EURO SECURITY

Das deutsche Fachmagazin für Sicherheit und Management in der DACH Region

Retter sind schneller am Unglücksort

www.vodafone.de/business/mobilfunk

- **Perimeter Protection**
  Rückblick auf die Messe mit KI, physikalischen Lösungen + Organisation
- **Border Control**
  Reisende und Unternehmen sind für Digitalisierung aufgeschlossen
- **KRITIS**
  KI prüft Fußgängerverhalten im Kontext zum Management

ISSN 09481249 • 1-2023 • ZKZ 16724 Postvertriebsstück bezahlt • 80383 BAY Germany ©SEC Global • euro-security.de

Inhalt

Inhaltsangabe 2
Impressum 3
Editorial 4

BORDER CONTROL

Digitalisierung an Grenzen 24
Reisenden und Unternehmen sind technologiebasierten Lösungen an internationalen Grenzen aufgeschlossen

DATENSCHUTZ

Europäischer Datenschutztag 16
Genetec gibt Best-Practice-Empfehlungen zum Datenschutz bei der physischen Sicherheit
Rohde & Schwarz 20
Datenschutz gleich Katastrophenschutz

DIGITALISIERUNG

BITKOM 12
Sprachassistenten im Auto werden wichtiger. Nutzung von Sprachbefehlen auf der Straße nimmt deutlich zu

EINZELHANDEL

Der Baumarkt ein Paradies für Diebe 38

IT-SICHERHEIT

DataLocker 36
Professionelle USB-Speichermedien mit Level 3 Zertifizierung und Selbstzerstörungsmodus
Swisscom Trust Services 36
Schafft die Passwörter ab!
G DATA 37
Sicherheitslücke in VMware ESXi – Patch dringend erforderlich

GEBÄUDETECHNIK

ASSA ABLOY 42
Tribut an eine heterogene Wohnbevölkerung
SALTO Systems 48
Hotelschließsysteme als Teil einer digitalen Gästereise
Labor Strauss 49
Besseres Handling für Feuerwehren
ASSA ABLOY 54
Energierückgewinnung mit ASSA ABLOY PULSE

HOCHSICHERHEIT

Milestone Systems 73
Sicherheitskonzept für Diamanten

KRITISCHE INFRASTRUKTUREN

Europäischen Tag des Notrufs 4
Notruf kann Leben retten
Europäischer Tag des Notrufs 112 6
Standort-Übertragung via Mobilfunk: Retter sind jetzt schneller am Unglücksort
Gesetz für Kritische Infrastrukturen 8
KÖTTER Security fordert stärkere Berücksichtigung privater Sicherheitsdienstleister
Hexagon 50
GeoAI-Lösung für das Abwassermanagement in Köln entwickelt

KÜNSTLICHE INTELLIGENZ

Marktstudie: 12% nutzen KI 18
Accenture Studie: Nur 12% der Unternehmen weltweit nutzen Künstliche Intelligenz effektiv
Hikvision Videotechnik 26
Mehr Automatisierung mit KI-Lösungen
Forschung-Prototyp 51
KI-System deutet Fußgängerverhalten, um Interaktion zwischen Auto und Passanten zu ermöglichen

LIEFERKETTEN

TrendTage im März zu aktuellen Themen 32
Angriffe auf Lieferketten, sicheres Active Directory, Managed SOC und Attack Path Management
Dokumenten-Management unterstützt neue Regeln 34
Seit erstem Januar ist das neue Lieferkettensorgfaltspflichtengesetz in Deutschland in Kraft. Für Unternehmen bedeutet das in erster Linie noch mehr Dokumentation.

MARKTTRENDS

Axis Communications 28
Sechs Trends für die Sicherheitsbranche im Jahr 2023
Berg Insight 78
Straftäterüberwachung: Der Markt für die Fernüberwachung von Straftätern wird bis 2026 um über 10 % wachsen

PERIMETER PROTECTION

Nürnberg Messe 56
Erfolgreich wie nie zuvor
Dneprometiz 60
Ukraine: Hochwertige Drahtwaren
Aaronia 60
Durchsagesystem zur Bevölkerungswarnung
Arrowtec 60
Arrow-401 Drohnensystem
ASO Safety Solutions 61
Autosecure 62
Kommunikationssäule und Webplattform
Axis Communications 62
PTZ-Kamera mit Langstrecken-IR

Inhalt

INOVA 63
Integrierte Freigeländesicherung
DroneTracker 63
Klassifizierung und Entschärfung von Gefahren durch Drohnen
deister electronic 64
eyeFOUR - Intelligent Vision Sensor
FEIG ELECTRONIC 65
Frequenzumrichter-Steuerung
www.magnetic-access.com 66
Passagierabfertigung
Perimeter Protection 67
Belgischen Stadt entscheidet sich für CityProtector
www.benincagroup.com 68
Standard für hydraulische Poller
SORHEA 69
Messehighlight SOLARIS NG
Stagnoli Accessories 70
ARGO steuert automatische Tore
sysco-gmbh/neopoint 70
Schutz für flexible Infrastrukturen
TRL Funksysteme 70
Für die Industrie: Funkfernsteuerung Sesam 800
HEALD 72
Eletromechanische Pollersysteme
ZABAG 72
Premiumprodukt Faltflügeltor

PRODUKTFÄLSCHUNGEN

AIM / Konsortialpartner 31
Im Fokus: Identifikation von Produktfälschungen

STANDARDS

BHE 53
Norm-Entwurf DIN VDE V 0826-20
Euralarm 82
Position Paper: Cyber Resilience Act
MOBOTIX 83
M16 Therma: Brandschutz-Zertifizierung auch in Österreich
DKE 83
DKE legt Entwurf für Vornorm Perimeterschutz vor

UNTERNEHMEN /VERBÄNDE

Paxton Neuer Vertriebspartner 10
HID Übernahme GuardRFID 10
PMRExpo Koelnmesse übernimmt 11
dormakaba Fabrik in Indien 40
Accenture SKS-Gruppe erworben 41
Klüh Security Airportgroßauftrag 41
ipoque Neue Kooperation 76
HMF Smart Solutions 77
Comelit/BAB Technologie 77

WISSENSCHAFT

North Carolina State University 79
Flüssigmetall stoppt Gase und Feuchtigkeit
Quantensichere Identitäten für eine digitale Zukunft 79
Deutscher Forschungsverbund startet Projekt »Sichere Quantenkommunikation für Kritische Identity Access Management Infrastrukturen – Quant-ID«
Hikvision 26
Mehr Automatisierung mit KI-Lösungen

Europ. Tag des Notrufs 112

Standort-Übertragung via Mobilfunk: Retter schneller vor Ort

Gute Nachricht zum Tag des Notrufs am 11. Februar: Die Retter – Feuerwehr, Notarzt, Rettungswagen – sind jetzt überall in Deutschland schneller am Unglücksort als noch vor drei Jahren. Denn das neue Notrufsy- stem AML (Advanced Mobile Location) wird nunmehr von praktisch allen Einsatzleitstellen eingesetzt. Ab dem Jahr 2019 hatten die drei Mobilfunk-Betreiber Vodafone, Deutsche Telekom und Telefónica AML in ihre Netze eingebaut.

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*

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

Editorial

Verläßlichkeit für Rettungskräfte

Am 11. Februar 2023 ist der Europäische Tag des Notrufs 112. In Deutschland besteht ein gut funktionierendes System Notrufe abzusetzen und Rettung anzufordern.

Durch die Digitalisierung Hilfskräfte in die Lage versetzt, per Standort-Übertragung via Mobilfunk schneller über Notsituationen, Unfälle und Katastrophen informiert: Mit diesem Weg sind Retter jetzt noch schneller am Unglücksort. Auch die einheitliche Notrufnummer stellt sicher, dass jeder in Notzeiten Hilfe anfordern kann.
Auch wenn dies eine positive Entwicklung ist, steht es mit der Gesamtsituation unser Rettungskräfte nicht gut: Nachwuchsmangel im professionellen Umfeld, zu wenig Ehrenämtler und immer wiederkehrende Aggressionen gegen die Einsatzkräfte im Alltag prägen die Wirklichkeit vieler Beschäftigter und deren Arbeitswelt.

Respekt und technischer Fortschritt

Für die technische Weiterentwicklung der Notrufsysteme ist auch eine Auf- und Nachrüstung der Leitstellen wichtig.
Das Leitstellenmanagement ist eine Zukunftsaufgabe und ist umso entscheidender, wenn man die Einsatzplanung bzw. die Einsatzbegleitung mehr in den Vordergrund rückt. Denn schließlich brauchen die Einsatzkräfte im aktiven Dienst auch eine Unterstützung und die Leitstellen können hier erheblich Einfluss nehmen.
Neben der Einforderung von mehr Respekt gegenüber den Hilfeorganisationen (Sanitär- und Feuerwehrwesen) sollten auch neue Technologien wie Body Worn Kameras entabliert werden.

Dr. Claudia Mrozek

Europäischen Tag des Notrufs

Notruf kann Leben retten

"Die Notrufnummer 112 rettet Leben", sagte Bayerns Innenminister Joachim Herrmann anlässlich des Europäischen Tags des Notrufs am 11. Februar. Der jährliche Aktionstag erinnert an die Bedeutung und Reichweite der Notrufnummer für Feuerwehr und Rettungsdienst.

"Mit einer einheitlichen Nummer erhalten Sie innerhalb der EU und weiteren europäischen Ländern kostenlos und schnelle Hilfe im Notfall", erklärte der Minister. "Alleine im Jahr 2022 erreichten die bayerischen Integrierten Leitstellen rund 3,1 Millionen Notrufe." Der Minister dankte den vielen Einsatzkräften, die tagtäglich Enormes leisten, um die Anrufe zu bewältigen. Wichtig sei hierbei jedoch auch eine moderne Technik: "Der Freistaat Bayern investiert daher kräftig mit rund 45 Millionen Euro in ein neues Einsatzleitsystem samt Kommunikationssystem in allen Integrierten Leitstellen." Ebenso werde die Integrierte Lehrleitstelle bei der Feuerwehrschule Geretsried komplett erneuert: "Hiermit wollen wir eine einheitliche und moderne Ausbildung unserer Leitstellendisponenten auch in Zukunft sicherstellen", erklärte Herrmann.

Gleichzeitig appellierte Herrmann mit Blick auf immer mehr unnötige Alarmierungen von Notärzten und Rettungsdiensten: "Nicht für alle Fälle ist die 112 die richtige Nummer. Besonders bei medizinischen Anliegen, bei denen nicht jede Minute zählt, sollte der Hausarzt angerufen werden oder die 116117 des Kassenärztlichen Bereitschaftsdienstes, die außerhalb der Praxisöffnungszeiten zeitnahe medizinische Hilfe vermittelt. Helfen Sie bitte mit, wichtige Ressourcen für echte Notfälle zu schonen. So erweisen wir auch unseren Einsatzkräften Respekt, die in zeitkritischen Situationen schnell handeln müssen."

[www.notruf112.bayern.de]

EuroShop

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

Messe Düsseldorf GmbH
Postfach 101006
40001 Düsseldorf _ Germany
Tel. +49(0)211/45 60-01
Fax +49(0)211/45 60-668
www.messe-duesseldorf.de

Messe Düsseldorf

PRIME SITE.

KEIN HALLENPLAN.
IHR BUSINESSPLAN.

Halle/Hall 1	Expo & Event Marketing
Hallen/Halls 3, 4	Retail Marketing
Hallen/Halls 4, 5, 6, 7a	Retail Technology
Halle/Hall 9	Lighting
Hallen/Halls 10, 11, 12	Shopfitting, Store Design & Visual Merchandising
Halle/Hall 13	Store Design, Materials & Surfaces
Halle/Hall 14	Food Service Equipment
Hallen/Halls 14, 15, 16, 17	Refrigeration & Energy Management
Halle/Hall 7	Specials

Europäischer Tag des Notrufs 112

Standort-Übertragung via Mobilfunk: Retter sind jetzt schneller am Unglücksort

Gute Nachricht zum Tag des Notrufs am 11. Februar: Die Retter – Feuerwehr, Notarzt, Rettungswagen – sind jetzt überall in Deutschland schneller am Unglücksort als noch vor drei Jahren. Denn das neue Notrufsystem AML (Advanced Mobile Location) wird nunmehr von praktisch allen Einsatzleitstellen eingesetzt. Ab dem Jahr 2019 hatten die drei Mobilfunk-Betreiber Vodafone, Deutsche Telekom und Telefónica AML in ihre Netze eingebaut.

231 von 232 Rettungsleitstellen setzen die Notruf-Technologie AML ein. Bei nahezu allen Handy-Notrufen in Deutschland wird damit der genaue Standort des Anrufers übermittelt.

„In Notfällen zählt jede Sekunde, um Leben zu retten. Hierbei hat sich die von Vodafone mit initiierte AML-Technologie in der Praxis bewährt: Weil der Standort des Notrufs automatisch an die Rettungsleitstelle übermittelt wird, treffen die Retter wesentlich schneller am Unglücksort ein – und umso schneller können sie Erste Hilfe leisten", so Tanja Richter, Netz-Chefin von Vodafone Deutschland.

Vodafone Management: Tanja Richter ist als Geschäftsführerin Technik die Netz-Chefin von Vodafone Deutschland.
© Vodafone

Im Notfall gilt: Ruhe bewahren und die 112 wählen – häufig mit dem Handy via Mobilfunk. Oftmals ist den Anrufern der genaue Standort nicht bekannt. Gerade im Wald, am Straßenrand oder in unbekannten und unübersichtlichen Gebieten fällt die Antwort auf die Frage nach dem Unglücksort meist schwer.

Hier hilft AML: Im Notruf-Gespräch mit der Leitstelle können sich Anrufer auf vier Fragen konzentrieren: Wer? Was? Wann? Wie? Niemand braucht sich mehr um das „Wo" zu sorgen.

Über 15 Millionen Notrufe im Jahr

AML-Mitinitiator Henning Schmidtpott von der Integrierten Leitstelle Freiburg-Breisgau-Hochschwarzwald, streicht die Bedeutung der noch jungen Technologie heraus: „Über 15 Millionen Notrufe gibt es pro Jahr in Deutschland. Wird das Smartphone für den Notruf an die 112 genutzt, können die Standortdaten des Anrufers dank AML-Technologie direkt an die entsprechende Rettungsleitstelle übermittelt werden. So können die Rettungskräfte den Standort des Anrufers bis auf wenige Meter genau lokalisieren und infolgedessen schneller zum Einsatzort aufbrechen und diesen finden." Die lebensrettende Notruf-Technologie ist in allen deutschen Mo-

Der Notruf wird digital: Vodafone und EmergencyEye wollen Ersthelfern helfen zu helfen. © iStock/AndrejPopov

bilfunk-Netzen implementiert und wird von den gängigen Smartphone-Betriebssystemen Android und iOS unterstützt.
Bei rund 75 Prozent aller Notrufe in Deutschland wird der Standort automatisch übermittelt – lediglich bei Anrufen aus dem Festnetz ist das nicht möglich, aber in diesem Fall können die Anrufer wesentlich öfter ihren genauen Standort mitteilen. Die dazu erforderlichen Daten laufen über zwei unabhängige Server in Freiburg und Berlin. Bereits eine Stunde nach dem Notrufeingang werden alle Daten wieder gelöscht

Notrufe: Retter erhalten virtuellen Einblick vom Einsatzort

Seit über 30 Jahren engagiert sich Vodafone beim Notruf. So hat das Unternehmen 1992, als erster Netzbetreiber in Deutschland, den kostenlosen Notruf per Mobilfunk eingeführt. Seitdem unterstützt Vodafone das Rettungswesen und treibt die Digitalisierung auch in diesem wichtigen Bereich voran. Gemeinsam mit dem Grevenbroicher Unternehmen Corevas entwickelte Vodafone beispielsweise die Notruf-Software 'EmergencyEye', mit der jeder Mensch zum Ersthelfer werden kann. Wenn ein Notruf bei der Leitstelle eingeht, senden die Rettungskräfte dem Anrufer einen Link per SMS. Dafür hat Vodafone eine Schnittstelle eingerichtet, die den Einsatzzentralen und Ersthelfern kostenlos zur Verfügung steht. Mit einem Klick baut sich nach Zustimmung des Ersthelfers eine Live-Videoverbindung mit der Leitstelle auf. Damit erhalten die Profis in der Rettungsstelle einen virtuellen Einblick vom Einsatzort. Auch hochauflösende Bilder oder Dokumente können über die Anwendung schnell und einfach verschickt werden. Das hilft die Situation besser einzuschätzen, die beteiligten Personen ggf. zu beruhigen und im Videotelefonat die entscheidenden Erste-Hilfe-Maßnahmen anzuleiten. Eine Chat-Funktion mit zwölf Sprachen hilft zudem bei der Verständigung.

Unterstützung für Krisen- und Katastrophenstäbe

Seit der Einführung 2019 war die EmergencyEye Technologie mehr als 200.000 Mal im Einsatz. Rund 1.000 Mal pro Woche wird der Dienst von Rettungsleitstellen in Deutschland und der Schweiz genutzt, um sich aus der Ferne direkt an den Unfallort zu schalten. EmergencyEye funktioniert per Videoverbindung mit jedem üblichen Smartphone und unabhängig vom vorhandenen Datenvolumen.
Es ist nicht nötig eine App zu installieren. Mittlerweile kommt die EmergencyEye-Technologie nicht mehr nur im Rettungsfall zum Einsatz, sondern kann bei Gefahrenabwehr auch Krisen- und Katastrophenstäbe unterstützen. Auch die systemrelevante Infrastruktur nutzt den Video-Support per Smartphone.

Überall dort, wo aus der Ferne Entscheidungen gefällt werden müssen, oder Beratungen stattfinden, kann die EmergencyEye-Technologie helfen, besser, schneller und zielgerichteter zu helfen. Über 50 Einrichtungen in Hessen, Niedersachsen und Rheinland-Pfalz greifen für ihre Ferndiagnosen auf das System zurück.

Gesetz für Kritische Infrastrukturen

KÖTTER Security fordert stärkere Berücksichtigung privater Sicherheitsdienstleister

Sabotageakte gegen Bahnstrecken und Cyberangriffe auf öffentliche Einrichtungen haben die Sicherheit für Kritische Infrastrukturen (KRITIS) zuletzt wieder verstärkt in den öffentlichen Fokus gerückt. KÖTTER Security begrüßt vor diesem Hintergrund das jüngst von der Bundesregierung beschlossene Eckpunktepapier für ein Gesetz zum Schutz Kritischer Infrastrukturen. Gleichzeitig mahnt das größte Familienunternehmen der Sicherheitsbranche aber eine deutlich stärkere Einbeziehung der privaten Sicher-heitswirtschaft bei der Neuausrichtung der KRITIS-Sicherheit an.

- **Familienunternehmen begrüßt geplante Rahmengesetzgebung der Bundesregierung**
- **Sicherheitsbeirat: Sicherheitswirtschaft bereits heute wichtiger Eckpfeiler**
- **Gesetz bietet riesige Chance für Vergabe nach verbindlichen Qualitätsstandards und Bestbieter-Verfahren**

Die private Sicherheitswirtschaft ist seit Langem wichtiger Eckpfeiler beim Schutz der Kritischen Infrastruktur. Die Dienstleister unterstützen seit Jahren Unternehmen der betroffenen Sektoren mit ganzheitlichen Risiko- und Business Continuity Management-Konzepten und übernehmen u. a. durch Sicherheitsdienste und -technik den Schutz von Kraftwerken, Rechenzentren und Internetknoten, (Flug-)Häfen, den Öffentlichen Personenverkehr (ÖPV), Behörden etc.

„Eine Schlüsselfunktion somit, die im Eckpunktepapier der Bundesregierung für die geplante Rahmengesetzgebung aber noch nicht ausreichend Berücksichtigung findet", sagt Dr. Harald Olschok, Mitglied des KÖTTER Sicherheitsbeirates. „So werden dort als Ziel zwar u. a. Vorgaben für die physische Sicherheit angeführt; ansonsten bleibt das Papier aber allein auf die staatlichen Behörden und die KRITIS-Betreiber ausgerichtet. Konkrete Ausführungen zu den Dienstleistern, welche die personellen und technischen Schutzmaßnahmen bereits heute umfassend erbringen, fehlen leider gänzlich. Diese Inhalte sollten daher im Rahmen der Gesetzgebung genauso Einzug finden wie die Anerkennung der Sicherheitswirtschaft als eigener KRITIS-Sektor. Denn die Einstufung als systemrelevanter Sektor ist ein weiterer zentraler Faktor, um ihre Rolle als wichtigen Eckpfeiler der inneren Sicherheit zusätzlich zu stärken."

Dies unterstreicht auch Wolfgang Bosbach, ebenfalls Mitglied des KÖTTER Sicherheitsbeirates und einer der versiertesten Innenexperten Deutschlands: „Ein Eckpunktepapier ist zwar noch kein Gesetzentwurf und ein Gesetzentwurf noch kein Gesetz – dennoch sollte man die Bedeutung solcher Papiere nicht unterschätzen. Die private Sicherheitswirtschaft tritt nicht in Konkurrenz zu den staatlichen Si-

cherheitsorganen auf, sie will nicht deren Aufgaben in privater Verantwortung übernehmen. Sie ist aber unbestritten ein wichtiger, unverzichtbarer Bestandteil einer soliden Sicherheitsarchitektur. Dies gilt insbesondere für den Bereich der Prävention, denn je wirksamer Gefahrenabwehr funktioniert, desto mehr werden die staatlichen Stellen entlastet.
Es wäre nicht nur wünschenswert, sondern unabdingbar notwendig, dass dies auch vom Gesetzgeber erkannt und im Rahmen des anstehenden Gesetzgebungsverfahrens berücksichtigt wird. Sollte das federführende Bundesministerium des Innern und für Heimat dies nicht in eigener Verantwortung berücksichtigen, wäre es Aufgabe des Gesetzgebers hier für eine Korrektur, genauer gesagt: Ergänzung, zu sorgen. Schließlich gilt auch hier das sog. Struck`sche Gesetz: Kein Gesetz verlässt das Parlament so, wie es eingebracht wurde."
KÖTTER Sicherheitsbeirats-Mitglied Fritz Rudolf Körper hebt die besondere Möglichkeit hervor, die sich aus der von der Bundesregierung geplanten Übernahme der „EU-Richtlinie über die Resilienz kritischer Einrichtungen (Critical Entities Resilience/CER-Richtlinie)" ergibt, die Ende 2022 auf europäischer Ebene verabschiedet wurde und nunmehr innerhalb von 21 Monaten in nationales Recht zu überführen ist.
„Diese Regelung ist ein Meilenstein, da erstmals in einer EU-Richtlinie KRITIS-Betreibern verbindlich empfohlen wird, ausschließlich auf Basis fester Standards mit privaten Dienstleistern zusammenzuarbeiten."

Eine Verankerung in der in Folge anzupassenden deutschen Gesetzgebung biete somit die riesige Chance, das vom Europäischen Dachverband der privaten Sicherheitsdienste (CoESS) seit Langem für Vergaben empfohlene „Bestbieter-Prinzip" sowie dessen hohe Qualitäts¬stan¬dards für alle Anbieter Kritischer Infrastrukturen in Verbindung mit den hierbei nach Vorgabe der CER-Richtlinie (Art. 16) anzuwendenden Normen verbindlich zu implementieren.
Eine wichtige Orientierung bietet hierbei im Sinne der CER-Richtlinie die europäische Normenreihe EN 17483 „Private Sicherheitsdienstleistungen - Schutz kritischer Infrastrukturen", welche mit den grundlegenden Anforderungen im Teil 1 bereits veröffentlicht ist und sukzessive ergänzend sektorspezifische Anforderungen an Sicherheitsdienstleister im KRITIS-Umfeld in den dazu bereits in Erarbeitung befindlichen Normteilen definieren wird.
Die Teile 2 und 3 für die Bereiche „Flughafen- und Luftsicherheitsdienstleistungen (Airport and aviation security services)" bzw. „Sicherheitsdienstleistungen für Seeschifffahrt und Seehäfen (Maritime and port security services)" folgen noch in diesem Jahr.

Paxton

Neuer Vertriebspartner im Nahen Osten

Paxton kündigt exklusive Vertriebspartnerschaft mit Stebilex Systems an Paxton, der internationale Hersteller von Sicherheitstechnik, und Stebilex Systems, der Anbieter von Zugangskontrolllösungen, haben für das Jahr 2023 eine exklusive Vertriebspartnerschaft für den Markt im Nahen Osten geschlossen. Stebilex Systems wird dazu beitragen, die Produkte von Paxton weiter zu vermarkten und gemeinsam auf die sich verändernden Sicherheitsanforderungen des Marktes einzugehen.

Dan Drayton, Paxton's Divisional Director - EMEA Sales Region, sagte: "Wir arbeiten seit 2019 mit Stebilex zusammen, und ihr Team hat bemerkenswerte Leistungen bei der Förderung des Markennamens Paxton in der Region gezeigt. Da Stebilex eine breite Palette von Zutrittskontroll- und Automatisierungsprodukten anbietet, können sie unsere Systeme mit Integrationslösungen, einschließlich Biometrie und Torschranken, erweitern. Wir sind davon überzeugt, dass die Kunden im Nahen Osten durch unsere Zusammenarbeit einen One-Stop-Shop für alle ihre Sicherheitsanforderungen und die umfassendste Benutzererfahrung haben werden."

HID Global

Übernahme GuardRFID

Das Angebot an Ortungslösungen für das Gesundheitswesen wird erweitert Mit der Übernahme von GuardRFID, einem Anbieter von RTLS-Hardware und -Software im Gesundheitswesen, erweitert HID sein Angebot an Echtzeitortungslösungen (RTLS) für das Gesundheitswesen.

GuardRFIDs aktive Lesegeräte, Lesegeräte und Erreger sowie Software unterstützen vier primäre Anwendungsfälle, die für Kunden im Gesundheitswesen wichtig sind: Säuglingssicherheit, Bedrohung des Personals, Verfolgung von Vermögenswerten und umherwandernde Patienten.

Das TotGuard-Säuglingssicherheitssystem verhindert die Entführung von Säuglingen und die Verwechslung von Mutter und Kind, indem es tragbare Tags für Mütter und Säuglinge bereitstellt. Die Lösung arbeitet sowohl mit den Zugangskontroll- als auch mit den Netzwerk-Videosystemen eines Krankenhauses zusammen.

RFID-Etiketten sorgen für Echtzeit-Transparenz der Anlagen im Gesundheitswesen und ermöglichen es dem Personal, die benötigten Geräte

schnell zu finden. Dies verbessert die Auslastung der Anlagen, spart Arbeitskosten und reduziert Diebstähle.

Wenn Risikopatienten, wie z. B. ältere oder psychisch kranke Menschen, mit Tags versehen sind, werden sie an Ausgangstüren, Treppenschächten und Aufzügen sofort erkannt. Die Türen können so konfiguriert werden, dass sie verriegelt werden und ein Alarm ertönt, was Patienten und Pflegepersonal ein zusätzliches Maß an Schutz bietet. "Mit der Aufnahme von GuardRFID und seiner innovativen RTLS-Technologie in die HID-Familie können wir unsere Präsenz im Gesundheitswesen ausbauen, um Patienten und Personal besser zu schützen", sagt Björn Lidefelt, Leiter von HID Global. "Diese Lösungen werden den Anbietern helfen, das zu tun, was sie am besten können - dafür zu sorgen, dass es ihren Patienten schneller besser geht." Die Lösungen ergänzen die hochmoderne Location Services-Plattform von HID für das Gesundheitswesen, die eine skalierbare Echtzeit-Ortung und Überwachung von Klinikpersonal, Patienten und Anlagen ermöglicht.

HID Location ist ein vernetzter Internet of Things (IoT)-Dienst, der Echtzeit-Transparenz bietet. HID Location wurde unter Verwendung eines offenen Standards für Bluetooth Low Energy- und Wi-Fi-Netzwerke und einer Cloud-Plattform entwickelt und ermöglicht es Organisationen im Gesundheitswesen, alles unter demselben Ökosystem zu verfolgen, ohne die aktuellen Anwendungsinvestitionen aufzugeben.

GuardRFID wurde 2007 gegründet und hat seinen Hauptsitz in Vancouver, Kanada, und ist nun Teil des HID-Geschäftsbereichs Identification Technologies. Das GuardRFID-Angebot wird in den IoT-Geschäftsbereich von HID integriert und profitiert von den Vertriebs- und anderen Funktionen von HID.

PMRExpo

Koelnmesse neuer Veranstalter der PMRExpo

Die Koelnmesse GmbH ist neuer Veranstalter der PMR-Expo. Oliver Freese, COO der Koelnmesse, und Michael Rosenzweig, Geschäftsführer des PMeV – Netzwerk sichere Kommunikation und der PMeV Services GmbH, haben eine entsprechende Kooperationsvereinbarung unterzeichnet. Der PMeV ist Initia- tor und ideeller Träger der PMRExpo, die erstmals im Jahr 2000 stattfand. 2009 zog sie von Leipzig nach Köln um. Ab der PMRExpo 2023 fungiert die Koelnmesse nun gleichermaßen als Gastgeber und Veranstalter.

PMeV und Koelnmesse wollen europäische Leitmesse weiter vorantreiben

Gemeinsames Ziel von PMeV und Koelnmesse ist es, das im Rahmen der Digitalisierung wichtige Themenfeld der sicheren Kommunikation auf alle relevanten Branchen auszuweiten sowie die Internationalisierung der PMRExpo als europäische Leitmesse für sichere Kommunikation noch weiter voranzutreiben. Hierzu soll auch das Auslandsnetzwerk der Koelnmesse eingebunden werden. „Der sehr positive Verlauf der PMRExpo 2022 bestärkt den PMeV in seinen Zielen, nach dem coronabedingten Zwischenstopp die PMRExpo kontinuierlich auf Wachstumskurs zu halten, noch weiter zu professionalisieren und unter Beibehaltung des hervorragenden Markenkerns als europäische Leitmesse für sichere Kommunikation noch vielfältiger und internationaler aufzustellen", erklärt Bernhard Klinger, Vorsitzender des PMeV-Vorstandes. Für die Umsetzung seiner Ziele habe der PMeV mit der Koelnmesse einen starken neuen Veranstaltungspartner gewinnen können. Die Koelnmesse ist eine der bekanntesten national und international tätigen Messegesellschaften Deutschlands.

Mit weltweit 1.000 Mitarbeitenden organisiert und betreut sie jedes Jahr rund 80 Messen, Gastveranstaltungen und Corporate Events in Köln und in den wichtigsten Auslandsmärkten. Darunter sind globale Leitmessen wie Anuga, imm cologne, DMEXCO und ISM. Ab 2023 wird nunmehr auch die PMRExpo unter ideeller Trägerschaft des PMeV Teil dieses exklusiven Veranstaltungsportfolios sein.

BITKOM

Sprachassistenten im Auto werden wichtiger

Nutzung von Sprachbefehlen auf der Straße nimmt deutlich zu

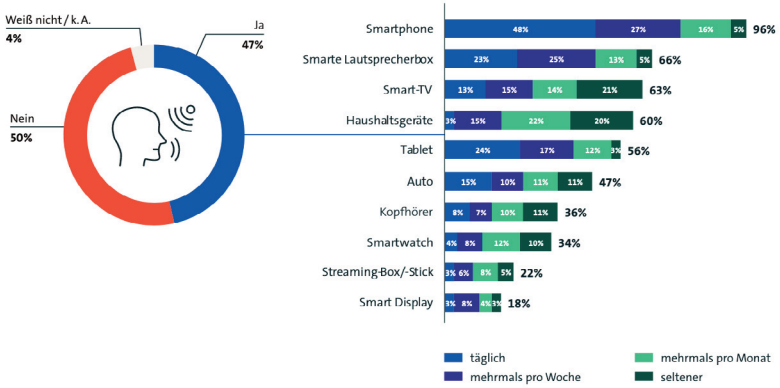
Zuhause und unterwegs: Die Nutzung von Sprachassistenten nimmt in Deutschland weiter zu. Über alle Geräte hinweg verwenden 47 Prozent aller Internetnutzerinnen und -nutzer ab 16 Jahren digitale Sprachassistenten zumindest hin und wieder – 2020 waren es noch 39 Prozent und 2021 44 Prozent. Das ist das Ergebnis einer repräsentativen Befragung unter 1.163 Personen in Deutschland ab 16 Jahren im Auftrag des Digitalverbands Bitkom. Männer (50 Prozent) verwenden sie demnach eher als Frauen (43 Prozent), die Jüngeren eher als die Älteren. Das Smartphone (96 Prozent), smarte Lautsprecherboxen (66 Prozent) und Smart-TVs (63 Prozent) sind unter den Nutzerinnen und Nutzern digitaler Sprachassistenten dabei die meistverwendeten Geräte. Den größten Schritt nach vorn hat zuletzt jedoch das Auto gemacht: Schon fast die Hälfte (47 Prozent) der Nutzerinnen und Nutzer erteilt dem Pkw Sprachbefehle – sei es etwa, um das Navi auf Kurs zu bringen, eine Playlist zu starten oder Nachrichten vorlesen zu lassen. Gegenüber dem Vorjahr hat das Auto damit um 17 Prozentpunkte zugelegt. „Die Automobilhersteller haben die Sprachsteuerung in Fahrzeugen in den vergangenen Jahren massiv ausgebaut.", sagt Dr. Sebastian Klöß, Bitkom-Experte für Consumer Technology. „Sprachsteuerung vergrößert nicht nur den Komfort am Steuer, sondern macht das Fahren vor allem sicherer. Sprachassistenten werden sich als dominierender Weg etablieren, die Funktionen des Fahrzeugs unterwegs zu bedienen."

Die Digitalisierung von Mobilität und Fahrzeugen war eines der dominierenden Themen auf der CES (Consu-

So verbreitet sind die digitalen Sprachassistenten

Nutzung von Sprachassistenten

Nutzen Sie die Möglichkeit, per Sprache Informationen abzufragen und Geräte zu steuern?
Wie häufig nutzen Sie die folgenden Geräte für die Sprachsteuerung?



Basis: Internetnutzerinnen und -nutzer ab 16 Jahren (links), Nutzerinnen und Nutzer von Sprachassistenten (rechts) | Hinweis: Werte gerundet | Quelle: Bitkom Research

mer Electronics Show) in Las Vegas, die Anfang Januar 2023 stattfand.

Die technischen Möglichkeiten bei der Sprachsteuerung im Auto sind dabei noch lange nicht ausgeschöpft.
Klöß: „Die technische Idealvorstellung eines digitalen Sprachassistenten ist perspektivisch, dass er nicht nur Sprachbefehle empfängt und umsetzt, sondern in möglichst vielen Lebenslagen assistiert – so wie K. I. T. T. aus »Knight Rider«".
Gleichwohl sind Nutzerinnen und Nutzer von Sprachassistenten im Moment noch zurückhaltend, Sprachassistenten als quasi-menschlichen Teil ihres Lebensumfeldes zu betrachten.

Nur 18 Prozent würden sich beispielsweise von einem Sprachassistenten ein Buch vorlesen lassen. Und nur eine kleine Minderheit (10 Prozent) würde sich aktuell gerne mit einem digitalen Sprachassistenten so unterhalten wie mit einem echten Menschen. „Das könnte sich jedoch künftig ändern. Sprachmelodie und Betonungen werden bei digitalen Sprachassistenten stetig weiterentwickelt, so dass sie immer weniger mit der teils ungelenken Sprachausgabe früherer Sprachassistenten zu tun haben", betont Klöß.

Hinweis zur Methodik: Grundlage der Angaben ist eine Umfrage, die Bitkom Research im Auftrag des Digitalverband Bitkom durchgeführt hat. Dabei wurden 1.163 Personen, darunter 1.012 Internetnutzerinnen und -nutzer in Deutschland ab 16 Jahren telefonisch befragt. Die Umfrage ist repräsentativ. Die Fragen lauteten: „Nutzen Sie hin und wieder die Möglichkeit, per Sprache Informationen abzufragen oder Geräte zu steuern?"; „Welche Geräte nutzen Sie für die Sprachsteuerung?"; „Inwieweit treffen die folgenden Aussagen zu Sprachassistenten auf Sie zu bzw. nicht zu?"

Fact Sheet: Digitale Sprachassistenten 2022/23

So verbreitet sind die digitalen Sprachassistenten

Nutzung von Sprachassistenten

Nutzen Sie die Möglichkeit, per Sprache Informationen abzufragen und Geräte zu steuern? Wie häufig nutzen Sie die folgenden Geräte für die Sprachsteuerung?

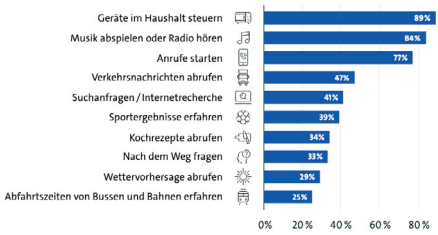
Knapp die Hälfte aller Internetnutzerinnen und -nutzer in Deutschland (47 Prozent) greift zumindest gelegentlich auf die Möglichkeit zurück, per Sprache Informationen abzufragen oder Geräte zu steuern. Klar an der Spitze liegen die 16- bis 29-jährigen Internetnutzerinnen und -nutzer: 61 Prozent. Für Sprachbefehle wird vor allem das Smartphone verwendet (96 Prozent), smarte Lautsprecher liegen bei 66 Prozent.

Die Sprachsteuerung wird sehr häufig verwendet, um Geräte im Haushalt zu steuern – 89 Prozent der Nutzerinnen und Nutzer von digitalen Sprachassistenten tun das. Das sind 7 Prozentpunkte mehr als im Jahr zuvor. Knapp dahinter liegt das Aufrufen von Musiktiteln oder Radiosendern (84 Prozent). Smarte Haushaltsgeräte per Sprache zu steuern, ist in allen Altersgruppen nahezu gleich beliebt. Bei der Musikauswahl hingegen sind es vor allem die Jüngeren, die ihre Sprache einsetzen.

Hierfür werden digitale Sprachassistenten eingesetzt

Der Einsatz von Sprachassistenten – Top 10

Wofür werden Sprachassistenten verwendet?

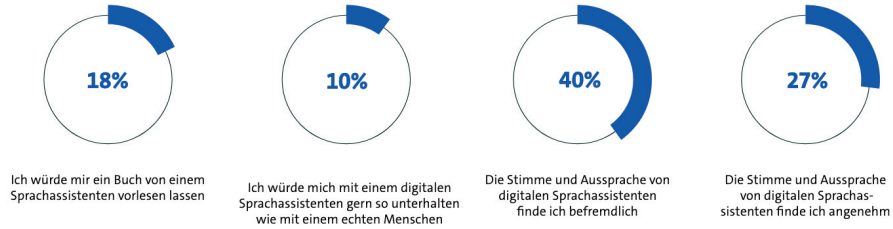


Basis: Nutzerinnen und Nutzer digitaler Sprachassistenten | Quelle: Bitkom Research

Erwartungen an digitale Sprachassistenten

Was Nutzerinnen und Nutzer von Sprachassistenten erwarten

Welche Aussagen treffen auf Ihre Erwartungen zu?



Basis: Nutzerinnen und Nutzer digitaler Sprachassistenten | Quelle: Bitkom Research

Erwartungen an digitale Sprachassistenten

Was Nutzerinnen und Nutzer von Sprachassistenten erwarten. Welche Aussagen treffen auf Ihre Erwartungen zu?

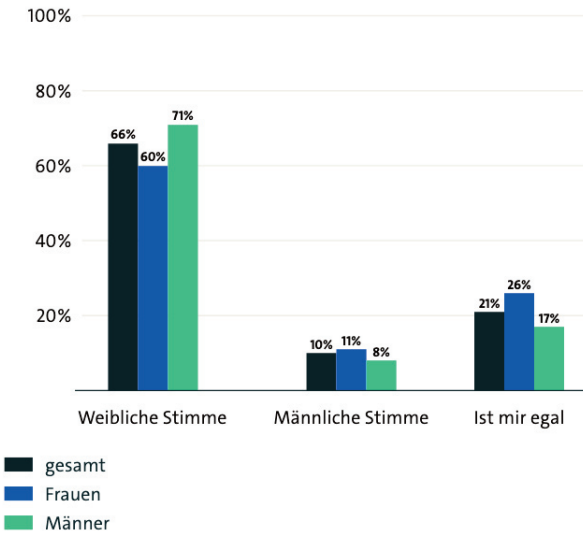
Nutzerinnen und Nutzer von Sprachassistenten sind zurückhaltend dabei, Sprachassistenten als (quasi-menschlichen) Teil ihres Lebensumfeldes zu betrachten. Nur 18 Prozent würden sich von einem Sprachassistenten ein Buch vorlesen lassen, nur 10 Prozent sich mit einem

Gründe, digitale Sprachassistenten nicht zu nutzen

Basis: Bevölkerung ab 16 Jahren | Quelle: Bitkom Research

Weibliche Stimmen werden bei Sprachassistenten bevorzugt

Würden Sie lieber mit einem digitalen Sprachassistenten mit einer weiblichen oder männlichen Stimme kommunizieren?



Basis: Nutzerinnen und Nutzer digitaler Sprachassistenten | Quelle: Bitkom Research

Sprachassistenten unterhalten wie mit einem echten Menschen.

Gegenüber Stimme und Aussprache der Sprachassistenten sind die Nutzerinnen und Nutzer recht neutral eingestellt. 40 Prozent finden sie befremdlich – eine Mehrheit empfindet das also nicht so. 27 Prozent finden Stimme und Aussprache von Sprachassistenten angenehm. Männer scheinen mit Stimme und Aussprache zufriedener zu sein: Von ihnen empfinden 36 Prozent Aussprache und Stimme als befremdlich, 30 Prozent als angenehm, bei den Frauen sind es 44 bzw. 23 Prozent.

Weibliche Stimmen kommen besser an

Zwei Drittel (66 Prozent) der Sprachassistentennutzerinnen und -nutzer möchten lieber mit einem Sprachassistenten mit weiblicher Stimme kommunizieren. 2016 waren es lediglich 42 Prozent derer, die sich damals schon für Sprachassistenten interessierten. Eine männliche Stimme wird derzeit von 10 Prozent der Nutzerinnen und Nutzer von Sprachassistenten bevorzugt, 21 Prozent ist es egal, ob die Stimme weiblich oder männlich ist.

Gründe, digitale Sprachassistenten nicht zu nutzen

Der Hauptgrund dafür, keine Sprachassistenten einzusetzen, sind Bedenken hinsichtlich des Datenschutzes und der Datensicherheit. 59 Prozent der Nicht-Nutzerinnen und -Nutzer beantworten die Frage, wieso sie aktuell keine Sprachsteuerung verwenden, mit der Sorge um ihre Daten. 53 Prozent haben Angst, dass Dritte die Sprachsteuerung hacken und abhören könnten

Alle Ergebnisse zu digitalen Sprachassistenten und weitere Fakten rund um Audio- und Videostreaming, Gaming, das Metaverse sowie Augmented und Virtual Reality finden sich in der Bitkom-Studie »Die Zukunft der Consumer Technology«

[https://tinyurl.com/4uye8f96]

Europäischer Datenschutztag

Genetec gibt Best-Practice-Empfehlungen zum Datenschutz bei der physischen Sicherheit

Genetec, Technologie-Anbieter für vereinheitlichtes Sicherheitsmanagement, öffentliche Sicherheit und Business Intelligence, stellte anlässlich des Europäischen Datenschutztages am 28. Januar Best-Practice-Empfehlungen für den Datenschutz bei der physischen Sicherheit vor. Die Empfehlungen sollen Verantwortlichen für physische Sicherheit dabei helfen, Privatsphäre und Daten zu schützen, ohne die physische Sicherheit zu beeinträchtigen – eine Voraussetzung für das Vertrauen von Kunden, Mitarbeitern, Geschäftspartnern und Dienstleistern.

Der Datenschutz hat nicht nur in Europa, sondern mittlerweile auch weltweit höchste Priorität. 71 % aller Länder haben Datenschutzgesetze eingeführt. Unternehmen, die keine angemessenen Maßnahmen zum Schutz von Daten ergriffen haben, müssen bei Verstößen mit Geldstrafen bis in dreistelliger Millionenhöhe rechnen. In der physischen Sicherheitsbranche ist die Erfassung digitaler Informationen wie Videoüberwachungsdaten, Fotos und Nummernschilder notwendig, um Menschen und Vermögenswerte zu schützen. Gleichzeitig sind diese Daten eine wertvolle Quelle für relevante Geschäftsinformationen.

"Sicherheit und Datenschutz schließen sich gegenseitig nicht aus", so Christian Morin, Chief Security Officer bei Genetec Inc. "Wenn Unternehmen die Best-Practice-Empfehlungen befolgen und sicherstellen, dass der Datenschutz in ihren physischen Sicherheitslösungen integriert ist, können sie die Privatsphäre respektieren, Datenschutzgesetze einhalten und trotzdem ein Höchstmaß an Sicherheit erreichen."

Zu den Best Practices, die sicherstellen, dass Videoüberwachungs-, Zutrittskontroll- und automatische Nummernschilderkennungssysteme die Datenschutzstandards erfüllen, gehören:

- **Erfassen und speichern Sie nur Daten, die das Unternehmen wirklich benötigt.**
  Reduzieren Sie Ihr Risiko im Falle einer Datenpanne mit einfachen Maßnahmen. Stellen Sie das Sichtfeld einer Kamera so ein, dass keine Videoaufnahmen von Bereichen erfolgen, die nicht überwacht werden müssen. Legen Sie Protokolle fest, um physische Sicherheitsdaten je nach Relevanz automatisch zu archivieren oder zu löschen. Und kontrollieren Sie sorgfältig, welche und wie viele Daten wie lange an andere Organisationen weitergegeben werden dürfen.
- **Beschränken Sie den Zugriff auf sensible Daten.**
  Gewähren Sie nur denjenigen Zugriff auf Daten, die diese für ihre Arbeit benötigen. Überwachen Sie diese Aktivitäten, um sicherzustellen, dass identifizierende Informationen wie Bilder und Zutrittsereignisse nur wie vorgesehen verwendet werden. Überprüfen Sie die Zutrittsberechtigungen regelmäßig, damit die Privilegien mit den Benutzeranforderungen übereinstimmen. Die Verwendung einer Identitätsnachweislösung wie Microsoft Active Directory kann ebenfalls dazu beitragen, menschliche Fehler zu vermeiden, indem Prozesse wie das Hinzufügen/Entfernen von Sicherheitsbenutzerkonten, der Gewährung von Rechten oder des Entfernens von Benutzern, die das Unternehmen verlassen haben, automatisiert werden.
- **Automatische Anonymisierung der Datenerfassung.**
  Neue Technologien können den Zugriff auf persönliche Daten automatisch einschränken und schützen. Ziehen Sie den Einsatz von datenschutzkonformen Maskierungslö- sungen wie Genetec KiwiVision™ Privacy Protector in Betracht. Da- mit werden Bilder

Datenschutztag: Ihre Daten, Ihre Rechte

Das EU-Datenschutzrecht gewährt Menschen eine Reihe von Rechten, wenn ihre Daten von einer EU-Einrichtung verarbeitet werden.

Informationsblatt unter >>
https://edps.europa.eu/system/files/2022-01/22-01-21_infographic_dataproday22_en.pdf

von Personen automatisch anonymisiert. So können Sie weiterhin Überwachungsdaten erfassen, ohne die Privatsphäre zu verletzen. Diese Technologie bietet auch eine zusätzliche Sicherheitsebene, die sicherstellt, dass nur autorisierte Benutzer das unmaskierte Videomaterial "entsperren" und ansehen können. Audit Protokolle bleiben dabei jederzeit unberührt.

- **Vereinheitlichen der Sicherheitslösungen**.
  Wenn Videoüberwachung, Zutrittskontrolle, Be- weismittelverwaltung und Sensoren über eine Plattform verwaltet werden, ist es viel einfacher, über eine einzige Schnittstelle auf alle Daten zuzugreifen, sie zu verwalten und Berichte für eine Vielzahl von Systemen und Sensoren zu erstellen. Ein vereinheitlichtes System vereinfacht die Überprüfung des System- und Gerätezustands sowie das Aufspielen von Software- und Firmware-Updates – ein wichtiger Punkt, um das Risiko möglicher Datenschutzverletzungen zu reduzieren.
- **Arbeiten Sie mit zertifizierten Partnern zusammen.**
  Vergewissern Sie sich, dass Ihre Systemanbieter ordnungsgemäß zertifiziert sind (Zertifizierung nach DIN EN-ISO 27001, 27017, Cybersicherheitszertifizierung nach dem US-amerikanischen Standard UL 2900-2-3 Level 3 und SOC2-Konformität; ein europäisches Zertifizierungsrahmenwerk wird aktuell von der European Cyber Security Certification Group erarbeitet) und dass Datenschutzprinzipien bereits bei der Technologieentwicklung berücksichtigt werden. Ein cyberresistentes physisches Sicherheitssystem trägt dazu bei, dass alle von IoT-Geräten und Sensoren über die physische Sicherheitsinfrastruktur gesammelten Daten privat bleiben.

Weitere Informationen zur Einhaltung des Datenschutzes ohne Beeinträchtigung der Sicherheit: https://www.genetec.com/de/blog/cybersicherheit/was-sie-uber-datensicherheit-wissen-sollten

12% nutzen KI

Accenture Studie: Nur 12 Prozent der Unternehmen weltweit nutzen Künstliche Intelligenz effektiv, mehr als 60 Prozent experimentieren noch Accenture entwickelt neuen Index für den KI-Reifegrad von Unternehmen.

Weltweit steckt der Einsatz von Künstlicher Intelligenz (KI) noch in den Kinderschuhen. Die Mehrheit der Unternehmen, die KI einsetzen, experimentieren in diesem Bereich noch. Lediglich 12 Prozent nutzen die Technologie mit einem KI-Reifegrad, der einen starken Wettbewerbsvorteil bringt, so das Ergebnis einer aktuellen globalen Studie des Beratungsunternehmens Accenture.

Die unter dem Titel „The Art of AI Maturity: Advancing from Practice to Performance" veröffentlichte Studie zeigt auf Basis eines holistischen Frameworks Strategien für den KI-Erfolg auf. Zu diesem Rahmenwerk gehört ein neuer Index, der den KI-Reifegrad von Unternehmen auf einer Skala von 0 bis 100 beziffert. Laut der Studie bezeichnet der KI-Reifegrad das Maß, in dem Unternehmen ihre Wettbewerber mithilfe einer Kombination

„Wir glauben, dass alle Teile eines jeden Unternehmens durch Technologie, Daten und KI verändert werden müssen, was in einigen Fällen zu einer Neuerfindung des Unternehmens führt. Die ‚AI Achievers' zeigen ihren Wettbewerbern, was möglich ist, wenn man das volle Potenzial von Talenten und Technologien freisetzt, die im Tandem und unterstützt von einer klaren Vision und dem Willen zum Wandel arbeiten." Aber selbst diese am weitesten fortgeschrittene Gruppe habe noch viel Spielraum für Wachstum. Und obwohl es in den meisten Branchen „AI Achievers" gebe, unterschieden sich diese stark darin, wie weit sie insgesamt im Bereich KI seien und welche Sprünge sie machten.

Dr. Andreas Braun, Managing Director und Applied Intelligence Lead bei Accenture für Deutschland, Österreich und die Schweiz.

grundlegender und differenzierender Fähigkeiten mit KI-Bezug übertreffen. Diese Fähigkeiten umfassen sowohl die Technologie – Daten, KI, Cloud – als auch die Unternehmensstrategie, eine verantwortungsvolle Nutzung, die Unterstützung durch die Führungsebene sowie die Talententwicklung und Unternehmenskultur.

Laut der Studie liegt der durchschnittliche KI-Reifegrad von Unternehmen gegenwärtig bei einem moderaten Wert von 36. Für die meisten Unternehmen ergeben sich also erhebliche Möglichkeiten, durch den gezielten Einsatz von KI größeren Mehrwert zu erzielen. Die Studie hebt eine kleine Gruppe (12 %) von Unternehmen hervor, die KI bereits nutzen, um ihre Wettbewerber zu übertreffen. Diese Gruppe, von den Studienautoren als „AI Achievers" bezeichnet, erreicht auf der Reifeskala mit 64 einen Wert, der fast doppelt so hoch ist wie der durchschnittlicher Unternehmen. Diesen gegenüber zeigt sich eine Korrelation mit einem um 50 Prozent höheren Umsatzwachstum.

In der Analyse wird außerdem deutlich, dass die meisten Unternehmen (63 %) „AI Experimenters" sind, die mit einem KI-Reifegrad von 29 kaum an der Oberfläche des KI-Potenzials kratzen. „AI Innovators" (13 %) mit einem Wert von 50 und „AI Builders" (12 %) mit einem Wert von 44 sind in ihrem KI-Reifegrad etwas weiter fortgeschritten, nutzen das Potential von KI aber auch noch nicht gänzlich aus.

Die Autoren der Studie geben des weiteren Beispiele für den aktuellen und den prognostizierten Stand des KI-Reifegrads nach Branchen:

- Technologieunternehmen haben mit einem Wert von 54 bereits einen hohen KI-Reifegrad, der bis 2024 moderat auf 60 ansteigen wird, womit sie im Branchenvergleich weiterhin an der Spitze des KI-Reifegrads stehen.
- Im Gegensatz dazu werden Automobilhersteller und -zulieferer von einem moderaten Wert von 39 heute auf 57 in zwei Jahren ansteigen, da sie auf einen erheblichen Anstieg der Verkäufe von KI-gesteuerten selbstfahrenden Fahrzeugen setzen.
- In ähnlicher Weise werden Einzelhandelsunternehmen ihren KI-Reifegrad von heute 38 auf 54 im Jahr 2024 steigern. Bemerkenswert ist, dass viele Einzelhandelsunternehmen ein stärkeres Engagement bei der KI-Transformation zeigen als andere Branchen. Walgreens Boots, beispielsweise, ist im Rahmen seiner Bestrebungen, ein stärker datengesteuertes Unternehmen zu werden, das seinen Kunden einen hochgradig personalisierten digitalen Service bieten kann, von alten Datenbanken auf fortschrittliche Cloud-Datenbanken und -Analysen migriert. Außerdem hat das Unternehmen mehr als 100 hochwertige KI-Produkte entwickelt, die detaillierte Kundenprofile erstellen und dabei helfen, Bestand und Preise zu optimieren.

Künstliche Intelligenz

Branchenunabhängig nimmt der Einfluss von KI auf Unternehmen zu und beschleunigt sich. Bei den weltweit größten Unternehmen, die in ihren Gewinnmitteilungen im Jahr 2021 über KI sprachen, war die Wahrscheinlichkeit für Aktienkurs-Steigerungen um 40 Prozent höher – verglichen mit 23 Prozent im Jahr 2018. Darüber hinaus nehmen Investitionen in KI zu. Im Jahr 2021 verwendeten 19 Prozent der befragten Unternehmen mehr als 30 Prozent ihrer Technologiebudgets für KI-Projekte. Bis 2024 wird der Anteil der Unternehmen, die mehr als 30 Prozent ihres Technologiebudgets in KI investieren, auf 49 Prozent steigen.

Die für die Studie verwendeten Machine-Learning-Modelle deuten darauf hin, dass sich der Anteil der „AI Achievers" bis 2024 von derzeit 12 Prozent auf 27 Prozent mehr als verdoppeln wird. Im gleichen Zeitraum wird der allgemeine KI-Reifegrad von heute 36 auf 50 ansteigen.

„Die Einführung von KI in großem Maßstab und ihre tiefere Einbettung in alle Geschäftsaspekte ist nicht länger eine Wahlmöglichkeit, sondern eine Notwendigkeit und Chance für jede Branche, jedes Unternehmen und jede Führungskraft", ist Braun überzeugt. Während die Wissenschaft der KI bahnbrechend und inspirierend sei, sei ihre gesamtheitliche Nutzung eine Kunst, die Führungskräfte kontinuierlich üben müssen. „Unsere Studie enthält umsetzbare Empfehlungen, wie man die KI-Reife vorantreiben kann, um sich in die Reihen der ‚AI Achievers' einzureihen."

Über die Studie

Die Studie mit dem Titel „The Art of AI Maturity: Advancing from Practice to Performance" basiert auf finanziellen und nicht-finanziellen Daten von 1.176 Unternehmen, die KI einsetzen, sowie auf Umfragedaten von 1.615 Führungskräften, die von August bis September 2021 in 16 Branchen (Luft- und Raumfahrt & Verteidigung; Automotive; Konsumgüter & Dienstleistungen; Chemie; Energie; Finanzdienstleistungen; Gesundheitswesen; Industrieausrüstung; Biowissenschaften; natürliche Ressourcen; öffentlicher Dienst; Einzelhandel; Technologie; Telekommunikation, Medien & Unterhaltung; Reisen & Transport; Versorgungsunternehmen) und 15 Ländern (Australien, Brasilien, Kanada, China, Frankreich, Deutschland, Indien, Israel, Italien, Japan, Singapur, Südafrika, Spanien, Großbritannien, USA).

Die Daten flossen in Modelle des maschinellen Lernens ein, die die Leistung der Unternehmen in Bezug auf eine Reihe von KI-bezogenen Fähigkeiten ermittelten – in erster Linie „grundlegende" Fähigkeiten, die Unternehmen benötigen, um im Bereich KI konkurrieren zu können.

Ergänzend dazu wurden „Differenzierungsfähigkeiten" bewertet, die Unternehmen einen Wettbewerbsvorteil durch KI verschaffen. Die Ergebnisse der beiden Modelle wurden in einem Index zusammengefasst, der den KI-Reifegrad auf einer Skala von 0-100 misst. **[www.accenture.de]**

Datenschutz
gleich Katastrophenschutz

Wenn kritische Infrastrukturen (KRITIS) von Hackern angegriffen werden, kann das dramatische Folgen haben. Doch während Rechenzentren oft Hochsicherheitstresoren gleichen, lassen sich Schaltbefehle beispielsweise von Bahnunternehmen, Energieversorgern oder Wasserwerken leicht manipulieren. Wenn sich diese Unternehmen vor folgenschweren Angriffen schützen wollen, sollten sie auf Verschlüsselungstechnologien „Made in Germany“ setzen.

Der Autor
Christian Stüble
Chief Technology Officer, Rohde & Schwarz Cybersecurity

Ein Vorfall aus dem vergangenen Frühjahr zeigt, dass Angriffe auf KRITIS längst keine Szenarien aus Katastrophenfilmen mehr sind: Die satellitengestützte Kommunikation von Windrädern in ganz Deutschland war im Februar 2022 durch einen Hackerangriff für mehrere Wochen unterbrochen worden. Die Fernwartung war infolgedessen gestört. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde eingeschaltet. Die Störung hatte zwar keinen Einfluss auf die Stromproduktion. Aber im Falle eines Problems hätte dieses nicht aus der Ferne behoben werden können. Ein weiterer Vorfall: Unbekannte hatten am 8. Oktober 2022 Glasfaserkabel der Deutschen Bahn durchtrennt. Eine Störung des digitalen Funksystems der Deutschen Bahn war die Folge. Der Zugverkehr im Norden und Westen Deutschlands kam zum Erliegen.

Diese Angriffe machen deutlich, wie groß die Auswirkungen sind, wenn KRITIS sabotiert werden. Und diese Angriffe waren nur möglich, weil die betroffene Infrastruktur ungeschützt war. So liegen z.B. Kabel praktisch für jeden zugänglich in Kabelschächten entlang der Bahntrassen. Ebenso ungeschützt sind die Daten, die durch die Kabel fließen und die Befehle für Weichen oder Signalanlagen übertragen.

Unverschlüsselte Daten an der Tagesordnung

KRITIS-Unternehmen sind zwar gesetzlich dazu verpflichtet, angemessene organisatorische und technische Vorkehrungen zum Schutz ihrer IT-Systeme zu treffen. Wenn aber zwischen verschiedenen Standorten oder Rechenzentren hochsensible Informationen übertragen werden, sind diese Daten häufig nicht oder nur unzureichend vor Manipulationen geschützt. Das gilt nicht nur für Datentransfers über öffentliche Netze, sondern bereits bei Verbindungen, die zwar durch private Leitungen, aber über öffentlichen Grund und Boden laufen. Denn: Die vorhandene Netzwerkinfrastruktur und auch der -schutz sind veraltet und mit geringem Aufwand und unverdächtigem Standardwerkzeug angreifbar. Nur eine hochsichere Verschlüsselung kann die Daten wirklich schützen.

Ungeschützte Datenübertragungen sind bei vielen Unternehmen allerdings noch immer an der Tagesordnung. Hacker können die Daten mitlesen, eigene Daten einspeisen oder die Datenübertragung stören. Die größte Gefahr geht bei Schaltbefehlen von einer Manipulation der Daten aus. Die Angriffsszenarien sind vielfältig: Manipulierte Befehle für Weichenstellungen und Signale können zu katastrophalen Bahnunfällen führen. Auch die Stromversorgung ist in Gefahr, wenn ein Signal eines Energieversorgers an ein Umspannwerk von Unbefugten verändert wird. Ein Blackout kann die Folge sein. Ein anderes Beispiel: Wasserversorgung. Wasserwerke senden Befehle an verschiedene Pumpenstandorte, um dort Grundwasser zu fördern. Durch eine Manipulation der Daten könnten alle

Pumpen herunterfahren, wodurch die Wasserversorgung zusammenbrechen würde. Verhindern lässt sich eine solche Manipulation von Daten, indem man diese kryptografisch absichert. Nur Sender und Empfänger haben dann schreibenden und lesenden Zugriff auf den Inhalt der Nachricht.

Netzwerkverschlüsseler dringend benötigt

Wer die Integrität und Vertraulichkeit seiner Kommunikationsdaten schützen will, wenn diese das Firmengelände verlassen, benötigt daher einen Netzwerkverschlüsseler. Die Geräte schützen vor Spionage und Manipulation von Daten, die per Internet oder Ethernet über Festnetz, Richtfunk oder Satellit übertragen werden. Sobald die Daten den Unternehmenssitz oder das Rechenzentrum verlassen, werden sie für den Transport zur Zieladresse verschlüsselt. Am Zielort angekommen wird der Befehl mit Hilfe eines weiteren Gerätes wieder entschlüsselt.

Die Herausforderung: Die kryptografische Absicherung sollte zwar hochsicher sein und Daten vor Angreifern schützen, gleichzeitig aber eine Übertragung nicht verlangsamen. Der entscheidende Faktor ist hier die Latenz – also die Zeit, die Daten benötigen, um von einem Punkt in einem Netzwerk zu einem anderen zu gelangen.

Effiziente Absicherung ohne Performanceverlust

Entscheidend für die Latenz ist u.a., auf welcher Ebene des Übertragungsnetzes die Verschlüsselung stattfindet. Für Unternehmen, die über ein Ethernet-Netzwerk verfügen, bietet sich eine Layer-2-Verschlüsselung an. Eine Verschlüsselung auf dieser Schicht ermöglicht eine Grundsicherung mit minimalem Performanceverlust. Nutzer profitieren von voller Leitungsgeschwindigkeit bei extrem geringer Latenz. Die Verschlüsselung ist in Echtzeit möglich. Layer-2-Verschlüsseler eignen sich für den Einsatz an zentralen Standorten von kritischen Infrastrukturen und in Rechenzentren und sichern auch große und komplexe Netze auf einfache Weise ab.

Ausschlaggebend für die Wahl des richtigen Verschlüsselungsgerätes ist es zudem, dass dieses selber vertrauenswürdig ist. Denn manipulierte Bauteile stellen heute eine steigende Bedrohung bei der Herstellung von Hardwarekomponenten dar. Aus diesem Grund sollten nur Geräte gewählt werden, die vollständig in Deutschland hergestellt wurden. Grundsätzlich gilt die Faustregel: Je tiefer die Fertigungstiefe ist, umso sicherer die Geräte. Ein weiterer Vorteil der Fertigung vor Ort: Die Geräte können kundenspezifisch angepasst werden. Zudem sind die nach speziellen Industriestandards konzipierten Geräte sehr robust - auch dann, wenn sie sich in Umspannwerken oder an Bahntrassen befinden und extremen Temperaturschwankungen ausgesetzt sind.

Ein weiteres Kriterium spielt eine Rolle bei der Wahl des richtigen Verschlüsselers: Beim Umgang mit kritischen Daten ist die Nutzung geprüfter Produkte empfehlenswert. Mit Netzwerkverschlüsselern, die vom BSI für die Verarbeitung von Verschlusssachen zugelassen wurden, sind KRITIS bestens ausgestattet. Eine BSI-Zulassung zeichnet Produkte und Lösungen aus, die für den Schutz von Verschlusssachen entsprechend den Einsatz- und Betriebsbedingungen genutzt werden können. Die Zulassung ist dabei immer zeitlich begrenzt und macht eine stetige Überprüfung und Aktualisierung notwendig. So sind die vom BSI zugelassenen Lösungen immer auf dem aktuellsten Stand.

IT Security Made in Germany

Einer der Hersteller, der solche zugelassenen Netzwerkverschlüsseler anbietet, ist das deutsche Unternehmen Rohde & Schwarz Cybersecurity. Die Firma ist zudem Träger des Vertrauenszeichens „IT Security Made in Germany" des Bundesverbandes für IT-Sicherheit „TeleTrusT". Unternehmen erhalten das Zeichen, wenn sie u.a. bestätigen, dass ihre Produkte keine versteckten Zugänge – sogenannte Backdoors - enthalten, dass der Unternehmenshauptsitz in Deutschland ist und auch die Forschung und Entwicklung auf heimischem Boden stattfindet. Hergestellt werden die Geräte vollständig in den eigenen Werken des Mutterkonzerns Rohde & Schwarz in Deutschland. Das Unternehmen ist Pionier hochsicherer Verschlüsselungstechnologien und verfügt über 30 Jahre Erfahrung in der Entwicklung von Verschlüsselungsprodukten. Aktuell forscht man an der Kryptografie für das Quantenzeitalter, um auch bereit zu sein für die Sicherheit von morgen.

Weitere Informationen zum Schutz von KRITIS:
https://tinyurl.com/253dznbv

Digitalisierung an Grenzen

Reisenden und Unternehmen sind technologiebasierten Lösungen an internationalen Grenzen aufgeschlossen

Im September 2022 hat Accenture einen neuen Marktbericht herausgefertigt, der zeigt, dass zwei Drittel der nternationalen Reisenden und Import-/Export-Händler den Einsatz bestehender und neuer Technologielösungen durch Grenz-, Einwanderungs- und Zollbehörden zur Verbesserung der Abläufe im Personen- und Warenverkehr befürworten. Darüber hinaus stimmten drei Viertel (75 %) der Befragten zu, dass sich die Abläufe an den Grenzen bis 2030 drastisch verändern werden.

Der Bericht Future borders 2030: From vision to reality (Zukünftige Grenzen 2030: Von der Vision zur Realität) enthält Daten aus 2022 Umfragen unter Reisenden und Händlern, die im internationalen Import und Export tätig sind, in neun Län-

dern (Australien, Kanada, Finnland, Frankreich, Deutschland, Saudi-Arabien, Singapur, Vereinigtes Königreich und Vereinigte Staaten) und stützt sich auf eine kürzlich durchgeführte länderübergreifende Umfrage unter Mitarbeitern von Grenzbehörden.

Die Ergebnisse des Berichts zeigen, dass eine Beibehaltung des Status quo für die Grenzbehörden keine Option ist. Siebenundfünfzig Prozent der internationalen Reisenden gaben an, dass sie ihr Reise- oder Aufenthaltsziel danach auswählen, ob sie glauben, dass die Grenzkontrollen nahtlos und einfach verlaufen werden, während 28 Prozent ihr Reise- oder Aufenthaltsziel gewechselt haben, weil sie eine schwierige Grenzkontrolle erwarteten. Die Importeure und Exporteure verhalten sich ähnlich: 17 % gaben an, dass sie Verträge aufgrund schlechter Erfahrungen mit den Zollverfahren in bestimmten Ländern gestoppt haben.

Der Bericht ergab auch, dass etwa ein Drittel der Menschen (30 %) plant, mehr internationale Reisen zu unternehmen als vor der Pandemie. Auch der globale Handel nimmt zu, angetrieben durch den Boom des elektronischen Handels, für den derzeit ein Anstieg von 4,21 Billionen Dollar im Jahr 2020 auf 17,53 Billionen Dollar im Jahr 2030 prognostiziert wird. Allerdings erwarten 85 % der Importeure in den nächsten drei Jahren eine höhere Volatilität als in den drei Jahren zuvor.

"Wir müssen die Technologie nutzen, um reibungslosere Erfahrungen für Reisende und den Warenverkehr zu schaffen", sagte Prasanna Ellanti, der bei Accenture den Bereich Grenzdienstleistungen leitet. "Dazu gehört es, sich auf die Erwartungen der Kunden zu konzentrieren, die Datenkapazitäten zu verbessern und aufkommende Technologien wie das Metaverse zu nutzen."

Drei Technologietrends:

1. **Reibungslos durch Design:** Die Erfahrungen an den Grenzen werden immer reibungsloser und konzentrieren sich darauf, die Bedürfnisse und Wünsche der Nutzer nach sichereren, schnelleren und reaktionsfähigeren Reisen zu erfüllen.

2. **Vertrauen in die Wahrheit:** Zunehmende Erfassung und Nutzung von Daten für Bewertungen vor und während der Grenz- und Zollinteraktionen.

3. **Virtuelle Grenzen:** Das Aufkommen und die Beschleunigung des Metaversums und seine Auswirkungen auf die Grenzen für die Ausbildung des Personals, die Erleichterung von Kontrollen und die Abwicklung von Reisenden und Handel.

"Wir gehen davon aus, dass sich diese Veränderungen bis 2030 recht schnell vollziehen werden", so Prasanna weiter. "Reisende und Händler befürworten den Einsatz neuer und aufkommender technologischer Fortschritte sehr stark, und wir sehen wachsende Anforderungen und Druck auf die Behörden, die eine Periode echter Neuerfindung der Art und Weise, wie sie Grenzdienstleistungen erbringen, einleiten.

Über die Studie

Accenture führte im März 2022 zwei Umfragen (Global Traveler Survey und Global Trader Survey) in neun Ländern durch: Australien, Kanada, Finnland, Frankreich, Deutschland, Saudi-Arabien, Singapur, Vereinigtes Königreich und die Vereinigten Staaten.

An der Global Traveler Survey nahmen 5 000 Personen teil, die in den letzten vier Jahren mindestens einmal ins Ausland gereist waren. Die Global Trader Survey umfasste 1.000 Befragte aus Unternehmen, die als Exporteure und/oder Importeure tätig sind.

Darüber hinaus befragte Accenture fünf der weltweit führenden Zukunftsforscher, die Unter- nehmen bei der Planung langfristiger Zukunftsszenarien beraten.

Für die Ausarbeitung dieses Papiers hat Accenture Ideen von mehr als 1.000 Fachleuten aus der globalen Grenzindustrie eingeholt und getestet.

Schließlich stützt sich diese Arbeit auf Teilbereiche früherer globaler Umfragen, einschließlich einer Umfrage unter 500 Grenz-, Einwanderungs- und Zollbeamten in fünf Ländern (Australien, Deutschland, Singapur, Vereinigtes Königreich und Vereinigte Staaten), die 2020 durchgeführt wurde.

Hikvision

Mehr Automatisierung mit KI-Lösungen

Im Zuge des technologischen Fortschritts wird künstliche Intelligenz (KI) auf immer vielfältigere Weise eingesetzt, um automatisierte Sicherheitsmaßnahmen zu realisieren. Sie wird jetzt auch in Unternehmensszenarien eingesetzt, wo sie komplexe Probleme lösen oder langwierige Aufgaben mit minimalem Aufwand erledigen kann. KI-gestützte Anwendungen wie automatische Ereigniswarnungen, Fehlalarmreduzierung, ANPR (automatische Kennzeichenerkennung) und Personenzählung haben sich bereits in einer Vielzahl von Szenarien durchgesetzt.

Sicherheitsfachleute müssen schon heute innovative Lösungen mit KI-Funktionen anbieten können, um ihre Wettbewerbsfähigkeit zu steigern. Zu ihrer Unterstützung bei der Bewältigung allgemeiner und spezieller Herausforderungen bietet Hikvision eine Reihe von Produkten und Lösungen mit der KI-gestützten AcuSense-Technologie sowie die DeepinView- und DeepinMind-Produktserien an. Mit ihnen lässt sich die Automatisierung von Sicherheitsmaßnahmen und Geschäftsabläufen optimieren und maximieren.

Bessere Perimetersicherheit mit AcuSense-Technologie

Herkömmliche Lösungen für den Perimeterschutz bieten bestimmte Erkennungsfunktionen, die auf der Analyse von Videoinhalten basieren, wie Bewegungserkennung, Erkennung von Linienüberquerung und Einbrucherkennung. Allerdings lösen sie leicht Fehlalarme aus, weil ein Tier, ein Schatten oder andere natürliche Bewegungen erkannt werden. Das Sicherheitspersonal muss dann jeden einzelnen Alarm untersuchen, wofür es Zeit braucht, die ihr für die Reaktion auf einen begründeten Alarm möglicherweise fehlt und was die Effizienz generell beeinträchtigt.

Hier können intelligentere Lösungen für die Perimetersicherheit mit "effektiver Fehlalarmreduzierung" und "Schnellzielsuche" hilfreich sein, die unerlaubtes Betreten des Perimeters in Echtzeit erkennen und darauf reagieren sowie das Durchsuchen von Bildmaterial automatisieren können, um wirkliche Vorfälle schnell darin zu finden.

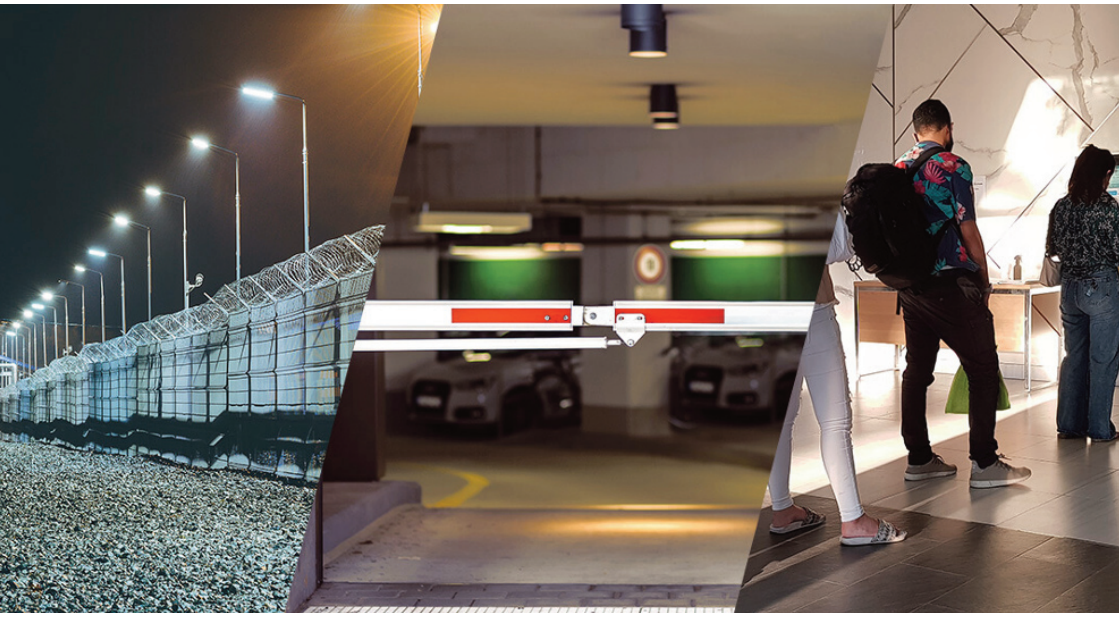
Die AcuSense-Technologie von Hikvision erfüllt diese Anforderungen mit modernen KI-Funktionen, die eine schnellere und effektivere Reaktion auf Sicherheitsvorfälle ermöglichen. Durch ihre Fähigkeit, zwischen Menschen, Fahrzeugen und anderen beweglichen Objekten zu unterscheiden, reduziert AcuSense die für Kunden kostspieligen Fehlalarme. Das bedeutet, dass sie reale Sicherheitsbedrohungen sofort überprüfen können und vom automatisierten Durchsuchen von Videoaufnahmen profitieren, indem sie nicht mehr stundenlang selbst Vidoes prüfen müssen.

Hikvision bietet eine Reihe von Front- und Backend-Produkten mit AcuSense-Technologie wie Kameras, NVR und DVR an, die sich zudem leicht installieren und konfigurieren lassen. So können Sicherheitsfachleute die Vorteile der KI für einen intelligenteren Perimeterschutz schnell und einfach für ihre Kunden realisieren, ohne dass zusätzliche Schulungen erforderlich sind.

Verbesserte Betriebseffizienz mit den DeepinView- und DeepinMind-Produktreihen

Mit den Fortschritten bei Algorithmen und Rechenleistung hat die KI-Technologie viel Potenzial für die Entwicklung von Intelligenz und Automatisierung für verschiedene Geschäftsprozesse. Neben dem Perimeterschutz dienen Überwachungskameras mit KI-Funktionen auch zunehmend dazu, alltägliche Abläufe in Unternehmen zu optimieren. Damit bietet sich für Sicherheitsfachleute die Gelegenheit, sich über ihren traditionellen Tätigkeitsbereich hinaus ein breiteres Geschäftsfeld zu erschließen.

Hikvision bietet DeepinView-Kameras und DeepinMind-NVR mit eingebetteten Deep-Learning-Algorithmen für ANPR, Personenzählung und Warteschlangenerkennung an, mit denen sich verschiedene intelligente Funktionen für Unternehmen realisieren lassen.
Im Einzelhandel beispielsweise liefert Personenzählung wertvolle Erkenntnisse für die Betreiber von Einkaufszentren. Mit ihr lassen sich etwa Muster in der Kundenfrequenz erken-



nen, um vorherzusagen, wann mit einem Besucheransturm zu rechnen ist, und die Personendichte unter Kontrolle zu halten. Gleichzeitig kann die Warteschlangenerkennung berechnen, wie lange die Menschen in der Schlange warten, und die Kassierer benachrichtigen, bevor ein Kunde die Geduld verliert.

Die Bewirtschaftung des Parkraums für Wohnhäuser, Bürotürme und Gewerbegebiete kann ebenfalls ein Problem darstellen. Deep-Learning-gestützte Kameras mit ANPR erfassen die Nummernschilder von Fahrzeugen, wobei Buchstaben und Ziffern scharf dargestellt werden.

Wenn diese Kameras an den Ein- und Ausfahrten von Parkplätzen installiert sind, können sie automatisch die Schranke öffnen oder schließen und bei Bedarf das Personal benachrichtigen, was die Parkraumbewirtschaftung erheblich effizienter gestaltet. Darüber hinaus können bei einigen Modellen der DeepinView-Kameraserie von Hikvision jetzt mehrere KI-gestützte Deep-Learning-Algorith- men in einem Gerät integriert werden. Die Algorithmen können umgeschaltet werden, so dass ein Gehäu- se im Grunde fünf oder sechs verschiedene Kameras enthält. Die Benutzer können manuell einen Algo- rithmus für eine bestimmte Anwendung aktivieren und später nach Bedarf zu einem anderen Algorithmus umschalten.

Darüber hinaus bietet Hikvision eine einheitliche Software an, HikCentral Professional, mit der Sicherheitsfachleute und Kunden problemlos mehrere Produkte und Systeme auf einer einzigen Plattform verwalten können.

HikCentral Professional kann verschiedene Anwendungen flexibel zusammenführen und ermöglicht es so den Benutzern, ein maßgeschneidertes System speziell für ihre eigenen Sicherheits- und Geschäftsanforderungen zu schaffen.

Durch diese Vereinigung wird nicht nur die Sicher- heitslage klarer einschätzbar, sondern sie setzt in der Alltagsroutine auch Ressourcen frei, die bislang durch die unverbundenen Systeme gebunden waren.

Sechs Trends

für die Sicherheitsbranche im Jahr 2023

Die Sicherheitsbranche ist ein Sektor, der zunehmend auf smarte Technologien setzt, sensible Daten verarbeitet und wie kein anderer von geopolitischen Fragen und deren Auswirkungen betroffen ist. Vor diesem Hintergrund sieht Axis Communications sechs grosse Trends, die die Branche im neuen Jahr massgeblich beschäftigen werden. Philippe Kubbinga, Regional Director Middle Europe bei Axis Communications, hat die Trends analysiert:

1. KI- und Machine-Learning-Analysen werden zur Grundlage für erkenntnisbasiertes Handeln

Das enorme Volumen von Daten und Metadaten, das inzwischen von Kameras und anderen Sensoren erzeugt wird, lässt sich manuell nicht mehr schnell genug sichten, interpretieren und verarbeiten. Eine auf künstlicher Intelligenz und Machine Learning basierende Analyse kann hier Abhilfe schaffen und als Fundament für erkenntnisbasiertes Handeln dienen: Das Ziel und der Schwerpunkt liegen dabei weniger auf der tatsächlichen Analyse der Daten, sondern auf den verwertbaren Ergebnissen, die sie für Echtzeit- und forensische Anwendungsfälle liefern. Es wird also weniger darum gehen, dass die Analyse erkennt, dass etwas nicht stimmt, sondern dass sie den Menschen bei Entscheidungen für bestimmte Massnahmen unterstützen kann. Das umfasst beispielsweise bei Zwischen- fällen die Aufforderung, den Notdienst zu rufen, oder den Verkehr in Städten umzuleiten, um Staus zu entschärfen. In stark frequentierten Einzelhandelsgeschäften wiederum lässt sich anhand der Informationen mehr Personal einsetzen oder in Gebäuden allgemein durch optimierte Beleuchtung und Wärmeverteilung Energie einsparen – die Szenarien sind vielfältig.

2. Die Wahl der Technologiearchitektur wird zunehmend vom Anwendungsfall bestimmt

Bei Sicherheitssystemen bieten hybride Technologiearchitekturen grundsätzlich eine Reihe von Vorteilen, da

Philippe Kubbinga, Regional Director Middle Europe bei Axis
(Copyright: Axis Communications)

sie sichere Server vor Ort, effiziente Da- tenverarbeitung in der Cloud und leistungsstarke Edge-Geräte kombinieren. Keine Architektur ist jedoch ausnahmslos für alle Anwendungsfälle geeignet. Dementsprechend wird die Betrachtung der spezifischen Situation in Zukunft noch ausschlaggebender für die Wahl der jeweiligen Architektur. Zum Beispiel ermöglichen es in Edge-Geräte eingebettete Echtzeit-Analysefunktionen, besonders schnell zu reagieren. Die Analyse von grösseren, forensischen Datenvolumen hingegen kann oftmals Erkenntnisse liefern, mit denen sich Prozesse und Effizienz verbessern lassen – diese Art der Analyse erfordert jedoch oft die Rechenleistung von Servern vor Ort oder in der Cloud. Darüber hinaus gibt es von Land zu Land und Region zu Region unterschiedliche Datenschutz- und Compliance-Anforderungen zu beachten, die eine Entscheidung zwischen Speicherung vor Ort oder in der Cloud beeinflussen können. Wichtig für Unternehmen wird es sein, sich nicht aus Prinzip oder Gewohnheit an eine einzige Architektur zu binden, sondern die Flexibilität, die hybride Architekturen bieten, zu nutzen, um die eigenen spezifischen Anforderungen bestmöglich zu erfüllen.

3. Kameras und Sensoren werden zur Schnittstelle für Anwendungsfälle, die über Sicherheit hinausgehen

Einer der wichtigsten Trends für den Sicherheitssektor – und damit eine ebenso grosse Chance – ist der Schritt über die Sicherheit hinaus. Während sich die Qualität von Kamera- und Sensordaten über die vergangenen Jahrzehnte hinweg kontinuierlich verbessert hat, lassen sich dank fortschrittlicher Analyseverfahren auf Basis von künstlicher Intelligenz und Machine Learning inzwischen auch Metadaten, sprich zusätzliche Informationen über die erhobenen Daten, erstellen.

Diese zusätzlichen Informationen können in Kombination mit weiteren Daten – zum Beispiel hinsichtlich Temperatur, Lärm, Luft- und Wasserqualität, Vibrationen oder Wetter – auch für Anwendungsfälle genutzt werden, die über den Bereich der Sicherheit hinausgehen. So entsteht ein fortschrittliches Sensornetzwerk, das

datengestützte Entscheidungen ermöglicht.

Zur Bewertung der Prozessqualität und der proaktiven Wartung von Maschinen werden solche Netzwerke bereits in der Industrie eingesetzt. Je nach Konfiguration der einzelnen Sensorknoten im Netzwerk und der Granularität der Datenanalyse sind den Anwendungsfällen, für die diese Art von Netzwerk genutzt werden kann, jedoch fast keine Grenzen gesetzt.

4. Cybersicherheit wird zum Eckpfeiler der Sicherheitsbranche

Nicht nur aufgrund neuer lokaler und internationaler Gesetze wie dem von der EU-Kommission vorgeschlagenen „Cyber Resilience Act" wird Cybersicherheit zu einem immer wichtigeren Aspekt der gesamten Technologie- und damit auch der Sicherheitsbranche, für die das Kundenvertrauen in die angebotenen Produkte und Services besonders wichtig sind. So ist beispielsweise im Bereich (Netzwerk-)Video eine umfassende Absicherung der einzelnen Geräte sowie des Netzwerks, in dem sie eingebettet sind, essenziell, um verlässliche Daten und Metadaten zu erhalten. Vor allem Massnahmen, mit denen die Authentizität der Daten bei der Erfassung und Übertragung von der Kamera in die Cloud gewährleistet werden kann, helfen dabei, das Vertrauen in die erhobenen Daten zu steigern. Als ein hochdynamisches Wachstumsfeld wird es herstellerseitig verschiedene neue und innovative Ansätze geben, um die Cybersicherheit ihrer Produkte über den gesamten Produktlebenszyklus hinweg zu steigern. Insbesondere „Bug Bounty"-Programme und „Bill of Materials"-Software (SBOM) werden als proaktive Lösungen in Zukunft häufiger zum Einsatz kommen.

5. Regulierung wird noch wichtiger

Der Technologiesektor wird das private und öffentliche Leben weiterhin signifikant beeinflussen und steht damit auch in Zukunft im Fokus nationaler und internationaler Regulatoren. Die Sicherheitsbranche als Teil des Technologiesektors wird aufgrund der Tatsache, dass sie an vielen Stellen kritische Infrastrukturen unterstützt, dabei ganz besonders ins Visier von Regulierungsbehörden und politischen Entscheidungsträgern rücken.
Vor allem in der Europäischen Union wird es im neuen Jahr voraussichtlich weitere Gesetzesentwürfe, Verordnungen und Richtlinien geben, die vor allem die Bereiche künstliche Intelligenz, Anforderungen an Cybersicherheit, Datenschutz, die Eindämmung des Einflusses von nichteuropäischen ‚Big Tech'-Konzernen und die Förderung von technischer und digitaler Souveränität der europäischen Staaten betreffen. Idealerweise wird sich die Regulierung dabei auf spezifische Anwendungsfälle von Technologien und nicht auf die Technologie an sich konzentrieren.
Dennoch werden sich Technologieunternehmen mit den für ihre Bereiche relevanten Regularien beschäftigen müssen, um rechtliche Fallstricke, Geldstrafen und Reputationsschäden zu vermeiden.

6. Nachhaltigkeit und einwandfreie Lieferketten bleiben hochrelevant

Das Thema Nachhaltigkeit bleibt angesichts des voranschreitenden Klimawandels branchenunabhängig hochrelevant – und nach dem zurückliegenden Jahr, in dem Unternehmen und Gesellschaft zusätzlich noch zahlreiche weitere Herausforderungen und Krisen zu meistern hatten, wird sich dieser Fokus 2023 noch weiter verstärken.
Von Unternehmen aller Branchen wird von der Öffentlichkeit und Gesetzgebern erwartet, dass dieses Thema auf der Agenda steht. Kunden setzen voraus, dass Unternehmen nachweisen können, dass Produkte und Dienstleistungen die eigenen Nachhaltigkeitsziele unterstützen.

Insbesondere für Technologieunternehmen endet diese Verantwortung nicht am eigenen Werkstor: Sie sollten nicht nur die eigenen Geschäftsabläufe überprüfen, sondern auch die ökologischen, gesellschaftlichen und geschäftlichen Praktiken ihrer Zulieferer messen und verbessern.

Denn selbst die ehrlichsten und umfassendsten Anstrengungen zur Reduzierung der eigenen Emissionen können untergraben werden, wenn die vor- und nachgelagerten Teile der Wertschöpfungskette nicht auf die gleichen Ziele ausgerichtet sind.

Mehr zu den Tech-Trends im Axis Blog Secure Insights: www.axis.com/blog/secure-insights-de/technologietrends-2023

AIM / Konsortialpartner

Im Fokus: Identifikation von Produktfälschungen

Die deutsche Volkswirtschaft erleidet über 50 Milliarden Euro Schaden durch Produkt- und Markenpiraterie pro Jahr. 97 Prozent der erfassten Plagiate stuften die EU-Marktaufsichtsbehörden als Waren mit ernsthaften Risiken ein. Produktions- und Logistikunternehmen sind machtlos gegen Plagiate: Weltweit gibt es keinen branchen- und grenzübergreifenden Lösungsansatz für die Verifizierung von Produkt-Identitäten. „Ebenso gibt es kein global anerkanntes Verfahren mit dem Unternehmen Produktfälschungen erkennen können, ohne dass dafür Informationen zu Lieferketten und volumina offengelegt werden müssen. Diese Lücke schließt nun das Projekt SPOQ", erklärt Stefanie Hildebrandt, Projektleiterin Technik und Innovation im VDE. Im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) erarbeitet der Technologieverband AIM und die Technologieorganisation VDE gemeinsam mit Partnern aus Wirtschaft und Wissenschaft jetzt eine Methodik für die fälschungssichere Produktkennzeichnung auf Originalprodukten zur Verifizierung der eineindeutigen Identität, die anschließend prototypisch auf Hersteller- und Endanwenderseite in die Praxis umgesetzt werden soll. Plagiaten wird damit der Kampf angesagt.

Methodik zur fälschungssicheren Produktidentität

Im Rahmen des vom BMWK geförderten Projekts „Standardisierte sichere Produktverifizierung zum Schutz von Originalität und Qualität" (SPOQ) entwickeln die Projektpartner AIM, KOBIL, PAV Card, Universität Würzburg sowie die Hochschule Mannheim unter der Leitung des VDE ein standardisiertes und damit global anwendbares Verfahren, das nicht nur eine fälschungssichere Produktidentität ermöglicht, sondern auch den Herstellern erlaubt, ihre Datenhoheit zu behalten. „Unser Ziel ist es, dass sie die Kennzeichnung ihrer Produkte selbst in dezentralen Datenbanken verwalten, beispielsweise im Rahmen einer Blockchain-Infrastruktur", führt Hildebrandt fort. Die Hersteller legen hierfür die Identität ihres Produktes mit charakteristischen physischen und schwer fälschbaren Merkmalen in einer Datenbank ab. Innerhalb eines festen Zeitraumes kann der Inverkehrbringer oder Endkunde die Identität des Produktes dann abrufen und durch Vergleich mit den Merkmalen die Echtheit feststellen.

Smartphone prüft Identität

Parallel prüfen die Projektpartner geeignete Technologien zur Verknüpfung eines physischen Produkts mit seiner digitalen Identität und erarbeiten Konzepte für das sichere Handling von Produkt- und Trackingdaten. Um auch für komplizierte Fälschungsszenarien gewappnet zu sein, kombinieren sie mehrere Methoden und Indikatoren zur Verifizierung der Echtheit eines Produkts. Im Rahmen eines Proof-of-Concept des standardisierten Ansatzes erfolgt dann die prototypische Entwicklung und Bereitstellung von Toolkits für Hersteller, Zwischenhändler und Endkunden, die an dezentralen Datenbanken angebunden sind. Hierbei setzen die Experten auf bereits massenhaft verbreitete Hardware, beispielsweise gängige Smartphones als Plattform, die für spezifische Anwendungsfälle auch mit Hardware-add-on oder in Handel und Logistik gängige mobile Lesegeräte für Barcodes und ähnliches ausgestattet sind.

Über das SPOQ-Projekt und die Projektpartner

Das SPOQ-Projekt des BMWK zielt auf die Erfassung und Aufarbeitung sowie Standardisierung und Umsetzung der sicheren Produktverifizierung und wird federführend durch den VDE e.V. in Zusammenarbeit mit folgenden Partnern realisiert:

- AIM-D e.V. (Industrieverband Automatische Identifikation, Datenerfassung und Mobile Kommunikation e.V.)
- Universität Würzburg, LS Informatik II, Secure Software Systems
- Hochschule Mannheim, Fakultät für Informationstechnik, ESM-Institut
- KOBIL GmbH, Sicherheitstechnologien
- PAV Card GmbH, RFID-Lösungen und IT-Services

Das Projekt ist Teil des Technologieförderprogramm "WIPANO - Wissens- und Technologietransfer durch Patente und Normen" des Bundesministeriums für Wirtschaft und Klima (BMWK). Im Rahmen des Projekts SPOQ hat der VDE darüber hinaus die Aufgabe, eine VDE SPEC zu erstellen, die anschließend in eine internationale Norm oder Normenfamilie münden soll.

Abkürzungen: RFID: Radiofrequenz-Identifikation; NFC: Near Field Communication; RTLS: Real-Time Locating Systems; ORM: Optical Readable Media (Barcode, 2D Code, OCR u.a.); QR: Quick Response Code; OCR: Optical Code Recognition.

TrendTage

im März zu aktuellen Themen

Angriffe auf Lieferketten, sicheres Active Directory, Managed SOC und Attack Path Management

cirosec, der Spezialist im IT-Sicherheitsbereich, veranstaltet im März 2023 wieder seine TrendTage rund um innovative Themen im IT-Sicherheitsbereich. Schwerpunkte bilden dieses Mal Angriffe auf Lieferketten, sicheres Active Directory, Managed SOC und Attack Path Management.

Nach einer kurzen Begrüßung stellt cirosec-Geschäftsführer Stefan Strobel Angriffe und mögliche Schutzmaßnahmen auf Lieferketten vor. Er beschreibt ausführlich zahlreiche Angriffe über Lieferketten aus der Vergangenheit und zeigt dabei die Besonderheiten sowie die unterschiedlichen Varianten dieser Angriffe auf. Zudem stellt er verschiedene Schutzmaßnahmen sowie ihre Grenzen vor und empfiehlt Strategien zur Absicherung der Lieferkette.

Im Anschluss präsentieren drei Hersteller ihre innovativen Produkte:

*** Managed SOC Services auf Basis von MS Sentinel oder Splunk in der Cloud - BlueVoyant**

Viele Unternehmen setzen Security-Produkte von Microsoft als AV-Lösung, EDR oder zur AD-Überwachung ein. Gleichzeitig steigt der Bedarf, solche Sicherheitssysteme zu überwachen sowie die dort erzeugten Alarme zu verifizieren und weiterzuverfolgen. Da die Events der diversen Microsoft Defender bereits in der Microsoft-Cloud liegen, werden neue SOC-Betriebsmodelle möglich, bei denen ein externer Dienstleister kein eigenes SIEM mehr betreiben muss, sondern nur noch Zugriff auf den Sentinel im Azure-Tenant seiner Kunden benötigt. BlueVoyant ist einer der erfolgreichsten Anbieter weltweit in diesem neuen Bereich.

*** Erkennung von Angriffen auf das Active Directory - Netwrix**

Voraussetzung für die Sicherheit des Active Directory ist eine übersichtliche, klar definierte und sorgfältig konfigurierte Verzeichnisstruktur, die engmaschig überwacht und kontrolliert wird.

Mit den Tools von Netwrix identifizieren, analysieren und priorisieren Sie Aktivitäten und Risiken in Ihrer Active-Directory-Umgebung, beispielsweise fehlerhaft konfigurierte Sicherheitsrichtlinien, die unrechtmäßige Vergabe von Berechtigungen sowie inaktive Benutzer- und Computerkonten. Darüber hinaus werden Angriffe im Kontext AD erkannt und gemeldet.

*** Attack Path Management: wie Angreifer Ihr Netzwerk sehen und Systeme kompromittieren – XM Cyber**

Trotz vieler Firewalls, neuer EDR-Lösungen und SOAR-Plattformen werden Unternehmen immer noch angegriffen und kompromittiert. Das Produkt von XM Cyber zeigt auf, wie Angreifer das Netzwerk ihres Opfers sehen, Schwachstellen ausnutzen können und diese mit Fehlkonfigurationen kombinieren. Ebenso lassen sich daraus Empfehlungen für Schutzmaßnahmen ableiten.

[www.cirosec.de]

Stationen der TrendTage sind Köln (20. März 2023), Frankfurt (21. März 2023), Stuttgart (22. März 2023) und München (23. März 2023). Die Teilnahme ist kostenlos.

Dokumenten-Management unterstützt neue Regeln

Seit erstem Januar ist das neue Lieferkettensorgfaltspflichtengesetz in Deutschland in Kraft. Für Unternehmen bedeutet das in erster Linie noch mehr Dokumentation. Stephan Feige, Market Director Logistics bei d.velop, erläutert, wie innovative Software-Lösungen dabei helfen können, komplexe Compliance-Anforderungen in den Griff zu bekommen.

Seit dem 01.01.2023 gilt das neue Lieferkettensorgfaltspflichtengesetz in Deutschland für Unternehmen mit mehr als 3.000 Beschäftigten. Ab Anfang 2024 wird es auch für Firmen mit mehr als 1.000 Mitarbeitenden zur Pflicht. Unternehmen müssen nun einen umfassenden Katalog von Verboten beachten, wozu unter anderem Zwangs- und Kinderarbeit sowie Missachtung von Gesundheitsschutz zählen. Die wichtige Neuerung dabei ist, dass Unternehmen nicht nur für eigene Werke oder Niederlassungen verantwortlich sind, sondern für ihre gesamte Lieferkette. Die unternehmerische Sorgfaltspflicht erstreckt sich also auch auf Aktivitäten von Vertragspartnern und Zulieferern. Das Gesetz sieht umfassende Dokumentations- und Aufbewahrungspflichten vor, bei deren Verletzung empfindliche Strafen drohen. Bis zu acht Millionen Euro oder zwei Prozent des weltweiten Jahresumsatzes können verhängt werden.

Für die Berichtspflichten, die sich aus dem Lieferkettengesetz ergeben, sind besonders diese Dokumente relevant:

- Vertragsdokumente
- Verhaltensvorschriften und Verhaltenscodizes
- Jahresberichte und Dokumentationen zur Einhaltung der Sorgfaltspflichten
- Grundsatzerklärungen
- Risikoanalysen und Risikoberichte
- Beschwerdeverfahren
- Lieferantenzertifizierungen

In großen Unternehmen können so schnell enorme Datenmengen entstehen. Dennoch brauchen Verantwortliche schnellen und zentralen Zugriff auf alle relevanten Informationen. Dokumenten-Management-Systeme helfen ihnen dabei, all das zu gewährleisten.

Dies sind die vier wichtigsten Vorteile:

1. Digitale Lieferantenakten sorgen für Überblick

Die Lieferkettenstruktur sowie eventuelle Verletzungen von Vorgaben und Maßnahmen sind kontinuierlich und vollständig zu dokumentieren. Anfallende Dokumente sollen die Transparenz von Produktionsabläufen sowie Lieferantenbeziehungen sicherstellen und müssen sieben Jahre aufbewahrt werden. Ohne entsprechende Lösungen, die der digitalen Ablage Struktur verleihen, kann hier schnell Chaos entstehen. Um die dadurch drohende Komplexität in den Griff zu bekommen, sollten Unternehmen auf ein Dokumenten-Management-System setzen, das die für das Lieferkettengesetz relevanten Dokumente in digitalen Lieferantenakten transparent und schnell zugänglich archiviert und so die geforderte ortsunabhängige Aufbewahrungspflicht sicherstellt.

2. Vertrags-Management schafft Transparenz

Durch einen Wechsel in das Vertrags-Management-System können Lieferantenverträge schnell und praktisch abgerufen, gemeinsam bearbeitet und Fristen automatisiert eingehalten werden.

Diese Vertragsdokumente spielen eine wichtige Rolle, wenn es darum geht, Transparenz in Produktionsabläufen sicherzustellen. Digitales Management dieser Unterlagen sorgt dafür, dass sie von überall aus abgerufen werden können, Fristen stets im Blick bleiben und die Verträge bei Bedarf einfacher abgeändert und sogar kollaborativ bearbeitet werden können.

3. Hinterlegte Risiken helfen bei Anpassungen

Das Gesetz fordert auch, mögliche Risiken in Lieferantenverträgen zu hinterlegen, um Aussagen über die Wahrscheinlichkeit von Anpassungen innerhalb einer Lieferkette treffen zu können.
Umsetzen lässt sich das beispielsweise über Listen innerhalb des Lieferantenvertrages, wo bestimmte Risiken beispielsweise für Umwelt oder Menschenrechtsverletzungen erfasst und in ihrer Schwere quantifiziert werden. Auch für die Verwaltung und Anpassung solcher komplexen Dokumente ist ein modernes Vertrags-Management-System eine enorme Hilfe.

4. Probleme erkennen mit digitalem Beschwerde-Management

Unternehmen müssen im Rahmen des Lieferkettengesetzes auch Beschwerdeverfahren einrichten. Dieses richtet sich sowohl an direkt Betroffene als auch an Mitarbeitende im Unternehmen, die Kenntnis von Verstößen haben.
Unternehmen stehen also vor der Herausforderung, ein System zu etablieren, zu dem alle Beteiligten entlang der Lieferkette Zugang haben. Dazu sollten Verantwortliche zunächst den Austausch mit Mitarbeitenden und Zulieferern suchen, um die individuellen Gegebenheiten zu analysieren.

Anschließend müssen alle Beschwerden erfasst und transparent für das Berichtswesen dokumentiert werden. Ebenso müssen Maßnahmen beschrieben sein, wie Verstöße in der Lieferkette künftig verhindert werden. Spätestens hier sollten digitale Lösungen zum Einsatz kommen, die das Management der Eingaben erleichtern.

DataLocker

Professionelle USB-Speichermedien mit Level 3 Zertifizierung und Selbstzerstörungsmodus

DataLocker Spezialist für verschlüsselte Speichermedien und USB-Sicherheit, senkt für externe Festplat- ten und SSDs der Serie DL4 FE bekannt.

DataLocker DL4 FE bietet ein kompaktes Format (12,3 x 7,7 x 2,1 cm) und einen integrierten, farbigen Touchscreen aus, über den die Konfiguration und die Authentifizierung erfolgen. Die Speicherlösung ist in Festplatten- und SSD-Varianten erhältlich und in Kapazitäten von 500 GB bis 15,3 TB verfügbar. Zur Ausstattung des unabhängig vom Betriebssystem einsetzbaren Laufwerks zählen eine USB-C Schnittstelle und ein Kensington Lock.

Wichtige Sicherheitsmerkmale der DL4 FE Serie:

Passwort-Komplexität und Passwortlänge
Der Administrator kann festlegen, ob Buchstaben, Ziffern und Sonderzeichen verwendet werden müssen und welche Mindestlänge ein Passwort erfüllen muss (8 – 64 Zeichen). Das US-amerikanische NIST (National Institute of Standards and Technology) empfiehlt für sichere Passwörter ein Minimum von acht Zeichen. Mit DL4 FE sind zudem echte alphanumerische Passwörter mit Sonderzeichen möglich. Dies stellt ein besonderes Sicherheitsmerkmal dar, da vergleichbare Produkte meist lediglich mit einer alphanumerischen Tastatur ausgestattet sind, die jedoch ausschließlich die Eingabe numerischer PIN-Codes ermöglicht.

Selbstzerstörungsmodus bei Brute-Force-Angriffen
Wird zu oft das falsche Passwort eingeben (konfigurierbar von 10 – 50 Fehleingaben), erfolgt automatisch ein Factory Reset (Zurücksetzen auf den Auslieferungszustand), bei dem der AES-Schlüssel und sämtliche Daten gelöscht werden, das Laufwerk jedoch wieder verwendet werden kann. Alternativ kann der sogenannte „Detonations-Modus" aktiviert werden, bei dem zusätzlich die Firmware gelöscht wird und das Laufwerk somit als physikalisch defekt gilt.

Silent Kill
Neben dem Administrator- und dem Benutzerkennwort lässt sich ein drittes Kennwort konfigurieren, bei dessen Eingabe sofort der Selbstzerstörungsmodus in Form von Factory Reset oder Detonations-Modus ausgeführt wird.

FIPS-140-2 Level 3 Zertifizierung
Diese Zertifizierung betrifft vor allem die physikalische Manipulierbarkeit des gesamten Laufwerkes und wird von vielen Organisationen als besonders sicher anerkannt.

Swisscom Trust Services.

Schafft die Passwörter ab!

Log-ins mit Nutzernamen und Passwort sind nicht nur lästig, sondern können auch gefährlich werden. Social Engineering und Phishing sind der einfachste Weg für Cyberkriminelle, um sich Zugang zu Nutzerkonten zu verschaffen. Es wird Zeit für nutzerfreundlichere und sicherere Alternativen, findet Mario Voge, Head of Growth Management bei Swisscom Trust Services.
„Laut dem Data Breach Investigations Report 2022 von Verizon sind Datendiebstähle mit etwa 40 Prozent der häufigste Angriffsvektor von Cyberkriminellen.

Diese Daten erbeuten sie auf relativ profanen Wegen wie Phishing oder Social Engineering, die keine besonderen IT-Kenntnisse voraussetzen. Dies bedeutet, heute kann praktisch jeder Cyberkrimineller werden, ‚Hacken' ist also gar nicht nötig. Wohl auch ein Grund dafür, warum das Cyber-Crime-Geschäft boomt.
Das ‚altbewährte' Passwort und seine Schwachstellen sind also ursächlich für eine Vielzahl von Cyber-Vorfällen. Seitdem es Passwörter gibt, predigen Experten, wie diese aussehen sollen, dass man sie häufig wechseln und nicht doppelt verwenden soll. Kaum jemand hält sich an all diese Empfehlungen und die Bequemlichkeit rächt sich allzu oft. Es wird Zeit für neue, innovative Konzepte zur Nutzerverifizierung im Netz, die sich nicht so einfach kompromittieren lassen und angenehmer in der Handhabung für die Nutzer sind. Bereits 2013 wurde die FIDO-Allianz gegründet, die sich für

eine passwortlose Zukunft einsetzt. An die Stelle von Passwort und Nutzername tritt bei diesem Ansatz asymmetrische Kryptografie. Ein Nutzer verifiziert seine Identität über einen privaten Schlüssel, der auf einem Gerät gespeichert ist. Das kann ein USB-Stick sein oder direkt die Hardware eines Mobiltelefons. Dieser Schlüssel muss das Gerät dabei gar nicht verlassen, was die Methode sehr sicher macht. Bei einer Authentifizierungsanfrage wird eine sogenannte Challenge an das jeweilige Gerät gesendet, deren Lösung nur mithilfe des privaten Schlüssels möglich ist und wodurch ein Nutzer seine Identität nachweist.

Ein entscheidender Aspekt, mit dem diese Form der digitalen Authentifizierung steht und fällt, ist die initiale Identifikation eines Nutzers. Schließlich muss sichergestellt werden, dass sich hinter einem privaten Schlüssel auch wirklich die angegebene Person verbirgt. Mit BankIdent oder KI-gestützter Videoidentifikation stehen uns dafür heute sehr effiziente und nutzerfreundliche Methoden zur Verfügung. Ein weitergreifendes Konzept stellt die Self-Sovereign Identity oder kurz SSI dar. Anwender erhalten hierbei die Möglichkeit, dezentral in einem Wallet eine Art digitales Abbild ihrer Identität zu erschaffen, um sich im digitalen Raum eindeutig identifizieren zu können.Dies macht das Leben in der vernetzten Welt an vielen Stellen erheblich einfacher: Kunden müssen sich beispielsweise nicht bei jedem Online-Shop aufs Neue anmelden und können sogar die Bezahlung über ihre zentrale Identität abwickeln, wenn sie dies wünschen. Es spricht nichts mehr dagegen, im Jahr 2023 nun wirklich das Ende des Passworts einzuläuten, das schon so oft angekündigt wurde."

G DATA

Sicherheitslücke in VMware ESXi - Patch dringend erforderlich

Eine kritische Sicherheitslücke in der Virtualisierungsplattform von VMware wird derzeit aktiv ausgenutzt, um Serversysteme in aller Welt anzugreifen. Ein Patch für die zwei Jahre alte Lücke ist verfügbar und sollte umgehend installiert werden.

Pünktlich zum Wochenende meldete unter anderem das französische CERT (CERT-FR) eine Angriffswelle gegen Systeme, auf denen VMware ESXi in den Versionen 6.5.x, 6.7.x sowie 7.x läuft (Details auf der Webseite von VMware).

Das Brisante daran: Die Sicherheitslücke mit der Kennung CVE-2021-21974 ist bereits seit zwei Jahren bekannt und gepatcht. Die Angriffe richten sich also gezielt gegen ungepatchte Systeme. Die Schwachstelle hat einen Kritikalitätswert von 9.8 – die höchstmögliche Zahl ist 10. Viel kritischer wird es also nicht.

Sofortmaßnahmen

Auf erfolgreich angegriffenen Systemen wird die Nevada-Ransomware installiert, die unter anderem die virtuellen Festplatten der Gastsysteme verschlüsselt (Dateiendungen *vmdk, *vmx, *vmsd und andere). „Wer bisher die Patches nicht installiert hat, sollte hier schnellstens aktiv werden", sagt Tim Berghoff, Security Evangelist bei der G DATA CyberDefense AG. „Verschlüsselte Systeme sorgen teilweise für Ausfälle, unter anderem bei einem italienischen Telekommunikationsanbieter." Um Angriffe zumindest vorerst zu blocken, wird empfohlen, das SLP-Protokoll auf ungepatchten Hypervisor-Systemen zu deaktivieren.

Dazu sind in der Shell die folgenden Kommandos erforderlich:

Ausführliche Informationen finden sich in der VMware Knowledge Base.

„Auch wenn es keine erkennbaren Zeichen eines Angriffs gibt, lohnt es sich nach IoC (Indicators of Compromise) zu suchen", rät Berghoff.

Altlasten rächen sich bitter

Diese aktuelle Angriffswelle zeigt wieder einmal, wie wichtig es ist, Patches zu installieren. Auch eine alte Sicherheitslücke kann zum Problem werden – manchmal auch erst Jahre später, wie in diesem Falle. Beispiele dafür gibt es genug. Eines der berühmtesten Beispiele, bei dem auch Heimanwender betroffen waren, ist WannaCry. Die hier zugrunde liegende Lücke war zum Zeitpunkt des Ausbruchs bereits seit einem Vierteljahr bekannt und gepatcht.

www.vmware.com/security/advisories/VMSA-2021-0002.html

Der Baumarkt
ein Paradies für Diebe

Die Verschönerung der eigenen vier Wände, Garten miteingeschlossen, ist ein großer Verbrauchertrend, der in erster Linie durch die pandemiebedingten Schließungen, aber auch durch Heimarbeit und aufstrebende Social-Media-Kanäle, die schöne Häuser und Gärten promoten, angetrieben wird. Einer der Gewinner dieser Entwicklung sind Baumärkte.

Aber wie es bei den meisten Dingen ist, gilt auch hier: Wo Licht ist, ist auch Schatten. Baumärkte sind nicht nur bei Käufern beliebt, sondern gelten mit ihrer Kombination aus leicht zu stehlenden Kleinteilen und hochwertigen Elektrowerkzeugen auch als „Paradies" für Diebe. Und da das Interesse am Heimwerken wächst, wissen Diebe, dass sie die gestohlene Ware leicht weiterverkaufen können, was Diebstähle noch interessanter und wahrscheinlicher macht.

Umso wichtiger ist es deshalb für Baumarktbetreiber, effektive Artikelschutz-Maßnahmen zu ergreifen – aber das ist leichter gesagt, als getan. Baumärkte stellen in Sachen Sicherheit eine Herausforderung dar, denn sie sind nicht nur sehr groß und haben in der Regel weitläufige Außenbereiche, sondern Baumarkt-Kunden sind es zudem gewohnt, nahezu alle Artikel in die Hand nehmen und testen zu können. Dies sind Schwach-

stellen, wenn es um den Warenschutz geht, denn es lässt Dieben viel Spielraum, Produkte unbemerkt zu verstecken, Kartons zu öffnen, Umreifungsbänder aufzuschneiden oder Artikel „einfach" zu entwenden.

Die Zukunft der Artikelsicherung

Checkpoint Systems bietet mit seinen EAS/RFID-Systemen der nächsten Generation eine Reihe von Schutzoptionen, um Produkte in diesem anspruchsvollen Umfeld zu schützen. Ein Beispiel sind die Alpha-Lösungen, die speziell für sehr diebstahlgefährdete Produkte konzipiert wurden. Zu dieser Lösungsklasse gehören CableLoks®, Mini NeedleLok™ Tag, Spider Wraps® zum Schutz großer, sechsseitiger Verpakkungen, offene Display-Lösungen und manipulationssichere Verpakkungsbänder, die einen lautstarken Alarm auslösen, wenn jemand versucht, die Verpackung zu öffnen. Neben der verbesserten Artikelsicherung ist der größte Vorteil der Alpha-Reihe, dass sie den potenziellen Käuferinnen und Käufern gestatten selbstständig Artikel zu berühren und auszuprobieren. Das sichert die Kundenzufriedenheit und wirkt sich positiv auf den Umsatz aus.
Ein weiterer Artikelschutz der nächsten Generation ist das neue RF Metal™-Etikett, das speziell zum Schutz von Metallgegenständen wie Farbdosen, Bohrer und Schraubenschlüssel entwickelt wurde. Bisher war die Sicherung metallischer Artikel ein Problemfeld und oftmals blieb nur das Wegschließen in Vitrinen. Der Grund: Das Metall absorbiert RF-Energie und macht dadurch die Elektronische Artikelsicherung so gut wie unmöglich. Das neue Metalletikett schließt nun diese Sicherheitslücke und bringt noch weitere Pluspunkte mit sich: Es kann zum Beispiel an der Quelle oder im Geschäft angebracht werden, hat nur minimale Auswirkungen auf das optische Erscheinungsbild der Produkte, und es wirkt visuell abschreckend auf potenzielle Diebe. Das ermöglicht es Einzelhändlern metallische Artikel offen an erstklassigen Stellen zu platzieren. Das RF-Metall-Etikett lässt sich mit allen EAS-Antennenlösungen von Checkpoint System kombinieren.
Auch im Bereich Antennenlösungen für Baumärkte wurden erhebliche Fortschritte gemacht. Besonders geeignet sind die Antennen der NEO-Reihe wie die robuste NEO™ NP10-Antenne. Der entscheidende Faktor bei diesen Lösungen ist, dass sie einen größeren Erfassungsbereich besitzen und deshalb weiter voneinander entfernt aufgestellt werden können. Dies ermöglicht nicht nur breitere Gänge in Baumärkten, sondern macht sie auch optisch weniger aufdringlich bei gleichzeitig verbessertem Produktschutz.
Sie bieten aber noch weitere Boni: Die integrierte drahtlose Konnektivität von NEO macht die Installation dieser Antennen einfacher und erfordert weniger Verkabelung. Zudem können die NEO-Lösungen direkt mit dem Filialnetz, dem Mobilfunknetz und der Checkpoint-Cloud-Plattform verbunden werden.

Zusätzlich zu diesen neuen und bewährten Lösungsklassen, bietet Checkpoint Baumärkten auch den Service Check&Secure®. Dieser beinhaltet einen Store-Audit geschützter und nicht geschützter Artikel, Beratung zur Optimierung der Artikelsicherung und einen Pilotversuch, der zeigt, wie EAS den Warenschwund reduzieren und den Umsatz steigern kann.

Alpha-Lösungen in der Praxis

Praxis ist eine der größten Baumarktketten in den Niederlanden und bietet eine Kombination aus kompakten City-Märkten, größeren mittelgroßen Filialen, Megastores und Online-Shopping. Vor kurzem testete das Unternehmen in vier Filialen die Sicherheitslösung Alpha S3vx von Checkpoint, um hochwertige Artikel besser vor Dieben zu schützen, die illegale Öffner verwenden, mit denen Produkte und deren Sicherheitsvorrichtungen voneinander getrennt werden.

Die Alpha S3vx verhindern illegale Öffnungen durch eine doppelte Sicherung: einen extrastarken Öffner und einen Verifizierungscode, der für jede Filiale einzigartig ist. Wie gut das funktioniert, zeigte sich in dem 4-monatigen Test. In diesem Zeitraum konnten die Diebstähle in den Praxismärkten um 50 Prozent gesenkt werden, u. a. bei Produkten von Bosch, Grohe, Makita und Worx. Und da die Verluste zurückgingen, verbesserte sich auch die Produktverfügbarkeit, was zu einem besseren Kundenerlebnis beitrug.

Nach dem erfolgreichen Pilotprojekt hat Praxis die Alpha S3vx-Lösung auf die Hälfte seiner Filialen ausgeweitet, die andere Hälfte soll noch in der ersten Hälfte des nächsten Jahres ausgestattet werden.

dormakaba

Produktionsstätte in Indien wird mit Solarenergie betrieben

Andy Jones, President Region Asia Pacific, weihte das Solarkraftwerk vor Ort ein. ©dormakaba

dormakaba gibt die Einweihung des Photovoltaik-Kraftwerks in seiner Produktionsstätte in Mahindra World City, Chennai, bekannt. Ausgestattet mit 440 Solarmodulen verfügt der Standort über eine installierte Leistung von 240 Kilowatt Peak (kWp), genug, um den aktuellen Energiebedarf aus eigenen erneuerbaren Energien zu decken.

Ein Kernelement von dormakabas Klimaschutz-Strategie ist die Ausweitung der Installation von Solarmodulen, insbesondere in Regionen, in denen Ökostrom nicht ohne Weiteres auf dem Markt verfügbar ist. Im Rahmen dieses Ansatzes hat dormakaba im Geschäftsjahr 2018/19 mit der Installation von Solarpanels auf dem Dach seiner Produktionsstätte in Chennai begonnen. Im letzten Geschäftsjahr 2021/22 wurde die Installation weiter ausgebaut und im Januar 2023 abgeschlossen. dormakaba hat sich im Rahmen seiner Strategie Shape4Growth verpflichtet, ein in der Branche füh- rendes Nachhaltigkeitskonzept mit mehr als 30 ambitionierten ESG-Zielen umzusetzen. Im Geschäftsjahr 2021/22 erreichte dormakaba eine Reduzierung der CO2-Emissionen (Scope 1 und 2) um 2.4% gegenüber dem Vorjahr. Per 30. Juni 2022 waren bei 67% der unternehmenseigenen Produktionsstandorte, lokalen Montagestandorte und regionalen Logistikzentren Energiemanagementsysteme eingeführt (Vorjahr: 21%). "Wir haben schrittweise Massnahmen ergriffen, um den CO2-Fussabdruck unserer Geschäftstätigkeit in Indien zu verringern. Die Investition in Sonnenkollektoren wird uns unabhängiger von fossilen Brennstoffen machen. Dies ermöglicht es uns, erneuerbare Energien zu nutzen und nachhaltige Produkte für die Zukunft zu entwickeln", sagt Natesh Balakrishna, Senior Vice President, Market India. "Mit diesem weiteren Ausbau der Solarenergieerzeugung demonstrieren wir unsere Führungsrolle beim Übergang zu einer kohlenstoffarmen Wirtschaft innerhalb der Branche für Zutrittslösungen und darüber hinaus", fügt Andy Jones, President Region Asia Pacific, hinzu, der das Solarkraftwerk vor Ort einweihte.

Nachhaltigkeitsbericht unter https://tinyurl.com/d7evrncy

Accenture

SKS-Gruppe erworben

SAP- und andere Regulatorien für Bankkunden in der DACH-Region im Fokus

Accenture hat vereinbart, die SKS-Gruppe zu übernehmen, ein Beratungsunternehmen, das Banken in Deutschland, Österreich und der Schweiz bei der Modernisierung ihrer technologischen Infrastruktur und bei der Erfüllung regulatorischer Anforderungen mit SAP S/4HANA-Lösungen unterstützt. Die Bedingungen der Transaktion wurden nicht bekannt gegeben.

Mit der Übernahme erweitert Accenture seine Kompetenzen in den Bereichen Technologie, Beratung und regulatorische Dienstleistungen und verbessert gleichzeitig seine Fähigkeit, spezialisierte Banken zu bedienen, wie zum Beispiel nationale Förderbanken, die lokale Unternehmen und Gemeinden finanziell und bei der Entwicklung unterstützen.
Das Team der SKS-Gruppe mit Hauptsitz in Hochheim, Deutschland, besteht aus rund 500 Fachleuten und wird von Accenture Technology übernommen. Die Transaktion umfasst alle Geschäftsbereiche der SKS-Gruppe, die Finanzinstitute bei der Entwicklung, der Implementierung und dem Betrieb von SAP-Lösungen für Kernbankdienstleistungen und Analytik unterstützen. Darüber hinaus verfügt die SKS-Gruppe über ein umfangreiches Angebot an Risiko-, Regulierungs- und Compliance-Funktionen, darunter das Observatory-Tool, das die regulatorischen Anforderungen abbildet und Banken bei der Verwaltung ihrer Meldeprozesse unterstützt.

Klüh Security

Airport-Großauftrag um fünf Jahre verlängert

Mitteldeutsche Flughafen AG setzt langjährige Partnerschaft mit Klüh Security fort

Die Mitteldeutsche Flughafen AG, Klüh-Kunde seit 2003, hat die bestehende Zusammenarbeit mit der Security-Sparte des Düsseldorfer Familienunternehmens zum 1. Januar 2023 um weitere fünf Jahre verlängert. Der Auftrag beinhaltet umfassende Sicherheitsdienstleistungen an den Flughäfen Dresden und Leipzig/Halle.

„Wir sind sehr stolz darauf, die Mitteldeutsche Flughafen AG schon so lange unterstützen zu dürfen. Dies zeigt uns, dass unsere Strategie aufgeht, Kunden flexible, genau auf sie zugeschnittene Lösungen auf Basis unseres fundierten Knowhows und unserer langjährigen Erfahrung zu bieten", erklärt Axel Hartmann, Geschäftsführer Klüh Security.

Zu dem breit gefächerten Aufgabengebiet der insgesamt rund 250 Sicherheitskräfte gehören Zugangskontrollen, Streifen- und Interventionsdienste,Terminalaufsicht sowie Luftsicherheits- und Frachtkontrolle.

Am Flughafen Dresden kommen noch weitere Services wie Parkaufsicht und Gepäckwagendienst hinzu. Für die technische Unterstützung setzt Klüh Security auf Röntgenscanner zur Durchleuchtung des Handgepäcks, Torsonden für Personenkontrollen sowie ein Wächterkontrollsystem, um alle abzusichernden Bereiche jederzeit teamübergreifend im Blick zu behalten. Eine Pkw-Flotte für die Streifenfahrten komplettiert die technische Ausstattung.

Tribut an eine heterogene Wohnbevölkerung

Übersich über Produkte, Konflikte in Wohngebäuden entschärfen

Jeder Mieter und jede Mieterin hat ganz unterschiedliche Bedürfnisse: die eine bestellt um 23 Uhr die erste Pizza, während der andere da längst schlafen will. Da gibt es Menschen mit Frühschicht, Spätschicht, Klavieren oder Haustieren, und es treffen oft ganz unterschiedliche Kulturen aufeinander.

Damit das gute Miteinander so reibungslos wie möglich gelingt, reichen oft wenige technische Nachrüstungen, die sehr große Effekte erzielen:

Für ruhebedürftige Bewohner:
Laut ins Schloss fallende Türen sind für viele ein Ärgernis. Vor allem, wenn sie ganz in der Nähe von Türen wohnen, die geschlossen bleiben müssen, wie Haustüren, Türen zu Tiefgaragen

oder Brandschutztüren. Hier hilft ein Türschließer mit Close-Motion-Technologie, der Türen erst abdämpft und dann sanft zuzieht. So entstehen weder ein störendes Geräusch noch eine Erschütterung. Zusätzlich können Absenkdichtungen (Foto oben) an Wohnungstüren oder Geschosstüren vor Lärm, Schmutz, Licht, Gerüchen und sogar Ungeziefer schützen. Diese schließen den störenden Spalt unter Türen und tragen so auch zur Energieeffizienz bei. Sie sind einfach und schnell auch nachträglich montierbar.

Für schutzbedürftige Bewohner: Der altbekannte Konflikt der offenen oder geschlossenen Haustür, der oft zwischen älteren und jüngeren Mietern entsteht, lässt sich durch den Mediator aus der Welt schaffen. Das selbstverriegelnde Fluchttürschloss

mit elektrischem Türöffner sorgt dafür, dass die Haustür von außen immer verschlossen ist, von innen aber jederzeit offen.

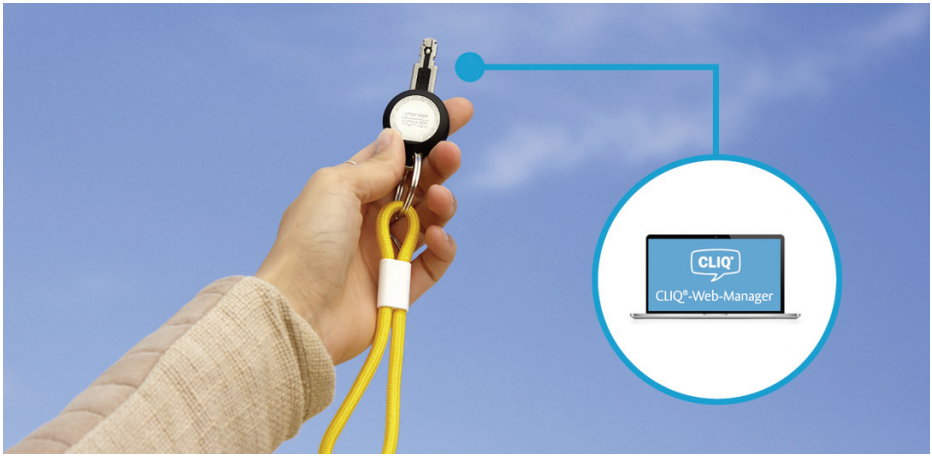
Für lebenslustige Bewohner:
Auch sie lieben den Mediator, da er Freunde und den Pizzaboten nachts ungehindert ins Haus und wieder hinauslässt, ohne dass man selbst zur Haustür laufen muss, um aufzuschließen (Foto oben).

Für kleine Bewohner und entspannte Eltern:
Kinderfinger sind zart und werden leider nur zu schnell in einen Türspalt geklemmt. Hier hilft ein Fingerschutzrollo, den Spalt zwischen Tür und Zarge zu schließen und die Finger zu schützen (Foto unten).
Es lässt sich schnell auch nachträglich installieren und an viele Bausituationen anpassen. Auch lassen sich Tast-

schalter zum Türöffnen in einer bestimmten Höhe anbringen, so dass kleine Kinder das Gebäude nicht unbemerkt verlassen können.

Für Hausmeister und Dienstleister:
Der Hausmeister hat Zugang zu allen für ihn wichtigen Räumen, der Paketbote darf aber nur bis zu den Briefkästen und das Putzteam nur in die Treppenhäuser. (Foto oben)Kein Problem: mit eCLIQ erhalten alle die passenden Zugangsberechtigungen und Zugangszeiten. So kann auch ein Missbrauch der Schlüssel zu anderen Zeiten ausgeschlossen und die Benutzung zu jeder Zeit nachvollzogen werden.

Für Schlüsselverlierer:
Verlorene Schlüssel führen meist zu hohen Kosten und daher zu Panik. (Foto unten) Bei mechanischen Schließanlagen müssen Zylinder in



der gesamten Anlage getauscht werden, weshalb viele den Schlüsselverlust möglichst lange verschweigen. Mit eCLIQ können verlorene Schlüssel einfach ausprogrammiert werden und es besteht keinerlei Sicherheitsrisiko mehr durch unehrliche Finder.

Für Altbaufans:
Selbst Nostalgiker und Verwalter historischer Bauten finden keine Argumente gegen den Einsatz von eCLIQ: Historische Türen werden nicht durch überstehende Zylinder oder Aufbauten „verschandelt", sondern sehen genauso aus wie zuvor (Foto oben). Sie müssen auch nicht verdrahtet oder verkabelt werden – die Substanz bleibt damit vollständig erhalten. Ein Beispiel von vielen ist das Referenzobjekt „Wohn-und Geschäftshaus in Erfurt".

Für alle, die eigentlich keine Veränderung mögen:
Neben der gewohnten Optik bleibt auch die gewohnte Handhabung: der eCLIQ Schlüssel wird wie ein mechanischer Schlüssel einfach in den Zylinder gesteckt und umgedreht. (Foto unten) Es ist also keinerlei Umgewöhnung nötig. Ganz im Gegenteil: der Wendeschlüssel macht die Handhabung sogar noch einfacher, ist es doch egal, wie man ihn in den Zylinder steckt.

Für Menschen mit Einschränkungen und Lieferdienste:
Schwellenlose Eingangstüren erleichtern den Zugang mit Rollstuhl, Rollator, Kinderwagen und Sackkarre. Hier sorgen Absenkdichtungen für Dichtheit gegen Schlagregen und Barrierefreiheit in einem.

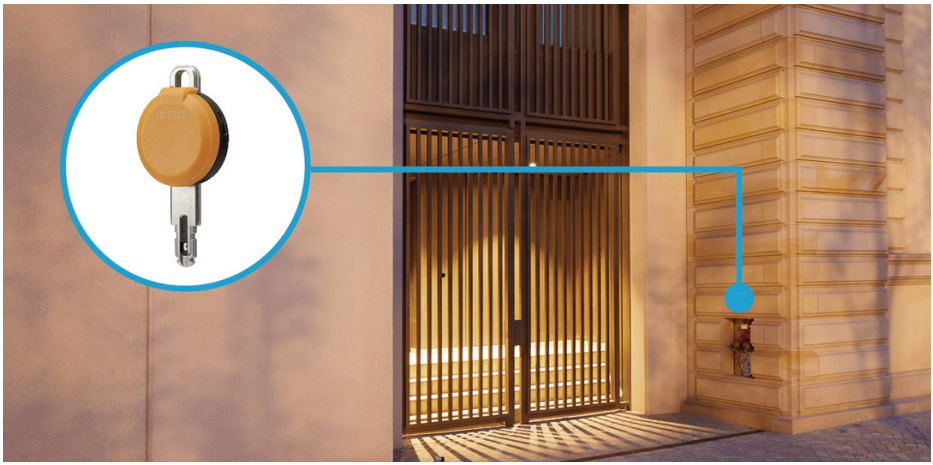
Türschließer mit Cam-Motion Technologie erfordern weniger Kraftaufwand für das Öffnen und Schließen von Türen als herkömmliche Türschließer.

Für Rettungskräfte:
Im Brandfall verhindern geschlossene Türen die Ausbreitung von Rauch und giftigen Gasen (Foto oben). Für Bewohner in Panik sind diese Türen aber stets in Fluchtrichtung offen: So beschleunigt Rettungswegtechnik die Entfluchtung des Gebäudes und erleichtert Rettungskräften den Zugang. Spezielle Schlüssel für die Feuerwehr erhöhen das Sicherheitslevel.

Für Leseratten:
Viele Verwalter, Investoren und Leiter Gebäudetechnik sind auf der Suche nach funktionierenden Gesamtlösungen, die das komplette System „Tür" im Blick haben. (Foto unten) Das garantiert ein perfektes Zusammenspiel der einzelnen Komponenten. Diese Lösungen rund um die Tür zeigt das eBook „Die komplette Sicherheitslösung für die Wohnungswirtschaft", das sichere und reibungslose Abläufe und Produkte für alle Wohnbereich vorstellt.

Für Filmfans:
Wer nicht lesen, sondern ganz konkret sehen möchte, wie sich der Einsatz moderner Sicherheitstechnik auf den Arbeitsalltag eines Leiters der Gebäudetechnik auswirkt, findet im Video „eCLIQ Schließanlagen in der Wohnungswirtschaft" dazu acht Situationen.

[https://youtu.be/ELZeuuKjeGQ]



SALTO Systems

Hotelschließ-systeme als Teil einer digitalen Gästereise

SALTO Systems ist in diesem Jahr erneut an zwei Ständen auf der INTERNORGA präsent. Das Unternehmen zeigt in der Halle A2 seine elektronischen Hotelschließsysteme als Teil der digitalen Gästereise bei der Unternehmenskooperation hotelnext.io am Stand 221 sowie bei dem Integrator Punktplanung am Stand 116.

SALTO ist mit seinen Hotelschließsystemen ein Vorreiter der Digitalisierung von Hotels. Die Lösungen verbessern die Sicherheit und tragen zu effizienteren Abläufen bei. Dank der vielfältigen Integrationen mit unterschiedlichen Hotelsystemen, z.B. Property Managementsysteme (PMS), digitale Hotelservices, Kiosksysteme, Raummanagement und Gebäudemanagement, lassen sich interne Prozesse automatisieren.
Das reduziert Kosten, vermeidet Fehler und gestaltet den Hotelbetrieb insgesamt effizienter. Entscheidend ist dabei das reibungslose Zusammenspiel der Systeme über geprüfte und stets aktuelle Schnittstellen. Dadurch können sich Hotelbetreiber auf eine zuverlässige Funktion verlassen und ihr Haus durchgängig digitalisieren. SALTO demonstriert die Vorteile der typischsten Integrationen – mit PMS und digitalen Hotelservices – mit seinen Partnern an beiden Ständen in Hamburg.

Die elektronischen Hotelschließsysteme von SALTO eignen sich für jede Art und Größe von Hotel. Sie ermöglichen die Türöffnung per RFID-Gästekarte, Mobile Access (BLE & NFC) und PIN.
Die Zutrittskomponenten binden Haupteingänge, Hotelzimmertüren, Seminarräume, Spa-Bereiche und Zufahrten sowie Büros, Service-Räume, Liftsteuerung, Verkaufsautomaten, Möbel und Spinde in eine einheitliche Zutrittslösung ein.

Die Hardware ist in diversen Oberflächen und zudem mit den unterschiedlichsten Drückergarnituren erhältlich. Sie fügt sich harmonisch in moderne wie klassische Inneneinrichtungen ein.
Die Hotellösungen von SALTO arbeiten nahtlos mit Drittsystemen zusammen, um Prozesse zu digitalisieren und zu automatisieren. Dazu gehören alle relevanten Hotel-PMS und Anbieter von digitalen Hotelservices sowie Raum- und Gebäudemanagementsysteme, Check-in-Lösungen, Kassenabrechnungssysteme sowie etliche Tourismuskarten.

SALTO Systems auf der INTERNORGA vom 10. bis 14. März 2023 in Hamburg: Halle A2, Stände 116 und 221.

Labor Strauss

Besseres Handling für Feuerwehren

MEP Feuerwehr Schlüsseldepot SD950 verspricht ein besseres Handling für Feuerwehren

Die Labor Strauss Gruppe ist ein führender europäischer Hersteller professioneller Gebäudesicherheitstechnik. Um den aktuellen Anforderungen der Brandschutzdienststellen zu entsprechen und den Feuerwehren im Ernstfall eine noch komfortablere Handhabung zu ermöglichen, hat die MEP Gefahrenmeldetechnik GmbH, eine Tochtergesellschaft der Labor Strauss Gruppe, das Schlüsseldepot SD950 entwickelt. Neben einem deutlich vergrößerten Innenraum bei gleichen Außenabmessungen punktet das Schlüsseldepot u. a. mit einer LED-Innenraumbeleuchtung sowie raffiniert positionierten Statusanzeigen. www.laborstrauss.com

Das neue Feuerwehr-Schlüsseldepot SD950 der MEP-Gefahrenmeldetechnik GmbH macht im Brandfall die schnelle und gewaltfreie Entnahme der diebstahl- und kopiergeschützten Objektschlüssel zu einer unkomplizierten Angelegenheit, denn die neue Generation von MEP-Schlüsseldepots bietet neben einer LED-Innenraumbeleuchtung zur Orientierung, bei gleichen Außenmaßen mehr Platz als sein Vorgänger. Es kann je nach Ausführung bis zu sechs überwachte Objektschlüssel aufnehmen, abhängig von Steckplatz und Variante der Konsole, auch in Überlänge bis zu 75 mm. Wer eine noch komfortablere Schlüsselentnahme bevorzugt, entscheidet sich für die optionale Flexkonsole, die bei Öffnung des Schlüsselkastens vorne schwenkt und so die Objektschlüssel im unmittelbaren Sichtradius des Bedieners bereitstellt.

In den Türknauf der Außentür haben die Entwickler von MEP elegant eine im Ruhezustand nicht wahrnehmbare Statusanzeige integriert, die bei entriegelter Außentür gelb blinkt bzw. rot blinkend einen Sabotagefall anzeigt. Falls die Objektschlüssel trotz hörbarem und haptisch wahrnehmbarem Einrasten unsachgemäß hinterlegt worden sein sollten, wird dies mittels integriertem Summer und zweifarbiger Statusanzeige, die bei geöffneter Außentür sichtbar ist, signalisiert.

Die serienmäßig eingebaute Heizung sorgt für ein ungehindertes Öffnen der Außentür auch bei niedrigen Temperaturen, zudem wird durch die Temperatur- und Feuchtigkeitsregelung die Betauung des Innenraumes auf ein Minimum reduziert.

Auch das solide Gehäuse in geschliffener V2A-Edelstahl-Ausführung überzeugt, denn bei optisch ansprechender Konstruktion mit einem fest verschweißten, integrierten Blendrahmen und einer bohrschutzüberwachten Außentür hält es sowohl mechanisch als auch elektrisch jedem Sabotageversuch stand. Zudem haben ungünstige Umwelteinflüsse aufgrund der hohen Korrosionsbeständigkeit keine Chance. Bei freistehenden Anwendungen in einer Schlüsseldepotsäule oder an/in Wänden mit Fassadendämmung wird eine sabotagesichere Einbauzarge mit Rundumbohrschutz verbaut.

Durch verschiedene Innentür-Varianten sind alle Feuerwehr-Schließungen realisierbar. Über den Anschlussadapter AD900-1 kann das Schlüsseldepot SD950 an Brandmelderzentralen beliebiger Hersteller angeschlossen werden.

Ein umfangreiches Zubehör für verschiedenste Anwendungsfälle, einfache Montagemöglichkeiten und im Lieferumfang enthaltenes Montagezubehör runden die überzeugenden Eigenschaften dieses gelungenen Produktes ab.

„Durch die enge Zusammenarbeit mit den Feuerwehren kennen wir die Anforderungen im Einsatzfall", erläutert Dipl.-Wirtschaftsing. (FH) Wolf-Dietrich Marschall, Vertriebsleiter der MEP-Gefahrenmeldetechnik GmbH. Die solide Ausführung und intelligente Konstruktion wurde auch beim FeuerTrutz-Award entsprechend gewürdigt: „Wir freuen uns, dass das MEP-Feuerwehr-Schlüsseldepot SD950 bei der Leserwahl zum Produkt des Jahres 2022 auf die Shortlist im Bereich „Anlagentechnischer Brandschutz" gewählt wurde" so Wolf-Dietrich Marschall.

Hexagon

GeoAI-Lösung für das Abwassermanagement in Köln entwickelt

Hexagons Safety, Infrastructure & Geospatial Division gab die erfolgreiche Bereitstellung einer GeoAI-Lösung (Geospatial Artificial Intelligence-Lösung) zur Rationalisierung des städtischen Abwasserbetriebs in Köln bekannt. Die Lösung erkennt automatisch Veränderungen von versiegelten Flächen, die sich auf die Entwässerung auswirken, und ermöglicht den Stadtentwässerungsbetrieben Köln, AöR (StEB Köln), die Abwassergebühren für private Grundstücke effizienter zu berechnen.

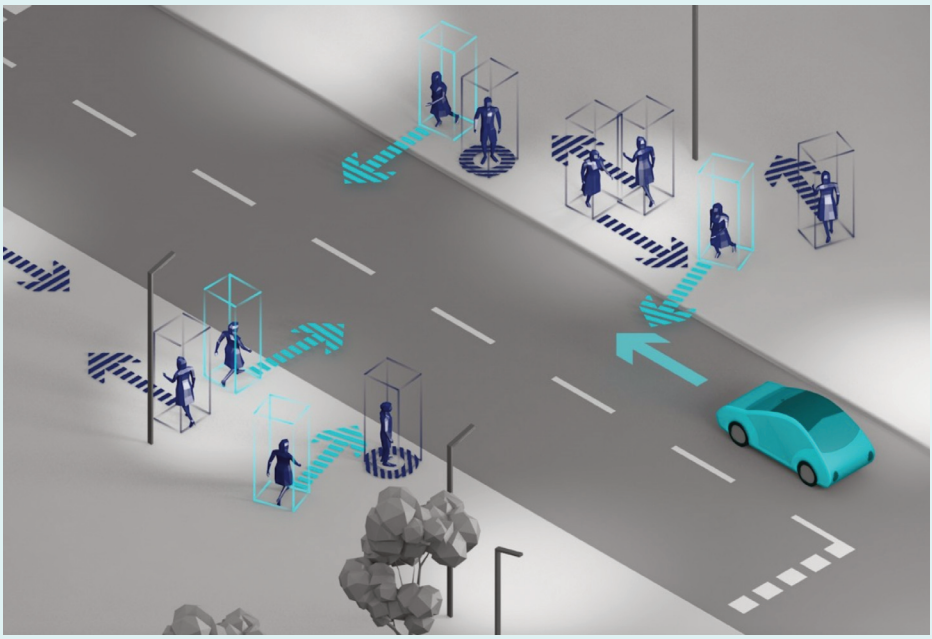
Vor dem Einsatz von GeoAI war das Steuerveranlagungsverfahren sehr arbeitsintensiv. Die Grundstückseigentümer meldeten nur selten die Vergrößerung oder Verkleinerung von versiegelten Flächen, so dass die StEB Köln die Informationen manuell erfassen und mit den Grundstückseigentümern abstimmen mussten.

Mithilfe von luftbild- und LiDAR-basierter Datenerfassung und auf Künstlicher Intelligenz gestützter Analysen identifiziert und klassifiziert die GeoAI-Lösung automatisch die Grundstücksflächen. Erkannt werden auch erschwerende Gegebenheiten wie Schatten, Vegetation und Dachüberstände, die die Auswertung beeinträchtigen könnten. Die daraus resultierenden Daten werden über eine Schnittstelle, die auf den Standards des Open Geospatial Consortium (OGC) basiert, im Unternehmens GIS der StEB zur Verfügung gestellt.

„Die Kernaufgabe der StEB Köln ist die Abwassersammlung und -reinigung, aber unsere Verantwortung erstreckt sich auf die gesamte Wasserwirtschaft der Stadt", sagt Jürgen Becker, stellvertretender Vorstand der StEB Köln. „Hexagon hat eine Lösung geliefert, die Prozesse automatisiert und es ermöglicht, uns auf die Qualitätskontrolle und die Verbesserung der wasserwirtschaftlichen Dienstleistungen für die Kölner Bürger zu konzentrieren."

Die GeoAI-Lösung von Hexagon umfasst den Leica CityMapper-2, ein hochleistungsfähiges luftgestütztes Bild- und LiDAR-Mappingsystem, die Bildanalysesoftware ERDAS IMAGINE und KI-Funktionen von Melowntech. Neben der Erkennung von Veränderungen an versiegelten Flächen kann die Lösung auch zur Simulation und Bewertung der Auswirkungen von Starkregenfällen und zur Identifizierung von Gebieten eingesetzt werden, die für eine Renaturierung zur Verbesserung des Stadtklimas geeignet sind.

„Die Nutzung von GeoAI zur Erstellung eines Digitalen Zwillings mit automatisierter Analyse bietet Kommunen leistungsstarke Anwendungen, um die urbane Lebensqualität zu verbessern", sagte Maximilian Weber, Senior Vice President EMEA, Hexagons Safety, Infrastructure & Geospatial Division. „Wir freuen uns, der Metropole Köln eine Lösung zur Verfügung stellen zu können, die sowohl die heutigen wasserwirtschaftlichen Dienste als auch das Klima der Stadt in Zukunft verbessern kann."



Forschung-Prototyp präsentiert

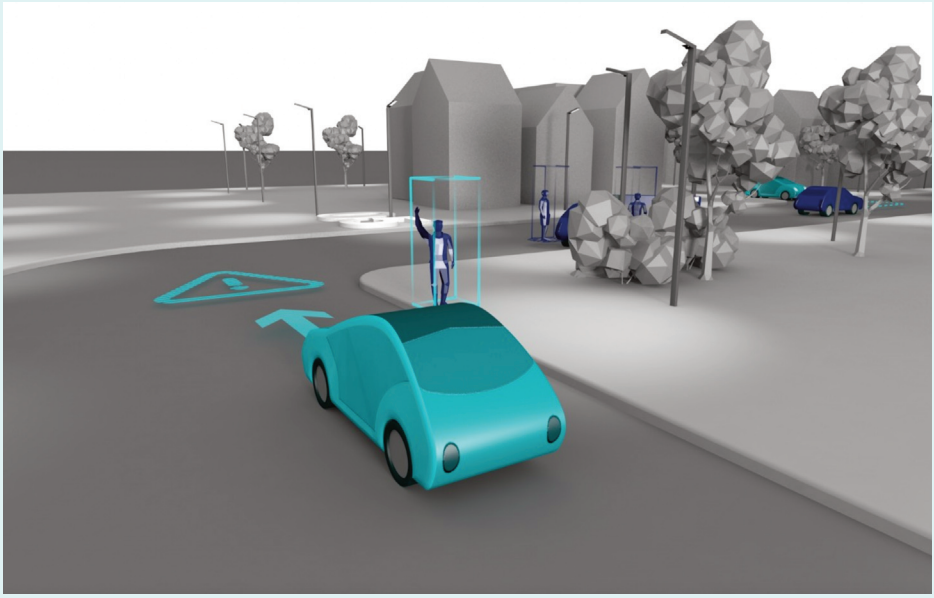
KI-System deutet Fußgängerverhalten, um Interaktion zwischen Auto und Passanten zu ermöglichen

Autofahren ist mehr als Gas geben, lenken und bremsen: Eine entscheidende Rolle spielt die Verständigung mit anderen Verkehrsteilnehmern.

Das autonome Fahrzeug der Zukunft muss deshalb unter anderem mit Fußgängern interagieren. Dazu muss es erkennen, welche Passanten relevant werden könnten, um sodann deren Verhalten zu erfassen und zu deuten. Einen Prototyp eines Systems, das mittels Künstlicher Intelligenz genau das leisten soll, hat nun das Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB in Karlsruhe vorgestellt.
Welche Passanten relevant sind für das Auto hängt davon ab, wo sie sich befinden und in welche Richtung sie laufen: Visualisierung eines im Projekt untersuchten Szenarios.

Ein weiteres Szenario im Projekt: Der Fußgänger winkt - das macht ihn relevant, auch wenn er keine Anstalten

Künstliche Intelligenz



macht, auf die Fahrbahn zu laufen. Will der Fußgänger die Straße überqueren oder nicht? Das ist für Manuel Martin eine Schlüsselfrage für seine Forschung.
Was ein menschlicher Autofahrer in der Regel intuitiv und ohne nachzudenken wahrnimmt, etwa anhand von Standort, Blickrichtung und Gestik, muss ein autonomes Fahrzeug erst beigebracht bekommen, um auch in einem Wohngebiet oder vor einer Schule sicher eigenständig agieren zu können. Verfahren der Künstlichen Intelligenz (KI) bieten das Potenzial, Videobilder dahingehend zu analysieren – aber müssen erst anhand großer Mengen an Trainingsdaten lernen, die richtigen Schlüsse zu ziehen.

Genau daran arbeitet der Diplom-Informatiker und wissenschaftliche Mitarbeiter des Fraunhofer IOSB im Rahmen des Forschungsprojekts »Intelligente Mensch-Technik-Kommunikation im gemischten Verkehr«, kurz INITIATIVE.

»Wir haben mittlerweile einen Forschungs-Prototypen umgesetzt, der abschätzt, ob ein Fußgänger die Straße überqueren möchte, seine Gesten analysiert und somit die Grundlage für die Interaktion schafft«, erklärt Martin. Das System bestehe aus einer Stereokamera, die räumlich »sehen« und somit die genaue Position von Passanten erfassen könne, und einem KI-Algorithmus, der die Positionen der Gliedmaßen erfasse und daraus Schlüsse ziehe. »Dieses System haben wir bei einer Projektpräsentation anlässlich der Halbzeit von INITIATIVE erfolgreich demonstriert«, so der IOSB-Forscher. »Nun geht es darum, die KI weiter zu trainieren und das System insgesamt zu verfeinern, damit es in allen denkbaren Situationen die Absichten der Fußgänger möglichst zutreffend erkennen kann.«

Das Fraunhofer IOSB vollzieht damit den Brückenschlag zwischen der Beobachtung des Fahrzeuginnen- und des Außenraums, wie der Leiter der Forschungsgruppe »Perceptual User Interfaces«, Dr. Michael Voit, hervorhebt: »Was bisher getrennte Welten waren, bringen wir nun zusammen: Die intelligente Erfassung des Verhaltens von Fahrer und gegebenenfalls Beifahrern durch unser Advanced Occupant Monitoring System – und die Erfassung anderer Verkehrsteilnehmer und ihrer Intentionen im Rahmen von

INITIATIVE.« Damit sei nun auch die Erfassung von Interaktionen zwischen Fahrer und Passanten möglich, was wiederum den Zugang zu neuen Forschungsfragen und Anwendungen eröffnet.

Auch im Forschungsprojekt INITIATIVE ist die Erkennung von Fußgänger-Intentionen nur ein Puzzleteil – das große Ziel ist hier, KI-gestützt die adaptive Kommunikation verschiedener Verkehrsteilnehmer zu ermöglichen, um automatisierte Fahrzeuge in gemischte Verkehrsszenarien integrieren zu können.

Dazu sollen letztlich umfassende Kommunikationsschnittstellen für die Interaktion des Fahrzeugs sowohl mit sonstigen Verkehrsteilnehmern als auch mit seinen eigenen Insassen entwickelt werden. Beispielsweise soll das Auto einem überquerungswilligen Fußgänger mittels einer unmissverständlichen Leuchtanzeige mitteilen können, dass es anhalten wird oder vorbeifahren möchte. Gestartet im April 2021, wird INITIATIVE vom Bundesministerium für Wirtschaft über drei Jahre mit insgesamt gut 4 Millionen Euro gefördert. Beteiligt an dem Projekt sind außerdem der Lichttechnik- und Elektronik-Zulieferer HELLA GmbH & Co. KGaA (Koordination), das Würzburger Institut für Verkehrswissenschaften (WIVW), die Electric Special Photronicsysteme GmbH, die version 1 GmbH, das Institut für Rechtsinformatik der Universität des Saarlandes sowie das Lichttechnische Institut und das Institut für Regelungs- und Steuerungssysteme des Karlsruher Instituts für Technologie (KIT).

BHE

Norm-Entwurf DIN VDE V 0826-20 – Vorstellung bei Perimeter Protection 2023

Insbesondere bei der Absicherung von kritischer Infrastruktur kommt den Perimeter-Sicherungs-Systemen (PSS) eine tragende Rolle zu. Der entscheidende Vorteil dieser Systeme liegt in der gewonnenen Reaktionszeit für Interventionsmaßnahmen durch eine frühzeitige Detektion im Außenbereich.
Der Entwurf der neuen Anwendungsregel DIN VDE V 0826-20 gilt als Meilenstein auf dem Weg zu hochwertigen Perimeter-Sicherheitslösungen mit dem Ziel, Sicherheit nachhaltig zu gewährleisten. Mit der Norm wurden erstmalig Qualitätsmaßstäbe für Betreiber, Planer und Errichter festgeschrieben.
Der Entwurf der DIN VDE V 0826-20, der durch den DKE Arbeitskreis „Perimeter Protection" entwickelt wurde, wurde auf der internationalen Fachmesse Perimeter Protection in Nürnberg im Januar 2023) erstmals offiziell der Fachwelt vorgestellt.
Einen umfassenden und intensiven Überblick über die Anforderungen der neuen DIN VDE V 0826-20, in Verbindung mit der DIN EN 16763 („Dienstleistungsnorm") für den Bereich PSS, bietet das BHE-Seminar "Perimetersicherung" am 01./02. März 2023 in Hünfeld.
Neben der Beschreibung der technischen Komponenten werden hier auch die für Errichterfirmen wichtigen Bereiche Planung, Projektierung, Installation, Inbetriebnahme und Instandhaltung von Perimetersicherungsanlagen erläutert.

PROGRAMM

Mittwoch, 01.03.2023
9.00 - 17.00 Uhr

- Grundlagen: Planung gem. DIN VDE (V) 0826-20 Betriebsanforderungen an das PSS
- Funktionalität / PSS-Grade Technologieauswahl / Sensorprinzipien
- Funktionalität / PSS-Grade Technologieauswahl / Sensorprinzipien
- Schnittstellen VSS, ZKS und GMS
- Inbetriebnahme und Abnahme

Donnerstag, 02.03.2023
8.00 Uhr - 14.30 Uhr

- Anlagenbeschreibung
- Instandhaltung
- Projektbeispiele / Kriterien für erfolgreiche Projektumsetzungen
- Abschlussprüfung

Kosten:
449,56 € (für Mitgliedsunternehmen, Behördenvertreter sowie Mitarbeiter von öffentlichen Einrichtungen
749,27 € (für externe Teilnehmer
(jeweils zzgl. gesetzlicher MwSt.)

Informationen:
https://tinyurl.com/je539dt3

Energierückgewinnung

Die elektronischen Schlösser ASSA ABLOY PULSE mit Energierückgewinnung passen zum Profil eines bahnbrechenden nachhaltigen Bauprojekts

Unternehmen in jedem Sektor stehen vor der Herausforderung, nachhaltiger zu arbeiten. Das Bauwesen ist nicht anders. Als Premium-Mitglied des Green Building Council Denmark suchte der Bauträger des neuen Wohnkomplexes A Place To" in Esbjerg nach einer effizienten Zugangskontrolle, die den zeitgenössischen Stil und den Nachhaltigkeitsgedanken ergänzt. Die Technologie zur Energiegewinnung war die Antwort.

In A Place To, Esbjerg, sind mehr als 400 Wohnungen mit gemeinsamen "Co-Living"-Bereichen verbunden. Es gibt ein Café, Fitness und Yoga, einen Großbildschirm, Leseecken und Arbeitsplätze, Gemeinschaftsküchen und vieles mehr. Nachhaltigkeit ist ein zentrales Element ihrer Vision. Im Zuge des Wachstums - bei zukünftigen Objekten in Kopenhagen, Horsens und darüber hinaus* - strebt A Place To an, dass der Betrieb und die Wartung aller Gebäude DGNB-zertifiziert sind.
Für eine effiziente Zugangskontrolle suchte man nach einer energiesparenden Lösung, die ohne Batterien oder Kabel funktioniert.
Weitere Prioritäten waren die Integrationsfähigkeit. Die elektronische Schließanlage von A Place To muss nahtlos mit anderen Gebäudetechnologien wie Online-Lesern und Türsprechanlagen zusammenarbeiten. Sie wollten eine Cloud-basierte Verwaltung, damit die Mitarbeiter rund um die Uhr und von jedem Ort aus die Kontrolle behalten können. Die Verantwortlichen wussten auch, dass jede Lösung zukunftssicher konzipiert sein muss: Neue Funktionen oder Kapazitäten können jederzeit erforderlich sein.

Energiegewinnendes Zutrittsmanagement in der Cloud

Elektronische PULSE-Schlüsselzylinder mit Energy-Harvesting-Technologie sichern jetzt mehr als 300 Wohnungen bei A Place To: "Wir haben uns für eine zukunftssichere Lösung entschieden, die wartungsfrei ist und bei der wir keine Batterien wechseln müssen", erklärt Peter Høpfner, COO und Gründer des Unternehmens.
Die PULSE-Geräte sind selbstversorgend und benötigen keine externe Energiequelle. Die verschlüsselte elektronische Sicherheit des Zylinders wird durch die beim Einstecken des Schlüssels erzeugte Energie gespeist. "Es war ein großes Plus von PULSE, dass Schlüssel und Schlösser batterie- und kabelfrei sind", fügt er hinzu.
Die Sicherheitsadministratoren von A Place To verwalten die Zugangskontrolle mit einer cloudbasierten Software. Sie können die Zutrittsberechtigungen von Personen online ändern. Die Benutzer aktualisieren ihre eigenen Schlüssel an integrierten Türsprechanlagen oder Online-Lesern. So wird sichergestellt, dass die Zutrittsberechtigungen der Bewohner immer aktuell sind.
Jeder PULSE-Schlüssel enthält außerdem einen RFID-Chip: Er dient gleichzeitig als Zugangskarte für den Eingang und die Gemeinschaftsbereiche, so dass die Mieter nur einen Ausweis für mehrere Öffnungen in der Wohnung mit sich führen müssen. Das ist bequemer und effizienter.

"Darüber hinaus verfügen mehrere PULSE-Zylindertypen über eine unabhängig bewertete Umweltproduktdeklaration (EPD), die bis 2026 gültig ist. Die EPD beschreibt die genauen Umweltauswirkungen eines Geräts während seines gesamten Lebenszyklus. EPDs enthalten viele Details, die für Projekte erforderlich sind, die eine Green-Building-Zertifizierung anstreben, die sich weltweit zunehmender Beliebtheit erfreut, da sie sowohl finanzielle als auch ethische Vorteile für den Gebäudeeigentümer bringen kann."

Daniel Totzeck, PULSE-Produktmanager bei ASSA ABLOY Opening Solutions EMEIA.

Wie PULSE die Herausforderungen des nachhaltigen Bauens meistert
Nach Schätzungen des UN-Umweltprogramms** werden rund 60 % des weltweiten Stroms in Gebäuden verbraucht. Die PULSE-Zutrittskontrolle kann dazu beitragen, den Energieverbrauch zu senken - ein Grund, warum die Technologie 2022 mit dem Danish Building Centres Energy Award*** ausgezeichnet wurde, dessen Ziel es ist, "innovative Produkte und Lösungen im Bauwesen auszuzeichnen und das Wissen über klimafreundliche
Baumaterialien zu erweitern".
Ein PULSE-Schließsystem ist selbstversorgend und kabellos und funktioniert im täglichen Betrieb ohne externe Stromquelle - weder Netz noch Batterien.

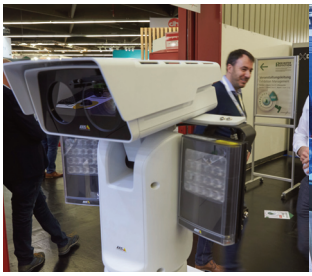
Auch die Installation erfolgt kabellos und mit geringem Aufwand, was den Stromverbrauch in der oft energieintensiven Phase des Lebenszyklus eines Systems minimiert. Bei einem Nachrüstungsprojekt muss der Installateur lediglich einen vorhandenen Zylinder gegen ein PULSE-Gerät austauschen. Das ist einfach und erfordert keine Bohrungen.

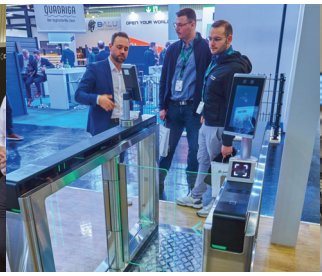
Weitere Informationen: https://campaigns.assaabloyopeningsolutions.eu/pulse.
*: www.aplaceto.com/en/corporation
**: www.euenergycentre.org/images/unep%20info%20sheet%20-%20ee%20buildings.pdf
***: www.dagensbyggeri.dk/artikel/118280-vinderne-af-byggeriets-klimapriser-imponerer

Erfolgreich wie nie zuvor

Mit 5.389 Fachbesuchern aus 55 Ländern (2020: 48) und einem Besucheranstieg von 27,7 Prozent zur Vorveranstaltung (2020: 4.227), geht am Donnerstag, 19. Januar 2023, die siebte Perimeter Protection erfolgreicher denn je zu Ende. Das Publikum informierte sich bei 198 Ausstellern (2020: 166) aus 22 Ländern auf rund 15.000 m² Bruttofläche über die neuesten mechanischen, elektrischen und elektronischen Lösungen der Freigelände- und Gebäudesicherheit. Besonders erfreulich:

Neben dem gesamten Ausstellerwachstum um 23 Prozent, stieg der Anteil der internationalen Aussteller auf ganze 50 Prozent. Somit ziehen die Unternehmen aus dem Ausland mit den deutschen gleich. Sehr guten Zuspruch fand auch in diesem Jahr wieder das Fachforum – mitten im Messegeschehen. Hier teilten an allen drei Messetagen renommierte Branchenexperten in zahlreichen Vorträgen wertvolle Tipps und Erfahrungen. Gelungene Premiere feierte die in die Fachmesse integrierte Sonderfläche U.T.SEC@Perimeter Protection. Die Aussteller schätzten vor allem die gute Qualität der Gespräche mit den Fachbesuchern: Über 94 Prozent erwarten aufgrund der geknüpften Kontakte ein Nachmessegeschäft.





„Die Perimeter Protection ist gefragter als je zuvor. Die Zahlen der diesjährigen Veranstaltung zeigen, mit welchem Erfolg die Fachmesse ihr konstantes Wachstum fortsetzt. Sie knüpft damit an ihre bisherige Erfolgsgeschichte an und bleibt unumstritten der Treffpunkt der Sicherheitsbranche in Europa“, so Frank Venjakob, Abteilungsleiter der Perimeter Protection bei der NürnbergMesse. „Wir freuen uns nicht

nur über den überaus erfolgreichen Restart, den die Perimeter Protection in diesem Jahr hingelegt hat – sie erreicht mittlerweile mit 50 Prozent an Ausstellern und knapp 30 Prozent an Besuchern auch international die Alleinstellung bei den Sicherheitsmessen", so Venjakob weiter.

Kai-Uwe Grögor, Geschäftsführer der Gütegemeinschaft Metallzauntechnik e.V., dem ideellen Träger der Perimeter Protection ergänzt: „Die Aussteller und Besucher aus dem Bereich Zaunbau berichten von einem sehr lebhaften Messegeschehen. Es ist deutlich zu spüren, dass es in den drei Jahren seit der vergangenen Perimeter Protection an persönlichen Kontakten zwischen Herstellern, Händlern und Zaunbauern gefehlt hat. Daher ist es sehr erfreulich, dass die Perimeter Protection so einen guten Neustart nach der Corona-Pandemie hingelegt hat. Das zeigt, dass die Veranstaltung als fester Termin in der Branche etabliert ist."

Qualitativ hochwertige Ausrichtung zog Besucher an

Während die Vorveranstaltung 2020 noch unter normalen Bedingungen stattfinden konnte, verschob sich der reguläre Termin der Perimeter Protection für 2022 pandemiebedingt auf dieses Jahr. Trotz der noch immer anhaltenden Corona-Pandemie, den Auswirkungen des Ukraine-Krieges sowie der derzeit bestehenden Energiekrise war die Fachmesse in den vergangenen Tagen sowohl aussteller- als auch besucherseitig ein reinster Erfolg. 198 Aussteller, davon 99 international (2020: 78), präsentierten den 5.389 interessierten Messe- und Forumsbesuchern ihr fachliches Know-how und Angebot rund um Perimeterschutz, Zauntechnik und Gebäudesicherheit. Aussteller und Besucher lobten besonders die an optischer Qualität gewonnenen Stände sowie das hochkarätige Neukundengeschäft. Das gestiegene Niveau der gesamten Veranstaltung und die Vielzahl an neuen Kontakten fand großen Gefallen.

Zu den Höhepunkten zählte auch das zum zweiten Mal in die Fachmesse integrierte, kostenfreie Fachforum, dessen Themen- und Referentenplanung der Verband für Sicherheitstechnik (VfS) innehat. Ergänzend zur Produktschau überzeugten die zahlreichen Vorträge wieder das Fachpublikum. Gerade die

qualitativ hochwertige Gestaltung der Inhalte kam sowohl bei Besuchern als auch Ausstellern sehr gut an.

Wilfried Joswig, Geschäftsführer des VfS, stellt zufrieden fest: „Das Fachforum traf auch in diesem Jahr wieder absolut den Nerv der Zeit und die Interessen der Teilnehmer. Die vielfältigen Themen der Referenten aus unterschiedlichen Fachgebieten stießen bei den Zuhörern auf großes Interesse und boten viel Raum für intensiven Wissenstransfer. Teilweise wurden sogar Stehplätze in Kauf genommen, um den Vorträgen zu folgen – und das, obwohl das Fachforum in diesem Jahr ohnehin bereits größer war als in 2020. Die Vorfreude auf die nächste Perimeter Protection war überall zu spüren."
Drohnendetektion und -abwehr als Sonderfläche verschärfter im Fokus
Als weiteres Highlight bestach die Sonderfläche U.T.SEC@Perimeter Protection mit zwölf Ausstellern die interessierten Messebesucher. Die thematische Planung der Vorträge übernahm der UAV DACH e.V. – Verband für unbemannte Luftfahrt, Berlin, Partner der Perimeter Protection. Die erstmals in die Fachmesse integrierte Fläche bildete als weltweit erste Plattform das Zukunftsthema der unbemannten Technologien ab. Sie ergänzte dadurch überaus gelungen den bestehenden Bereich der Drohnendetektion und -abwehr.

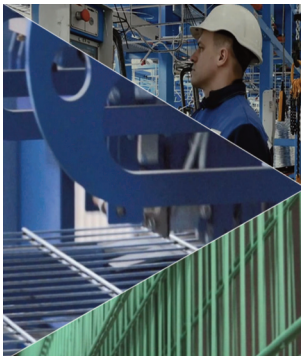
Alleinstellung sorgt für erhebliches Wachstumspotential

„Keine andere Messe verknüpft die Kombination aus Zaun-, Tor- und Sicherheitstechnik so umfassend wie die Perimeter Protection. Die Spezialmesse findet einen wirklich tollen Anklang und zeigt einmal mehr ihr überdurchschnittliches Potential für diese spannende Branche", resümiert Thomas Preutenborbeck, Mitglied der Geschäftsleitung und Bereichsleiter der Perimeter Protection.
Die diesjährigen Ausstellerstimmen spiegeln ebenfalls das Wachstum wider: Durch den unerwarteten Besucheransturm hätten einige Unternehmen größere Stände benötigt, um den enormen Andrang besser zu bedienen.

Perimeter Protection 2025: Termin vormerken! Die nächste Perimeter Protection findet vom 14. bis 16. Januar 2025 auf dem Messegelände in Nürnberg statt.

Dneprometiz

Hochwertige Drahtwaren aus der Ukraine



Das Unternehmen ist einer der führenden Eisenwarenhersteller in der Ukraine und spezialisiert auf die Herstellung von Drähten mit niedrigem und hohem Kohlenstoffgehalt. Die Produkte von PrJSC "Dneprometiz" werden im Maschinenbau, Bauwesen, in der Landwirtschaft, bei Reparaturarbeiten, im Dienstleistungssektor und in anderen Tätigkeitsbereichen eingesetzt. Schon seit zwei produziert 3D- und 2D-Schweißgittern für Sektionszäune. Das Rohmaterial für geschweißte Gitter ist Zink- und Zink-Aluminium-beschichteter Draht. Die Korrosionsbeständigkeit von 3D- und 2D-Profilen wird durch die spezielle Behandlung von verzinktem Draht um das 5-fache erhöht. Drahtabschnitte 3D und 2D durchlaufen fünf Stufen der Oberflächenvorbereitung in einem automatischen Tunnel, Besonderes Augenmerk wird nach Angaben des Herdtellers auf die Qualität der Produkte gelegt.

[www.en.dneprometiz.com]

Aaronia

Durchsagesystem zur Bevölkerungswarnung

Steigende Drohnenverkäufe bedeuten auch zunehmende Sicherheitsrisiken im Luftraum. Sowohl im zivilen als auch im militärischen Bereich nimmt die Bedrohung durch handelsübliche Drohnen rapide zu. Wiederholt haben unautorisierte Drohnenflüge weltweit Sicherheitsvorfälle ausgelöst – über Flughäfen, Haftanstalten und Grenzübergängen. Frei erhältliche Drohnen werden immer wieder dazu missbraucht, um Privatpersonen, Grundstücke und Prominente auszuspionieren. Das Ziel von Aaronia ist es, der wachsenden Bedrohung durch Mikro- und Mini-UAVs stets einen Schritt voraus zu sein.

Zu den neuesten Ergänzungen des AARTOS DDS gehört der optionale Ultra Long Range Communication Speaker (AARTOS Long Range Speaker) – ein voll integriertes Durchsage- und Sirenensystem zur Bevölkerungswarnung, das automatisch Warnmeldungen abspielt, wenn sich eine Drohne in einer Gefahrenzone befindet. Diese Option ermöglicht es dem Benutzer, den Drohnenpiloten vor dem Eintritt in eine Gefahrenzone zu warnen, bevor er Gegenmaßnahmen ergreift. Das 360°-System mit Sektorschaltung ist für hohe Reichweiten optimiert (ca. 2000 m bei 120 dBA) und bietet beste Sprachverständlichkeit durch neue Strahlertechnologie.

High-End Detection-System - AARTOS HF Detektion

Ein Hochfrequenzdetektor (RF-Detektor) ist ein Gerät, das zur Erkennung des Vorhandenseins von RF-Wellen in einem physikalischen Übertragungsmedium verwendet wird. Das AARTOS-System verwendet den RF-Detektor, um Drohnen und Drohnenpiloten zu erkennen. Die künstliche Intelligenz identifiziert sogar die Art der Bedrohung durch den Vergleich verschiedener Frequenzmuster. Das System erkennt jedes Funksignal und kann Drohnen durch erlernte Muster leicht von z.B. WiFi-Signalen unterscheiden und identifiziert fast alle Arten von Bedrohungen. Zusätzlich wird der Standort des Drohnenpiloten ermittelt. Ein Vorteil dieser Methode ist die Erfassungsreichweite. Während das Radar nur eine Kegelreichweite von ca. 3 km erreicht, erzielt der RF-Detektor eine Kuppelreichweite von bis zu 14 km. Das System ist skalierbar und kann an die Anforderungen und das Budget angepasst werden.

[drone-detection-system.com]

Arrowtec

Arrow-401 Drohnensystem

Das Drohnensystem überwacht vollautomatisiert Liegenschaften durch

Patrouillen Flüge und Alarm Verifikation. Die integrierte KI liefert dabei bereits ausgewertete Lagebilder und ermöglicht eine schnelle und exakte Intervention. Die Technologie lässt sich mit bewährter Sicherheitstechnik zu einem robusten Sicherheitskonzept kombinieren. Arrowtec verfügt hierfür über eine EU-weite Genehmigung für den Betrieb autonomer Drohnen ohne Piloten notwendig sind. Im Fokus stehen der Schutz kritischer Infrastruktur und großen Liegenschaften, der Schutz von Fahrzeugkonvois, sowie die Überwachung von unbefugten Personen auf Grundstücken. Auch die Kontrolle von Umgebungen zum Zweck der Brandfrüherkennung oder die Inspektion, z.B. von Solaranlagen und Hochspannungsanlagen gehören zum Aufgabenspektrum.

Kosten stehen im Fokus

Durch die steigenden Lohnkosten für traditionelle Sicherheitsdienste wird der Einsatz von Drohnen immer interessanter. Allerdings besteht bei manchen Drohnen das Problem, dass sie ohne langwierige Ausbildung schwer zu handhaben sind. Aus der Sicht von Arrow sind auch Kameratürme nicht die richtige Lösung, da die Installationszeit zu lang ist und ihnen eine gewisse Flexibilität fehlt.Bird's eye view als Lösung Arrowtec zeigte auf der Perimeter Protection eine autonome Drohne in Kombination mit Hangar- und IoT-Sensoren, die ungewünschten Personen in den Standortbereich (Wasserversorgung, Industriegebiete, Grenzen usw.) erkennt. Die Vorteile der Lösung listet der Hersteller wie folgt auf:

- 105% effizienter als Patrouillen
- 72% billiger als herkömmliche Drohnen
- 18-mal schnellerer Aufbau als mit herkömmlichen Kameratürmen
- 90% weniger Arbeitskräfte erforderlich

[www.arrowtec.de]

ASO Safety Solutions

Installationszubehör als Kernkompetenz

Außerdem bietet der Hersteller auch die DRICO Torsteuerungen an, die unter extremen Bedingungen, wie z.B. im Tiefkühlbereich eingesetzt werden kann.

Auf der Perimeter Protection wurde auch Zubehör für Installationen rund um Perimeterschutzlösungen gezeigt. ASO Safety Solutions bietet die Sicherheitskontaktleisten SENTIR edge, druckempfindliche Sensoren zur Schließkantensicherung, mit optimalen Nachlaufwegen und einem schnellen Schaltverhalten.
Das Plug'n'Sense-Selbstkonfektionssystem ermöglicht die Konfektion einer Schaltleiste ohne Werkzeug

und ohne Verkleben innerhalb kürzester Zeit und unabhängig von Umgebungsbedingungen, z.B. im Service-Fall direkt am Tor.

Mit dem neuen, innovativen drahtlosen Signalübertragungssystem ELMON wicom sorgt ASO Safety Solutions für eine sichere und bidirektionale Signalübertragung an allen automatischen Torsystemen. Das System besteht Sender und Empfänger, die per Funk sicher miteinander verbunden sind. Es zeichnet sich unter anderem durch eine hohe Verbindungsqualität, eine lange Batterielebensdauer sowie eine schnelle Reaktionszeit aus. Zudem können mehrere Sendeeinheiten eingebunden werden.

autosecure

Kommunikationssäule und Webplattform

Das Unternehmen autosecure aus Münster bietet eine Lösung, die die Digitalisierung der Standortsicherheit organisiert. Das autosecure Ecosystem ist eine neue Highend-Webplattform für die Integration in folgende durch autosecure angebotene Services:

- Web-Plattform für die maximale Vereinfachung von Geschäftsabläufen
- Cloudbasierter User-Account
- Erhebliche Reduktion von E-Mail Korrespondenz, Telefonaten oder Suchaufwand
- Zentralisierte Bereitstellung von Informationen und Dokumentationen
- Maximale Transparenz für Ereignisselm autosecure Eco-System werden standardmäßig alle verfügbaren Dokumente wie Kamerapläne, abgestimmte Alarmpläne und Objektinformationen hinterlegt.

Außerdem findet man hier vereinbarten Zeitpläne und sonstige Objektbemerkungen, die für Fahrer, die auf das Logistikgelände fahren relevant sind. Alle relevanten Informationen sind so an einem Ort vereint und Zeit kann eingespart werden.
Außerdem wird die Kommunikation zur Leitstelle verbessert, denn Ereignisse werden durch das Eco-System erfasst und in einer gesammelten Übersicht in Echtzeit zur Verfügung gestellt.

Axis Communications

PTZ-Kamera mit Langstrecken-IR

Die AXIS Q6225-LE wurde speziell für die Überwachung über große Entfernungen hinweg mit hochpräzisem PTZ und OptimizedIR für hohe Reichweiten entwickeltt. Sie verfügt über einen ½"-Sensor, einen 31-fachen optischen Zoom und integrierte Analysefunktionen, über die Sie bei Bedarf benachrichtigt werden. Es bietet eine auflösung von HDTV 1080 px und einen 31-fachen optischen Zoom. Durch den 1/2"-Sensor und OptimizedIR ist eine hohe Reichweite möglich. Für eine störungsfreie Erfassung von Bilder exisiziert eine elektronische Bildstabilisierung. Außerdem ist das System MIL-STD-810G- und NEMA TS-2-konform und die KI AXIS Object Analytics ist vorinstalliertEbenfalls auf der Messe zu sehen: AXIS Q1656-DLE Radar-Video Fusion Camera und AXIS A8207-VE Network Video Door Station.

INOVA

Integrierte Freigeländesicherung aus einer Hand

Der Hersteller und Systemanbieter Berlemann Torbau GmbH ist einer der führenden Hersteller und Systemanbieter für Anlagen zur Freigeländesicherung (Perimeterschutz) unter den Markennamen INOVA in Deutschland. Das Schwesterunternehmen, Peri-Net GmbH, bietet mit der elektronischen Vernetzung von Perimeterschutzkomponenten, und bei Bedarf einer Integration von Übersteig- und Durchbruchsdetektion, die ideale Lösung für die elektronische, intuitive Ansteuerung und Überwachung von Perimetern.

Korridorschloss mit Ziehfixsperre

Das mehr als 200 Jahre alte Unternehmen Bever & Klophaus stellt das Turrus-Sicherheitschloss mit Ziehfixsperre her. Das Bever-Korridorschloss „Turrus" (Foto links) mit Ziehfixsperre (DBGM) ist ein wesentliches Sicherheitselement im Gesamtkonzept der Korridortürsicherung. Neben seinen diversen Sicherheitselementen, wie Fallenverriegelung und Rückdrucksicherung, wirkt seine Ziehfixsperre speziell gegen die verbreitete Einbruchsmethode nach dem Ziehfix- oder Korkenzieherverfahren.

Gladius" - Das selbstverriegelnde Korridorschloss

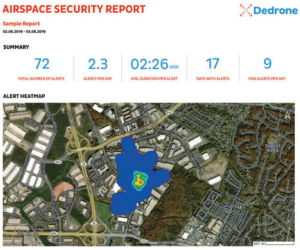
Das Bever-Korridorschloss 271P „Gladius" ist ein Türschloss mit Anti-Panikfunktion, dass eine Reihe von Besonderheiten aufweist:Das Schloss verriegelt sich automatisch beim Schließen der Tür. Damit wird das Abschließen mit Schlüssel überflüssig.Die Stulpe ist aus Edelstahl, der Riegel ist aus solidem Stahl, die Falle Messing vernickelt.Das Schloss ist mit einer Panikfunktion ausgestattet, d.h. durch Betätigung der Türklinke kann die verriegelte Tür von innen geöffnet werden.Das Schloss ist für DIN Linke und DIN Rechte Türen verwendbar, da Falle und Stulpe umlegbar sind.Die Stulpe des Schlosses kann ausgetauscht werden.

Auch im Programm ist das Rohrrahmenschloss „Scuteus" (Foto) mit drei besonderen Merkmalen, die eine höhere Einbruchsicherheit gewährleisten: Es verfügt über einen kräftigen Riegel mit innenliegendem Stahlkern, der sich 22mm herausschließen lässt.Die Falle wird zusätzlich mitverriegelt, sodass zwei Verriegelungspunkte entstehen.Für ein exklusives Erscheinungsbild und zusätzliche Stabilität sorgt die Stulpe aus rostfreiem Stahl.

DroneTracker

Klassifizierung und Entschärfung von Gefahren durch Drohnen

Die Drohnentechnologie entwickelt sich rasant weiter, und nur eine softwarebasierte Lösung kann mit den permanenten Veränderungen Schritt halten. Durch intelligente Mustererkennung mittels DroneDNA detektiert und klassifiziert die von Dedrone entwickelte DroneTracker Software Drohnen automatisch. Dazu wertet



sie die Daten verschiedener Sensoren wie Funkfrequenz-Sensoren, PTZ-Kameras und Radarsystemen aus. Das Sensornetzwerk ist beliebig skalierbar und hängt von der Größe und Beschaffenheit des zu schützenden Geländes sowie den Anforderungen des Kunden ab.

Die DroneDNA-Datenbank ist eine selbstlernende Software und ein Klassifizierungssystem, das Drohnen aller Art erkennen kann. Trainiert mit Millionen von Bildern und Datenpunkten, kann die DroneDNA Drohnen von anderen zwischen Flugobjekten wie Vögeln, Hubschraubern oder Flugzeugen unterscheiden und sogar

verschiedene Drohnenmodelle erkennen. Die Software stellt Ergebnisse zu Drohnenhersteller, -modell, Flugdauer, Flugrouten sowie -zeiten in Form eines umfangreichen Berichts automatisch zur Verfügung. Auf diese Weise werden auffällige Aktivitätsmuster sichtbar gemacht und Sicherheitsverantwortliche können gezielt Schutzmaßnahmen planen und umsetzen.

Cloud-Managed Airspace Security

Die Dedrone Cloud vereinfacht die Installation und macht Server vor Ort überflüssig. RF-Sensoren verbinden sich automatisch via LTE mit der Cloud, und regelmäßige Software-Aktualisierungen stellen sicher, dass der Luftraum auch vor neuen Drohnenmodellen geschützt ist. Für Umgebungen, die ein Datenmanagement vor Ort erfordern, sind auch lokale Management-Konfigurationen verfügbar.

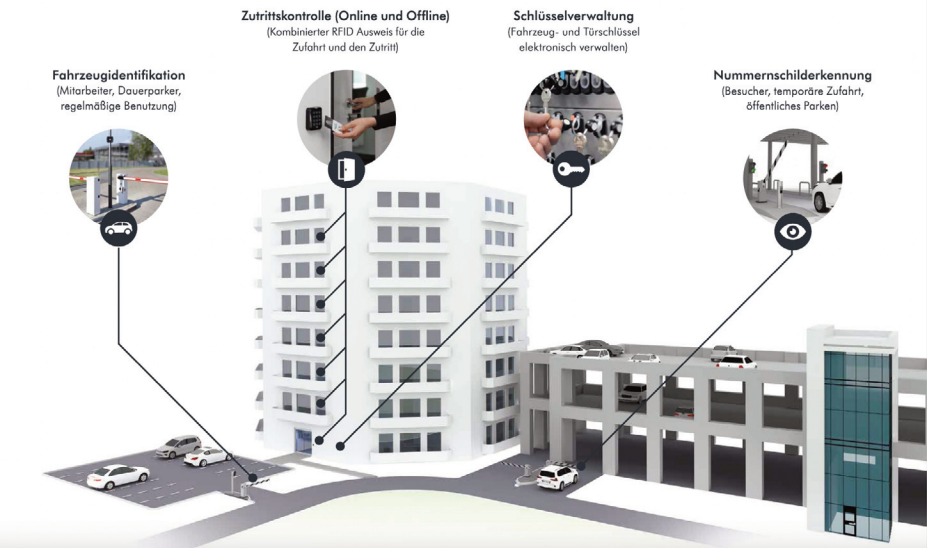
RF-100 - Wie viele Drohnen sind in Ihrem Luftraum?

Der RF-100 hat eine Reichweite von bis zu zwei Kilometern. Anhand von Funksignalen detektiert und klassifiziert dieser Sensor zuverlässig alle kommerziellen, Hobby- und selbstgebauten Drohnen und die gesamte DJI-Produktlinie. Die DroneTracker Software verarbeitet und analysiert die Daten des RF-100 und generiert automatisch Berichte mit aussagekräftigen Informationen über Drohnenaktivitäten im überwachten Luftraum. Auf dieser Basis kann das Detektionssystem optimal angepasst und erweitert werde

deister electronic

eyeFOUR - "Intelligent Vision Sensor"

KameraDas Konzept der eyeFOUR ist, als Plattform für innovative Lösungen zu dienen, mit denen sich reale Herausforderungen in Anwendungen wie die Parkraumbewirtschaftung, das Transportwesen, die Zutrittskontrolle usw. bewältigen lassen. Dabei kann die Kamera an die spezifischen Anforderungen modular angepasst werden – sowohl in der Hardware, als auch in der Software. Ziel der eyeFOUR ist es, eine leistungsstarke Plattform zu bieten, die für die Anwendung optimal konfiguriert werden kann, um Fehlalarme zu reduzieren und beste Ergebnisse zu erzielen. Der modulare Aufbau der eyeFOUR ermög-



licht die Integration anwendungsspezifischer Bildsensoren und Optiken. Zudem verfügt die eyeFOUR über integrierte Hochleistungs-IR-LEDs, einen Flash-Speicher und eine USB-Schnittstelle für optionale Funktionsmodule.

Die eyeFOUR wurde als „Intelligent Vision Sensor" Kamera konzipiert. Qualifizierte, auf künstlicher Intelligenz basierende Algorithmen können für unterschiedliche Aufgabenfelder eingesetzt werden:

Perimeter Überwachung, Objekt- und Personenerkennung oder Kennzeichenerkennung. Die eyeFOUR ist eine sogenannte Edge-Intelligence Kamera. Sie braucht keinen zentralen Server, eine aufwendige Infrastruktur oder nachgelagerte Videoverarbeitung. Alles passiert in der Kamera. Alle relevanten Einstellungen zur Konfiguration der Bildparameter der Kamera und zur gezielten Anpassung der Eigenschaften der installierten Applikationen können bequem über das Webinterface vorgenommen werden, welches auf der Kamera selbst gehostet wird. **[www.eyewatch.de]**

Perimeter Protection 2023 - Rundgang mit Innenminister Joachim Herrmann
Urheber: NuernbergMesse / Frank Boxler

FEIG ELECTRONIC

Frequenzumrichter-Steuerung vorgestellt

Im Umfeld der Perimeter Protection stellte Feig electronic Steuerungen für Industrietore, Poller und Schranken seine RFID-basierten Lösungen für die Zufahrtskontrolle sowie weitere RFID- und Sensorik-Komponenten vor.

Auf dem Stand wurde eine Frequenzumrichter-Steuerung - nicht nur für den Antrieb zum Öffnen und Schließen des Schrankenbaums gezeigt. Darüber hinaus ist sie mit zwei RFID-Zufahrtskontrolllesern (UHF für die Weitbereichserkennung und HF für den Nahbereich) und einem Schleifendetektor nebst Schleife als Impulsgeber zum Öffnen und Schließen der Schranke verbunden.

Ein kontaktloses Bezahlterminal für die Begleichung der Parkgebühr komplettiert das Modell. Messebesucher aus dem Bereich der Gebäudesicherheit interessierten sich vor allem für die neue PROFINET Netzwerkkarte TST RCCA, durch die Torsteuerungen netzwerkfähig werden und Tore direkt mit einer übergeordneten Steuereinheit kommunizie- ren können.

Bei Anwendungen im Gebäudemanagement, können die Toranlagen in die Klimasteuerung, das Alarmsystem und das Wartungssystem eingebunden werden. So können die Tore beispielsweise auto- matische Lüftungsfunktionen übernehmen. Eine Zentralsteuerung von Toren ist ebenfalls problemlos realisierbar.

www.magnetic-access.com

Passagierabfertigung mit Momentum am Flughafen

Vilnius Airport (VNO) ist der mit Abstand größte Flughafen in Litauen. Mehr als 6,5 Millionen Passagiere flogen 2019 von hier aus zu ihren Zielen – vor allem ins Vereinigte Königreich, nach Deutschland und Skandinavien. Die Corona-Pandemie hat diesen Trend kurzzeitig unterbrochen, aber der staatliche Betreiber Lithuanian Airports verzeichnete bereits 2022 eine Erholung und rechnet mit weiter steigenden Passagierzahlen.

Damit all diese Reisenden in Zukunft schnell und bequem zu ihrem Flugzeug gelangen, hat Lithuanian Airports ein neues Passagierabfertigungssystem zur Vergabe ausgeschrieben. Beim Betreten des Sicherheitsbereichs sollte die automatisierte Kontrolle der Bordkarten folgende Ziele erreichen:

- Erhöhung des Passagierdurchsatzes
- Bessere Orientierung der Passagiere im Terminal-Gebäude
- Erhöhte Sicherheit und Überwachung der Passagiere
- Verbesserte Erfahrung der Passagiere auf dem Flughafen

Die Betreibergesellschaft entschied sich schnell für die hochwertigen Sicherheitsschleusen mPass von Magnetic. Die neue Momentum® Serie überzeugte die Projektverantwortlichen durch ihre hohe Flexibilität und die konsequente Ausrichtung auf die Anforderungen von Flughäfen:

- Intuitive Benutzerführung mit Beleuchtungselementen und Display
- Schnelle Überprüfung der Bordkarte, um die Wartezeit der Passagiere zu verkürzen
- Intuitive Konfiguration und Parametrierung über die Sperren-Steuerung oder die grafische Benutzeroberfläche

Das Projekt im Überblick

Insgesamt wurden am Eingang des Sicherheitsbereichs vier mPass instal-

liert, drei in Standardausführung und eine in einer breiteren Ausführung für PRMs. Sechs Monate nach der ersten Installation wurden die Personensperren mit einem Gantry-System nachgerüstet. An der Gantry befindet sich derzeit ein Bildschirm, auf dem flughafenbezogene Informationen angezeigt werden.
An diesem speziellen Standort war es aufgrund der begrenzten Platzverhältnisse nur möglich, vier Reihen einzurichten, aber dank der benutzerfreundlichen Aufstellung und der intuitiven Gestaltung der Momentum mPass Personensperren ist es ein Leichtes, den derzeit hohen Passagierdurchsatz zu bewältigen.

Das litauische Flughafenunternehmen ist mit der Lösung, die Magnetic und NT Services, der lokale Partner vor Ort, geliefert haben, zufrieden. Das Unternehmen bestätigt seine Absicht, auch andere Bereiche des Flughafens Vilnius damit auszurüsten, was auch für die Flughäfen in Kaunas und Palanga in Erwägung gezogen wird – weil sich die Passagier- abläufe mit Momentum so einfach gestalten lassen.

Projekt:
Lithuanian Airports,
Vilnius, Litauen

Installierte Produkte:
VierWartereihen mit mPass, da-von drei in Standard- und eine in Wide-Lane-Ausführung, ausge-stattet mit Bordkartenleser und Gantry

Installationspartner vor Ort:
NT SERVICE, Kaunas, Litauen

Stand 2021

Perimeter Protection

Belgischen Stadt entscheidet sich für CityProtector

Die Beziehung zu unserem Distributor in Belgien, Noyez NV, hat sich über mehrere Jahre entwickelt und ist aufgrund der guten Kommunikation, der Qualitätsprodukte, der Unterstützung, des guten Rufs und letztlich des Vertrauens erfolgreich. Als also der Vorschlag zur Installation eines physikalischen Schutzes an einem großen Verkehrsknotenpunkt in Belgien zur Ausschreibung kam, arbeiteten wir zusammen, um eine Lösung vorzuschlagen, die nicht nur die geforderte Spezifikation erfüllen, sondern auch einige der standortspezifischen Einschränkungen überwinden würde.

Zu bewältigende Herausforderungen

Der Standort ist ein belebter öffentlicher Bereich, die Lösung musste für Fußgänger zugänglich sein.

- Für verschiedene Standorte innerhalb des Geländes waren zwei Schutzvorrichtungen erforderlich.
- Die Lösung sollte nahtlos und ohne offensichtliche Inkonsistenz der Produkte sein.
- Die Lösung sollte dauerhaft mit einer abnehmbaren Ausführung sein, da Servicefahrzeuge gelegentlich Zugang benötigen.
- Beschränkung auf eine Fundamenttiefe von 450 mm.
- Eine Tiefgarage befindet sich unter dem geplanten Schutzbereich.

Innovativ und dynamisch

Der PPG CityProtector Poller erwies sich als die ideale Lösung. Wir wussten sofort, dass der Poller zu einem modernen, pulsierenden Ort passt und eine innovative, dynamische Alternative zu einem herkömmlichen Poller mit runder Form darstellt. Die Tests nach IWA 14-1 und PAS 68 mit Fahrzeugen der Klassen N2 und N2A erwiesen sich sowohl bei 64 km/h als auch bei

80 km/h als erfolgreich und erfüllten somit die geforderte Spezifikation. Der CityProtector hat ein einheitliches Design und stellt somit eine nahtlose Lösung dar, ohne dass verschiedene Pollerformen und -größen erforderlich sind.

Standardmäßig demontierbar

Die üblichen auf dem Markt erhältlichen, herausnehmbaren Poller, sind wie folgt aufgebaut. Oft sitzt eine äußere Hülse tiefer im Fundament, wobei das Pollerrohr in die äußere Hülse eingeschoben wird. Bei dieser Lösung muss die Position des herausnehmbaren Pollers oder des Zufahrtsbereichs für Fahrzeuge vor der Installation festgelegt werden, was bei einer begrenzten Fundamenttiefe nicht immer möglich ist. Der CityProtector wiederum ist modular aufgebaut, so dass jeder CityProtector standardmäßig von Hand demontierbar ist, was Zeit und Geld spart. Es ist nicht erforderlich, eine Aufsicht für schwere Hebemaschinen einzuplanen oder Bereiche abzusperren, damit die Entfernung stattfinden kann. Ein CityProtector Poller kann einfach für kurze oder längere Zeit entfernt und dezent mit einer eleganten Edelstahlabdeckung verschlossen werden.

Das vorgegebene flache Fundament von 450 mm konnte problemlos eingehalten werden, für den CityProtector wurden nur 220 mm benötigt. Die sorgfältige Konstruktion des Pollers reduziert den Zeit- und Ressourcenaufwand für die Installation und ist damit auch kosteneffizient.

www.benincagroup.com

Neuer Standard für hydraulische Poller

Seit dem Jahr 2021 ist Spartacus eine Pollerreihe von Rise auf dem Markt und wurde nun auf der Perimeter Protection von der Benincà-Gruppe auch dem deutschen Markt vorgestellt. Die neue Lösung ist ein ölhydraulischer Poller mit einer unabhängigen Hydraulikpumpe für jeden Poller.

Die Poller sind ideal für die Verwaltung und den Schutz der Zufahrt von Straßenfahrzeugen in private Bereiche, aber auch ein unverzichtbares Werkzeug, wenn ein Durchbruchschutz an hochsensiblen Orten wie z.B. vor Bankfilialen oder Juweliergeschäften. Auch können Poller dort eingesetzt werden, wo Fußgängerzonen, Gehwege oder Radwege geschützt werden müssen.

Durch ihren versenkbaren Mechanismus und ihr minimalistisches Design entsprechen die Straßenpoller den ästhetischen Bedürfnissen in allen Bereichen, in denen sie eingesetzt werden – von Stadtzentren bis hin zu Privatbereichen. Die hydraulische Technologie ist ideal, um den Verschleiß und

die Beanspruchung der mechanischen Komponenten zu minimieren, aber dar- über hinaus wurde auf Qualität und Funktionalität geachtet.

Jeder Poller ist mit einer unabhängigen Hydraulikpumpe ausgestattet, die Arbeitszyklen von bis zu 3500 pro Tag garantiert. Der hydraulische Poller Spartacus hat einen Durchmesser von 275 mm und ist in zwei Höhenvarianten erhältlich: 600 und 800 mm. Für das Design stehen zwei Optionen zur Verfügung: eine schwarze Graphitlackierung, die eine hohe Beständigkeit gegen Oberflächenkorrosion gewährleistet, oder eine Edelstahlverkleidung. Jedes Modell der Spartacus-Linie ist mit LED-Systemen zur optischen Signalisierung des Hindernisses und einem Sicherheitssystem ausgestattet, das die Entriegelung im Falle eines Stromausfalls erleichtert.

[youtu.be/4Do_0B4R6aI]

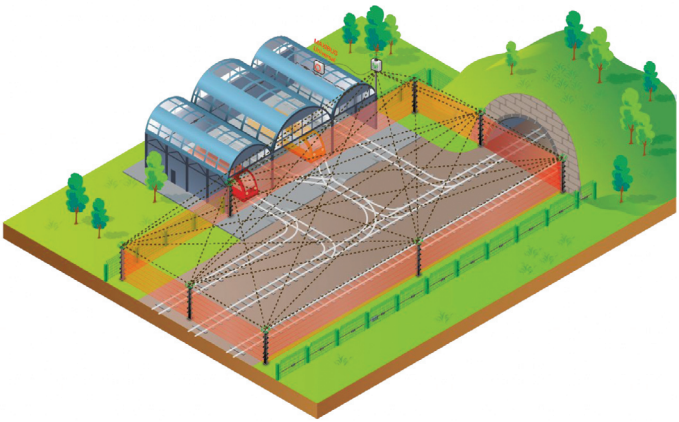
SORHEA

SOLARIS NG in Nürnberg präsentiert

Die neue Generation von SOLARIS, einer autonomen Infrarotschranke mit einer Reichweite von 100 Metern, wurde im September 2022 vorgestellt.

Die autonome Aktiv-Infrarot-Lichtschranke SOLARIS wurde in den vergangenen Jahren an zahlreichen Standorten in Europa und weltweit installiert. Die Lösung kann mittels Solarenergie autonom betrieben werden. SOLARIS wurde schon im Jahre 2009 von SORHEA konzipiert und war die erste Low-Power-Infrarotbarriere auf dem Markt für Perimetersicherheit. Der sehr geringe Energieverbrauch ermöglicht einen Allwetterbetrieb mit einer Reichweite von 100 Metern. Die Solarenergie wird durch eine Batterie ergänzt, die den Betrieb für zwei Monate in völliger Dunkelheit (ohne Solarenergie) garantiert. So konnte auch in Skandinavien und anderen weniger sonnenreichen Breitengraden eine Installation vorgenommen werden. Die Übermittlung der Alarminformationen erfolgt ebenfalls ohne Verkabelung, da SOLARIS eine Mesh-Funkkommunikation nutzt. Da keine Verkabelung erforderlich ist, kann das System einfach installiert

werden, während die Kosten für Erdarbeiten gering bleiben. Mit zehn Infrarot-Zellen auf drei Meter hohen Säulen ist die SOLARIS NG heute die einzige existierende autonome Infrarotschranke, die eine derart hohe Infrarotdichte über eine Reichweite von 100 m bietet. Die SOLARIS NG profitiert auch von SORHEAs technologischen Fortschritten im Bereich der Funktechnologie. Die vollstän-



dige Verschlüsselung des Funknetzes der SOLARIS ermöglicht eine hohe Datensicherheit, und die Kommunikation über das LoRa-Protokoll bietet eine große Reichweite, geringe Leistung und sehr gute Störungsresistenz.

Neue Funktionen integriert

SORHEA kann auf eine 35-jährige Erfahrung in der Infrarottechnologie zurückblicken und hat die traditionellen Kompetenzen bei verdrahteten Säulen auf die autonomen Säulen übertragen.
Die Funktion „Discrimination-Train", die bisher nur bei den MAXIRIS-Schranken verfügbar war, ist nun auch bei den autonomen SOLARIS NG-Schranken verfügbar. Ein Algorithmus ermöglicht, die Durchfahrt eines Fahrzeugs (Zug, U-Bahn, Lkw oder sogar Flugzeug) zwischen den zwei Säulen und kann diese von durchgehenden Personen unterscheiden. Falschalarme werden vermieden und das Perimeter-Sicherheitssystem kann ohne physikalische Unterbrechung betrieben werden.

Stagnoli Accessories

ARGO steuert automatische Tore

Automatische Tore werden immer häufiger für die Kontrolle des Zugangs zu Häusern und Wohnkomplexen verwendet und funktionieren mit einem Elektromotor und Fotozellen. Zwischen den beiden ARGO-Komponenten (Sender und Empfänger) verläuft ein Infrarotstrahl, der eine echte unsichtbare Barriere bildet. Wird diese durch ein Objekt (ein Fahrzeug oder eine Person) durchbrochen, sendet sie ein Signal an die angeschlossene Zentrale, die entsprechend reagiert, um einen Aufprall zu verhindern. Neben Industrie- und Wohngebäuden finden die Lösungen auch in komplexeren Systemen wie Parkplätzen, Be- und Entladestellen oder überall dort, wo fremde Objekte erkannt werden müssen, Anwendung. Die Lichtschranke ARGO für Tore bietet die Schutzart IP65 und schützt vor Insekten und Leckagen und verfüg über einen von Stagnoli entwickelten Vandalismusschutz.

Die AFAPC-Abdeckung aus satiniertem Aluminium schützt die Lichtschranke außerdem vor Diebstahl und Vandalismus.Die Lichtschranken für Hauseingänge zeichnen sich durch eine Reichweite von 20 Metern aus, die auch unter schwierigen Bedingungen wie starker Sonne, Nebel, Regen oder Schnee funktionieren. Das optisches System ist von +-180°H, +30° -10° V einstellbar und benötigt eine 12 - 24 V AC/DC-Stromversorgung.

www.sysco-gmbh.de/neopoint

Schutz für flexible Infrastrukturen

Das Sensorsystem NEOPOINT ist eine neue Lösung zur Überwachung von Zäunen, Fassaden, Dächern oder anderen festen Strukturen. Das System der Produktlinie NEOLINE wurde konzeptionell auf eine äußerst einfache Installation mit einer möglichst flexiblen Infrastruktur ausgelegt. Dieses System zielt klar auf Anwendungen im industriellen und militärischen

Umfeld. Die Möglichkeit einer redundanten Verkabelung im Ring-Bus ermöglicht es, im Falle einer Kabelsabotage alle Sensoren ohne technische Verluste weiter zu betreiben. Der Bus NEOIO kann in die Lösung eingezogen werden und verfügt über die volle Sensorfunktionalität des NEOPOINTs. So können Anlagen flexibel auf alle kundenspezifischen Anforderungen angepasst werden. Mit dem neuen RADARPOINT300 verfolgt SYSCO einen komplett neuen Lösungsansatz zur Freigeländeabsicherung.

Als Anwendung kommen alle Bereiche in Frage, in denen unauffällig und ohne großen Montageaufwand weite Geländeabschnitte überwacht werden sollen. Somit ist die neue Technologie sowohl für den Hochsicherheitsbereich sowie für industrielle Anwendungen geeignet. Zur Lösung gehört ein kompaktes Wetterschutzgehäuse. Der Sender- und Empfänger befinden sich in einem Gehäuse. Mit einer großen Reichweite ist die Lokalisierung von Objekten, die richtungs- bzw. geschwindigkeitsabhängige Detektion und eine Einteilung in Meldeabschnitte möglich. Es besteht ein LAN- und RS485 Anschluss und der IO's ist integriert.

TRL Funksysteme

Für die Industrie: Funkfernsteuerung Sesam 800

Sesam heißt die Produktfamilie von Funkfernsteuerungen für Industrieanwendungen, wie z. B für das Öffnen und Schließen von Schranken und Toranlagen, das Ein- und Ausschalten von Ventilatoren und Flutlichtsystemen sowie für mobile Anwendungen wie Winden für Geländewagen und Forstmaschinen. Das einfache und flexible System basiert auf moderner Digitaltechnologie. Die Sesam 800 ist eine komplette Produktfamilie aus Sendern und Empfängern. Die Sender sind ausgesprochen einfach zu bedienen. Die robuste und dauerhafte Konstruktion ist durch einen Gummischutz am Gehäuse besonders stoßfest. Dank Schutzart IP67 können die Geräte permanent Staub, Feuchtigkeit und Spritzwasser ausgesetzt werden. Die Sender haben einzelne,

leicht zu drückende Qualitätsdrucktasten, die auf über 1 Million Betätigungzyklen ausgelegt sind. Das Sesam 800 Funksystem arbeitet auf dem 868MHz Frequenzband. Die Kommunikation zwischen Sender und Empfänger ist bidirektional, was eine Rückmeldeanzeige am Sender ermöglicht, die zeigt, wann ein Relais angesprochen wird.

Das System verwendet 16,7 Millionen einmalige Codierungen. Prüfsummen garantieren eine fehlerfreie Befehlsübertragung. Für Anwendungen mit noch höheren Sicherheitsanforderungen kann das System für verschlüsselte Datenübertragung konfiguriert werden.Die Empfänger sind in verschiedenen Ausführungen erhältlich: Gerät für Aufputzmontage mit Display, Gerät für Aufputzmontage ohne Display und ein kleines Gerät für DIN-Schienenmontage. Dank Display lassen sich leicht neue Sender und Systembenutzer hinzufügen und entfernen. Der Empfänger besitzt außerdem eine herausnehmbare Speicherkarte für betriebskritische Systeme, so dass er mit einer großen Anzahl Sender eingesetzt werden kann. Einstellungen des Empfängers können mit einem vierstelligen Zahlencode passwortgeschützt werden, um bestimmte Funktionen nur autorisierten Benut-

zern zugänglich zu machen. Einstellungen und Zugangskontrolle lassen sich einfach mit dem Tastenfeld am Displayempfänger vornehmen.

HEALD

Eletromechanische (EM) Pollersysteme

Aufbauend auf den Erfolg der bisher größtenteils hydraulisch angetrieben HEALD-Produktpalette, hat HEALD nun entsprechende elektromechanischen (EM) Zufahrtsschutzsysteme entwickelt. Die EM-Produkte bieten die gleichen Standards wie die bestehenden Produkte mit einer Vielzahl von zusätzlichen Vorteilen. Einer der Hauptvorteile von EM gegenüber einem hydraulischen System ist die Möglichkeit, die Produkte schneller einzusetzen, da die Motoren innerhalb des Produkts installiert sind, was die Notwendigkeit einer zusätzlichen Einheit zur Unterbringung von Steuerungen und die Installation von Hydraulikleitungen für den Betrieb der Produkte überflüssig macht. Ein weiterer Vorteil der EM-Reihe von HEALD ist die geringere CO2-Bilanz, da für den Betrieb im Durchschnitt über 60 % weniger Strom benötigt wird. Das EM-Sortiment wird u.a. auch den preisgekrönten HEALD Matador erweitern.

Der Matador wird insbesondere die temporäre Sicherheit und die Sicherheit kleinerer Veranstaltungen revolutionieren, da er nur eine geringe Fundamenttiefe hat und mit einem Generator oder einer temporären Stromversorgung betrieben werden kann.

ZABAG

Premiumprodukt ist ein Faltflügeltor

Der zertifizierte Flachfundamentpoller ist vor allem für die Sicherheit und den Schutz von Personen auf belebten Plätzen und innerstädtischen Bereichen geeignet. Aufgrund der flachen Fundamenttiefe von 300 mm ist der Z-HFFP 273 ideal in Fußgängerzonen und auf Rad- sowie Gehwegen einsetzbar. Die örtlichen Gegebenheiten – z. B. Versorgungsleitungen – werden dank des flachen Fundaments nicht berührt. Durch das Einbetonieren gewährleistet der feststehende Poller einen dauerhaften Zufahrtsschutz. Eine Zertifizierung von Pollern und Durchfahrtssperren erfordert reale Testszenarien in Form eines Crashtests. Dieser wird durch eine akkreditierte Prüfstelle durchgeführt, die bei erfolgreich bestandenem Test die amtliche Zulassung erteilt.

Premiumprodukt ist das Faltflügeltor MAPO FGZ. Dieses ist sowohl in der Basic-, Professional- als auch der Hochsicherheitsvariante erhältlich. Das MAPO FGZ überzeugt durch seine hohe Funktionalität und Wirtschaftlichkeit. Es kann durch seine platzsparende Bauweise sowohl in beidseitig begrenzten Durch- und Einfahrten als auch bei eingeschränktem Flügelschwenkbereich eingesetzt werden und überzeugt gleichzeitig durch seine hohe Öffnungs- und Schließgeschwindigkeit. Durch verschiedene Sonderausstattungen wie Gefälleanpassung, Durchbruchhemmung, Öffnungswinkel bis zu 110°, Übersteigschutz oder Sonderfüllungen und -beläge kann das MAPO FGZ individuell Ihren Bedürfnissen angepasst werden.

Sicherheitskonzept für Diamanten

Bharat Diamond Bourse (BDB) ist eine der größten Zentren für die Bearbeitung von Edelsteinen und speziell Diamanten weltweit. Mit über 4.000 Mitarbeitern, die sich mit dem Import und Export, dem Vermarkten von rohen und geschliffenen Diamanten beschäftigen, hat BDB unternehmerisch geschaffen, um ihre Transaktionen in höchstem Grad an Komfort und Sicherheit durchzuführen. Die Börse wurde ursprünglich erschaffen, um primär notwendige Infrastrukturanlagen für die Promotion der Diamantenausfuhr zu errichten, einschließlich Diamantenschmuck aus Indien, und um zu diesen Zwecken Hilfs- und Diensteinrichtungen darzubieten, um Indien letztendlich zu einem internationalen Handelszentrum für Diamanten, Juwelen und Schmuck zu machen.

Komplexe Infrastruktur

BDB Complex ist in einem weitläufigen Komplex mit einer Grundstücksfläche von 20 Hektar und einer bebauten Fläche von 186.000 qm untergebracht. Sie schließt zwei Keller mit zusätzlichen Quadratmetern für Parkmöglichkeiten und Versorgungsinfrastruktur ein. Ein hochmodernes Sicherheits- und Überwachungssystem rund um die Uhr und hat ein gewidmetes, gut ausgerüstetes und schnell reagierendes Team, um Krisen zu bewältigen. Solche sicherheitskritische Gebäude- und Unternehmenskomplexe benötigen grundsätzlich eine hochmoderne Sicherheits- und Überwachungsinfrastruktur.

Die Börse hat eine tägliche Mitarbeiter- und Besucherfrequenz von über 70.000 Personen und stellt angesichts der Millionenwerte einen kritischen Anlagenbetrieb dar. Die Sicherheit in den Unternehmensbereichen muss rund um die Uhr gewährleistet werden, was für BDB der wesentliche Grund war, eine Hochsicherheitslösung zu suchen.

„Wir haben nach etwas gesucht, das mehr ist als nur Sicherheitskameras und analoge Überwachung. Für die Diamantenbranche ist der höchste Standard an Sicherheit und Schutz

notwendig und mit einem noch fortgeschritteneren und offenen VMS-Überwachungssystem setzen wir einen hohen Maßstab für Sicherheitsstandards. Das dänische Unternehmen Milestone Systems wurde ausgewählt," führt Samir Jha, Head Security & Fire Safety, BDB, aus.

„Die Plattform hat sich als sehr benutzerfreundlich erwiesen, nicht nur in Sachen Installation und Konfiguration, sondern auch in Sachen Anwendung."

Samir Jha, Head Security & Fire Safety, BDB

Offenheit und Stabilität

Um alle Lücken in Sicherheitsmaßnahmen zu schließen, entschied sich BDB für Milestone Systems und vertraute der offenen VMS-Plattform. Das System zeichnet sich durch eine benutzerfreundliche Plattform aus, die allen Konformitätsanforderungen entspricht.

„Das Beste an Milestone war die Offenheit und Skalierbarkeit, mit der man jedes Kameramodell oder andere Systeme auf Milestone auswählen kann. Die Plattform hat sich als sehr bedienerfreundlich herausgestellt, nicht nur in Sachen Installation und Konfiguration, sondern auch in Sachen Anwendung. Sie hat alle unsere Anforderungen lokal und vor Ort mit hoher Verfügbarkeit in Sachen Videodaten erfüllt. Auch von unterwegs z.B. mit Smartphones und Tablets kann auf das Überwachungssystem zugegriffen werden.

Für die ordnungsgemäße, flächendeckende Installation aller rund 3.500 Plus Cameras benötigte man ungefähr zwei Jahre. Außerdem war nach den Installationen eine Verdoppelung der Systeme geplant, sowie eine Integration in das Zutrittskontrollsystem (ACS) und dem Videoanalysensystem (VA).

Viederbeschaffungsrate verbessert

Anbetracht des immensen Wertes von Diamanten ist das Wiederauffinden von gestohlenen Edelsteinen sehr wichtig. Dank der Sicherheitslösung von Milestone Systems konnten im Jahr 2020 beie BDB zu 100 % alle abhanden gekommenen Edelsteine wiederbeschafft werden.

„Die XProtect Mobile-App hat den unmittelbaren Zugriff auf das Überwachungssystem unterwegs durch Smartphones und Tablets unterstützt. Durch die App kann unser Sicherheitsteam, das jeden Tag raus auf Patrouille geht, Videos ansehen, abspielen und exportieren, sich Audiodateien anhören und durch die Kameras sprechen sowie auf Zutrittskontroll-Anfragen reagieren und Push-Benachrichtigungen über Ereignisse erhalten, die direkt auf einem Mobilgerät als Alarme ausgelöst werden können. Bestimmte andere Funktionalitäten wie MAPs, Smart Wall, Karussellansicht, Matrix usw. sind auch sehr hilfreich bei der proaktiven Überwachung".

Walter Crasto, Head IT, BDB. Fire Safety, BDB

„Es wird immer Leute geben, die versuchen, unsere Diamanten zu stehlen. Aber mit dem offenen VMS von Milestone System wird das für sie um einiges schwieriger werden. Sogar unsere verlorenen Diamanten kommen am Ende zu uns zurück. Wir setzen einen neuen Maßstab für Sicherheitsstandards. Für die Kontrolle der Sicherheit des gesamten Areals haben wir uns auf Milestone gestützt." Samir Jha, Head Security & Fire Safety, BDB

Auch außerdem des Betriebsgeländes kommt die VMS-Plattform ebenfalls zum Einsatz: So unterstützt BDB die Mumbai Stadtpolizei bei der Verkehrsüberwachung per Video in der Umgebung des Unternehmensareals mit Hilfe der offenen VMS-Plattformen.

Bharat Diamond Bourse

BDB hat im Bandra-Kurla Complex in Mumbai 2010 gestartet und hat jetzt über 4.000 Mitarbeiter, die sich mit dem Im- und Export, der Herstellung und dem Vermarkten von rohen und geschliffenen Diamanten beschäftigen. BDB hat einen Geschäftsrahmen geschaffen, um ihre Transaktionen in höchstem Grad an Komfort und Sicherheit durchzuführen.

Tagtäglich zieht die Börse hunderte an inländischen und internationalen Fachgemeinschaften für den Verkauf und Ankauf von Diamanten in jeder Größe, Form und Qualität, Diamanten jeden Grades und natürlich gefärbten Diamanten in jeder Schattierung an. Die Fähigkeit, jede Art von Waren zu liefern, macht Indien zu einem wichtigen Zentrum für Diamantenbearbeitung für Diamantenhändler weltweit.

ipoque

Kooperation zwischen Rohde & Schwarz und der Technischen Universität Chemnitz

Zweijähriges Kooperationsprojekt mit der TU Chemnitz verbindet Forschung und Entwicklung für eine innovative Softwarelösung zur Erhöhung der Cybersicherheit in 5G- und 6G-Kommunikationsnetzen

Die ipoque GmbH, ein Unternehmen von Rohde & Schwarz, kooperiert mit der Technischen Universität Chemnitz in einem Forschungsprojekt zu Cybersicherheit und digitaler Souveränität. Dabei arbeitet ipoque als Marktführer im Bereich Deep Packet Inspection (DPI) an einer weiteren technischen Innovation. Im Mittelpunkt des Projekts steht der Schutz vor DDoS- (Distributed Denial of Service) und Jamming-Angriffen. Derzeit gibt es nur wenige praktikable Lösungen für dieses Problem. Das gibt ipoque die Chance, mit einer passenden Lösung zu den Ersten auf dem Cybersecurity-Markt zu gehören.

Die Ausschreibung des Bundesamtes für Sicherheit in der Informationstechnik, der ipoque im September 2022 gefolgt ist, trägt den Titel "Cyber-Sicherheit und digitale Souveränität in den Kommunikationstechnologien 5G/6G".
Im Mittelpunkt des Projekts von ipoque steht die Erforschung eines Systems, das es Providern ermöglicht, Mobilfunknetze sicher zu betreiben. ipoque hat sich in Kooperation mit der Professur für Kommunikationsnetze (Dr.-Ing. Thomas Bauschert) und der Professur für Nachrichtentechnik (Prof. Dr. Klaus Mößner) der Technischen Universität Chemnitz beworben. Es ist eine optimale Synergie zwischen Forschung und Entwicklung.
Zudem planen wir eine ständige Kommunikation mit namhaften Mobilfunkanbietern, um ein möglichst breites Nutzerspektrum zu gewährleisten. Damit unterstützt die Realisierung dieses Projektes nicht nur den Wissenstransfer, sondern sichert auch Arbeitsplätze, fördert die Unabhängigkeit der Mobilfunk- und Sicherheitsindustrie und trägt zur digitalen Souveränität Deutschlands bei.

Das Know-how für dieses Projekt stammt aus dem aktuellen Produktportfolio von ipoque, das sich durch hochperformante Analytiklösungen auszeichnet. Die DPI-Engines R&S® PACE 2 und R&S®vPACE identifizieren und klassifizieren Tausende von Anwendungen und Protokollen und extrahieren Metadaten in Echtzeit, selbst wenn der Verkehr verschlüsselt oder verschleiert ist. Das User- und Control-Plane-Korrelationsmodul R&S®GSRM ermöglicht es Anbietern von Mobilfunklösungen, teilnehmerspezifische GTP-Sitzungen zu filtern, weiterzuleiten und einen Lastausgleich durchzuführen.

Bislang arbeiten die meisten 5G-Netze nach dem sogenannten "Security by Obscurity"-Ansatz. Mobilfunknetzbetreiber und Unternehmen preisen das Netz als sicher an, aber die Sicherheit der Systeme selbst kann nicht nachgewiesen werden, ohne ihre Funktionsprinzipien offenzulegen.
Das macht es Angreifern leichter, Schwachstellen zu identifizieren und auszunutzen, die den Betreibern möglicherweise unbekannt sind. ipoque entwickelt diese Lösung, um dies zu verhindern und gleichzeitig die Sicherheit von 5G- und 6G-Mobilfunknetzen zu bewerten und zu gewährleisten. Nutzer und Betreiber profitieren beide von den neuesten verfügbaren Technologien.

HMF Smart Solutions

Aus Hytera Mobilfunk wird die HMF Smart Solutions GmbH

Hytera Mobilfunk firmiert nun offiziell unter dem neuen Namen HMF Smart Solutions GmbH.
Mit dem offiziellen Eintrag im deutschen Handelsregister ist es jetzt amtlich: Hytera Mobilfunk firmiert nun offiziell unter dem neuen Namen HMF Smart Solutions GmbH. Damit ist ein weiterer großer sichtbarer Schritt zur Transformation des niedersächsischen Unternehmens getan.

„Die ganze PMR-Branche und wir als Unternehmen befinden uns mitten im Wandlungsprozess. Als HMF Smart Solutions haben wir uns für die Zukunft neu aufgestellt. Mit unserem Firmennamen machen wir auf den ersten Blick deutlich: Wir sind nicht nur die Spezialisten für maßgeschneiderte Kommunikationslösungen im Bereich Professioneller Mobilfunk, sondern auch kompetenter Lieferant und Partner für smarte Digitalisierungslösungen und Systemintegration", begründet CEO Matthias Klausing die Namensänderung.

Die Wenigsten wird der neue Name überraschen: „Wir sind als HMF in der Branche bereits seit vielen Jahren fest etabliert", erläutert Marketingleiterin Dr. Katharina Tadje. „HMF Smart Solutions – wir freuen uns auf die Zukunft. Mit neuem Namen. Mit smarten Lösungen und innovativen Technologien. Gemeinsam mit unseren Partnern und Kunden."

Comelit/BAB Technologie

Kooperation von zwei Hidden Champions

Mit dem INTERCOM MODULE von BAB-Technologie ist die volle Integration einer Video-Türsprechanlage in die Gebäudevisualisierung möglich. Jetzt gilt das auch für alle IP-basierten Video-Türsprechanlagen von Comelit. Damit ergeben sich ganz neue Möglichkeiten, nicht nur für Comelit-Kunden. Die strategische Kooperation der beiden Hidden Champions dient dem weiteren Ausbau der KNX Smart Home Möglichkeiten im Bereich der Gebäudeautomation und definiert den neuen Standard im Segment Sicherheitstechnik.

"Die Integration von Videosprechanlagen unterschiedlicher Hersteller in smarte Umgebungen ist eine der häufigsten Anforderungen unseres Marktes. Mit dem INTERCOM MODULE haben wir eine flexible Lösung zur einfachen Umsetzung dieser Aufgabe geschaffen. Wir freuen uns ganz besonders, dass wir nun einen der gefragtesten Hersteller an Bord willkommen heißen dürfen und allen Anwendern von Comelit-Produkten die Möglichkeit bieten können, diese in KNX Systeme zu integrieren", so Stefan Mainka, Business Development Manager bei der Dortmunder BAB TECHNOLOGIE.

"Wir können es kaum erwarten, interessierten Installateuren auf der bevorstehenden Fachmesse für Elektrotechnik in Dortmund, die Möglichkeiten dieser Kooperation vorzustellen und unseren Anspruch, der sich in unserem Slogan -With You Always- wiederfindet, noch einmal zu bestätigen. Wir freuen uns zudem mit der BAB-Technologie als starken Partner der gesamten Branche ganz neue Perspektiven mit Comelit-Produkten aufzeigen zu können", ergänzt Daniel Latzke, Technischer Leiter Comelit.

Berg Insight

Straftäterüberwachung

Der Markt für die Fernüberwachung von Straftätern wird bis 2026 um über 10 % wachsen

Berg Insight hat einen neuen Marktbericht über den Sektor der elektronischen Straftäterüberwachungslösungen veröffentlicht. Diese zweite Ausgabe des Berichts analysiert die neuesten Entwicklungen beim Einsatz von RF- und GPS-Tracking-Lösungen in den Strafjustizsystemen in Europa, Nord- und Südamerika.

Die durchschnittliche Zahl der täglich überwachten Personen in Europa, Nordamerika und Lateinamerika belief sich im Jahr 2021 auf etwa 50.000, 371.000 bzw. 96.000.

Berg Insight schätzt, dass die Zahl der täglichen Nutzer bis 2026 auf 77.000 in Europa, 821.000 in Nordamerika und 184.000 in Lateinamerika steigen wird.

Der Marktwert im Jahr 2021 erreichte 947 Millionen US-Dollar in Nordamerika, 224 Millionen US-Dollar in Europa und 75 Millionen US-Dollar in Lateinamerika.

Der Gesamtmarktwert in den drei Regionen zusammen wird voraussichtlich mit einer CAGR von 10,8 Prozent von 1,2 Milliarden US-Dollar im Jahr 2021 auf 2,1 Milliarden US-Dollar im Jahr 2026 wachsen.

Elektronische Überwachungsprogramme (EM) wurden erstmals in den frühen 1980er Jahren in den USA eingeführt. Heute ist die elektronische Überwachung in ganz Europa und Nordamerika sowie in einigen lateinamerikanischen Ländern eine etablierte Alternative zur Inhaftierung. Die elektronische Überwachung kann in verschiedenen Phasen des Strafrechtssystems eingesetzt werden, u. a. in der Voruntersuchung, bei der Verurteilung und nach einer Haftstrafe.

Es gibt zwei vorherrschende Technologien für die elektronische Überwachung - Radiofrequenz (RF) und GPS. Die RF-Technologie war die erste Technologie, die eingesetzt wurde und es den Behörden ermöglichte, aus der Ferne zu überwachen, ob Straftäter, die zu einer Ausgangssperre verurteilt wurden, die Regeln des Programms einhielten. RF-basierte Systeme sind heute in den meisten europäischen Ländern die gängigste Art von Lösung. In den USA, Brasilien und anderen lateinamerikanischen Ländern sind GPS-basierte Lösungen üblicher.

Eine Reihe von Privatunternehmen und Behörden sind an der Bereitstellung von EM beteiligt, einschließlich der Lieferung und Installation von Geräten, der Überwachung und der Durchsetzung. In Nordamerika, Lateinamerika und in einigen europäischen Ländern sind private Unternehmen stark involviert. In den meisten europäischen Ländern liefern private Unternehmen hauptsächlich Geräte und Software, während die Behörden für die Installation, Überwachung und Durchsetzung zuständig sind.

North Carolina State University

Flüssigmetall stoppt Gase und Feuchtigkeit

Neues ideales Verpackungsmaterial für Elektronik

Forscher der North Carolina State University (www.ncsu.edu) haben erstmals eine elastische Folie entwickelt, die weder Flüssigkeiten noch Gase passieren lässt. Laut Wissenschaftler Michael Dickey ließe sich dies als ideales Verpackungsmaterial für hochwertige elektronische Geräte nutzen, die empfindlich auf äußere Einflüsse reagieren. "Seit Langem gilt, dass Elastizität und Gasdichtheit einander ausschließen. Grundsätzlich sind Werkstoffe, die gut darin sind, Gase fernzuhalten, hart und steif. Und Dinge, die Elastizität bieten, lassen Gase passieren. Wir haben uns etwas einfallen lassen, das die gewünschte Elastizität bietet und gleichzeitig Gase fernhält", so Dickey. Die neue Technik, an deren Entwicklung auch Tao Deng von der Shanghai Jiao Tong University (en.sjtu.edu.cn) beteiligt ist, nutzt eine eutektische Legierung aus Gallium und Indium (EGaIn). Eutektisch bedeutet, dass die Legierung einen niedrigeren Schmelzpunkt hat als die beiden Metalle, aus denen sie besteht. Das EGaIn ist bei Raumtemperatur flüssig. Dickeys Team hat daraus einen dünnen Film hergestellt und ihn mit einem elastischen Polymer umhüllt. Die Innenfläche des Polymers haben die Fachleute mit mikroskaligen Glasperlen besetzt, die verhindern, dass sich das EGaIn an bestimmten Stellen konzentriert. Das Ergebnis ist ein elastischer Beutel aus flüssigem Metall, der keine Gase oder Flüssigkeiten ein- oder auslässt."

Die flüssigen Metalle sind ziemlich teuer. Wir sind jedoch optimistisch, dass wir die Technik optimieren können, indem wir zum Beispiel den EGaIn-Film dünner machen, um die Kosten zu senken", sagt Deng. Derzeit würde ein einzelner Beutel mehrere Dollar kosten. "Wir suchen nach Industriepartnern, um das Verfahren zu kommerzialisieren", ergänzt Dikkey. Das neue Material käme auch für Dichtungen bei flexiblen Rohrleitungen infrage - oder als Hülle für flexible Batterien.

Quantensichere Identitäten für eine digitale Zukunft

Deutscher Forschungsverbund startet Projekt »Sichere Quantenkommunikation für Kritische Identity Access Management Infrastrukturen – Quant-ID«

Die Sicherheit digitaler Identitäten wird durch zukünftige Quantentechnologien bedroht. In den Händen von Angreifern werden Quantencomputer auch in der Lage sein, klassische Verschlüsselungsverfahren zu brechen. Um solche Angriffe abzuwehren, forschen vier Partner in dem Projekt Quant-ID an der Entwicklung von neuartigen Verfahren und Systemen,

die auf Basis von Quantenzufallszahlen und Post-Quantum-Kryptographie die kryptographische Sicherheit auch langfristig garantieren. Gerade hochsensible Bereiche, wie staatliche Einrichtungen, Banken, Krankenkassen oder Versicherungen werden dadurch den notwendigen Schutz erhalten. Das vom BMBF geförderte Projekt startete im September 2022 mit einer Laufzeit von drei Jahren.

Um eine größere Akzeptanz für die Digitalisierung von Dienstleistungen und Geschäftsprozessen in der Gesellschaft zu erreichen, müssen benutzerfreundliche, zuverlässige und die Privatsphäre schützende Verfahren etabliert werden. Im Projekt »Sichere Quantenkommunikation für Kritische Identity Access Management Infrastrukturen (Quant-ID)« forschen deshalb die Quant-X Security & Coding GmbH, das Fraunhofer-Institut für Photonische Mikrosysteme IPMS, die MTG AG sowie die Universität Regensburg gemeinsam an verlässlichen digitalen Identitäten. Die Verwendung von aktuell genutzten Netzwerkprotokollen soll hierbei den Übergang von klassischen Verschlüsselungsalgorithmen zu quantensicheren Verfahren erleichtern. Abweichend vom ursprünglichen physikalischen Begriff bezeichnet Quantensicherheit dabei hier den Schutz gegen Angriffe durch Quantencomputer.

»Unser Ziel ist die Entwicklung einer quantensicheren Autorisierung von Nutzern in einer IAM-Architektur (Identity Access Management) unter Zuhilfenahme von Quantenzufallszahlen und Post-Quanten-Kryptographie«, erklärt Dr. Alexander Noack, Gruppenleiter am Fraunhofer-Institut für Photonische Mikrosysteme IPMS. Unter Post-Quanten-Kryptographie (PQC für engl. Post Quantum Cryptography) werden kryptographische Algorithmen verstanden, die zwar auf klassischer Hardware verwendet werden, welche jedoch Sicherheit gegenüber Angriffen mit Quantencomputern versprechen. Die für diese Verfahren notwendigen echten Zufallszahlen sollen im Projekt zur Steigerung der Sicherheit durch einen Quantum-Random-Number-Generator (QRNG) erzeugt werden.

»Zusätzlich wollen wir auch die Netzwerkkommunikation, Signaturen und Datenbankverschlüsselung durch Post-Quanten-Kryptographie absichern«, so Dr. Alexander Noack. Ein weiteres Ziel des Gemeinschaftsprojekts ist die Entwicklung eines quantensicheren »Single-Sign-On« Ansatzes, der den Zugriff auf verschiedene Dienste mit einer einzigen zentralen Anmeldung ermöglicht. Zum Projektende werden die digitalen Identitäten und die quantensichere Autorisierung in einem Demonstrator in einer realistischen Anwendung über bestehende Netzwerkprotokolle erprobt. Dabei werden die Fähigkeiten des entwickelten Systems mit klassischen Verfahren verglichen. Die Ergebnisse der Teilprojekte werden auch modular anwendbar sein. Dies bietet Netzwerkadministratoren und Systemverantwortlichen die Möglichkeit, entweder das gesamte System oder nur Teilaspekte zu intgrieren.

Durch die Konzeptentwicklung in Deutschland wird die Souveränität mit Blick auf die Sicherheit nationaler informationstechnischer Systeme gestärkt. Vor diesem Hintergrund ergibt sich ein besonders hohes Marktpotenzial der Projektlösung in hochsensiblen Bereichen und kritischen Infrastrukturen wie im Bereich der Banken, Versicherungen, Unternehmen des Gesundheitsbereiches sowie Behörden und staatlichen Einrichtungen. Gerade diese Marktteilnehmer sind darauf angewiesen, hohe Sicherheitsstandards zu erfüllen, da sie vielfach immer komplexer werdenden Angriffsstrukturen ausgesetzt sind.

Um die Verwertung des Quantenzufallsgenerators zu unterstützen, wird zudem eine Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) angestrebt. Motivation des Konsortiums ist es, ein interdisziplinäres Projektteam aufzubauen, Partnerschaften in Deutschland für Gesamtlösungen zu etablieren und Absicherungstechnologien gegen Angriffe mit Quantencomputern jedermann zugänglich zu machen.

»Mit diesem Projekt wollen wir die Grundlage für interdisziplinäre Kooperationen zur effizienten Realisierung von Quantensicherheit in

Deutschland schaffen«, so der Gruppenleiter des Fraunhofer IPMS. Die daraus entstehende quantensichere Version von OpenID Connect soll der Allgemeinheit für geringe Kosten als Open-Source-Bibliothek zugänglich gemacht werden.

Somit schafft Quant-ID die Grundlage für einen hochsicheren Schutz in kritischen Infrastrukturen in einer End-to-End-Lösung in Deutschland. Durch den Use Case »Quantensichere eID« wird das Sicherheitsniveau gegen Cyberangriffe für alle ansässigen Unternehmen und staatlichen Einrichtungen erhöht.

Gleichzeitig wird eine Grundlage für die langfristige Sicherheit von Identitätsdaten und anderen sensiblen Daten deutscher Bürger geschaffen. »Das Projekt verfolgt über diesen Weg den Ansatz, die ethischen, gesellschaftlichen und wirtschaftlichen Werte Deutschlands früh genug vor fremden staatlichen und kriminellen Angriffen zu schützen«, so Dr. Alexander Noack abschließend.

Die internationale Positionierung als deutsches Konsortium in einer neu zu schaffenden öffentlichen OpenID-Working-Group mit dem Ziel der Definition von »OpenID-Quantum« garantiert außerdem den parallelen Anschluss an internationale Standardisierungsvorhaben.

[www.quant-id.de]

Beteiligte Einrichtungen des Quant ID

Verbundkoordinator:

Quant-X Security & Coding GmbH ist ein Startup mit Schwerpunkt Informationssicherheit. Die Expertise der Firma beruht auf 10 Jahren Beratungserfahrung für Fintechs und Banken. Die Beratungsleistungen umfassen Konzeption, Planung, Entwicklung, Steuerung, und Qualitätssicherung im Bereich Informations- sicherheit. Experten von Quant-X wurden mit Implementation und Troubleshooting von IAM-Infrastrukturen in mehreren Projekten beauftragt, unter anderem für VWFS, Deutsche Bank und die Bundesdruckerei. Mit verschiedene Quantentheorie- und Sicherheits-Experten untersucht Quant-X ausgewählte offene Fragen zum Thema Quantensicherheit mit Fokus auf konkrete Anwendungen.

Das **Fraunhofer-Institut für Photonische Mikrosysteme IPMS** erforscht mikroelektronische und mikromechanische Low-Power-Sensoren, Aktoren sowie optische, drahtlose Hochgeschwindigkeitsdatenkommunikation. Als innovativer Entwicklungsdienstleister für elektronische und photonische Mikrosysteme finden sich in allen großen Märkten – wie Information und Kommunikation, Fahrzeugtechnik, Halbleiter, Mess- und Medizintechnik - innovative Produkte, die auf am IPMS entwickelten Technologien basieren. Auch Hochgeschwindigkeits-FPGA- und Mixed-Signal-ASIC-Design gehören zum Portfolio. Die elektronische Ansteuerung und Auswertung von Qubits und aktiven photonischen Einzelelementen bis hin zu Rechenbeschleunigern über dedizierte integrierte Elektronik liegen dabei im Fokus.

Seit der Gründung im Jahr 1995 ist die **MTG AG** einer der Spezialisten für anspruchsvolle Verschlüsselungstechnologien in Deutschland. Die innovativen IT-Security Lösungen von MTG sichern kritische Infrastrukturen und das Internet der Dinge effektiv ab. MTG beteiligt sich an dem Förderprojekt QuantumRISC des Bundesministeriums für Bildung und Forschung (BMBF) und hat das Förderprojekt Use-A-PQClib des Hessischen Ministerium für Wissenschaft und Kunst (HMWK) erfolgreich abgeschlossen. Im Rahmen dieser beiden Forschungsprojekte hat MTG umfangreiche Erfahrungen in der Entwicklung und Integration von PQC-Verfahren in Software gesammelt.

Die **Universität Regensburg (UR)** ist eine bayrische Volluniversität, deren jüngste Fakultät, die Fakultät für Informatik und Data Science (FIDS), erst im Jahr 2020 gegründet wurde. Seit 2021 wird der Lehrstuhl für Datensicherheit und Kryptographie von Prof. Dr. Juliane Krämer besetzt. Die Arbeitsgruppe QPC (Quantum and Physical attack resistant Cryptography) von Prof. Krämer erforscht alle fünf Familien der Post-Quantum- Kryptographie bzgl. verschiedener Aspekte, z.B. [ABB+20, GHK+21, GKS21, KS20, RKK20]. Die Gruppe ist Teil verschiedener Forschungsprojekte, z.B. DFG-SFB CROSSING, QuantumRISC, Aquorypt, 6G-RIC. In das vorliegende Projekt Quant-ID bringt Prof. Krämer ihre umfangreiche Expertise in der Analyse, Entwicklung und Integration von PQC-Verfahren ein.

Euralarm hat ein Position Paper zum Cyber Resilience Act veröffentlicht. (Photo: © Artur Szczybylo)

Euralarm

Position Paper zum Cyber Resilience Act

Euralarm hat ein Position Paper zum Cyber Resilience Act veröffentlicht. Das Position Paper enthält die Ansicht von Euralarm zu den Elementen des vorgeschlagenen Cyber Resilience Act, die für die veröffentlichte Gesetzgebung beibehalten werden sollten, identifiziert einige Unklarheiten, die, wenn sie beibehalten werden, unsere Hersteller in eine gewisse Rechtsunsicherheit führen würden, und schlägt mehrere Änderungen des Textes vor. Das Cyber Resilience Act ist der Vorschlag für eine Verordnung über Cybersicherheitsanforderungen für Produkte mit digitalen Elementen. Mit dem Gesetz sollen die Cybersicherheitsvorschriften gestärkt werden, um sicherere Hardware- und Softwareprodukte zu gewährleisten. Die vorgeschlagene CRA enthält viele Grundsätze, die Euralarm als positive Beiträge zum europäischen Binnenmarkt begrüßt.

Die Bewertung des Verordnungsvorschlags durch Euralarm und die Gespräche mit dem CRA-Team der GD CONNECT haben jedoch gezeigt, dass es noch Raum für Verbesserungen gibt, um die Rechtssicherheit für die Hersteller und die Verhältnismäßigkeit des Geltungsbereichs und der Kategorisierung zu gewährleisten und gleichzeitig das Gesamtziel der Erhöhung der Cyber-Resilienz der europäischen Gesellschaft zu wahren. Euralarm hat in seinem Position Paper Verbesserungsmöglichkeiten aufgezeigt und Vorschläge zur Klärung des Textes und zur Verbesserung der Verhältnismäßigkeit der Verordnung unterbreitet. Euralarm fordert die Mitgesetzgeber auf, diese sorgfältig zu prüfen.

Exemplare des neuen Euralarm Position Papers können von der Euralarm-Website heruntergeladen werden.

MOBOTIX

M16 Therma: Brandschutz-Zertifizierung auch in Österreich

Die Prüfstelle für Brandschutztechnik des österreichischen Bundesfeuerwehrverbandes (PBST) bestätigt der MOBOTIX M16 Thermal-Infrarot Kameraeinrichtung zur Temperaturüberwachung die erfolgreichen Prüfungen zum Einsatz in Brandmeldeanlagen. Mit dieser Prüfung nach TRVB 123 S - Brandmeldeanlagen (TRVB = Technische Richtlinien vorbeugender Brandschutz) und dem positiven Prüfbericht kann die MOBOTIX Kamera auch in Österreich selbst in bestehende Brandmeldeanlagen eingebaut werden.

„Die von der PBST geprüfte Kamera ist eine M16 Thermal TR, die zusätzlich einen optischen Sensor mitverwenden kann. Diese Kombination aus Thermal- und optischem Bild wurde vom Prüfer als zusätzlicher Benefit besonders positiv vermerkt. Dieses Vertrauen und den Rückenwind möchten wir am attraktiven Markt rund um die Brandprävention gerne gewinnbringend umsetzen. In Österreich sind bereits eine Roadshow in Linz und weitere lokale Partner-Events geplant", so MOBOTIX Vice President Sales EMEA, Christian Heller. Der Markt der Brandschutztechnik in Österreich erreichte 2021 bei einer Steigerung von 4 % zum Vorjahr ein Gesamtvolumen von 233 Millionen Euro. (Quelle: Verband der Sicherheitsunternehmen Österreichs).

Die MOBOTIX Thermal-Kameratechnologie ist bereits von drei international anerkannten Institutionen zertifiziert: VdS (VdS Schadenverhütung GmbH), EN 54-10 (EU-Norm) und CNPP (Französisches nationales Zentrum für Prävention und Schutz).

DKE

DKE legt Entwurf für Vornorm Perimeterschutz vor

Vom Freibad bis zum Flughafen – E DIN VDE V 0826-20 beschreibt Qualitätsmaßstäbe für Betreiber, Planer und Errichter von Perimeter-Sicherungs-Systemen. Perimetersicherung bietet Lösungen für unterschiedlichste Angriffs-Szenarien. Es geht darum, unerwünschten Zutritt frühzeitig zu erkennen, um Zeit für Intervention zu gewinnen.

Perimeter-Sicherungs-Systeme (PSS) werden direkt an der Grundstücksgrenze eingesetzt und sind vor allem zur Absicherung kritischer Infrastruktur zentral. Sie sollen helfen, Liegenschaften besser zu schützen, indem unerwünschter Zutritt möglichst früh erkannt wird. Dabei sind die Aufgabenstellungen divers und reichen vom Freibad zur Verhinderung von Vandalismus bis hin zur Absicherung von Flughäfen oder Industrie-Parks. Der DKE Arbeitskreis Perimeter Protection liefert nun wichtige Qualitätsmaßstäbe für Betreiber, Planer und Errichter von PSS. Der Entwurf der Vornorm E DIN VDE V 0826-20 wurde auf der Fachmesse Perimeter Protection in Nürnberg offiziell vorgestellt. Er gilt als Meilenstein auf dem Weg zu hochwertigen Perimeter-Sicherheitslösungen.

Radar-Technologie und Drohnendetektion

Die Perimetersicherung nutzt mechanische und elektronische Systeme bis hin zu Radar-Technologie und Drohnendetektion und bietet Lösungen für unterschiedlichste Angriffs-Szenarien. Der entscheidende Vorteil liegt in der gewonnenen Reaktionszeit für Interventionsmaßnahmen durch eine frühzeitige Detektion im Außenbereich. „Ereignisse wie die Blockade von Flughäfen oder die Sabotage von Bahn- oder Energieinfrastruktur zeigen, dass der Schutz vor und an der Grundstücksgrenze ein elementarer Baustein jedes Sicherungskonzepts sein sollte", sagt Jürgen Schiller, Vorsitzender des DKE Arbeitskreises Perimeter Protection.

Mit der Vornorm will DKE ein Rahmenwerk schaffen, um Betreiber und Errichter von PSS zu helfen, Anforderungen zu definieren und zu dokumentieren. So soll Planern geholfen werden, geeignete Lösungen für ihr Schutzziel und den damit verbundenen Risiken zu finden. Ziel soll sein, alle normativen Anforderungen zu erfüllen und die Investitionen nachhaltig zu machen.

VfS
Verband für Sicherheitstechnik eV

VFS KONGRESS 2023

KRISE HEUTE – CHANCE MORGEN!

危机

SAVE THE DATE

25./26. APRIL, LEIPZIG
www.vfs-hh.de