitstellen ein optimales Produkt für ihre vielfältigen Aufgaben zur Verfügung stellen. Wir sind stolz auf dieses Vorzeige-Projekt ILS Saarland und das Vertrauen des ZRF Saar in Frequentis."

Sepura

## 500.000stes TETRA-Funkgerät in Deutschland in Betrieb genommen

Sepura hat sein 500.000stes TETRA-Funkgerät in Deutschland in Betrieb genommen, wobei das Gerät im U-Bahn-Netz der Stadt München zum Einsatz kommen wird. Die Stadtwerke München errichten im Netz der Münchner U-Bahn-Netz aktuell im Rahmen eines Projektes ein neues Digitalfunksystem als Ersatz für die bisherige analoge Funktechnik. Als Teil der neuen Lösung liefert die Firma Sepura - über ihren deutschen Exklusivpartner SELECTRIC Nachrichten-Systeme GmbH – im Rahmen einer Ausschreibung über 1.800 Sepura SC20 TETRA-Funkgeräte und Zubehör für das neue Netz.

Sepura hat sein 500.000stes TETRA-Funkgerät in Deutschland in Betrieb genommen, wobei das Gerät im U-Bahn-Netz der Stadt München zum Einsatz kommen wird. Die Stadtwerke München errichten im Netz der Münchner U-Bahn-Netz aktuell im Rahmen eines Projektes ein neues Digitalfunksystem als Ersatz für die bisherige analoge Funktechnik. Als Teil der neuen Lösung liefert die Firma Sepura - über ihren deutschen Exklusivpartner SELECTRIC Nachrichten-Systeme GmbH – im Rahmen einer Ausschreibung über 1.800 Sepura SC20 TETRA-Funkgeräte und Zubehör für das neue Netz.

Hendrik Pieper, Geschäftsführer der SELECTRIC, arbeitet mit Sepura seit dem Markteintritt des Herstellers in Deutschland zusammen. Er sagte:

"Die Produkte von Sepura sind weltweit als robuste und zuverlässige Produkte bekannt. Wir haben auf dem größten TETRA-Markt der Welt Erfolg, indem wir Sepura-Produkte mit einem hervorragenden Kundenservice für Nutzer in der öffentlichen Sicherheit und in kommerziellen Organisationen im ganzen Land kombiniert haben. Wir freuen uns darauf, diese Kunden auch in Zukunft zu unterstützen."

Das Angebot von SELECTRIC umfasste neben den Sepura Handfunkgeräten auch Faustmikrofone und Ladestationen, die von WETECH speziell nach den Spezifikationen des Kunden für den Einsatz in den Fahrzeugen entwickelt wurden. SELECTRIC kümmerte sich auch um die Integration des TETRA-Kommunikationsnetzes in die bestehende Leitstelle, programmierte die Sepura TETRA-Funkgeräte, führte Schulungen für die Funkgerätebenutzer durch und begleitete den Einsatz mit umfassender technischer Unterstützung. Die vollständige Übernahme in den aktiven Betrieb wird für Ende 2023 erwartet.

Hooman Safaie, Regional Sales Director bei Sepura, sagte: "Wir sind stolz darauf, den Meilenstein von einer halben Million installierter Funkgeräte in Deutschland zu erreichen. Wir beobachten zunehmend, dass kommerzielle Organisationen mit einsatzkritischen Anforderungen, wie z.B. die Stadtwerke München, sich für Sepura-Funkgeräte entscheiden und von dem bewährten, robusten Design und den flexiblen Funktionen profitieren, die auf ihre betrieblichen Anforderungen abgestimmt werden können. Wir freuen uns darauf, deutschen Anwendern noch viele Jahre lang erstklassige Kommunikationslösungen zu bieten.

Johnson Controls

# Brandschutz- und Sicherheitslösungen für Gebäude

**Moderne CKS-Softwarelösungen für Leitstellen inklusive des neuen CEUS Alarmdisplays Web sowie erweiterte Funktionen des Tyco Integrated Systems Managers (TISM), der dazu beiträgt, die Sicherheit und Effizienz in Gebäuden zu steigern – das waren nur einige der innovativen Lösungen, die Johnson Controls auf der diesjährigen PMRExpo gezeigt hat.**

In den drei Tagen drehte sich alles darum, Prozesse und Arbeitsabläufe für eine sichere digitale Kommunikation effektiver und nachhaltiger zu gestalten. Bei Johnson Controls schließt das vernetzte Gebäudesicherheitssysteme und Leitstellensoftware ein. „Für die Fachbesucher der Messe haben wir ein umfangreiches Portfolio im Gepäck", kündigt Jörg Keßler, General Manager Deutschland bei Johnson Controls, an. „Neben den intelligenten Softwarelösungen CELIOS, CEVAS und CKS Datawarehouse präsentieren wir in Köln beispielsweise erstmalig unser neues CEUS Alarmdisplay Web der Öffentlichkeit."

Ein weiteres Messe-Highlight von Johnson Controls waren die neusten Entwicklungen der Plattform TISM, die eine vollständige und zuverlässige Integration der gesamten Gebäudesicherheits- und Kommunikationstechnik in einer zentralen Softwareplattform ermöglicht. Dadurch werden Gebäude und Umgebungen einmal mehr sicherer – und das auf effiziente Weise.

## Der PMRExpo Messestand von Johnson Controls im Detail:

### 1. Intelligente Softwarelösungen Rettungsdienst, Feuerwehr + C.o

### / Einsatzleitsystem CELIOS

Von der Annahme eines Einsatzes bis

hin zu dessen Verwaltung: Das Einsatz- und Gefahrenmanagementsystem CELIOS von CKS Systeme unterstützt die Leitstellen von Rettungsdienst, Feuerwehr und Polizei seit vielen Jahren. Johnson Controls zeigt in Köln seine Software-Innovationen unter anderem für die Bereiche Meldungs- und Statusübersicht, Maßnahmenbearbeitung sowie Webclient und Schnittstellen.

### / CEVAS Feuerwehr

Das CEVAS Feuerwehr System eignet sich speziell für die Berichterfassung und Statistik von Feuerwehreinsätzen. Es unterstützt Leitstellen dabei, ihr Berichtswesen zu optimieren und die Qualität zu sichern – zum Beispiel indem es die Erstellung von Statistiken und Dokumentationen automatisiert und stark vereinfacht. So nutzt es Daten aus dem Leitstellensystem CELIOS, erstellt eigenständig Berichte auch mit Bildanhängen und beinhaltet eine umfassende Stammdatenverwaltung. Ebenso unterstützt CEVAS Feuerwehr Leitstellen bei der Einsatzabrechnung.

### / Statistikmodul CKS Datawarehouse

Die Datenbank CKS Datawarehouse erweitert CELIOS, CEVAS Feuerwehr und CEUS für eine noch effizientere Einsatzplanung, indem sie alle relevanten Daten auf interaktiven Dashboards übersichtlich bereitstellt und Einsatzkräfte so dabei unterstützt, noch schneller und datenbasiert gute Entscheidungen zu treffen.

### / CEUS Alarmdisplay Web

Aktuell laufende Einsätze der Leitstelle stellt das neue CEUS Alarmdisplay Web nun auf einer modernen Oberfläche im Browser dar – unabhängig von Betriebssystemen und ohne umfangreiche Installation. Über die Alarmansicht des Add-Ons sehen die Verantwortlichen nicht nur den jeweiligen Status ihrer Fahrzeuge, sondern auch die wichtigsten Einsatzparameter. Ebenfalls wird ihnen der Einsatzort in einem Satellitenbild oder als klassische Karte angezeigt. Im Ruhezustand bietet die Wachanzeige zusätzliche Informationen wie eine Wetterkarte oder einen Live-TV-Stream.

## 2. Vernetzte Sicherheits-, Gebäude- und Kommunikationstechnik

### / Sicherheitsplattform TISM

Mit dem Tyco Integrated System Manager (TISM) bietet Johnson Controls eine unabhängige und bedienerfreundliche Lösung für die Integration von Sicherheitssystemen in einer zentralen Softwareplattform. Indem er die Ereignisse, Daten und Informationen angebundener Sicherheitssysteme etwa für Video-, Zutritts- oder Einbruchmeldeanlagen sammelt, protokolliert und visualisiert, ermöglicht es TISM seinen Nutzern, Situationen besser und schneller zu identifizieren und zu analysieren – und dadurch deutlich effizienter zu werden.

**Ob Leitstellen oder Gebäude ganz anderer Art:** Zusätzlich entlasten Maßnahmenpläne sowie automatisch im Hintergrund ablaufende Routinen die Anwender und sorgen dafür, dass die Sicherheits- und Gebäudemanagementsysteme reibungslos laufen.

### Das Einsatzleitsystem der CKS Systeme GmbH für Feuerwehr- und Rettungsdienst- sowie Polizei- und Industrieleitstellen

Die Anforderungen an Disponenten in Leitstellen unterliegen einem starken Wandel: Verschärfte Bedrohungslagen, veränderte Einsatzbedingungen, Normungsarbeit, fortschreitende Vernetzung und Digitalisierung erfordern ein hohes Maß an Flexibilität, sowohl was die Arbeitsabläufe angeht als auch die Leitstellen-Technologien. Ein Einsatzleitsystem muss heute verschiedensten Ansprüchen gerecht werden, sich schnell und einfach an immer neue Kundenanforderungen anpassen. Um dies zu erreichen, sollte vor allem die zugrundeliegende Leitstellen-Software skalierbar ausgerichtet sein.

**Whitepaper-Download**: **https://tinyurl.com/5cbcsn2p**

# Einsatzkräfte erhalten neue sicherheitskritische Applikationen

## Integrierte Kommunikationslösungen können die Arbeitsweise und -abläuft von Einsatzkräften optimieren und die Sicherheit im Einsatz nachhaltig verändern

Motorola Solutions zeigte auf der PMRExpo 2022 in Köln, wie sein integriertes Gesamtportfolio Behörden und Organisationen mit Sicherheitsaufgaben (BOS), aber auch Unternehmen im geschäftskritischen Umfeld hilft, ihren Einsatzkräften die Informationen zur Verfügung zu stellen, die sie benötigen, um bessere und sichere Entscheidungen zu treffen.

Zu den Highlights der PMRExpo-Messe gehört die erste mobile, sicherheitskritische Softwarelösung basierend auf Apple CarPlay, die Einsatzkräften aus dem Auto heraus die Möglichkeit bietet, über eine einzige, intuitive Schnittstelle auf Daten zuzugreifen und sie einsatzbezogen zu

verarbeiten. Die neue Lösung wird bereits von mehr als 6.000 Beamten der Western Australia Police genutzt, die über die neue App monatlich rund 84.000 Einsätze koordinieren. Die neue Softwarelösung ist Teil des umfassenden und vollständig integrierten Portfolio von Motorola Solutions, bestehend aus TETRA und zukunftsweisenden Breitbandlösungen, Bodycams und Video-Sicherheitslösungen, Softwareapplikationen sowie Cyber Security und Managed Services. „Mit unserer Innovationskraft helfen wir Ersthelfern, ihre Arbeit im Einsatz an vorderster Front zu vereinfachen und zu optimieren", erklärt Axel Kukuk, Country Manager Deutschland bei Motorola Solutions. „Unser Portfolio integriert Endgeräte, Videolösungen und Infrastruktur, die häufig separat gesehen werden, in einer Gesamtlösung. Das hilft den Einsatzkräften, auf Daten zuzugreifen, die sie für effektivere Entscheidungen benötigen."

- Digital Policing: PSCore, die neue intelligente mobile Anwendungsplattform für die öffentliche Sicherheit, ist die weltweit erste ihrer Art, die mit Apple CarPlay funktioniert. Sie lässt sich nahtlos in viele öffentliche Sicherheitssysteme integrieren und vereinfacht die Arbeitsabläufe der Beamten, indem sie über eine einzige, intuitive Schnittstelle Zugriff auf wichtige Details bietet.
- Nahtloses Zusammenspiel von Breitband-MCPTT und LMR: WAVE PTX ist ein Push-to-Talk Dienst, der Teams über verschiedene Geräte, Netzwerke und Technologie miteinander verbindet. Mit Critical Connect zeigt Motorola Solutions eine cloud-basierte Kommunikationslösung, die Barrieren zwischen verschiedenen Kommunikationsnetzen beseitigt und eine nahtlose Sprach- und Datenkommunikation über verschiedene Sicherheitsorganisationen und über Landes- und Netzgrenzen hinweg unterstützt. Ziel ist es, die Kommunikation zwischen Behörden bei großen Einsatzlagen oder grenzüberschreitenden Katastrophenfällen entscheidend zu verbessern.
- TETRA- und LTE-Geräte: Das MXP7000 ist ein tragbares All-in-One-Gerät für die einsatzkritische Kommunikation. Es vereint TETRA- und 4G-LTE-Sprach- und Datenkommunikation, um das Lagebewusstsein, die Sicherheit und die Produktivität von Einsatzkräften zu verbessern.
- Das vielseitige MXM7000 kann mit seiner LTE-Konnektivität jedes Fahrzeug in einen mobilen Breitband-Hotspot verwandeln. Es erweitert die Anbindung und Reichweite, indem eine Reihe von Kommunikationsgeräten miteinander verbunden werden.
- Cyber Security: Die Managed Security Platform ActiveEye von Motorola Solutions bietet kontinuierliche Einblicke in sicherheitsrelevante Aktivitäten mit automatischen Benachrichtigungen und Berichten. Sie basiert auf einer flexiblen Architektur, die sich mit modernen IT-Systemen weiterentwickeln lässt.
- Videosicherheit und Zugangskontrolle: Auf der PMRExpo stellt Motorola Solutions sein skalierbares Video-Portfolio vor. Dazu gehören die VB400 Bodycam- und Videomanagement-Lösungen, das M500 In-Car-Videosystem und das mobile ANPR-System L5M (Automatic Number Plate Recognition), das die Erkennung und Datenerfassung maximiert. Außerdem die schlüssellose Zugangslösung Openpath, die eine zuverlässige Zugangskontrolle mit intelligenten Video- und Intercom-Funktionen, cloudbasierter Software und einem offenen Ökosystem bietet.

## Euro Security TV: Videos-Statements vom Motorola-Stand auf der PMR Expo 2022

Ricardo Gonzalez
MSSSI VP EMEA Strategy and Marketing, MOTOROLA SOLUTIONS

Darren Wood
Solution Architect - International Mobile Video, MOTOROLA SOLUTIONS

Kostyantyn Steblovskyy
End User Video Account Executive, MOTOROLA SOLUTIONS

Airbus

## Was ist Tactilon Agnet?

### Tactilon Agnet bringt sichere Gruppen-Kommunikation auf smarte Geräte

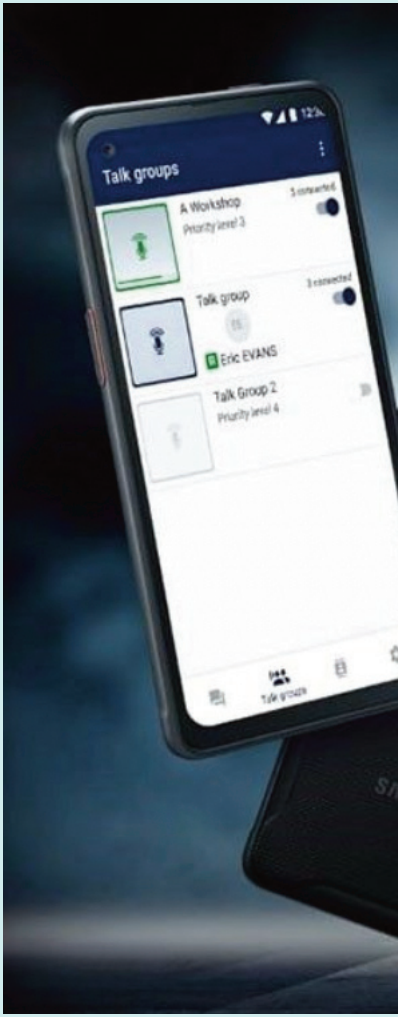
Mit Tactilon Agnet, werden Nutzer von smarten Geräten Teil der professionellen Welt – Sprach-, Daten-, Video- und Lokalisierungsdienste stehen alle zur Verfügung und bieten die Verlässlichkeit und Sicherheit, die professionelle Nutzer erwarten. Tactilon Agnet ist eine erweiterbare Lösung für die Zusammenarbeit, die alle Vorteile der Smartphone-Funktionen auf sichere und kontrollierte Weise nutzt.

Die für einen Einsatz benötigten Mitarbeiter können einfach und sicher verbunden werden, auch wenn sie verschiedene Geräte und Technologien nutzen. Tactilon Agnet erfüllt die Anforderungen von Organisationen der öffentlichen Sicherheit genauso wie die von gewerblichen Nutzern. Tactilon Agnet läuft auf herkömmlichen oder robusten smarten Geräten und bietet eine sehr einfache und intuitive Benutzeroberfläche für die Mitarbeiter im Einsatz.

Airbus

## Download Datenblatt für Tactilon Agnet 900

Tactilon Agnet 900 bietet Apps für Sprache, Bilder, Standortbestimmung und andere professionelle Anwendungen über Breitband in zentral gesteuerten Nutzergruppen. All dies beinhaltet Servicequalitäts-Management und End-to-End-Verschlüsselung nach 3GPP-Standard für einsatzkritische Dienste. Agnet 900 wurde für den professionellen Einsatz in den Bereichen Polizei, Feuerwehr, Gesundheitswesen, Verteidigung und für SWAT-Teams entwickelt und ist perfekt für die Gruppenkommunikation mit unterschiedlichen Anforderungen. Die Anwendung läuft auf herkömmlichen oder robusten Smartphones und Tablets und bietet eine sehr einfache und intuitive Benutzeroberfläche für die Mitarbeiter im Einsatz.




securelandcommunications.com

## Samsung arbeitet mit Airbus an einem Smartphone mit integrierter Tactilon Agnet-Lösung

Samsung hat gerade ein neues XCover6 Pro-Smartphone auf den Markt gebracht, das Nutzern kritischer Kommunikationen neue und verbesserte Optionen bietet. Das neue Samsung-

Smartphone in Kombination mit der Airbus Tactilon Agnet MCX-Lösung hat die ICCA-Auszeichnung als beste MCX-Lösung des Jahres erhalten und ermöglicht eine erfolgreiche einsatz- und geschäftskritische Kommunikation selbst unter anspruchsvollen Bedingungen.

Airbus hat die Tactilon Agnet-Lösung zusammen mit Samsung entwickelt und getestet, und das gerade auf dem Markt eingeführte XCover6 Pro-Smartphone liefert neue Lösungen für die Servicebereitstellung und MCX-Dienste für anspruchsvolle Nutzer.
Samsung Knox-Produkte ergänzen die Bereitstellung von Tactilon Agnet mit einem benutzerfreundlichen Firmware Management, einem Lizenzserver für die Offline-Aktivierung, einer Massenregistrierung und zahlreichen weiteren Funktionen zur Unterstützung von Benutzern kritischer Kommunikationen.

Mit Samsung Knox Security kann das Sicherheits- und Qualitätsmanagement sogar noch effizienter implementiert werden. „Diese Ankündigung zeigt, dass ein globales und führendes Technologieunternehmen die einsatzkritischen Nutzeranforderungen für Endgeräte erfüllen kann. Die Tactilon Agnet-Lösung von Airbus für Samsung Knox-fähige Smartphones gewährleistet eine schnelle und einfache Bereitstellung, Nutzung und Sicherheit von MCX-Diensten", erklärt Samuel Gustafsson, Head of European Sales bei Airbus.

Samuel Gustafsson fährt fort: „Der Tactilon Agnet-Dienst auf dem neuen XCover6 Pro bietet Nutzern neue Funktionen ohne Kompromisse bei der Effizienz und Sicherheit, die bei der kritischen Kommunikation einen immer höheren Stellenwert einnehmen."

„Sicherheit und Nutzbarkeit sind für Regierungsorganisationen von überragender Bedeutung bei der Auswahl mobiler Technologien", betonte Neil Barclay, Head of B2G, Samsung Europe. „Auf unsere Sicherheits- und Staging-Tools der Unternehmensklasse gestützt haben wir zusammen mit Airbus eine einzigartige und einfach bereitzustellende Plattform eingerichtet, die sensibelste und vertrauliche Informationen auf einem erstklassigen PTT-Gerät verwaltet und schützt."
Das neue Samsung XCover6 Pro (Bild unten) bietet zahlreiche Funktionen für den Feldeinsatz, darunter Schutz unter anspruchsvollen Bedingungen, programmierbare Hardwareschlüssel, ein Hochleistungsakku mit Schnellladetechnologie und

ein Monolautsprecher für klare Sprachkommunikation.
Darüber hinaus bietet das Samsung XCover6 Pro einen Chipset zur Unterstützung von LTE und 5G und die Verbesserung der Qualität von Video-Streaming- und Videokonferenzfunktionen.

Die International Critical Communications Awards 2022 haben Airbus Tactilon Agnet 500 als beste MC-X-Lösung des Jahres ausgezeichnet.

# Hexagon unterstützt Smart-City-Umbau in Brasilien

**Die brazilianische Stadt Manaus setzt eine Hexagon-Lösungen in ihrem City Cooperation Center (CCC) ein und unterstützt damit die Transformation der Stast zur Smart-City. Die integrierten Technologien gebern in Echtzeit einen Betriebsüberblick über die Stadt und die jeweiligen Automatisierungsinitiativen sowie die KI-basierten Services, die eine Reaktion auf Notfälle beschleunigen und öffentliches Arbeiten verbessern.**

**Das 2021 eingerichtete Manaus CCC beherbergt den Zivilschutz, die städtische Wache, den Verkehr und die städtischen Mobilitätsbehörden. Das Zentrum soll die Lebensqualität von 2,2 Millionen Einwohnern verbessern, indem es durch eine bessere Zusammenarbeit zwischen den öffent- lichen Organisationen die Bedürfnisse der Bürger besser vorhersagen und darauf reagieren kann.**

Die Lösungen von Hexagon liefern die Informationen und Funktionen, die es dem CCC ermöglichen, die Erkennung von und Reaktion auf Vorfälle zu automatisieren - von Notfällen im Bereich der öffentlichen Sicherheit über Parkverstöße bis hin zu Reparaturen der Infrastruktur. Durch die Integration von Daten aus Überwachungssystemen, Wetterstationen, öffentlichen Anwendungen und Sensoren in der gesamten Stadt werden die Hexagon-Systeme Benachrichtigungen generieren, die automatisch analysiert und der zuständigen Abteilung zur Reaktion zugewiesen werden. Die neuen, koordinierten Arbeitsabläufe werden es den Behörden ermöglichen, Probleme und Notfälle schneller zu erkennen und zu beheben.

"Dies ist eine bedeutende technologische Entwicklung, denn sie ermöglicht es uns, Vorfälle in Echtzeit zu überwachen und darauf zu reagieren", so Sandro Diz, Superintendent des Kooperationszentrums der Stadt Manaus. "Der nächste Schritt ist die Integration anderer Behörden und Dienste außerhalb der Stadtverwaltung, so dass die Stadt noch besser vernetzt sein wird.
Manaus CCC nutzt HxGN OnCall Dispatch, die branchenführende computergestützte Dispatch-Lösung von Hexagon, zur Zentralisierung von Dispatching- und Störungsreaktionsda- ten und Workflows, einschließlich HxGN OnCall Dispatch | Smart Advisor, einer unterstützenden Lösung für künstliche Intelligenz (KI), die Betriebsdaten auswertet und das Personal bei sich abzeichnenden Situationen warnt. Das Zentrum wird auch die PSIM-Funktionen (Physical Security Information Management) von Hexagon nutzen, um Daten von Sensoren und anderen Systemen zu integrieren und auszuwerten und so eine Echtzeitüberwachung und ein noch nie dagewesenes Situationsbewusstsein zu ermöglichen.

Die Mitarbeiter werden auch die M.App Enterprise von Hexagon nutzen, um Daten zu visualisieren und zu

analysieren und so die Planung und den Betrieb durch intuitive kartenbasierte Dashboards und Anwendungen zu verbessern. "Durch die Integration, Modernisierung und Digitalisierung der städtischen Abläufe unterstützt Hexagon Manaus dabei, sein Smart-City-Projekt zum Leben zu erwecken", so Sergio Nunes, Senior Vice President für Lateinamerika bei Hexagons Geschäftsbereich Safety, Infrastructure & Geospatial. "Der Einsatz neuartiger Technologien wie der KI-Hilfslösung Smart Advisor macht Manaus zu einem Vorreiter unter den Städten Südamerikas, und wir sind stolz darauf, ihre Bemühungen zu unterstützen."

---

**Was ist HxGN OnCall Dispatch?**

## Die Einsatzleitsoftware für Notfall- und Katastrophenmanagement

**Die HxGN OnCall Dispatch Produktsuite bietet Polizei, Feuerwehr, Rettungswesen und Industrie-Leitstellen hochwertige Einsatzleitfunktionen, um die Arbeitslast der Mitarbeiter zu minimieren und die Leistungsfähigkeit der Leitstellen zu erhöhen – sowohl bei Vorfällen als auch bei Großereignissen.**

HxGN OnCall Dispatch ist die flexible Einsatzleitsystem-Produktsuite der nächsten Generation. Geboten werden Einsatzleitfunktionen für Leitstellen aller Art und Größe – inklusive der Anbindung mobiler Einsatzkräfte.
Die HxGN OnCall Dispatch Produktsuite wird entweder vor Ort installiert, in der Cloud oder als SaaS (Software as a Service) bereitgestellt.

Die Produktsuite dient zur Bearbeitung von Ereignissen in Leitstellen und Notruf- zentralen, abgesetzten Dienststellen, bei den mobilen Einheiten und überall, wo Ersthelfer und Notfallhilfe benötigt werden.

### HxGN OnCall Dispatch dabei:

- die Kapazität des Einsatzmanagements zu steigern
- die Lagebeurteilung und Koordination zu verbessern
- die Kommunikation zu optimieren
- die organisationsübergreifende Zusammenarbeit zu optimieren
- das Berichtswesen und die Transparenz zu verbessern
- das Vertrauen der Öffentlichkeit in die Arbeit von BOS zu steigern.

Die Produksuite wird mittels Browser und / oder mobiler App aufgerufen . HxGN OnCall Dispatch lässt sich auf Bedürfnisse und neue Technologien schneller und kostengünstiger anpassen als herkömmliche Systeme. Dank der flexiblen Lizenzierungsstruktur und Funktionalität umfasst Advantage auch HxGN OnCall Dispatch | Dashboard für dynamische visuelle Übersichtsdarstellungen von Ereignissen, Einheiten und Aufgaben.

HxGN OnCall Dispatch | Viewer ist eine Möglichkeit, den Zugriff auf Informationen aus dem Einsatzleitsystem um grundlegende Funktionen zu erweitern und gleichzeitig die Arbeitsbelastung der Mitarbeiter zu verringern.
Der Viewer ist eine benutzerfreundliche Webanwendung, mit der auch Nutzer außerhalb des Leitstellenraums Ereignisse anzeigen, Echtzeit- und Verlaufsinformationen durchsuchen und Vorfälle – sofern es keine Notfälle sind – anlegen können.

## Notrufzentrale und Einsatzleitstelle

In Notrufzentralen und Einsatzleitstellen zählt oft jede Sekunde. Die Call-Taker und Dispatcher müssen vorfallrelevante Informationen unkompliziert aufnehmen und rasch Maßnahme einleiten können. Advantage liefert ein klares Bild zur Lage und ermöglicht schnellere Verfahrensabläufe, ohne den Anwender mit unnötigen Informationen zu überfrachten. Advantage optimiert die Koordination zwischen der Leitstelle und den Einsatzkräften und unterstützt die Zusammenarbeit über Organisationsgrenzen hinweg.
Die Lösung umfasst:

- Eine innovative Benutzererfahrung (UX)
- Schnellere Verfahrensabläufe
- Optimierte Workflows
- Ein umfassendes Lagebild
- Automatische Nutzerunterstützung
- NG112 und eine nachrichtenbasierte • Kommunikation mit der Leitstelle
- Einen Kartenanbieter Ihrer Wahl
- Unkomplizierte Konfiguration

# Gebäudeplanung mit modernen IP-Video-Systemen

## Integration der Videosicherheit in Baupläne mit AXIS Plugin für Autodesk® Revit®

**Netzwerk-basierte Videosicherheit, Audio und andere vernetzte Sensoren sind heute ein wichtiger Teil jedes neuen Gebäudes. Früher wurden Videosicherheitslösungen höchstens nachträglich in fertige Gebäude eingefügt, doch heute werden sie bereits als integraler Bestandteil der Gebäudeinfrastruktur geplant. In diesem Artikel zeigen wir, wie Axis dies über das AXIS Plugin für Autodesk® Revit® unterstützt, eine der beliebtesten Softwarelösungen zur Gebäudeplanung weltweit.**

**Neben anderen Gebäudesystemen und Infrastrukturen – von der Stromversorgung zur Netzwerkverkabelung, von Heizung, Lüftung und Klimatisierung (HVAC) bis zu den Rohrleitungen: Netzwerk-basierte Videosicherheit, Netzwerk-Audio und die zugehörigen Sensoren sind heute wichtige Bestandteile jedes neuen Gebäudes.**

Während diese Technologien immer umfangreichere und fortschrittlichere Funktionen erhalten und angesichts der Innovationen bei fortschrittlichen Analysen auf der Grundlage von Deep Learning erhalten Netzwerk-Video, -Audio und die damit verbundenen Sensoren neben der Gewährleistung der Sicherheit noch weitere wichtige Aufgaben.

Durch Kombination der Technologien kann die Gebäudenutzung optimiert, die Energieeffizienz erhöht und natürlich der Schutz der Menschen sichergestellt werden, die das Gebäude nutzen und bewohnen.

### Integration von Netzwerk-Video in die Struktur eines Gebäudes

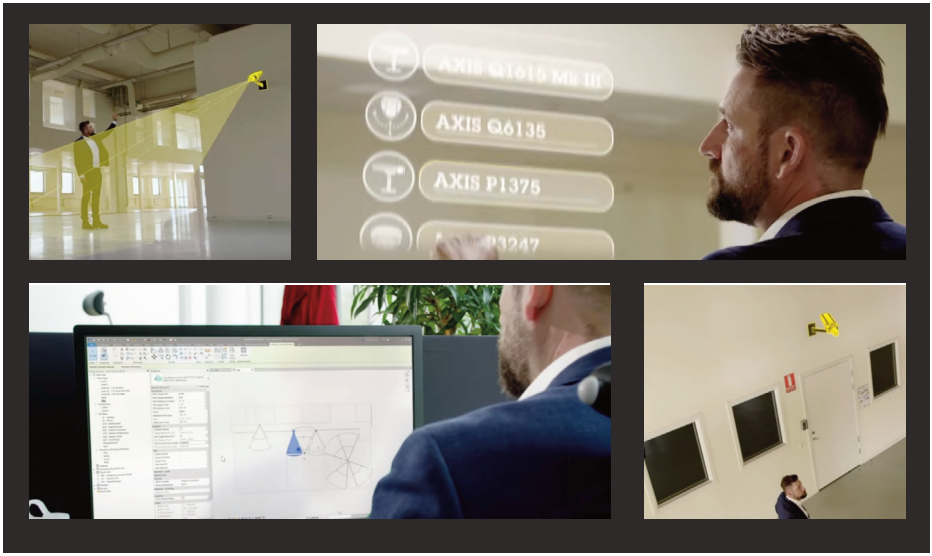
Angesichts ihrer großen Bedeutung müssen die Architekten Netzwerk-Video und -Audio schon von Beginn an neben den anderen wichtigen Services und Komponenten in die Struktur eines neuen Gebäudes einplanen. Dafür müssen sie die Geräte und zugehörige Technologie direkt in ihre Planungslösung einfügen können. Mit dem AXIS Plugin für Autodesk Revi erhalten Architekten und Gebäudeplaner Zugriff auf das gesamte Portfolio von Axis Technologien.

Autodes Revit ist eine der beliebtesten BIM-Softwarelösungen (Building Information Modelling, Modellierung der Bauinformationen). Mit der Software können Architekten, Designer, Statiker, Mechaniker, Elektroingenieure, Planer und Bauprofis Gebäude und Strukturen sowie deren Komponenten in 3D entwerfen und koordinierte Designs und Pläne von der Idee bis zur Fertigstellung erstellen. In Autodesk Revit kann jeder Aspekt des Gebäudes geplant und vorgegeben werden, von den Fundamenten bis zur Möblierung.

Das AXIS Plugin für Autodesk Revit unterstützt alle aktuellen Versionen von Autodesk Revit (einschließlich der neuesten Version 2023) und bringt das Axis-Portfolio an Netzwerkgeräten in den Gebäudeentwurf des Planers. Das Plugin erlaubt nicht nur die gezielte Auswahl eines bestimmten Axis Produkts und dessen Integration in die 3D-Projekte, sondern kann sogar die Abdeckung einzelner Sicherheitskameras oder Lautsprecher anzeigen, visualisieren und gemäß den Anforderungen des Kunden anpassen.

### Volle Interaktivität in der Planung der Sicherheitslösung

Natürlich hat jede Axis Kamera ihre speziellen technischen Merkmale und optimalen Einsatzgebiete. Deshalb ist es wichtig, dass Gebäudeplaner die technischen Parameter des modellspezifischen Geräts berücksichtigen,




wenn sie die Videosicherheits- oder Audiolösung in einem Gebäude planen. Mit Axis Camera Viewer kann sich der Designer beim Einfügen einer Kamera in ein Projekt eine komplette 3D-Visualisierung des abgedeckten Bereichs aus dem Blickwinkel der Kamera anzeigen lassen. Dies ist eine intuitive Möglichkeit zur Überprüfung der Kamerapositionierung und einstellungen. Diese Visualisierung ist unverzichtbar, wenn man die Kundenerwartungen schon frühzeitig beim Design berücksichtigen möchte.

Fügt man eine Kamera in ein Projekt ein, simuliert das Plugin die Hardwaresteuerung der Kameras. Sobald die Kameraposition ausgewählt und die Montagekonfiguration festgelegt ist, werden die Kamerahöhe, der Schwenk- und Neigungswinkel sowie der Zoom eingestellt, um das Sichtfeld der einzelnen Geräte festzulegen. Es gibt mehrere Einstellungen für die Pixeldichte (PPM/PPF), um das Sichtfeld für Branchenstandards zu illustrieren – von der Erkennung bis zur Identifizierung – und die Übereinstimmung mit den tatsächlichen Ergebnissen sicherzustellen. Und schließlich gibt es noch eine Einstellung zur Veranschaulichung des Korridorformats, eine 90°-Drehung des Kameraobjektivs, um zu überprüfen, ob eine Szene vollständig abgedeckt wird.

Sobald die gewünschten Einstellungen für alle Kameras festgelegt sind, werden feste oder transparente Objekte im projizierten Sichtfeld mit der Funktion Collision Detection erkannt. Diese Wiedergabe liefert eine realitätsnahe 2D-Darstellung des Kamerasichtfelds und zeigt genau an, was die Kamera erkennen kann.
Die Perspektive des Designers

Nathan Mudler, Produktionsleiter bei Guidepost Solutions LLC, nutzt das AXIS Plugin für Autodesk Revit jede Woche. Er erklärt dessen Vorteile:

„Das Plugin erweitert Autodesk um nützliche Funktionen, sowohl als Unterstützung des Lösungsdesigns als auch, indem es einfachen Zugang zu aktuellen Inhalten von Axis bietet, wie Produktinformationen und Konfigurationen."

„Wir nutzen es in Designprojekten für den Gewerbe-, Gesundheits- und Bildungsbereich, und ich finde die 3D-Ansicht und Collision Detection unglaublich praktisch, um Arbeiten zu automatisieren, die ich bisher manuell ausführen musste.
Wir haben zum Beispiel kürzlich ein Projekt abgeschlossen, bei dem wir 3D-Ansichten entwickelt und Collision Detection auf einen Plan mit 120 Axis Kameras angewendet haben.
Durch die Automatisierung haben wir viel Zeit gespart, außerdem konnten wir den Installateuren vor Ort ein sehr detailliertes Design bereitstellen, was außerdem für eine effizientere Systeminstallation sorgte."
Netzwerk-basierte Videosicherheit, Netzwerk-Audio und Analytik sind inzwischen genauso wichtig für die Infrastruktur eines Gebäudes wie jeder andere grundlegende Service.
Mit dem AXIS Plugin für Autodesk Revit erfolgt ihre Integration intuitiv in das grundlegende Planungswerkzeug für Architekten und Bauplaner weltweit.

**[https://youtu.be/5t-s8AiXyfk]**

ASSA ABLOY Opening Solutions

## Openings Studio-Software rationalisiert den Spezifikationsprozess für ein Luxusprojekt in Dubai

**Qualität und Genauigkeit sind ausschlaggebend für die Realisierung von Luxusprojekten, die ihr Versprechen einlösen und Investitionen lohnen. Für das Six Senses, The Palm, Dubai - ein 5-Sterne-Hotel und Markenresidenzen - suchte das preisgekrönte Architekturbüro Brewer Smith Brewer Group nach einem Partner, der das Building Information Modelling (BIM) und die Spezifikation der Beschläge rationalisiert. Die Wahl fiel auf die Experten und die Software von ASSA ABLOY Opening Solutions.**

Die Brewer Smith Brewer Group (BSBG) ist ein langjähriger Befürworter des BIM-Prozesses. Sie hat die Erfahrung gemacht, dass dieser Prozess die Produktivität steigert und die Lieferzeiten verkürzt. Es hat ihnen geholfen, ein Portfolio zu schaffen, das sowohl bei der Planung als auch beim Bau branchenführende technische Effizienz aufweist.
Sie setzen BIM bereits in der Konzeptphase ein, um den Informationsfluss zwischen Designern, Ingenieuren und externen Auftragnehmern zu koordinieren. Die richtige BIM-Zusammenarbeit verbessert die Arbeitsabläufe und fördert die Kreativität und einen methodischen, technisch versierten Ansatz bei der Gebäudeplanung. Sie gewährleistet außerdem eine offene, transparente Kommunikation während der gesamten Pro-

jektdauer. Die weitreichende Erfahrung und das Wissen der ASSA ABLOY-Spezifikationsteams machten sie zum idealen Partner für die Zusammenarbeit bei einem solch prestigeträchtigen Projekt in Dubai.

### Beschleunigung der Projektabwicklung

Ein wichtiges Instrument zur Optimierung der Zusammenarbeit zwischen BSBG und ASSA ABLOY bei Six Senses, The Palm, war die Software Openings Studio. "Openings Studio von ASSA ABLOY wurde aufgrund der BIM-Integration mit der Revit-Modellentwicklung und der einfachen Kommunikation zwischen den Architekten und den Beschlagspezialisten bevorzugt", erklärt Adam Drawl, Senior Architect bei BSBG.

Detaillierte Spezifikationen für Türlösungen können in Openings Studio erstellt und dann in die Design-Software exportiert werden, wenn der Projektmanager sie benötigt. Die Integration in Revit vereinfacht die gemeinsame Nutzung von Informationen und die Aktualisierung von Beschlagsätzen innerhalb der BIM-Umgebung.

Im Laufe der Planung vereinfacht Openings Studio die Aktualisierung und verhindert unerwünschten Informationsverlust. Daten zu Hardware und Zertifizierungsanforderungen, einschließlich Brand- und Ausstiegsklassen, waren jederzeit verfügbar. Die Zusammenarbeit beschleunigte die Spezifikation einer breiten Palette von ASSA ABLOY-Lösungen für rund 3.500 Öffnungen - von Stahl- und Holztüren bis hin zu Zutrittskontrolllesern, elektromechanischen Schlössern und Türschließern.

"Unsere Spezifikationsteams können eine ganze Reihe von Projektunterstützung anbieten", sagt Bala Vignesh von ASSA ABLOY Opening Solution EMEIA. "Da sie in ganz Europa und im Nahen Osten angesiedelt sind, verfügen sie über fundierte Kenntnisse der lokalen Normen und Zertifizierungen - zum Beispiel für grünes Bauen oder Brandschutz."
"Sie bieten auch eine Reihe von Tools, die die Zusammenarbeit unterstützen und Architekten und Projektmanagern Zeit sparen. Nicht nur Openings Studio, sondern auch eine BIM-Bibliothek, die leicht importiert werden kann, um jeden Planungs- oder Bauablauf zu unterstützen."

"Das Onboarding und die Nachbetreuung waren ausgezeichnet", bestätigt Herr Drawl. "Das ASSA ABLOY-Team war immer schnell verfügbar und hat proaktiv an der Entwicklung der Beschläge mitgewirkt und aufgetretene Probleme angesprochen. Ihr Fachwissen ist der Schlüssel.

**[Pdf-Download https://tinyurl.com/yc4uaxd7]**

In der Heliosklinik Cuxhaven werden die Zugangsanlagen von dormakaba gewartet - im Auftrag von VAMED.
©Adobe Stock dormakaba

## VAMED vertraut bei der Wartung ihrer Tür- und Toranlagen auf dormakaba

# Zugangslösungen für einen reibungslosen Betriebsablauf

Die VAMED-Gruppe mit Sitz in Wien ist ein weltweit anerkannter Partner für die Planung, Ausstattung, Errichtung und Betriebsführung von Gesundheitseinrichtungen. Seit vier Jahrzehnten hat VAMED weltweit mehr als 1.000 Gesundheitsprojekte in 98 Ländern realisiert. In Deutschland verwirklicht der Krankenhaus-Dienstleister ebenfalls seit 40 Jahren effiziente Modelle für die Errichtung und Modernisierung sowie den technischen Betrieb von Krankenhäusern.
VAMED Deutschland steht für eine effiziente und moderne Infrastruktur

Links Automatische Drehtüren für einen schnellen und sicheren Transport von Krankenbetten. ©dormakaba

Auch in der Helios Klinik Kiel werden die Türsysteme regelmäßig gewartet.
©Adobe Stock dormakaba

im Krankenhaus. Das Unternehmen plant, errichtet, modernisiert und betreibt Technik und Gebäude so, dass Ärzte und Pflegekräfte ihre Patienten optimal und effizient zugleich versorgen können. Mit VAMED als Partner können sich Krankenhäuser ganz auf ihre Kernaufgaben Medizin und Pflege konzentrieren.

Moderne Krankenhäuser und Gesundheitseinrichtungen benötigen eine starke Infrastruktur aus Technik und Gebäuden. Nur wenn im Hinter-

Bundesweit über 250 hochqualifizierte Servicetechniker von dormakaba sorgen für die Wartung und Reparatur von Türsystemen in über 100 von VAMED betreuten Kliniken.
©dormakaba

grund alles reibungslos funktioniert, können sich Ärztinnen und Ärzte sowie Pflegekräfte ganz auf ihre Arbeit konzentrieren. Für einen reibungslosen Betriebsablauf setzt VAMED auf intelligente Zugangslösungen, die den Personenfluss steuern, für barrierefreien, hygienischen Zugang für das Personal und Besucher sorgen und Sicherheit und Brandschutz gewährleisten. So werden beispielsweise in den Fluren automatische Drehtüren für einen schnellen, problemlosen Transport von Krankenbetten eingesetzt, automatische Schiebetüren ermöglichen den schnellen Zugang zu Behandlungsräumen.
Gerade in Krankenhäusern sind Funktionsfähigkeit, Langlebigkeit und Qualität von Türsystemen über den gesamten Lebenszyklus essenziell. Insbesondere in sicherheitsrelevanten Bereichen, wie z. B. Operationssälen oder Intensivstationen, ist ein störungsfreier Betrieb unabdingbar. Die Türen müssen funktionieren- und zwar immer.

Um dies zu gewährleisten, hat VAMED 2020 einen Service-Partner für die Reparatur und Wartung der Automatiktüren und Vereinzelungsanlagen in den über 100 vom Unternehmen betreuten Kliniken in Deutschland gesucht. „Unsere wichtigsten Anforderungen waren Kompetenz, Qualität, Zuverlässigkeit und kurze Reaktionszeiten", erklärt Sebastian Keim, Leitung Arbeitsgruppen Betriebstechnik der VAMED VSB-Betriebstechnik Süd-West GmbH. Mit dem Tür- und Sicherheitsspezialisten dormakaba, der mit bundesweit über 250 hochqualifizierten, vom Werk top geschulten Servicetechnikern eines der dichtesten Servicenetze der Branche bietet, entschied man sich für einen starken Rahmenvertragspartner. Die Mitarbeiter der Servicehotline sind auf Wunsch 24 Stunden am Tag, 365 Tage im Jahr erreichbar und können oft bereits am Telefon „Erste Hilfe" leisten.

## Starker Vertragspartner

Der herstellerunabhängige Service von dormakaba umfasst Schiebetüren, Karusselltüren, Drehtürantriebe, Glasschiebewände, Faltflügel- und Raumspartüren, Türschließer, spezielle Türprodukte rund um die Themen Fluchtweg und Brandschutz, Drehsperren und Drehkreuzen, Personenschleusen, Sensorschleusen und Tore. Darunter befinden sich natürlich auch viele Türsysteme von dormakaba selbst.

Nachdem der Rahmenwartungsvertrag mit dormakaba seit zwei Jahren besteht, bestätigt Sebastian Keim die gute Zusammenarbeit: „Wir haben bisher gute Erfahrungen mit dem Service von dormakaba gemacht und sind mit der Zusammenarbeit sehr zufrieden."

Karusseltüren tragen dazu bei, den Energiebedarf zu senken, da sie den Luftzug von außen verringern. Sie werden regelmäßig überprüft.
© dormakaba

# Umfrage zur Lage der physischen Sicherheit 2022

**Bedenken hinsichtlich Cybersicherheit • Daten aus der physischen Sicherheitstechnologie werden als "unternehmenskritisches" Instrument für den Geschäftsbetrieb angesehen • Die Industrie setzt auf hybride Cloud-Infrastrukturen und vereinheitlichte Lösungen.**

Genetec,Technologie-Anbieter für vereinheitlichtes Sicherheitsmanagement, öffentliche Sicherheit und Business Intelligence, hat die Ergebnisse seiner "Umfrage zur Lage der physischen Sicherheit 2022" veröffentlicht. Mehr als 3.700 Expertenaus dem Bereich der physischen Sicherheit weltweit (einschließlich

Endusern und Systemintegratoren / Installateuren/Anbietern) teilen darin ihre Erfahrungen zu den in ihren Unternehmen eingesetzten Sicherheitsstrategien, um die Herausforderungen einer sich verändernden Realität effektiv zu meistern.

## Die Zukunft der Sicherheit ist hybrid

Rund 54 % der befragten Enduser gaben an, dass ihr Unternehmen für die Sicherheitsstrategie einen Mix aus lokalen und Cloud-basierten Lösungen plant.
Der hybride Ansatz ermöglicht es Unternehmen, ihre bestehenden Investitionen vor Ort weiter zu optimieren und gleichzeitig sinnvolle Cloud-Optionen zu nutzen, um Kosten zu senken, Sicherheit und Effizienz zu steigern und den Fernzugriff auf Systeme und Sensoren zu ermöglichen.

## Die Sorgen um die Cybersicherheit nehmen zu

Die Konvergenz von Informationstechnologie (IT) und Sicherheit führt zu neuen Ansätzen für die Umsetzung und Verwaltung einer starken Cybersicherheitsstrategie. 64 % der Befragten aus dem IT-Bereich und 54 % der Befragten aus dem Sicherheitsbereich gaben an, dass Tools für die Cybersicherheit in diesem Jahr ein zentrales Thema sind.

## Nutzung der physischen Sicherheit für den Geschäftsbetrieb

Im Rahmen der Umfrage bestätigten fast zwei Drittel (63 %) aller Befragten und sieben von zehn Unternehmen mit mehr als 10.000 Mitarbeitern, dass die physische Sicherheit und die damit verbundenen Daten als "unternehmenskritisch" angesehen werden. In den letzten Jahren hat sich die physische Sicherheit zu einer strategischen Ressource entwickelt, um eine Vielzahl von Herausforderungen zu bewältigen, die über die reine Risikominimierung hinausgehen. Darüber hinaus spielt physische Sicherheit nun eine deutlich wichtigere Rolle bei der digitalen Transformation von Unternehmen.

## Physische Sicherheit wird vereinheitlicht

Die meisten Befragten (64 %) gaben an, dass sie sowohl Videoüberwachung als auch Zutrittskontrolle in ihren physischen Sicherheitsanlagen einsetzen. Rund 77 % davon bestätigten, dass ihre Organisation entweder eine Integration zwischen Videoüberwachungs- und Zutrittskontrollsystemen verschiedener Anbieter oder eine vereinheitlichte Videoüberwachungs- und Zutrittskontrolllösung von einem Hersteller implementiert hat.

"Jedes Unternehmen möchte die neueste Technologie nutzen. Angesichts von Budgetbeschränkungen, Fachkräftemangel und sich ständig verändernden Prioritäten müssen Sicherheitsverantwortliche jedoch mit weniger mehr erreichen", sagt Pervez Siddiqui, Vice-President of Offerings and Transformation bei Genetec. "Eine vereinheitlichte Sicherheitsplattform bietet Unternehmen die Möglichkeit, ihre veralteten Systeme zu modernisieren und dabei ihre bestehende Infrastruktur weiter zu nutzen, ohne teure und komplexe kundenspezifische Lösungen entwickeln zu müssen."

## Methodik der Umfrage

Genetec befragte vom 25. August bis zum 21. September 2022 Fachleute für physische Sicherheit. Nach einer Überprüfung der eingereichten Antworten wurden die Ergebnisse von 3.711 Befragten in die analysierte Stichprobe aufgenommen. Die Umfrage wurde in den Regionen Nordamerika, Mittelamerika, Karibik, Südamerika, Europa, Naher Osten, Afrika, Ostasien, Südasien, Südostasien, Zentralasien, Westasien und Australien-Neuseeland durchgeführt.

**Der vollständige Bericht kann heruntergeladen werden unter https://www.genetec.com/a/physical-security-report**

FeuerTrutz 2023

IDIS

# Videoüberwachung in Hotels - für Sicherheit und Gästemanagement

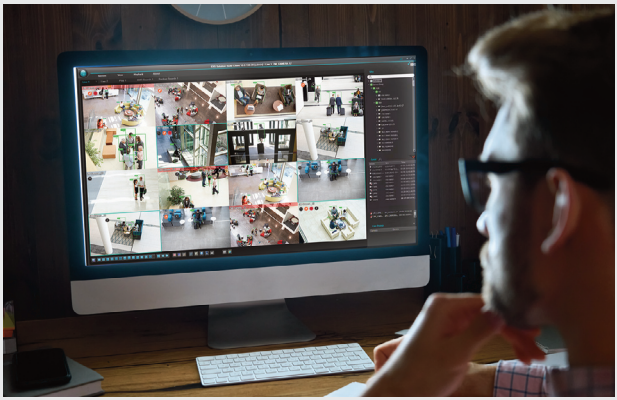
## Ein eBook zeigt Vorteile der Videoüberwachung im Beherbergungsgewerbe

Informativer Leitfaden zeigt auf, wie umfassende Videotechnik eine Reihe von Herausforderungen im Gastgewerbe bewältigen und sich positiv auf das Geschäftsergebnis auswirken kann

Das im September erschienene eBook von IDIS, einem koreanischen Videohersteller, zeigt auf, warum es für Hoteliers und Gastronomen entscheidend ist, die Vorteile der Videotechnologie der nächsten Generation zu nutzen, um die betriebliche Flexibilität in turbulenten Zeiten zu verbessern.

Das neueste eBook des Unternehmens wurde geschrieben, um Sicherheitsplaner zu unterstützen und ihren Systemintegratoren zu helfen, zu verstehen, wie sie eine Reihe von Herausforderungen mit den neuesten Videotools angehen können - einschließlich der Stärkung der Sicherheit, der Erhöhung der Gästesicherheit und der Verbesserung der betrieblichen Effizienz: Die Bedürfnisse des europäischen Gastgewerbes mit modernster Videotechnik erfüllen.

Nach den Auswirkungen der COVID-19-Pandemie sieht sich das europäische Gastgewerbe einem anhaltenden Druck durch steigende Energiekosten, Inflation und die Lebenshaltungskostenkrise ausgesetzt. Infolgedessen müssen die Hotels überlegen, wie sie ihre Flexibilität und Wider-

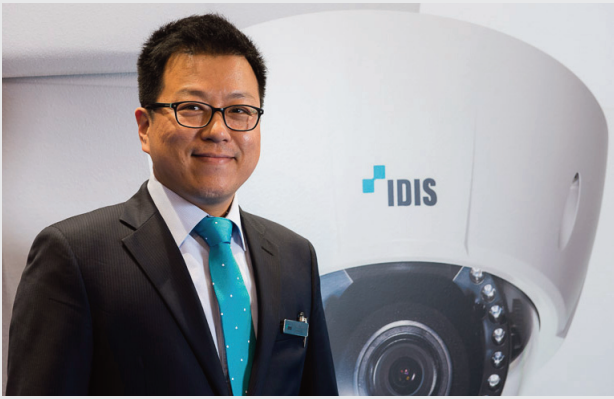


standsfähigkeit verbessern und auf die sich ändernden Kundenanforderungen reagieren können.
Sicherheit hat für die Gäste nach wie vor höchste Priorität und ist für VIP- und Firmenkunden oft ein entscheidender Faktor bei der Auswahl ihres Aufenthaltsortes. Sicherheitsmängel können schnell zu direkten Verlusten führen, einschließlich der Kosten für die Behebung, der Schädigung des Rufs und des Verlusts künftiger Geschäfte. So sind Diebstähle nach wie vor ein großes Problem für Hoteliers, wobei nicht nur das Eigentum der Gäste gestohlen wird, sondern auch das des Hotels. Eine Umfrage von Wellness Heaven ergab, dass "Diebstähle in Luxushotels sprunghaft ansteigen", wobei der Diebstahl von Matratzen in den letzten drei Jahren um 35 % und der Diebstahl von Fernsehern um 11 % zugenommen hat.

Gut konzipierte Videosysteme sind eines der wirksamsten Instrumente zur Bekämpfung von Sicherheitsrisiken, insbesondere wenn sie mit anderen Gebäudemanagement- und Back-of-House-Systemen integriert werden.

Darüber hinaus bietet die neueste Generation von Videolösungen Vorteile, die den Hotels auch aus geschäftlicher Sicht einen Wettbewerbsvorteil verschaffen.

Für wettbewerbsfähige Hotels wird Video nicht mehr nur zur Kostenreduzierung und Risikominderung eingesetzt, sondern auch zur Verbesserung der Servicebereitstellung und der Effizienz in einer Art und Weise, die dem Kundenangebot einen Mehrwert verleiht. KI-gestützte Videoanalysen können beispielsweise für die Überwachung von Warteschlangen und Belegungen eingesetzt werden, um Manager zu alarmieren, damit sie das Personal entsprechend umleiten können, sowie für die Erstellung von Heatmappings historischer Daten, um Spitzenzeiten zu verstehen und den Betrieb zu optimieren, um einen gleichbleibenden Service zu gewährleisten.




"Das neue eBook von IDIS zeigt auf, wie Videotechnologie genutzt werden kann, um das Gastgewerbe bei seiner Weiterentwicklung und Modernisierung zu unterstützen", sagt James Min, Managing Director von IDIS Europe (Foto links). "Unsere Erfahrung in diesem Sektor hat gezeigt, dass die neueste Generation von Videolösungen nicht nur die Sicherheit von Hotelpersonal und Gästen erhöhen und den Schutz von Eigentum und Vermögenswerten verbessern kann, sondern auch die betriebliche Flexibilität und Widerstandsfähigkeit des Unternehmens."

## Museum und Denkmal aus dem 13. Jahrhundert

# Videotechnik im Schloss Ujazdowski

## Schutz von Besuchern und Kunstwerken mit Hanwha Techwin KI-Kameras im Austellungsraum im Schloss Ujazdowski, Zentrum für zeitgenössische Kunst in Warschau

Das Zentrum für zeitgenössische Kunst im Schloss Ujazdowski ist ein Ort, der Besucher durch Kunst zum Nachdenken über die Welt anregt. Er soll zur Diskussion über die Werke einladen, in denen verschiedene Kunstdisziplinen in kreativen Arbeiten miteinander verschmelzen. Der im Herzen Warschaus gelegene Ort beherbergt Veranstaltungen, Ausstellungen, ein Kino, eine Buchhandlung, eine Bibliothek und ein Aufenthaltsprogramm für Künstler.

### State-of-the-art

Das Zentrum für zeitgenössische Kunst im Schloss Ujazdowski, benötigte ein Sicherheitssystem, das sich flexibel an die unterschiedlichen Räume des Museums anpassen lässt

und zur Ästhetik des Baus aus dem 13. Jahrhundert passt. Das Team entschied sich für die Investition in innovative IP-Kameras mit modernsten Video- und Audioanalysen, um Personen, Vermögenswerte und Kunstwerke zu schützen.
Aufgrund der integrierten Deep-Learning-Analysen und dem intuitiven und benutzerfreundlichen Wisenet WAVE Video Management System (VMS) sowie der WAVE Video Wall (zur gleichzeitigen Anzeige mehrerer kritischer Bereiche) fiel die Wahl auf die Wisenet-KI-Kameras der P- und X-Serie.

## Tiefe und Weite

Die Kameras der Wisenet P-Serie werden eingesetzt, um bestimmte Bereiche besonders konzentriert zu überwachen, zum Beispiel wertvolle Kunstwerke oder Ein- und Ausgänge. Die Fisheye-Kameras der X-Serie überwachen hingegen ganze Räume, um den Betreibern einen umfassenden Überblick über das Geschehen im Museum zu geben. Die KI-Kameras der P-Serie verfügen über KI-Analyse und Geräuschklassifizierung, um zu erkennen, wenn sich Personen den Ausstellungsstücken zu sehr nähern. Deep Learning minimiert Fehlalarme, insbesondere in Räumen mit schwacher Beleuchtung, die dafür anfällig sind.

Da das System während der Covid-19-Pandemie installiert wurde, unterstützten die KI-Kameras der P-Serie zusätzlich die Zählung der anwesenden Personen und die Erkennung von Mund- und Nasenschutz, um sicherzustellen, dass alle offiziellen Sicherheitsmaßnahmen eingehalten wurden.

## Audio Integration

Das mit WISENET WAVE betriebene Videoüberwachungssystem ist mit einem Zwei-Wege-Audiokommuni-

kationssystem verbunden, so dass das Personal Besucher auffordern kann, den Abstand zu den Exponaten einzuhalten. Besonders wichtig sind diese Warnungen für das Sicherheitsteam des Museums, wo sich Exponate in der Mitte eines Raumes befinden oder hervorstehen oder sich in einem Bereich befinden, den die Besucher durchqueren und erleben sollen.

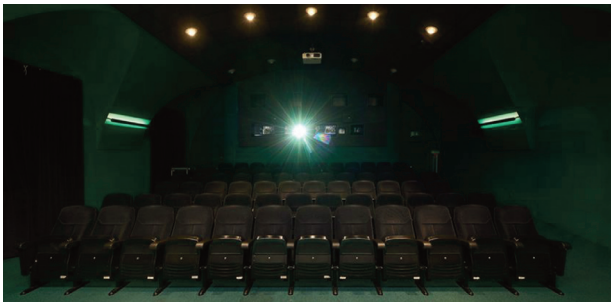
Die Videoanalyse umfasst zudem die Erkennung von virtuellen Linien und unbefugtem Zutritt, was automatische Warnungen an den Kontrollraum und definierte Maßnahmen auslöst (z. B. das Sperren eines Bereichs).

## Einfache Verwaltung

„Unser Personal kann alles einfach über Wisenet WAVE verwalten, einschließlich der Alarme, so dass niemand durch wiederholte Fehlalarme abgelenkt wird. Anhand von KI-Attributen und verschiedenen Parametern können die Mitarbeiterinnen und Mitarbeiter Regeln definieren, die bestimmte Prozesse automatisieren. All dies trägt dazu bei, dass unsere Sicherheit intelligenter und effizienter geworden ist“, erklärt Rafał Filipowicz, Head of IT and Multimedia von Schloss Ujazdowski. WAVE ist außerdem mit einer intelligenten De-Warping-Funktion ausgestattet, die eine Verzerrung durch das Fisheye-Objektiv reduziert. Das Personal kann damit deutlicher erkennen, was in einem Raum passiert.

## Alles im Blick

Die WAVE-Videowall-Funktion ermöglicht es dem Team von Schloss Ujazdowski, mehrere Ansichten der wichtigsten Museumsbereiche zu erstellen, z. B. der wertvollsten Exponate. Die Mitarbeiter können so aktiv überwachen, was in diesen besonders wichtigen Räumen passiert. Die im Hintergrund laufende Videoanalyse gibt bei Ereignissen, die untersucht werden müssen, automatisch Warnmeldungen aus – so wird sichergestellt, dass den Mitarbeiterinnen und Mitarbeitern nichts entgeht.



# Segelclub in Finnland vertraut auf PULSE

**Ein finnischer Segelclub spart seinen Mitgliedern Zeit, indem er seine Räumlichkeiten mit Cloud-verwalteten, energiesparenden Schlössern sichert**

**Viele Unternehmen kennen das Problem. Die Sicherung von verstreuten Standorten stellt Facility Manager vor besondere Probleme. Der Austausch von Zylindern bei Verlust eines Schlüssels ist oft mit Reisen und hohen Kosten verbunden. Alle alternativen Zugangskontrollsysteme, die auf Strom angewiesen sind, können an abgelegenen Standorten nur schwer oder gar nicht eingesetzt werden. Batterielose, kabellose elektronische Schlösser, die über eine Cloud-Software aus der Ferne verwaltet werden, helfen, diese Herausforderungen zu meistern.**

Der Näsijärvi Sailing Club in Finnland hat mehrere Stützpunkte über den gesamten Näsijärvi-See verteilt, von denen einige bis zu 2 Segelstunden voneinander entfernt sind. Es waren viele mechanische "Skipper-Schlüssel" im Umlauf, die es den Clubmitgliedern ermöglichten, diese Einrichtungen aufzuschließen und zu nutzen. Die Register der Schlüsselinhaber und der Verbleib vieler traditioneller mechanischer Schlüssel waren jedoch nicht mehr auf dem neuesten Stand. Dies stellte ein Sicherheitsproblem dar, das weder durch mechanische Sicherheitsvorkehrungen noch durch herkömmliche Zugangskontrollen gelöst werden konnte. Der Segelclub suchte nach einer Lösung, um seine Sicherheit zu erhöhen und gleichzeitig Aufwand und Kosten zu sparen.

Um eine neue, effizientere Lösung zu finden, suchte der Segelclub nach einem programmierbaren digitalen Schlüsselsystem, mit dem er die Kontrolle über die Sicherheit seiner Einrichtungen zurückgewinnen konnte. Er benötigte drahtlose Schließvorrichtungen, die für die abgelegenen Standorte des Clubs geeignet sind und über den Benutzerschlüssel mit Strom versorgt werden.

Um alles verwalten zu können, wurde eine Software benötigt, mit der Systemverwaltungsaufgaben von jedem Ort aus erledigt werden können: ein System, mit dem es einfach ist, fehlenden Schlüsseln die Zugangsrechte zu entziehen, und eine Audit-Trail-Funktion, mit der Sicherheitsadministratoren die Zugangsprotokolle überprüfen können, wenn ein Problem auftritt.

## Mehr Kontrolle mit programmierbaren Smart Keys

Der Näsijärvi Sailing Club entschied sich für die schlüsselbetätigte PULSE-Zutrittskontrolllösung von ASSA ABLOYs Konzernmarke ABLOY, um sein Gelände zu sichern und den Zugang für die Clubmitglieder zu verwalten. Rund 55 PULSE-Zylinder wurden an verschiedenen Standorten des Segelclubs eingesetzt.
Berechtigte Mitglieder tragen nun einen individuellen Schlüssel bei sich, mit dem sie alle zugelassenen PULSE-Schlösser rund um den See öffnen können.

## Warum ist PULSE die beste Lösung für Clubs mit abgelegenen Standorten?

PULSE-Schlösser sind ideal für eine Umgebung wie den Näsijärvi-See geeignet, wo die Zugangspunkte verstreut sind. Sie erzeugen den gesamten Strom, den sie für die Schlosselektronik benötigen, aus dem Schlüsselschub.
Diese innovative Technologie zur Energiegewinnung bedeutet, dass weder Kabel noch Batterien benötigt werden, was dem Segelclub Betriebs- und Wartungskosten erspart.

Das PULSE-Zylindersortiment umfasst Türschlösser, Nockenschlösser, Möbelschlösser und Vorhängeschlösser, die auch in den rauesten Klimazonen im Freien eingesetzt werden können. Fast jeder Zylinder kann gegen ein PULSE-Gerät ausgetauscht und ohne Kabel oder Bohren angeschlossen werden.

Ein weiterer Vorteil ist, dass ein PULSE-System so einfach zu verwalten ist. Der Club verwaltet es selbst und spart damit auch zusätzliche Verwaltungskosten.

Sichere Einrichtungen können Stunden mit dem Boot entfernt sein: PULSE spart unnötige Fahrten.
"Das PULSE-System ermöglicht es, Schlüssel über Lesegeräte und den Cloud-Service jederzeit zu aktualisieren und zu deaktivieren", sagt Ari Karjalainen, CEO von Ajan Lukko Lock und Mitglied des Näsijärvi Sailing Club.

Vorfälle lassen sich leicht untersuchen, indem man die Prüfprotokolle von Schlüsseln oder Schlössern einsieht: "In Fällen von Vandalismus kann anhand des Zugangsregisters überprüft werden, wer wann mit welchem Schlüssel das Gebäude betreten hat", fügt Karjalainen hinzu.

# Aus der Wissenschaft

Vanderbilt University

## Künstliche Intelligenz beseitigt Autobahnstaus

**Forschern der Vanderbilt University glücken Experimente mit speziell ausgerüsteten Fahrzeugen**

Künstliche Intelligenz in vernetzten Autos verhindert Staus auf Autobahnen, die scheinbar grundlos auftreten. Das hat ein Team um Daniel Work von der Vanderbilt University (www.vanderbilt.edu) experimentell nachgewiesen. Die Wissenschaftler haben 100 Autos so ausgestattet, dass sie per Funk miteinander kommunizieren und Verkehrsinformationen austauschen, ohne dass der Fahrer sich einschalten muss.

### Automatischer Sicherheitsabstand

Die Fahrzeuge wurden zudem mit Adaptive Cruise Control (ACC) ausgestattet. Diese Technologie ermöglicht es dem Fahrer, die Geschwindigkeit seines Autos einzustellen, die präzise eingehalten wird, wenn kein Hindernis auftaucht. Dann bremst das Auto selbstständig ab, hält also den Sicherheitsabstand ein, und beschleunigt wieder, wenn das Hindernis verschwunden ist. Für das Experiment haben die Forscher ACC so modifiziert, dass es auf der Basis von Künstlicher Intelligenz auf den gesamten Verkehrsfluss reagiert, auch auf das, was voraus passiert.

Derart ausgerüstet, rollten die Fahrzeuge zwischen 6 Uhr und 9.45 Uhr über ein 24 Kilometer langes Teilstück der Interstate 24 (I-24), immer hin und her. Die These war, dass Phantomstaus nicht auftreten, wenn fünf Prozent der Autos mit modifiziertem ACC und Künstlicher Intelligenz ausgestattet sind.

### 300 Sensoren für Verkehrskontrolle

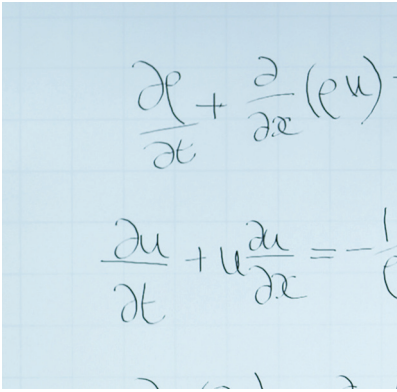
Die Entscheidungsfindung der Autos fand auf zwei Ebenen statt. Auf der Cloud-Ebene wurden Infos über die Verkehrslage zur Erstellung eines Gesamtgeschwindigkeitsplans genutzt. Diesen Plan erhielten die Autos, die Algorithmen der Künstlichen Intelligenz verwendeten, in Echtzeit, sodass sie die Fahrweise optimieren konnten. Die Forscher ermittelten die Auswirkungen der vernetzten Autos auf den morgendlichen Verkehrsfluss auf einem mit 300 Sensoren ausgestatteten, 6,4 Kilometer langen Abschnitts der I-24.Da die Fahrzeuge gewissermaßen weit vorausschauen konnten, passten sie ihre Geschwindigkeit so an, dass sie möglichst ohne zu bremsen durchkamen. So glätteten sie den Verkehrsfluss und verhinderten Schnellfahrten ebenso wie plötzliches Bremsen, das bei dichtem Verkehr Staus auslöst. Wer hinter dem Bremser herfährt, muss wegen der Reaktionszeit schärfer bremsen als sein Vordermann. Das setzt sich nach hinten fort, sodass es irgendwann zum Stillstand kommt.

National Institute of Standards and Technology

## Internet-Router überwacht künftig die Atmung

**Verzerrung der Signale ist laut National Institute of Standards and Technology ein Warnsignal**

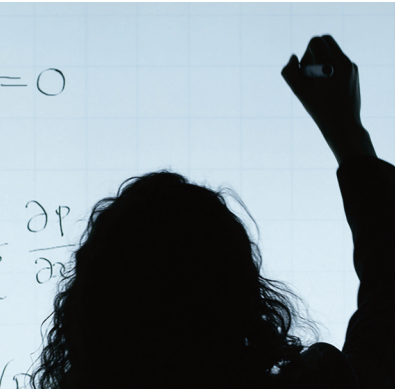
Die von Internet-Routern ausgesendeten Signale lassen sich nicht nur nutzen, um Tablets und Smartphones



mit dem Netz zu verbinden. Mithilfe des Wireless Access Points lässt sich auch die Atemfrequenz einer Person im Raum messen - und zwar wenn sich der in mobilen Endgeräten verbaute Wireless Adapter mit einem Local Area Network (LAN) oder einem anderen kabelgebundenen Datennetz verbindet. Der Router wird laut Experten des National Institute of Standards and Technology (www.nist.gov) (NIST) somit zum Frühwarngerät für gesundheitsgefährdende Atemstörungen.

### Elektromagnetische Wellen

Die elektromagnetischen Wellen, die Router aussenden, prallen an manchen Hindernissen ab oder durchdringen Materie, auch menschliche Körper. Wenn sie sich bewegen, etwa beim Atmen, werden sie zusätzlich verändert. Diese Interaktionen unterbrechen die Internetverbindung nicht, aber sie können signalisieren, dass jemand in Schwierigkeiten ist, jedenfalls mit dem neuen System der NIST-Forscher. Im Jahr 2020 wollten NIST-Wissenschaftler Ärzten helfen, die COVID-19-Pandemie zu bekämp-



fen. Patienten wurden isoliert und Beatmungsgeräte waren knapp. Frühere Forschungen hatten die Verwendung von WLAN-Signalen untersucht, um Personen oder Bewegungen zu erfassen - mit nur mäßigem Erfolg.
Die Forscher um Jason Coder haben die Kanalstatusinformation (CSI), also das Signal, das Laptops, Smartphones und andere Endgeräte aussenden, genutzt. Es ist immer dasselbe, und der Access Point, der die CSI-Signale empfängt, weiß, wie es aussehen soll. Aber wenn die CSI-Signale durch die Umgebung wandern, werden sie verzerrt. Der Access Point analysiert das Ausmaß der Verzerrung, um die Verbindung anzupassen und zu optimieren. Das Team hat die Firmware auf dem Router modifiziert, um diese Signale bis zu zehnmal pro Sekunde abzufragen, um ein detailliertes Bild davon zu erhalten, wie sich das Signal ändert.

### Trefferquote 99,54 Prozent

Um das System zu trainieren, haben die KIST-Wissenschaftler eine Puppe genutzt, die für Ausbildungszwecke entwickelt worden war. Sie simuliert alle denkbaren Arten von normaler Atmung über abnormal langsame und abnormal schnelle Atmung sowie Asthma bis hin zu Lungenerkrankungen. In all diesen Fällen bewegt sich der Körper auf eine ganz spezielle Art. Die Atembewegungen der Puppe verändern den Weg des CSI-Signals. Mit Deep Learning ist es den Ingenieuren schließlich gelungen, eine Trefferquote für Erkrankungen der Atemwege von 99,54 Prozent zu erreichen.

**Georgia Institute of Technology**

## Neue Druckertinte ist transparent und leitfähig

**Mit dem Verfahren der Georgia Tech lassen sich flexible Leiterbahnen und auch Filme herstellen**

Forscher des Georgia Institute of Technology (www.gatech.edu) (Georgia Tech) haben eine neue Druckertinte entwickelt, mit der sich flexible Leiterbahnen und Filme herstellen lassen, die zudem transparent sind. Die Wissenschaftler haben mit dem beliebten Polymer PEDOT (Poly-3,4-ethylendioxythiophen) begonnen, das die Forderungen nach Leitfähigkeit und Transparenz erfüllt, aber unlöslich ist. Dadurch ist es für die Herstellung einer Druckertinte ungeeignet.

### Seitenketten für Löslichkeit

James Ponder, selbst Chemiker, und ein Team von Chemikern und Ingenieuren hatten dann eine glänzende Idee. Sie hängten an die PEDOT-Moleküle andere an, die sogenannte Seitenketten bildeten. Jetzt waren die neu gebildeten Moleküle zwar löslich, doch damit gedruckte Leiterbahnen oder Filme nicht mehr sonderlich leitfähig, denn die Seitenketten bestehen aus einer Art Wachs, das zu den Isolatoren gehört.

"Wir wollen die Seitenketten für die Verarbeitung, aber wir wollen sie nicht in unserem Endprodukt. Also fügen wir Seitenketten hinzu, die wir, sobald wir mit dem Druck fertig sind, gewissermaßen abwaschen können", sagt Ponder. So haben die Team-Mitglieder das Polymer mit Seitenketten erstellt, drucken oder sprühen es auf, spalten die Seitenketten chemisch und waschen sie mit gängigen industriellen Lösungsmitteln weg. Mit einem letzten Umwandlungsschritt entsteht ein flexibler, hochleitfähiger, stabiler Film.

### Für Bioelektronik ideal nutzbar

Es gibt bereits Unternehmen, die an der Lizenzierung der Technologie interessiert sind, da die Filme einige wichtige Vorteile haben. Einer der am weitesten verbreiteten transparenten Leiter für Flachbildschirme, Fotovoltaik, intelligente Fenster und andere Anwendungen ist Indiumzinnoxid. Das Material hat jedoch einige Nachteile, sagt John Reynolds, Doktorvater von Ponder.
"Es ist ziemlich schwierig, mit diesem Material gebogene und flexible Geräte herzustellen, weil es spröde ist." Die PEDOT-Variante sei dagegen flexibel und unter anderem bestens geeignet für elektronische Geräte, die direkt auf der Haut befestigt oder gar implantiert werden. "Hier, in der Bioelektronik, wird das neue Material glänzen", glaubt Reynolds.

intersec

17 - 19 January, 2023
Dubai, UAE

## Uniting the worlds leading industry specialists for the safety & security of future generations

Meet us at our stand at Intersec, a global nexus for the fire, emergency services, security and safety industry.

→ REGISTER TO VISIT

**@intersecexpo I #intersecexpo**