EURO SECURITY

Das deutsche Fachmagazin für Sicherheit und Management in der DACH Region

- **Drohnentechnik**
  Neue Partnerschaft: Erster digitalen Risiko-Check für Drohnenflüge
- **Schließanlagen**
  Schutz des geistigen Eigentums in der Automobilbranche
- **Cybersecurity**
  Report: Mehr Datenschutzverletzungen und höhere Ausfallzeiten

ISSN 09481249 • 3-2023 • ZKZ 16724 Postvertriebsstück bezahlt • 80383 BAY Germany ©SEC Global • euro-security.de

Inhalt

KRITISCHE INFRASTRUKTUR

STANDARDS

TITELSTORY

UNTERNEHMEN

VERBÄNDE

VIDEOTECHNOLOGIE

Das Titelbild

Die INTUS Zutrittsleser-Familie bietet Modelle für alle Einsatzmöglichkeiten

- Integration in Schalterprogramme und Türsprechanlagen
- Alle gängigen Leseverfahren (aktuelle RFID-Technologie) wie LEGIC prime, LEGIC advant, MIFARE® Classic, MIFARE® DESFire EV1/EV2/EV3
- Nutzung der App ID.mobile mit Bluetooth© Low Energy (ab Leserversion Lx6)
- Für höhere Sicherheitsanforderungen: Zwei-Faktor-
- Authentifizierung mittels PIN und/oder Biometrie
- Verschlüsselte Datenübertragung zum Zutrittskontrollmanager [www.pcs.com]

ZUTRITTSKONTROLLE

Editorial

Wenn der Kunde aufs Abstellgleis geschoben wird

Arlo mit dem Mehrheitseigner Netgear ist Anbieter von smarten Überwachungskameras. Nach eigenen Angaben wurden 2022 21,6 Millionen Geräte ausgeliefert, verfügt das Unternehmen über 5,82 Millionen registrierte Konten und hat rund 877.000 Kunden im Abo-Bestand. Arlo Kameras können zwar auch ohne Abonnement betrieben werden, haben aber in diesem Fall keine Konfigurationsmöglichkeiten, die den Schutz von Grundstücken und den eigenen Wänden eines Kunden individuell erhöhen. Damit bietet diese smarte Sicherheitslösung dem Kunden dieselbe Funktionspallette, wie Marktbegleiter Ring, welches ein Amazon Unternehmen ist. Ohne Abonnement als kein Mehrwert zu generieren. Ohne Updates erhalten Kunden auch keine sicheren und funktionell angepassten Bedien- und Leistungsoptionen. Dieser Fakt bringt von diesem Jahr an, Benutzer von älteren Arlo-Produkten an Ihre Grenzen. Denn seit Anfang des Jahres 2023 verfolgt Arlo eine neue EOL Policy (End Of Life Policy) und schließt damit auf Dauer diese Produkte vom Support aus. Bestimmte Kameras bekommen bald also keinen Support mehr. Schon ab April werden einige Arlo Sicherheitslösungen nicht mehr unterstützt, bekommen keine Updates mehr und es werden Cloud-Funktionen reduziert oder gar eingestellt. So gibt es den kostenlosen Cloud-Speicher nicht mehr und auch Benachrichtigungs-E-Mails sollen dem Kunden nicht mehr zugestellt werden. Eine kalte Enteignung und sicher nicht so leicht für die Kunden zu akzeptieren.

Zu verstehen wäre eine Veränderung eines Onlineservices, wenn die Qualität der Kamaeras bei der Videoüberwachung zu schlecht ist, die Funktionalität des Babyphones nur noch über Rauschen definiert werden kann oder wirklich ein Verschleiß bei der Hardware festzustellen wäre, aber einfach den Hahn zuzudrehen und vollendete Tatsachen zuschaffen, ist ethisch eine verfehlte Vertriebspolitik. Oder nicht? Die professionelle Sicherheitsbranche war bei Einführung der Arlo-Kameras nicht gerade erfreut. Doch das Marktsegment ‚Smart Home' hat sich nun mal als eigenständiger Markt in den letzten Jahren erheblich weiterentwickelt und zeigt an Hand der Marktdaten, wie gut sich Unternehmen wie Arlo und Ring etabliert haben. Sicherheit bedeutet für Menschen jedoch Verläßlichkeit. Die Sicherheitsbranche könnte eine Menge von Kunden zurückgewinnen, wenn der Aspekt ‚Produktlebenszeit' in Kombination mit Leitstellen- oder Cloudservices doch in den Vordergrund gestellt würde. Der Kunden möchte Vertrauen und wer will denn solchen Unternehmen vertrauen, die Kunden einfach auf dem Abstellgleis stehen lassen.

Dr Claudia Mrozek

Impressum

ISSN 09481249

Redaktion *Euro Security Fachmedien; Dr Claudia Mrozek; 83083 Riedering, Tel: +49 (0)8036 3035071; 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 Überbayern, Bestellungen und Druckvorlagen: anzeigen@euro-security.de*

NXP

Neue MCU für eine sichere und schnellere NFC-Authentifizierung

Die sichere, vernetzte Ein-Chip-Lösung kombiniert ein vollständiges NFC-Lesegerät, eine konfigurierbare Arm Cortex-M33-MCU und eine komplette Sicherheits-Toolbox, um eine schnellere und sicherere NFC-Authentifizierung und Kommunikation zu ermöglichen.

NXP Semiconductors stellt mit dem PN7642 eine Ein-Chip-Lösung mit einer kundenspezifisch anpassbaren MCU, einem NFC-Lesegerät und SESIP-Level-2-Sicherheit vor. Sie schafft die Grundlage für zahlreiche NFC-Anwendungen wie schnellere und sicherere NFC-Transaktionen für physische Zugangslösungen, Authentifizierung von Verbrauchsmaterialien, sichere Identitätsüberprüfung und vieles mehr.

NFC-Technologie ist zu einem grundlegenden Element für die sichere Authentifizierung geworden. Sie kann beispielsweise überprüfen, ob eine Person, die vor der Haustür steht, vom Hausbesitzer Zutritt erhalten hat. Oder sie kann bestätigen, dass das Verbrauchsmaterial, das in ein medizinisches Gerät eingelegt wurde, für die Verwendung mit diesem Gerät zugelassen ist.

„NFC ist für die sichere Authentifizierung sowohl von Personen als auch von Waren unverzichtbar geworden", sagt Alasdair Ross, Senior Director, NFC IoT Security, NXP. „Durch die Kombination einer konfigurierbaren MCU mit einer vom NFC-Forum zertifizierten NFC-Lösung und einer kompletten Sicherheits-Toolbox vereinfacht der PN7642 die Integration der NFC-Technologie in neue oder bestehende Authentifizierungslösungen."

Der PN7642 verfügt über einen hochleistungsfähigen, vom NFC-Forum zertifizierten NFC-Leser mit 2W Ausgangsleistung. Die integrierte konfigurierbare Arm Cortex-M33 MCU umfasst 180kB Flash, 20kB RAM und eine Vielzahl von Controller- und Host-Schnittstellen. Das Produkt verfügt zudem über eine SESIP-Level-2-Zertifizierung, eine vollständige Sicherheits-Toolbox, einen Krypto-Beschleuniger und einen sicheren Schlüsselspeicher, die allesamt durch Software unterstützt werden.

Hochschule Offenburg

Empathische Roboter revolutionieren Pflege

"EmoCare" hat die Akzeptanz und den Nutzen von Robotiksystemen untersucht

Empathische Robotiksysteme mit unterschiedlichen Erscheinungsbildern und Größen kommen bei Pflegebedürftigen gut an und könnten die Arbeit von Betreuungskräften erleichtern. Zu dem Schluss kommt das Forschungsprojekt EmoCare der Hochschule Offenburg (www.hs-offenburg.de).

Freude, Trauer, Angst und Ärger erkennen

Das System kann anhand spezifischer Sensoren Emotionen und mentale Zustände wie Freude, Trauer, Angst, Ärger oder Schmerz bei Pflegebedürftigen erkennen, klassifizieren und interpretieren. So ist es möglich, das Pflegepersonal dabei zu unterstützen, das Verhalten und die Stimmung der Bewohner besser zu verstehen und angemessen darauf zu reagieren.

In Kooperation mit dem St. Carolushaus (www.st-carolushaus.de) war EmoCare über einen Zeitraum von zwei Jahren auch erprobt worden. Interessierte Bewohner des Pflegeheims hatten sich für die notwendigen Tests zur Verfügung gestellt. Ziel dabei war es, das Robotiksystem zu trainieren und die Akzeptanz eines solchen Systems unter Realbedin- gungen wissenschaftlich zu untersuchen.

Hybride RFID-Technologie

Verlässliche Zeiterfassung und schnelle Zutrittskontrolle beim Logistik-Dienstleister LOXXESS

2022 erreicht LOXXESS einen weiteren Meilenstein: Im tschechischen Bor, in Grenznähe zu Deutschland, wird Ende des Jahres eine neue Logistikhalle mit 68.000 m2 in Betrieb genommen. Zukünftig wird hier die Warendistribution für einen Großkunden abgewickelt. Mit dieser Standorterweiterung schafft LOXXESS wichtige Ressourcen für das Wachstum des Kunden.

Für eine Logistik in dieser Größenordnung mit branchenüblichen Schwankungen und Auftragsspitzen bedarf es effizienter Prozesse in allen Unternehmensbereichen. Deshalb holte sich LOXXESS bei den ersten Planungen für die Infrastruktur der Halle Unterstützung vom langjährigen IT-Lösungspartner SOFT-CONSULT Häge GmbH. Bereits seit 2007 begleitet der Digitalisierungspartner den Kunden LOXXESS. Er betreut unter anderem die Lösungen für Zeitwirtschaft, Zutrittskontrolle sowie Lohn und Gehalt.

Herausforderung: Ältere und neue RFID-Technologie für Zeiterfassung und Zutritt.

Seit vielen Jahren nutzt LOXXESS an allen Standorten die INTUS-Zeiterfassungsterminals und -Zutrittssysteme von PCS Systemtechnik GmbH. Personalleiterin Jeanette Uhlmann fasst die Erfahrungen zusammen: „Die INTUS-Terminals laufen gut und sind viele Jahre bei uns im Einsatz. Manche Terminals werden mit umgezogen und am neuen Standort weiter genutzt". Im Sinne der Nachhaltigkeit wird die Hardware so lange erhalten, wie sie funktioniert. Allerdings stieß diese Philosophie in jüngster Zeit an ihre Grenzen. Denn die ältere RFID-Technologie entspricht inzwischen nicht mehr den aktuellen Standards. Neue Generationen arbeiten heute mit Verschlüsselung bei der Datenübertragung. Neue Transpondermedien verfügen über ein höheres Sicherheitsniveau, verbesserte Reaktionszeiten und eine größere Speicherkapazität. LOXXESS wird deshalb

Jeanette Uhlmann, Leitung Personal, LOXXESS

„Die Zusammenarbeit mit SOFT-CONSULT und PCS hat mich vor allem durch die große Professionalität überzeugt. Bei allen beteiligten Parteien stand immer die bestmögliche Lösung im Vordergrund. Auch wenn es mal schwieriger wurde, haben unsere Ansprechpartner immer schnell reagiert und gehandelt. Durch die Flexibilität und eine auf uns zugeschnittene Dienstleistung konnten wir gemeinsam eine gute Lösung entwickeln."

Abbildung 1 LOXXESS betreibt ab Ende 2022 im tschechischen Bor eine neue Logistikhalle mit 68.000 m2 Fläche.

nach und nach auf diesen neuen Standard umsteigen.

Kombinationstransponder ermöglichen hybriden Betrieb.

Bei der Ausstattung der Logistikhalle in Bor wird nur noch die neueste RFID-Technologie für Zeit und Zutritt genutzt, um zukunftsgerecht aufgestellt zu sein. Dadurch ergab sich eine komplizierte Situation, denn an anderen Standorten wird die ältere Hardware weiter genutzt, da sie problemlos läuft.

Was also tun? LOXXESS erkundigte sich bei den Experten von SOFT-CONSULT, ob ein paralleler Betrieb

Abbildung 2: Am robusten Zeiterfassungsterminal INTUS 5540 lassen sich Projektzeiten erfassen.

von alt und neu, mit nur einem Firmentransponder möglich sei. SOFTCONSULT schlug eine hybride Lösung in Form eines neuen Schlüsselanhängers vor.

Auf ihm befinden sich zwei Sektoren, sowohl für die ältere als auch für die aktuelle Technologie. Mit diesen Kombi-Transpon- dern kann jeder Zutrittsleser an jedem LOXXESS-Standort bedient werden.

Für das übergeordnete Zeiterfassungssystem war es allerdings etwas komplizierter: Die hybriden Buchungssätze mussten erst harmonisiert werden, damit sie in der übergeordneten Software verarbeitet werden können. Hier wurde von PCS Systemtechnik eine individuelle Lösung programmiert, welche das alte System mit dem neuen verbindet.

Die Tests am Standort Bor ergaben, dass die Kombi-Transponder die Arbeitszeiten richtig übertragen und somit konnten die neuen Transponder an alle Mitarbeiter ausgegeben werden.

Seither nutzen auch weitere LOXXESS-Standorte in Deutschland die neuen Transponder, um nach und nach die alte Technik gänzlich abzulösen.

Zuverlässiges Zeiterfassungsterminal mit Folientastatur und Barcode-Scanner.

Bei LOXXESS arbeiten die Mitarbeiter im Mehrschichtbetrieb rund um die Uhr. Die Dienstleistungen werden kundenindividuell vereinbart und reichen bis zum Fulfillment mit Rechnungsstellung. Damit dies für jeden Kunden korrekt abgerechnet werden kann, buchen die Mitarbeiterinnen und Mitarbeiter ihre Arbeitszeiten auf Kundenkostenstelle. Diese Buchungen werden an einem INTUS 5540-Zeiterfassungsterminal erfasst, das über eine haptische Folientastatur verfügt. So kann das Terminal auch von Beschäftigten mit Handschuh bedient werden. Ein zusätzlicher Scanner am Gerät ermöglicht das Lesen von Barcodes für die Zuordnung der Projektzeiten.

Schnelle Reaktionsgeschwindigkeit ist in der Zutrittskontrolle essenziell.

Bei der Auswahl der Zutrittskontrolle spielt Zuverlässigkeit eine große Rolle. In Bor treffen zu Schichtbeginn am Morgen gleichzeitig mehrere hundert Personen an insgesamt drei Halleneingängen ein. Um die Personen- ströme zu kanalisieren, wurden pro Eingang zwei bis drei Drehkreuze installiert, die mit den Zutrittslesern INTUS 620 bedient werden. Auch hier bewähren sich die aktuellen Modelle, die mit schnellen Reaktionszeiten die Mitarbeitenden rasch passieren lassen.

Verlässliche HR-Prozesse über alle Standorte sind sehr wichtig.

Bei einem Unternehmen mit 28 Standorten ist es besonders wichtig, dass die Prozesse über alle Standorte hinweg funktionieren. Deshalb legt Personalleiterin Jeanette Uhlmann besonders viel Wert darauf, papierlose Prozesse einzuführen: „Wir beschäftigen rund 2.600 Mitarbeitende – damit zählen wir immer noch zum Mittelstand. Wir holen uns für unsere Anforderungen Experten mit ins Boot, die mit uns zusammen un-

Profil LOXXESS AG

Die LOXXESS AG hat sich auf komplexe Outsourcing-Projekte in der Industrie- und Handelslogistik spezialisiert. Für die Kunden unterschiedlichster Branchen werden auf Basis individueller Konzepte maßgeschneiderte Logistik- und Fulfillmentlösungen entwickelt und umgesetzt.

Als Fulfillment-Dienstleister optimiert LOXXESS für seine Kunden nicht nur Beschaffung und Warenverteilung, sondern bietet Mehrwerte durch Customer Care Ser- vices, Value-Added-Services, Debitorenmanagement und E-Commerce-Fulfillment. Die LOXXESS AG hat ihren Hauptsitz in Tegernsee südlich von München, beschäftigt etwa 2.600 Mitarbeiter, verfügt über 28 Logistik-Standorte in Deutschland, Tschechien und Polen und bewirtschaftet 400.000 m2 Lagerfläche.

sere IT-Prozesse gestalten." Frau Uhlmann schätzt die Unterstützung von SOFT-CONSULT bei der Einrichtung der HR-Prozesse, denn Änderungen können komplex sein. Die hinterlegten Schichtmodelle dürfen nicht unbeabsichtigt geändert werden.

Zu einem gelungenen HR-Workflow tragen auch die qualitativ hochwertigen INTUS-Zeiterfassungsterminals bei. Eine wichtige Funktion ist, dass alle Buchungen in den INTUS-Terminals gespeichert werden. Eigentlich gedacht als Notfallspeicher für einen eventuellen Blackout, nutzt die HR-Abteilung die Funktion bei der Einstellung von neuem Personal. Neue Mitarbeiterinnen und Mitarbeiter bekommen bereits am ersten Tag einen Firmenschlüsselanhänger ausgehändigt und können sofort ihre Arbeitszeiten buchen.

Die eigentliche Anlage des Mitarbeiterstammsatzes in der Software erfolgt erst zu Beginn des nächsten Monats. Sobald der Stammsatz vorhanden ist, werden die schon erfolgten Buchungen aus dem Terminal abgeholt und richtig zugeordnet.

Da die Zahl der Mitarbeitenden saisonalen Schwankungen unterliegt, nutzt LOXXESS für Auftragsspitzen temporär beschäftigte Lohnarbeiterinnen und -arbeiter. Auch die Zeitarbeitsmitarbeiterinnen und -mitar- beiter buchen ihre Arbeitszeiten an den INTUS-Zeiterfassungs- terminals. Die Buchungsdaten werden gesammelt exportiert und an den Dienstleister übermittelt. So entfällt die manuelle Abrechnung von Lohnarbeitszeiten.

[www.pcs.com]

Einsparpotentiale

In jeder Phase ihres Lebenszyklus kann die drahtlose Zutrittskontrolle helfen, Geld zu sparen und den Energieverbrauch zu senken

Installation, Betrieb und Erweiterung: Die elektronische Zugangskontrolle ist in jeder Phase ihres Lebenszyklus mit Kosten verbunden. Diese Kosten sind jedoch nicht fix.

Die Entscheidung für eine drahtlose statt einer kabelgebundenen Schließanlage kann eine wichtige Rolle bei der Senkung des Energieverbrauchs - und damit der Ausgaben - spielen.

Kosteneinsparungen bei der Installation: schnellere, einfachere Montage
Die Einsparungen beginnen ganz am Anfang. Die Installationsphase trägt am meisten zu den potenziellen Kosteneinsparungen bei, wenn sich Unternehmen für eine drahtlose Zugangskontrolle entscheiden.

In Berechnungen für einen Kostenbericht untersuchten die Experten von ASSA ABLOY die voraussichtlichen Kosten für eine Installation mit 100 Türen. Die Einsparungen bei den Arbeitskosten betrugen 82,5 %* für diejenigen, die sich für kabellose gegenüber verkabelten Schlössern entschieden.
Und warum? Erstens, weil die drahtlose Installation viel schneller ist. Außerdem ist sie weniger invasiv. Bei den meisten kabellosen Schlössern sind nur wenige oder gar keine Bohrungen an der Tür erforderlich, während bei verkabelten Zutrittskontrollsystemen eine Verkabelung durch die Tür und teilweise auch um die Tür herum erforderlich ist - was wiederum spezialisierte Elektroinstallateure erfordert.

Durch die Wahl einer drahtlosen Lösung verbessern Unternehmen auch die Gebäudesicherheit, ohne das Personal zu belästigen oder die täglichen Arbeitsabläufe zu stören.

ASSA ABLOY Öffnungslösungen EMEIA: Drahtlose Schlösser wie Aperio® sind schneller zu installieren und verbrauchen im Betrieb viel weniger Energie als vergleichbare kabelgebundene Geräte

Kosteneinsparungen bei der Nutzung: weniger Energie, bessere Nachhaltigkeitsleistung

Im Jahr 2017 erklärte die Harvard Business Review Energieeffizienz zu einem der "wichtigsten Hebel für den Unternehmenserfolg "**. Diese Meinung könnte heute zutreffender sein als je zuvor.
Zwischen 2021 und 2022 steigen die Energiepreise für Nicht-Haushalte in allen EU-Ländern außer einem um mindestens 10 %. In Griechenland, Rumänien und Dänemark haben sich die Einheitspreise für Unternehmen mehr als verdoppelt***. Kabellose, batteriebetriebene Geräte können helfen, sich gegen Preissteigerungen und Preisschwankungen zu schützen.

Batteriebetriebene Schlösser verbrauchen weniger Energie als herkömmliche kabelgebundene Schlösser, die in der Regel über Magnete funktionieren, die permanent mit Strom verbunden sind. Drahtlose Schlösser funktionieren anders. Sie "wachen" nur auf, wenn ihnen ein Berechtigungsnachweis vorgelegt wird, um eine Zugangsentscheidung zu treffen.

Dies bedeutet eine zusätzliche Einsparung bei den Energiekosten: mehr als 70 %* bzw. Tausende von Euro über die Lebensdauer einer typischen Zutrittskontrolllösung.

Auch die anderen damit verbundenen Energie- und Materialkosten während der Nutzung sind geringer. Im Betrieb müssen drahtlose Schlösser nur einmal alle zwei Jahre ihre Standardbatterie - die wiederaufladbar sein kann - austauschen. Eine spezielle Wartung ist nicht erforderlich.

Kostenersparnis durch längere Lebensdauer: Wiederverwendung und Raumflexibilität

Kabellose Schlösser erhöhen auch die Flexibilität - und können die Kosten

senken -, wenn ein Unternehmen seine Büroräume umgestaltet oder vergrößert. Hochwertige, innovative kabellose Schlösser wie die Aperio®-Reihe von ASSA ABLOY können in der Regel ohne Beeinträchtigung der Zuverlässigkeit an einer anderen Tür wieder installiert werden. Sie können überall dort angebracht werden, wo es bequem ist.
Wenn ein Unternehmen seinen Arbeitsbereich überdenkt, um beispielsweise flexible oder hybride Arbeitsmodelle zu fördern, könnten die Kosteneinsparungen erheblich sein****. Typische Einsparungen bei Büroumzügen oder -erweiterungen werden auf ca. 30 %* geschätzt, wenn kabellose statt kabelgebundene Schlösser verwendet werden.

Senkung des Energieverbrauchs bei gleichzeitiger Erweiterung der Kontrolle: Universität von St. Andrews
Die Universität von St. Andrews, an der der renommierte St. Andrews Prize for the Environment verliehen wird, hat sich Nachhaltigkeit auf die Fahnen geschrieben. Für die Studentenwohnheime suchten die Verantwortlichen der Universität eine energieeffiziente Zutrittskontrolllösung, die diese Grundsätze respektiert und widerspiegelt.

Eine große Herausforderung für die Universität bestand darin, dass in den Studentenwohnheimen im Laufe der Jahre mehrere unterschiedliche, eigenständige Zugangskontrolltechnologien installiert worden waren. Um die Unterkünfte zu modernisieren, suchte die Universitätsleitung nach einer geeigneteren, integrierten Lösung.
Die Universität entschied sich für die batteriebetriebenen elektronischen Beschläge ASSA ABLOY Aperio. Bisher sind rund 1.600 Türen mit elektronischer Zutrittskontrolle ausgestattet - ohne Verkabelung*****.
Die Aperio-Geräte lassen sich vollständig integrieren und arbeiten flexibel mit dem bestehenden Zentralsystem der Universität und dem Studentenausweis zusammen. Die Sicherheitsverantwortlichen der Universität genießen weiterhin die Effizienzvorteile der Überwachung und Kontrolle des Zugangs von einem einzigen Punkt aus und in Echtzeit, auch für Türen in mehreren Gebäuden.

Energieeffizienz und mehr Kontrolle mit Aperio

Im Vergleich zu einer kabelgebundenen Zutrittskontrolllösung bieten die Aperio-Geräte erhebliche Vorteile in Bezug auf die Energieeffizienz. Da die Geräte kabellos sind, können sie mit geringem Energieaufwand installiert werden, ohne dass eine Verkabelung mit dem Stromnetz erforderlich ist. Sie verbrauchen im Ruhezustand keine Energie und werden mit Standardbatterien betrieben, die während des Betriebs nur wenig Strom verbrauchen.
Während des gesamten Produktlebenszyklus verbindet Aperio Zuverlässigkeit und Energieeffizienz mit Kosteneffizienz. Damit trägt Aperio zu den Nachhaltigkeitszielen der Universität bei.

Gleichzeitig hat die Online-Integration in das zentrale Managementsystem von St. Andrews den Zugang für alle Benutzer verbessert.

"Aperio ermöglicht uns eine zentrale Verwaltung und Kontrolle", sagt Pauline Brown, Associate Chief Information Officer an der University of St Andrews, "und trägt zu unserer preisgekrönten Erfolgsbilanz in Sachen Energieeffizienz bei."

Für mehr Informationen zur Umstellung auf kabellose Schlösser und Einsparpotentiale: Leitfaden unter tinyurl.com/4c8t8s96

* **https://campaigns.assaabloyopeningsolutions.eu/aperio-cost-savings**
** **https://hbr.org/2017/01/energy-strategy-for-the-c-suite**
*** **https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity_price_statistics#Electricity_prices_for_non-household_consumers**
**** **www.ifsecglobal.com/access-control/5-reasons-security-managers-make-lives-easier-connected-access-control/**
***** **www.youtube.com/watch?v=Zo8UxL0VYGE**

Karlsruher Institut für Technologie (KIT)

„Wir bestehen darauf, dass Menschen weiterhin das letzte Wort haben."

Der Deutsche Ethikrat hat seine Stellungnahme „Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz" veröffentlicht. Die 287 Seiten starke Schrift untersucht die Auswirkungen digitaler Technologien auf menschliches Selbstverständnis und gesellschaftliches Miteinander. „Der Ethikrat macht die Rolle des Menschen als bewusst handelndes Wesen mit Intentionen und Freiheit stark und schließt hieraus auf Regeln für den Umgang mit KI", erläutert Professor Armin Grunwald vom Karlsruher Institut für Technologie (KIT). Als Mitglied des Ethikrats gehörte Grunwald der multidisziplinären Arbeitsgruppe Mensch/ Maschine an, welche die Stellungnahme federführend erarbeitet hat. Eingebracht hat er hierbei insbesondere seine Expertise zum technischen Wandel, zur Technikfolgenabschätzung und zur digitalen Transformation.

Ein roter Faden in der Stellungnahme des Ethikrats ist die Frage, welche Folgen es hat, wenn Tätigkeiten an Maschinen delegiert werden – insbesondere Entscheidungen, die zuvor Menschen vorbehalten waren. Dies bedrohe den Wert, ja die Möglichkeit menschlicher „Autorschaft" überhaupt. „Wir bestehen darauf, dass Menschen weiterhin das letzte Wort haben", unterstreicht Grunwald, der am KIT eine Professur für Technikphilosophie innehat sowie das dortige Institut für Technikfolgenabschätzung und Systemanalyse (ITAS) leitet. „Unsere besondere Sorge gilt dabei dem sogenannten ‚Automation Bias', also der Tendenz, dass Menschen den Ergebnissen automatisierter Entscheidungsunterstützung tendenziell mehr Glauben schenken als menschlichen Überlegungen. Auf diese Weise könnte es zu einem schleichenden Verlust menschlicher Autonomie und Freiheit kommen."

Angeregt durch den Deutschen Bundestag unter Mitwirkung seines früheren Präsidenten Wolfgang Schäuble, hat der Rat in über zwei Jahren und einer Vielzahl von Beratungen eine Orientierung für Gesellschaft und Politik erarbeitet, die weit über viele vorliegende Ethik-Leitlinien bezüglich KI hinausgeht: „Statt nur zu schauen, welchen abstrakten Werten und Normen KI-Anwendungen folgen sollen, stellt der Ethikrat ein klar ausformuliertes Menschenbild an den Anfang seiner Überlegungen.
Danach bleibt die KI Mittel zu von Menschen gesetzten Zwecken, wird aber nicht zum Selbstzweck", sagt Grunwald, der auch das vom ITAS betriebene Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) leitet.
So kann (und soll) auch die KI-Unterstützung von Entscheidungen, die bislang von Menschen aufgrund ihres Sachverstands getroffen wurden, ja sogar die vollständige Delegation von Entscheidungen an KI-Systeme (automated decision-making), letztlich der menschlichen Autonomie dienen, so Grunwald.
„Freilich muss sichergestellt werden, dass weder Diskriminierungen erfolgen, etwa im Sicherheitsbereich oder im Sozialwesen, noch dass die menschliche Dimension des Einzelfalls verloren geht. Maschinen dürfen nicht nach den von ihren Herstellern einprogrammierten Regeln ohne fachkundige menschliche Kontrolle über menschliche Schicksale befinden."

Zugleich plädiert der Karlsruher Technikforscher im Umgang mit Künstlicher Intelligenz für differenzierte und fallbezogene Einschätzungen:
„Statt KI pauschal zu loben oder zu kritisieren, statt utopische Erwartungen zu pflegen oder den Untergang der Menschen zu befürchten, ist bei jeder einzelnen KI-Anwendung ethische Sorgfalt genauso angesagt wie die Berücksichtigung der je besonderen Umstände.

Auf vitalen Anwendungsgebieten wie Medizin, Bildung, Verwaltung sowie öffentlicher Kommunikation und Meinungsbildung", sagt Grunwald, „sehen wir vielfältige Potenziale, das Handeln und Entscheiden von Menschen durch KI-Systeme auf eine bessere Basis zu stellen, zum Beispiel durch gezielte Datenauswertung und Entscheidungsvorbereitung."

Genetec

Authorisierung von CVE Numbering Authority (CNA)

Unternehmen bringt sein Fachwissen im Bereich Cybersicherheit ein

Genetec, ein Technologieanbieter von Lösungen für vereinheitlichtes Sicherheitsmanagement, öffentliche Sicherheit, Betrieb und Business Intelligence, wurde vom Common Vulnerabilities and Exposures (CVE)-Programm als CVE Numbering Authority (CNA) autorisiert. Damit ist Genetec ein international starker Partner bei der frühzeitigen Identifikation von

Schwachstellen und Anfälligkeiten und dem Schutz gegen Cyberangriffe. Insbesondere DACH-Kunden mit internationaler Ausrichtung profitieren von diesem Know-how. Das CVE-Programm identifiziert, definiert und katalogisiert öffentlich bekannt gewordene IT-Sicherheitslücken. Es wird von der Cybersecurity and Infrastructure Security Agency (CISA) des U.S. Department of Homeland Security (DHS) finanziert und von der MITRE Corporation in enger Zusammenarbeit mit internationalen Experten aus Wirtschaft, Wissenschaft und öffentlicher Hand betrieben. MITRE ist eine Organisation, die durch Abspaltung vom Massachusetts Institute of Technology entstanden ist und verschie-

entrust.com

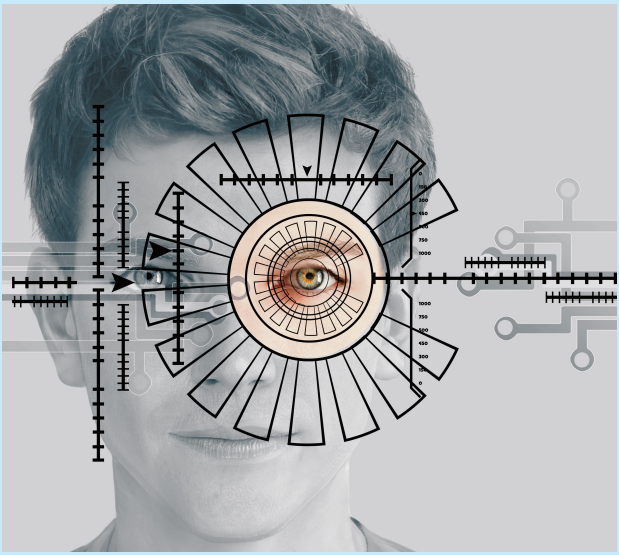
Biometrie löst Passwörter mehr und mehr ab

"The Future of Identity Report" von Entrust sieht Finger-Scan und Gesichtserkennung im Kommen

Passwörter haben ausgedient, Biometrie zur Authentifizierung hingegen gewinnt an Bedeutung. Laut "The Future of Identity Report" des Entrust Cybersecurity Institute (https://entrust.com) setzen 51 Prozent der 1.450 weltweit befragten User mindestens einmal im Monat ein Kennwort zurück, 15 Prozent sogar einmal pro Woche.

Biometrische Lösungen sicherer

Mehr als die Hälfte der Befragten hält biometrische Lösungen für sicherer, wobei 53 Prozent den Finger-Scan bevorzugen, gefolgt von der Gesichtserkennung (47 Prozent). Nur sechs Prozent der Verbraucher halten Passwörter noch für die sicherste An-



meldemethode. Vor die Wahl zwischen Biometrie und Passwort gestellt, entscheiden sich daher auch 74 Prozent aller Befragten laut Entrust mindestens bei der Hälfte aller Anwendungen für Biometrie. Ein Drittel würde sich immer für Biometrie entscheiden, sofern sie angeboten wird.

dene Forschungs- institute im Auftrag der Vereinigten Staaten betreibt.

Zentrales System verbessert Cybersicherheit

Ein zentralisiertes System und Verfahren zur Katalogisierung von IT-Sicherheitslücken hilft Beteiligten wie Softwareentwicklern, Geräteherstellern und IT-Teams, Informationen über Schwachstellen schnell zu entdecken und zu bewerten. Sie können dann Systeme besser vor Angriffen schützen. Fachleute aus den Bereichen IT und Cybersicherheit verwenden CVE Records einerseits um sicherzustellen, dass sie über dasselbe Problem sprechen, und andererseits, um die Schwachstellen zu priorisieren und zu beheben. Das CVE-Programm verhilft damit zu einem schnelleren Schwachstellenmanagement in einem frühen Stadium, einer besseren Koordination und einer effektiveren Cyberhygiene.

Als Partner des CVE-Programms ist Genetec berechtigt, CVE Records zu veröffentlichen, um einheitliche Beschreibungen von Schwachstellen zu kommunizieren. Die Verwendung dieser standardisierten und öffentlich zugänglichen CVE Records kann zu erheblichen Zeit- und Kosteneinsparungen führen. „Dass Genetec jetzt eine autorisierte CVE-Stelle ist, spiegelt unser fortwährendes Engagement für starke Cybersicherheitspraktiken wider", sagt Christian Morin (Foto), CSO & Vice President of Product Engineering bei Genetec. „Als Teil einer internationalen Gemeinschaft, auf die man sich bei der Identifizierung, Katalogisierung und Veröffentlichung von Schwachstellen verlässt, ermöglichen wir die schnelle Behebung dieser Sicherheitslücken. Dies gibt unseren Kunden die Gewissheit, dass ihre physischen Security-Lösungen geschützt sind und hohen Cybersicherheitsstandards entsprechen."

Nordrhein-Westfalen

Polizei NRW entscheidet sich bei Drohnenabwehr für ESG-Software ELYSION

Ende November 2022 gab die Polizei Nordrhein-Westfalen ihre Entscheidung zur Beschaffung der ESG-Software ELYSION bekannt. Damit nutzt die Polizei NRW künftig die hochspezialisierte Counter-UAS-Software der ESG für bestmöglichen Schutz vor Gefahren durch Drohnen.

Der Beschaffungsentscheidung gingen intensive Erprobungen durch das zuständige Landesamt für Zentrale Polizeiliche Dienste voraus – gut ein Jahr lang wurde ELYSION „auf Herz und Nieren" getestet, insbesondere auch im Rahmen des Einsatzes zur Absicherung von Großveranstaltungen. Dabei hat sich ELYSION bewährt. Wie die Einsatzberatungsstelle Drohnenabwehr beim LZPD NRW mitteilte, hat ELYSION seine Leistungsfähigkeit während der umfas-

senden Erprobungsphase bewiesen und konnte zudem seine Einsatzreife beim letztjährigen G7-Gipfel in Elmau unter Beweis stellen.Polizeibehörden von Bundes- und Landesdienststellen, der Bundeswehr sowie internationale Kunden nutzen ELYSION. Die dabei erarbeiteten Erfahrungen und die Möglichkeit zur Vernetzung bei behördenübergreifender Zusammenarbeit kommen daher künftig allen Nutzern zugute. ELYSION ist eine umfassende Weiterentwicklung des GUARDION-Softwarekerns bestehend aus verarbeitender Kernintelligenz und hochgradig vernetzter, kartenbasierter Lagedarstellung.

In die ELYSION-Software sind die umfangreichen Einsatzerfahrungen und das Feed-back von unterschiedlichen zivilen, (polizei-)behördlichen und militärischen Kunden und Nutzern direkt eingeflossen, so dass sie die vielfältigen hochkomplexen Anforderungen im Einsatz in idealer Weise abbildet. Nach der Erfolgreichen Abnahme des „Abwehrsystem gegen unbemannte Luftfahrzeuge – kurz ASUL" durch die Bundeswehr im Sommer 2022, stellt die Beschaffung von ELYSION durch die Polizei NRW einen weiteren wichtigen Erfolg für das Drohnenabwehr-Team der ESG dar. Beides unterstreicht die besondere Bedeutung des Themas Drohnenabwehr für die Bereiche innere und äußere Sicherheit und die führende Rolle der ESG als der verlässliche Partner für sicheren Schutz vor Gefahren durch unkooperative Drohnen.

Paxton

Prämienprogramm auf der ISC West vor

Paxton, die globale Marke für Zutrittskontroll-, Videoüberwachungs- und Gegensprechanlagen, wird auf der ISC West am Stand Nr. 14075 ihr brandneues Kundenbindungsprogramm Paxton Rewards vorstellen. Außerdem wird das Unternehmen auf der Messe eine exklusive Vorschau auf seine neue Türöffnungs-App präsentieren. Die ISC West war die erste Gelegenheit für Sicherheitshändler sein, das Rewards-Programm und die Entry-App in Aktion zu sehen.

Auch in diesem Jahr war Paxton wieder auf der ISC vertreten, um seinem US-Kundenstamm die Neuheiten zu präsentieren. Die Messe ist die größte Sicherheitsveranstaltung der Welt und fand vom 29. bis 31. März in der Venetian Expo in Las Vegas statt.

Das Paxton Rewards Programm ist ein neues Treueprogramm, das Kunden für Schulungen, den Kauf und die Installation von Paxton Produkten belohnt. Installateure scannen einfach Paxton-Produkte und führen Aktivitäten durch, um Punkte zu sammeln. Je mehr sie verdienen, desto höher steigen sie auf. Vom Paxton Rewards Partner der Einstiegsstufe bis zum exklusiven Platin-Partner-Level erhalten sie mit jeder Stufe weitere fantastische Vorteile, um ihr Geschäft anzukurbeln.

Jonathan Lach, Vice President of Sales bei Paxton, erklärte: "Wir freuen uns, dieses Jahr auf der ISC West persönlich mit unseren Kunden in Kontakt zu treten und unser neues Paxton Rewards Programm und die Entry App vorzustellen. Das Belohnungsprogramm ermöglicht es Installateuren, sich von der Masse abzuheben, indem sie ihre Paxton-Expertise mit ihrem Paxton-Partner-Abzeichen un- ter Beweis stellen.

"Installateure, die unseren Stand besuchen, hatten auch die Gelegenheit haben, die neueste1 Türöffnungs-App zu sehen. Die Entry-App ermöglicht es den Benutzern, Anrufe zu beantworten und den Zutritt mit unseren Videosprechanlagen auf intelligenten Geräten zu verwalten. Dies wird eine großartige Ergänzung zu unseren Türsprechanlagen sein und auch die Kundenerfahrung verbessern.

Neben einem kurzen Einblick in das Paxton Rewards-Programm und die Entry-App können Besucher an Vorführungen der neuesten Net2- und Paxton10-Updates sowie der jüngsten Versionen von Paxtons Video-Gegensprechanlage Entry und unserer drahtlosen Schloss-Produktlinie PaxLock teilnehmen.

Jeder, der am Stand eine Produktvorführung erhält, hat die Chance, Paxton-Produkte im Wert von $1.500 MSRP zu gewinnen. Diejenigen, die sich eine Produktvorführung ansehen, sich für die kostenlose Paxton-Installationsschulung anmelden und an der Schulung teilnehmen, nehmen automatisch an einer Verlosung teil, bei der sie am Mittwoch und Donnerstag der Messe eine Apple Watch gewinnen können.

Alle Paxton-Produkte haben eine fünfjährige Garantie, ein problemloses Rückgaberecht und werden von Paxtons branchenführendem Kundendienstteam unterstützt.

Suprema

NEUES AI-Gesichtserkennungs-OEM-Modul 'Q-Face Pro' auf den Markt

Suprema AI, ein Unternehmen, das sich auf integrierte Sicherheitslösungen auf Basis künstlicher Intelligenz spezialisiert hat, stellte am 29. März auf der ISC West, der größten Sicherheitsmesse Nordamerikas, offiziell ein leistungsstarkes OEM-Modul für die Gesichtserkennung mit dem Namen 'Q-Face Pro' vor. Q-Face Pro ist die Antwort von Suprema AI auf den wachsenden Bedarf an kontaktlosen Sicherheitslösungen in der Post-COVID-Welt.

Q-Face Pro ist mit einem erstklassigen KI-basierten Gesichtserkennungsalgorithmus und einer Neural Processing Unit (NPU) - der neuesten KI-Prozessortechnologie - ausgestattet, die eine schnelle und genaue Gesichtserkennungsleistung für bis zu 50.000 Benutzer bietet. Darüber hinaus bietet es ein hohes Maß an Genauigkeit bei der Erkennung falscher Gesichter sowie eine hochpräzise Authentifizierungsleistung, wenn sich die Gesichter der Benutzer ändern, z. B. beim Tragen verschiedener Arten und Farben von Masken, Frisuren, Hüten und Brillen.

Q-Face Pro erfüllt die europäischen GDPR-Bestimmungen und schützt Benutzerdaten vor externen Hakking-Versuchen, indem es einen separaten Secure Element (SE)-Chip enthält und die höchste Stufe der Verschlüsselungstechnologie für Benutzergesichtsdaten einsetzt. Darüber hinaus bietet es Zuverlässigkeit im Feld durch ein optimiertes Wärmestrahlungsdesign und unterstützt eine Reihe von kontaktlosen Authentifizierungsmethoden, einschließlich Gesichtserkennung, QR-Codes und Barcodes für einen erhöhten Benutzerkomfort.

Q-Face Pro verwandelt gewöhnliche physische Sicherheitsgeräte in hochentwickelte KI-Gesichtserkennungsprodukte. Es kann in verschiedenen Anwendungsfällen eingesetzt werden, z. B. in Zugangskontrollgeräten, Zeiterfassungsterminals, intelligenten Kiosken für die Kundenverwaltung, Rechenzentren, Geldautomaten, unbemannten Verkaufsautomaten, Türschlössern, Fahrzeugen und im IoT. Um Kunden bei der schnellen und einfachen Integration von Q-Face Pro zu unterstützen, bietet Suprema AI SDKs für alle wichtigen Betriebssysteme, einschließlich Android, sowie technische Support-Kanäle in Echtzeit zur Optimierung von Entwicklungslösungen. Bei den vor der offiziellen Markteinführung durchgeführten Produktevaluierungen erhielt Q-Face Pro positive Bewertungen von den weltweit führenden Herstellern physischer Sicherheitsprodukte in Nordamerika und Europa. Eine Reihe globaler Kunden bereitet nun die Einführung neuer Produkte mit Q-Face Pro vor.

"Q-Face Pro ist das Ergebnis eingehender Marktforschung und ein Gesichtserkennungs-OEM-Modul der nächsten Generation, das die Bedürfnisse von Großkunden widerspiegelt, die heute auf dem Weltmarkt führend sind", so Song Bong-Seop, CEO von Suprema AI. "Wir gehen davon aus, dass wir unsere weltweite Führungsposition im Bereich der Edge-KI-Lösungen weiter ausbauen werden, indem wir Anwendungsfälle in neuen Bereichen schaffen und den Markt erweitern."

Schutz des geistigen Eigentums in der Automobilbranche

Entwicklung und Bau von Automobilen ist ein wichtiges Standbein der deutschen Wirtschaft. Der ausgeprägte Wettbewerbsdruck sorgt für einen fortwährenden Innovationswettlauf auf globaler Ebene. Das bedeutet aber auch, dass hohe Anstrengungen unternommen werden müssen, das geistige Eigentum zu schützen – sowohl eigene Entwicklungen in entsprechenden Ingenieurbüros, als auch das der Kunden und weiterer Technologie-Partner. Eine zuverlässige Schließanlage bietet die Grundlage für einen umfassenden Schutz.

Antriebstechnik und Karosserie-Design, Batterie-Aufbau und Steuerungsprogrammierung, Werkstoff-Forschung und Fertigungsmethoden – die Automobilhersteller bauen ihren Erfolg auf zahlreiche Entwicklungsfelder, in denen Innovationen vorangetrieben und eigene Akzente gesetzt werden müssen, um im globalen Wettbewerb bestehen zu können. Die Hersteller setzen dabei auf eigene Entwicklungsabteilungen ebenso wie auf externe Ingenieurbüros, innovative Zulieferer von Komponenten und die Zusammenarbeit mit Technologielieferanten und Forschungseinrichtungen.

Daher gilt es nicht nur das eigene geistige Kapital zu schützen, sondern auch das der beteiligten Partner. Der Druck zu einem tragfähigen Schutzniveau ist so groß, dass sich die europäischen Hersteller und ihre Partner auf den gemeinsamen Sicherheitsstandard „TISAX" geeinigt haben, den jedes Unternehmen, das sich als Dienstleister einbringen will, einhalten muss.

Das Kürzel steht für „Trusted Information Security Assessement Exchange". Während vorher jeder Hersteller für sich überprüfte, ob ein potenzieller Partner vertrauenswürdig ist, kann sich ein Unternehmen nun gemäß TISAX zertifizieren lassen und die Ergebnisse der ganzen Branche zur Verfügung stellen. Alle drei Jahre muss die Zertifizierung erneuert werden, nach den jeweils aktuellen Anforderungen.

Zugangs- und Access-Management im Fokus

Ein wesentliches Element der Zertifizierung ist die Installation eines Information Security Management Systems (ISMS, engl. für „Managementsystem für Informationssicherheit"). In dessen Rahmen sind beispielsweise Fragen des physischen Zugangs zu beantworten, wie etwa die Einrichtung und Verwaltung von Sicherheitszonen oder der „physische Schutz von Informationswerten", wie es in den TISAX-Statuten heißt. Gemeint ist damit, dass beispielsweise Zeichnungen und Mock-up-Modelle aus dem 3D-Printer oder Laptops, Festplatten und Server mit digitalen Entwicklungsdaten vor Diebstahl und Zerstörung bewahrt werden müssen.

Ein weiterer Aspekt betrifft das Identity- und Access-Management, sprich: wie zuverlässig Identifikationsmittel wie Schlüssel, RFID-Karten, Token und ähnliches verwaltet werden. Denn eine Sicherheitszone nützt wenig, wenn die Prüfung der Zugangsberechtigung nicht wirksam ist.

Sichere Schließanlage, zuverlässige Verwaltung

Die Anforderungen der TISAX-Prüfung legen den Einsatz einer elektronischen Schließanlage wie dem eCLIQ-System von ASSA ABLOY nahe, denn diese bietet nicht nur eine komfortable und effiziente Verwaltung, sondern lässt sich auch flexibel an die Sicherheitsanforderungen anpassen und erleichtert es aufgrund der integrierten Dokumentation, die im Rahmen des Assessments geforderten Nachweise zu erbringen.

Ein weiterer Vorteil ist die große Typenvielfalt der Schließzylinder, die eine durchgängige Lösung für alle Bedürfnisse ermöglicht. Denn nicht nur alle Arten sicherer Türzylinder stehen zur Verfügung, sondern auch Möbelzylinder für Schreibtisch-Schubladen und Rollcontainer (V 184, V924), Vorhangschlösser zur sicheren Verwahrung von Komponenten und 3D-Modellen in Containern (V316) oder das Serverschrank-Schloss KS100, mit dem innerhalb des Rechenzentrums die zentrale IT zusätzlich geschützt werden kann. Insgesamt stehen mehr als 60 verschiedene Zylinder zur Verfügung.

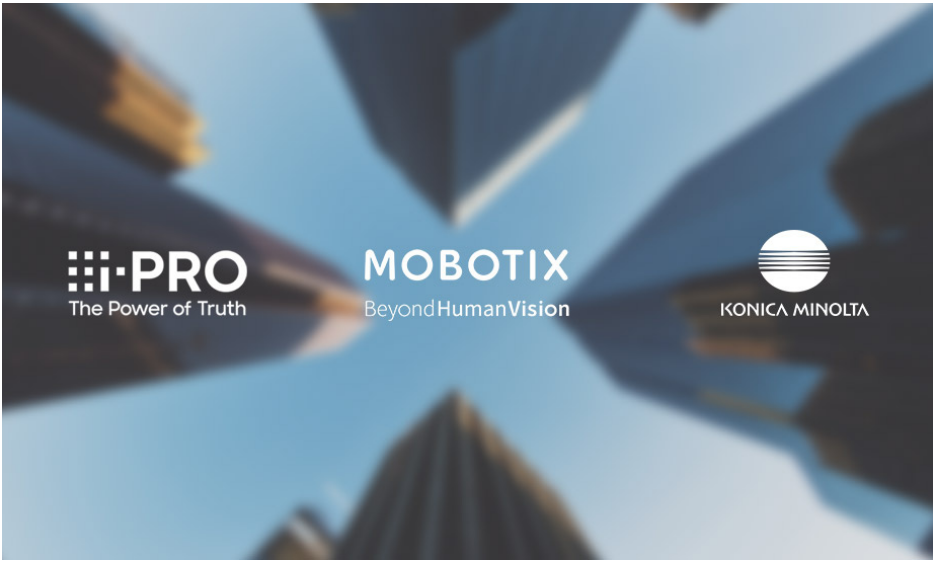
Jeder eCLIQ-Schlüssel ist individuell programmierbar

So können die Berechtigungen für jeden einzelnen Mitarbeiter maßgeschneidert angepasst werden. Für die Erteilung zeitlich begrenzter Zugangsberechtigungen – beispielsweise für Handwerker oder Wartungspersonal – stehen Tisch- oder Wandprogrammier- geräte zur Verfügung, oder auch ein mobiles Programmiergerät.

Mit dem elektronischen Nutzerschlüssel - „Connect Remote" können Berechtigungen sogar per Bluetooth-Schnittstelle des Smartphones erteilt werden. Alle Veränderungen sowie die jeweiligen Schlüsselaktivitäten werden in der Managementsoftware CLIQ Web Manager dokumentiert.

Branchenbezogene Expertise

Die Experten von ASSA ABLOY können Ihnen bei entsprechenden Projekten beratend zur Seite stehen. Sie haben sowohl Erfahrung bei der Sicherheitsprüfung gemäß dem TISAX-Standard der Automobil-Branche, wie auch bei ähnlichen Sicherheitsanforderungen anderer Branchen, etwa dem IFS Standard Food in der Lebensmittelverarbeitung



i-PRO, MOBOTIX, Konica Minolta

Strategische Zusammenarbeit intensiviert

i-PRO Co., Ltd. (i-PRO), MOBOTIX AG (MOBOTIX) und Konica Minolta, Inc. (Konica Minolta) verstärken ihre strategische Zusam- menarbeit durch die Kombination ihrer Produkte. Diese Zusammenarbeit wird es den Unternehmen ermöglichen, die Stärken des Portfolios von i-PRO und MOBOTIX, beides Spezialisten für Bildgebungs- und Sensortechnologien, gegenseitig zu nutzen und ihre Produkte mit FORXAI, einer hochmodernen Imaging-IoT-Plattform von Konica Minolta, zu kombinieren.

"Seit seiner Gründung im Jahr 2019 hat i-PRO Kooperationen mit Partnern auf der ganzen Welt aufgebaut und ist 2020 eine Partnerschaft mit Konica Minolta und MOBOTIX eingegangen. Konica Minolta, MOBOTIX und i-PRO sind Pioniere im Bereich bildbasierter und intelligenter Dienstleistungen und für die Qualität und Zuverlässigkeit ihrer Produkte und Lösungen bekannt. Ich bin davon überzeugt, dass diese Partnerschaft dazu beitragen wird, dass unser umfangreiches Angebot an Produkten, die KI-Technologie enthalten, zur Lösung einer Vielzahl von sozialen Problemen und Herausforderungen beitragen wird."

Shohei Ozaki, COO von i-PRO Co., Ltd

Zusammenarbeit von i-PRO und MOBOTIX mit IP-Kameras

i-PRO bietet eine breite Palette von Videoüberwachungsprodukten mit modernster KI-Technologie. Zusammen mit der bekannten Zuverlässigkeit und Langlebigkeit der japanischen Produkte hat dies dem Unternehmen ermöglicht, seine Präsenz auf dem globalen Markt zu erhöhen. MOBOTIX wiederum bietet weltweit IP-Kameras mit dezentraler Verarbeitung (Edge Computing) an, die die Standards für Made-in-Germany-Produkte erfüllen.

Die MOBOTIX High-End-Wärmebildkameras verfügen zudem über die entscheidende Fähigkeit, Temperatu-

"MOBOTIX und i-PRO teilen viele gemeinsame Werte und haben übereinstimmende Qualitätsstandards, insbesondere in Bezug auf Leistung und Cybersicherheit. Gemeinsam mit Konica Minolta können wir unsere Kompetenzen bündeln und innovative Lösungen – inklusive Thermotechnik und KI - für unsere zentralen vertikalen Märkte anbieten. Die Fokussierung der Videotechnologie auf die Datennutzung ist ein gemeinsamer Ansatzpunkt der Kooperationspartner. Intelligente Videotechnologie ist weit mehr als nur Sicherheit zu bieten. Es geht darum, effektiv zu arbeiten, Umsätze zu steigern und das Leben der Menschen einfacher und besser zu machen."

Thomas Lausten, CEO der MOBOTIX AG

ranomalien und -schwankungen genau zu erkennen. MOBOTIX, i-PRO und Konica Minolta haben bereits 2020 gemeinsam ein System aus visuellen und thermischen Kameras entwickelt. Die neue strategische Kooperation sieht vor, dass MOBOTIX ausgewählte Hochleistungs-Kamerahardware von i-PRO einsetzen wird. Kombiniert mit den einzigartigen MOBOTIX-DNA-Funktionen auf ODM/JDM-Basis (Original Design Manufacturing / Joint Development Manufacturing) wird die Hardware mit der bestehenden Systemlandschaft von MOBOTIX und Konica Minolta kom- patibel sein. Die Markteinführung des ersten Produkts ist bereits in diesem Jahr geplant.

Die Zusammenarbeit wird das Lösungsangebot für die vertikalen Märkte - z.B. Industrie & Produktion, Behörden, Gesundheitswesen, Logistik - gezielt mit leistungsfähigen End-to-End-Lösungen stärken. Sie ermöglicht es den Kunden, ihre Bedürfnisse hinsichtlich verbesserter Prozesse und höherer Gewinne zu erfüllen und die soziale Sicherheit in der Gesellschaft zu unterstützen.

Kombination von i-PRO- und MOBOTIX-Produkten mit FORXAI von Konica Minolta

Der Markt für Überwachungs- und Videolösungen verlangt heute weit mehr als nur Videoüberwachung und Verifizierung von Ereignissen. Zunehmend rücken die Erkennung, die Analyse und die Vorhersage mithilfe von KI sowie die Bereitstellung von Datendiensten, die diese nutzen, als neue Wachstumsbereiche in den Fokus. Die Verbindung von i-PRO- und MOBOTIX- Systemen mit der FORXAI Imaging IoT-Plattform von Konica Minolta ermöglicht die Integration und Nutzung verschiedener anderer Geräte und Systeme durch offene Partnerschaften. So wollen die Unternehmen einzigartige Lösungen auf der Grundlage der hochmodernen Imaging-KI-Technologie von Konica Minolta entwickeln, die Technologien von FORXAI- Partnerunternehmen integrieren, mit den neuen Lösungen ihren Kundenstamm erweitern und auch diese Daten kontinuierlich zur Optimierung und Erweiterung der KI-Lösungen nutzen.

"Wir freuen uns auf diese intensive Partnerschaft. Durch diese Zusammenarbeit zwischen Konica Minoltas Imaging-IoT-Plattform FORXAI, MOBOTIX und i-PRO sind wir zuversichtlich, dass sich unsere Kompetenzen, Qualitätsstandards und Stärken perfekt ergänzen. Die Zusammenarbeit wird eine Win-Win-Win-Situation für die drei Unternehmen sein. Die mit Abstand größten Gewinner werden dabei unsere Kunden und Nutzer sein."

Toshiya Eguchi, Konica Minoltas Executive Vice President und Executive Officer Responsible for Technologies and Imaging-IoT Solution Business

Schon jetzt die Sicherheit der Zukunft gestalten

Regierungserklärung des hessischen Innenministers: Die neue Sicherheitsstrategie

Innenminister Peter Beuth hat in seiner Regierungserklärung die strategischen Schwerpunktsetzungen der Landesregierung in der Inneren Sicherheit dargelegt. Fester Bestandteil ist dabei künftig eine noch stärkere Einbeziehung der Bürgerinnen und Bürger, die über Angebote wie das neue Sicherheitsportal immer unkomplizierter sicherheitsrelevante Angaben an Sicherheitsbehörden übermitteln, Anzeigen erstatten oder Mängel an Kommunen melden können.

„Wir gestalten schon jetzt die Sicherheit der Zukunft. Die Bürgerinnen und Bürger können dabei dank moderner Angebote eine immer aktivere Rolle spielen. Denn Sicherheit ist nicht nur ein Zustand, sondern auch ein Gefühl. Dieses Sicherheitsgefühl wollen wir weiter stärken und beteiligen deshalb die Bürger aktiv daran, Sicherheit in Hessen gemeinsam zu gestalten. Dies gelingt uns dank innovativer Technik und moderner Ausstattung der Sicherheitsbehörden. Wir wollen deutschlandweiter Schrittmacher der Polizeiarbeit von morgen sein und investieren entsprechend in modernste Ermittlungswerkzeuge. Wir haben moderne Rahmenbedingungen geschaffen, von denen die hessischen Sicherheitsbehörden und damit die Bürgerinnen und Bürger unmittelbar profitieren. Auch wenn es für den ein oder anderen mittlerweile selbstverständlich erscheinen mag, dass Hessen eines der sichersten Länder der Bundesrepublik ist. Es ist letztlich auf eine klare und konsequente Sicherheitspolitik ‚Made in Hessen' zurück zu führen. Wir haben klare Schwerpunkte gesetzt und zielgerichtet neue Wege bei der Modernisierung und Digitalisierung der Sicherheitsbehörden eingeschlagen", sagte Innenminister Peter Beuth (Foto).

Mit modernen Sicherheitsbehörden ist Hessen auch in Zukunft sicher

Die hessische Polizei wurde gezielt mit modernster Ausstattung für die Verbrechensbekämpfung gerüstet. Drohnen, Taser und Bodycams sind fester Bestandteil der hessischen Polizeiarbeit. Der Innovation Hub der hessischen Polizei ist zum Motor digitaler Eigenentwicklungen geworden. Zugleich hat die Landesregierung als eines der ersten Bundesländer die hessischen Polizistinnen und Polizisten mit modernen und besonders gesicherten Smartphones ausgestattet, auf denen die speziell entwickelten Applikationen den polizeilichen Arbeitsalltag revolutionieren. Hessens forciert auch weiterhin den Ausbau moderner digitaler Lösungen für die Polizeiarbeit. Beim Kampf gegen Kindesmissbrauch, Einbrecherbanden und Geldautomatensprenger kommen bereits innovative Software- und Analysetools zum Einsatz. Angesichts der Unmengen an Daten, die heute bei der Polizeiarbeit anfallen, hat sich Hessen als erstes Bundesland diesem polizeilichen Zukunftsthema beherzt angenommen und der Polizei mit hessenDATA eine modere Analyseplattform an die Hand gegeben.

„Die Polizeiarbeit der Zukunft muss effizient mit großen Datenmengen umgehen. Eine moderne und effektive Technik ist dabei im alltäglichen Polizeidienst unverzichtbar. Die Landesregierung nicht nur bewiesen, dass sie die Polizei bei der Verbrechensbekämpfung aktiv unterstützt, sondern auch, dass sie der Innovationstreiber der deutschlandweiten Polizeiarbeit ist. Denn viele Bundesländer eifern uns hier bereits nach", so der Innenminister.

Sicherheitsgefühl ist Teil der hessischen Sicherheitsstrategie

Bereits im Jahr 2017 hat Hessen mit dem KOMPASS-Programm ein neues Kapitel in der Sicherheitsstrategie des Landes aufgeschlagen. Über das Programm, an dem mittlerweile 138 KOMPASS-Kommunen teilnehmen, können hessische Städte und Ge-

meinden Sachverhalte, die das Sicherheitsgefühl beeinträchtigen können, selbständiger angehen und individuelle Lösungen für Sicherheitsbedarfe vor Ort entwickeln. Im Rahmen von KOMPASS wurden hessenweit zahlreiche Sicherheitsanalysen und Bürgerbefragungen zur Erkennung von Problemfeldern in Kommunen durchgeführt, die auch in die operative Polizeiarbeit einfließen, und darauf aufbauende Lösungsansätze entwickelt. Die Bürgerinnen und Bürger sind nicht mehr allein der passive Empfänger von Sicherheitsmaßnahmen des Staates. Sie können und sollen sich in Hessen ganz bewusst nunmehr noch aktiver an der Verbesserung der Sicherheit und des Sicherheitsgefühls in ihrem Nahbereich beteiligen und aktiv mitwirken. „KOMPASS hat den Grundstein für einen Paradigmenwechsel in der Sicherheitsstrategie des Landes gelegt. Aber wir ruhen uns auf den Erfolgen nicht aus. Mit dem ‚Sicherheitsportal Hessen' haben wir alle Sicherheitsprogramme für die Bürgerinnen und Bürger unter einem Dach gebündelt und den Leitgedenken des gemeinsamen Gestaltens von Sicherheit digital fortgeführt. Erneut untermauert die Hessische Landesregierung damit, dass sie sich unaufhörlich und mit einem klaren Plan dem Sicherheitsempfinden der Menschen annimmt", so Innenminister Peter Beuth.

Neues Online-Portal bündelt die Angebote zur Erhöhung der Sicherheit in Hessen

Das seit Februar 2023 bereitstehende Sicherheitsportal bündelt die Onlinewache der hessischen Polizei, die Meldestelle HessenGegenHetze sowie einen landesweiten Mängelmelder. Der Mängelmelder, an dem gegenwärtig rund 325 von 421 hessischen Kommunen teilnehmen, ermöglicht es den Bürgerinnen und Bürgern unkompliziert ihre Anliegen den Kommunen mitzuteilen. „Die erste Resonanz auf das Sicherheitsportal zeigt: Wir haben einen Nerv getroffen und das richtige Angebot unterbreitet. Die Bürgerinnen und Bürger profitieren davon. Denn Sie können nun unkompliziert der Kommune und den Sicherheitsbehörden ihre Anliegen mitteilen und auch öffentliche Orte melden, an denen sie sich unsicher fühlen. Jede Örtlichkeit und jeder Anlass werden individuell von Polizeibeamten mit Ortskenntnis bewertet und gemeinsam mit den Kommunen Lösungen erarbeitet", so der Minister.

Historisch gute Sicherheitswerte

Seit vielen Jahren gehört Hessen auch im bundesweiten Ländervergleich zu einem der sichersten Bundesländer. Deutlich wird dies bei der Häufigkeitszahl, die Zahl der polizeilich registrierten Straftaten je 100.000 Einwohner, mit der Hessen in den vergangenen Jahren stets einen Spitzenplatz unter den Ländern einnahm. Die absolute Zahl der Straftaten ist 2022 im Vergleich zu 2002 um mehr als 60.000 Delikte gesunken. In den vergangenen 20 Jahren konnte die Anzahl der Straftaten in Hessen damit um 17 Prozent gesenkt werden. Hinzukommt, dass heute 63,7 Prozent aller Straftaten und damit zwei von drei Delikten in Hessen aufgeklärt werden. 2002 lag die Aufklärungsquote noch bei 48,2 Prozent. Maßgeblichen Anteil an den guten Sicherheitswerten hat die Arbeit der hessischen Polizei, der Innenminister Peter Beuth auch im Namen der Hessischen Landesregierung ausdrücklich für ihre erfolgreiche Arbeit dankte.

Rekordinvestitionen in die Stärkung der hessischen Polizei

Die guten Sicherheitswerte gehen mit strategischen Schwerpunktsetzungen und gezielten Investitionen einher. Die finanzielle Ausstattung der hessischen Polizei befindet sich seit Jahren auf Rekordniveau und steigt in diesem Jahr mit 2,1 Milliarden Euro auf einen neuen Höchststand. Zugleich wurde die hessische Polizei massiv personell gestärkt: Seit einigen Wochen sind bereits mehr als 15.500 Polizistinnen und Polizisten für die Sicherheit der Bürger unterwegs. Allein seit Beginn dieser Legislaturperiode 2018 ist dies ein zusätzliches Plus von 1.400 Beamtinnen und Beamten. 2025 werden über 16.000 Polizistinnen und Polizisten Verantwortung für die Sicherheit übernehmen. Im Vergleich zum Jahr 2014, dem Beginn des Personalaufbaus, beträgt der Zuwachs dann satte 18 Prozent. „In unserem Bundesland gab es unter keiner Landesregierung zuvor mehr Polizei. Trotz dieses Rekords und trotz der sehr guten Sicherheitslage ist der Personalzuwachs bei der hessischen Polizei noch lange nicht zu Ende. Denn in den kommenden beiden Jahren kommen nochmals 500 zusätzliche Beamtinnen und Beamte hinzu. Der historische Zuwachs bei unserer Polizei wird Hessen noch sicherer machen", so Hessens Innenminister.

BVSW

11. BVSW-Wintertagung

Sicherheitsgipfel der deutschen Wirtschaft verbucht Teilnahme-Rekord

Angesichts der derzeitigen Weltlage war der Informationsbedarf enorm: Über 150 Gäste folgten der Einladung des BVSW an den Spitzingsee, um vom 8. bis 10. März bei der Wintertagung im Arabella Alpenhotel dabei zu sein. Knapp drei Tage lang bot die Wintertagung exklusive Informationen rund um die wichtigsten sicherheitsrelevanten Herausforderungen unserer Zeit.

„Mehrere Krisen finden aktuell parallel statt, sie bedingen und verstärken sich gegenseitig", so der BVSW-Vorstandsvorsitzende Johannes Strümpfel bei seiner Begrüßungsrede. „Für Unternehmen wird es deshalb immer wichtiger, jene Trends zu kennen, die Einfluss auf die Sicherheitslage in Deutschland haben. Mit unserer Wintertagung bieten wir alljährlich einen exklusiven Einblick in die wichtigsten Entwicklungen."

Für die Vorträge hatte der BVSW wie jedes Jahr herausragende Experten und Redner eingeladen:

Geopolitische Lage setzt deutsche Wirtschaft unter Druck

Zum Auftakt der Veranstaltung sprach Landespolizeipräsident Michael Schwald über die aktuelle Sicherheitslage in Bayern, das in Sachen Sicherheit noch immer Spitzenreiter unter den Bundesländern ist. Cyber-Kriminalität, steigende Fallzahlen beim CEO-Fraud, Enkeltrick sowie falscher Polizeibeamten, die Sicherheit von Großveranstaltungen und Nachwuchssorgen – das sind nur einige der Herausforderungen, mit denen die Bayerische Polizei zu kämpfen hat. Umso wichtiger ist die hervorragende und vertrauensvolle Zusammenarbeit zwischen Polizei, BVSW und Unternehmen in Bayern. Zum Erfolg trägt auch die Kooperationsvereinbarung zwischen BVSW, BDSW und der Polizei bei. Auch zukünftig plane die Polizei intensiv mit Unternehmen und Sicherheitsdienstleistern zusammenzuarbeiten, weil sich gemeinsam mehr erreichen ließe.

Den Eröffnungsvortrag des zweiten Kongresstages hielt Prof. Dr. Günther Schmid. Der Professor (em.) für internationale Politik erklärte, wie revisionistische Staaten daran arbeiten würden, das derzeitige globale Machtgefüge zu verschieben. Die aktuellen Krisen, insbesondere der Ukraine-Krieg und die Pandemie, hätten dazu geführt, dass sich der Systemwettbewerb zwischen den USA und China weiter verschärft.

Wie China seine Position in der Welt systematisch zu stärken versucht, prä-

(von links nach rechts) Landespolizeipräsident Michael Schwald, Caroline Eder, Geschäftsführerin des BVSW, BVSW-Vorstandsvorsitzende Johannes Strümpfel

sentierte Daniel Mauer, Leiter des Sachgebiets China-Außenwirtschaft beim BND. Der Plan „China Standards 2035" beispielsweise würde darauf abzielen, globale Standards für Zukunftstechnologien, wie Künstliche Intelligenz, IoT oder 5G zu etablieren. Das Programm sei ein weiterer Baustein in Chinas Plan, bis

2050 zur Weltmacht aufzusteigen, denn wer führende Industriestandards setzt, kann diese so ausgestalten, dass sie den eigenen Stärken und Ambitionen zu Gute kommen. Experten fordern deshalb, dass EU-Staaten Unternehmen unterstützen sollen, Vertreter in die Normierungsgremien zu entsenden. Ein weiteres wichtiges Thema an diesem zweiten Kongresstag war der Krieg in der Ukraine und seine Auswirkungen auf die Sicherheit in Bayern und in Deutschland. Dr. Burkhard Körner, Präsident des bayerischen Landesamtes für Verfassungsschutz, erklärte wie Extremisten unterschiedlicher Gruppierungen die Krisensituationen nutzen würden, um Misstrauen in den Staat zu säen und ihre verfassungsfeindlichen Ziele durchzusetzen. Auch ausländische Akteure würden versuchen, „Staatsverdrossene" anzusprechen und für sich zu gewinnen.
Während Extremisten neue Anhänger meist über das Internet zu rekrutieren versuchen, bekommen Unternehmen die Auswirkungen des zunehmenden Extremismus bereits ganz konkret zu spüren. Peter Kunkel, Leiter der Konzernsicherheit der Rheinmetall AG, zeigte, wie das Rüstungsunternehmen den teilweise gewalttätigen Protestaktionen begegnet. Zum Schutz von Werten und Mitarbeitern sei ein intensiver Austausch zwischen Polizei, Wirtschaft und Verfassungsschutz wichtig.

Risiken durch Cybercrime und Klimawandel

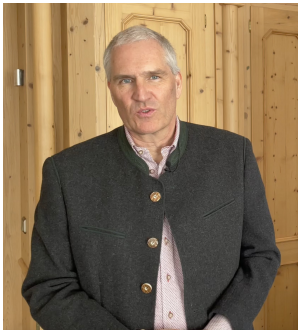
Austausch und gute Zusammenarbeit sind auch bei der Bekämpfung von Cybercrime von essentieller Bedeutung, wie die Kongressteilnehmer im Vortrag von Dr. Benjamin Krause erfuhren. Der Oberstaatsanwalt ist einer der führenden Köpfe der Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) bei der Generalstaatsanwaltschaft Frankfurt am Main. Er gehörte zu dem internationalen Ermittler-Team, das 2021 die Infrastruktur der Emotet-Schadsoftware zerschlagen hatte und so das Geschäftsmodell „Emotet" für einen längeren Zeitraum empfindlich stören konnte. Emotet galt bis dahin als der „König der Schadsoftware" und war weltweit verantwortlich für eine Vielzahl von schweren Cyber-Sicherheitsvorfällen. Trotz des signifikanten Erfolges, konnten nicht alle Täter der Gruppe gefasst werden, weshalb die Ermittlungen andauern. Den Abschluss des zweiten Kongresstages bildete der Vortrag von Prof Dr. med. Thomas J. Müller, Chefarzt und ärztlicher Direktor an der Privatklinik Meiringen im Berner Oberland. Der Mediziner forscht über den Zusammenhang zwischen Klimawandel und psychischer Gesund-

heit. Anhand unterschiedlicher Studien zeigte er, dass steigende Temperaturen und vermehrte Aggressivität korrelieren. Das macht sich beispielsweise durch steigende Kriminalität oder mehr Aufnahmen in der Psychiatrie an Hitzetagen bemerkbar. Zudem gibt es einen Zusammenhang zwischen Hitze und Hass im Internet.

Unternehmenssicherheit muss sich neu definieren

Der letzte Kongresstag startete mit einem Beitrag von Sven Weizenegger, Leiter des Cyber Innovation Hubs der Bundeswehr. Ziel dieser Einheit ist es, nach Start-up-Manier digitale Innovationen bei den deutschen Streitkräften umzusetzen. Wichtigster Erfolgsfaktor ist für ihn dabei die Agilität, die Dinge wie Flexibilität, Schnelligkeit und proaktives Handeln vereint.

Welche Auswirkungen die aktuellen Entwicklungen auf die Arbeitsweise der Security-Abteilungen in den Unternehmen haben werden, zeigte Prof. Dr. Marc Knoppe, Professor für Internationales Handelsmanagement, Strategisches Marketing und Innovationsmanagement an der TH Ingolstadt. Unternehmenssicherheit wird sich zunehmend auf die Analyse der vielen Daten stützen, die mittlerweile durch unterschiedliche Systeme bereitstehen. Durch ihr Wissen und ihre Fähigkeiten habe die Security zunehmend die Möglichkeit, einen echten Mehrwert für Unternehmen zu erbringen. Mit dem Ziel Sicherheitskräfte für ihre zukünftigen Aufgaben auszubilden, hat der BVSW den Bachelor-Studiengang an der TH Deggendorf etabliert. Peter Apfelbeck, Referent am Zentrum für akademische Weiterbildung an der Hochschule, präsentierte den Studiengang, bei dem die ersten Studenten demnächst ihren Abschluss machen werden.



Prof. Dr. Marc Knoppe, Professor für Internationales Handelsmanagement, Strategisches Marketing und Innovationsmanagement an der TH Ingolstadt

Damit auch kleinere und mittelständische Unternehmen eine umfassende Security leisten können, werden zukünftig Plattformen gefragt sein, die solche Leistungen anbieten können.
Durch die entstehenden Skaleneffekte lassen sich hier die Kosten senken. Gerald Ulmer, Leiter für Strategie und Digitale Transformation im Bereich Security der Siemens AG, baut derzeit eine solche Security-Plattform auf. Zum Abschluss der Tagung gab Dr. Benedict Franke Einblicke in die diesjährige Münchner Sicherheitskonferenz. Bislang, so Franke, war es die Geschlossenheit des Westens, die einen Sieg Putins verhindern konnte. Doch der Westen ist ebenso aufgefordert, seine Werte in der Welt besser zu vermitteln, um beispielsweise den Wettlauf um Partner im Globalen Süden nicht zu verlieren.
„Das spannende Tagungsprogramm bot reichlich Gesprächsstoff bei den Gästen, die die vielen Gelegenheiten zum Netzwerken zu nutzen wussten", so Caroline Eder, Geschäftsführerin des BVSW. „Auch wenn wir dieses Jahr eine lange Warteliste hatten, werden wir die Teilnehmerzahl zukünftig nicht weiter ausbauen. Demzufolge heißt es: Frühzeitig für die nächste Wintertagung anmelden!"

Die Wintertagung 2024 findet vom 6. bis 8. März statt, Buchungen sind ab sofort möglich.

Digital. Datenbasiert. DroNet.

Vodafone & Dimetor stellen ersten digitalen Risiko-Check für Drohnenflüge vor

- **Drohnenland Deutschland: Bis 2025 fast eine halbe Million Drohnen in Deutschlands Luftraum**
- **Immer mehr Drohnen im kommerziellen Einsatz für Logistik & Industrie**
- **Vodafone & UPLIFT-Partner Dimetor starten mit DroNet eine digitale Lösung für den Risiko-Check**
- **Das Ziel: Genehmigungsprozesse beschleunigen & mit anonymisierten Bewegungsdaten aus dem Mobilfunk-Netz Drohnenflüge sicherer machen**

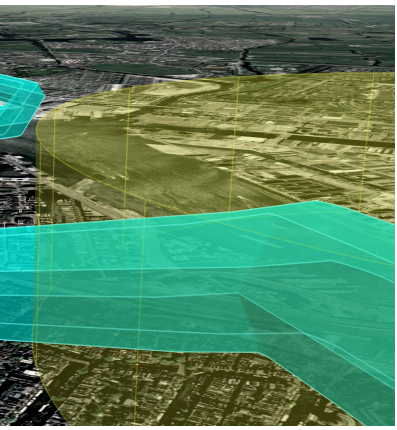
Mit DroNet brachten Vodafone und Dimetor am 23. März 2023 den branchenweit ersten digitalen Datenservice zum Risiko-Check für kommerzielle Drohnenflüge auf den Markt. Über eine digitale Schnittstelle können Operatoren und Genehmigungsstellen den Drohnen-Service von Vodafone nutzen, um mit Hilfe anonymisierter Bewegungsdaten aus dem Mobilfunk-Netz das Boden- und Konnektivitätsrisiko zu bewerten. DroNet liefert somit Antworten auf die Fragen: Wie viele Menschen halten sich unterhalb der Flugroute auf? Und wie stabil ist die Mobilfunk-Verbindung zwischen Pilot und Drohne? So soll der Geneh-

Drohnentechnik

migungsprozess beschleunigt und die Drohnenflüge sicherer gemacht werden.
Zeitmaschinen, Hoverboards und Blitzdings – nicht alle Erfindungen aus der Welt der Science-Fiction schaffen tatsächlich den Sprung in die Realität. Doch gibt es fast genauso viele, die heutzutage einfach nicht mehr aus unserem Alltag wegzudenken sind. Smartphones und Video-Calls zum Beispiel. Und voraussichtlich bald auch Drohnen. Bis 2025 soll sich laut Verband der unbemannten Luftfahrt die Anzahl der Drohnen in Deutschlands Luftraum auf rund 450.000 erhöhen. Haupttreiber dieser Entwicklung: der kommerzielle Drohnenmarkt.

Wir wollen dazu beitragen, die Genehmigungsverfahren für Drohnenflüge in Deutschland zu beschleu- nigen.
Michael Reinartz
Vodafone Innovationschef

Denn die unbemannten Flugobjekte sind im Einsatz als smarte, effiziente und ressourcenschonende Helferlein aus der Industrie und Logistik zukünftig nicht mehr wegzudenken. Damit die Vorteile gegenüber den Risiken, z. B. durch Abstürze oder Kollisionen, überwiegen, hat die EU klare Regeln für Drohnenflüge jeglicher Art definiert.
450000 Drohnen soll es bis 2025 laut Verband der unbemannten Luftfahrt in Deutschlands Luftraum geben.



Sicherheit bei Drohnenflügen – auf dem Boden und in der Luft

So gehören Flüge mit dem größten Effizienz-Potential für den kommerziellen Einsatz – also Flüge über größere Distanzen und somit außerhalb der Sichtweite des Piloten, oftmals automatisiert oder gar autonom – zu den genehmigungspflichtigen Flügen. Bei einer solchen Genehmigung werden zur Einschätzung des Risikos vor allem zwei Kriterien geprüft:

1. Wie viele Menschen halten sich unterhalb der definierten Flugroute auf?
2. Ist die Mobilfunk-Konnektivität auf der definierten Flugstrecke ausreichend und ohne Unterbrechungen gegeben?

Sichere Flüge von Drohnen

Mit DroNet bringen Vodafone & Dimetor den ersten digitalen Datenservice zum Risiko-Check für kommerzielle Drohnenflüge auf den Markt.

Bis ein solches Genehmigungsverfahren mit der Beantwortung dieser Fragen abgeschlossen ist, dauert es aktuell mehrere Wochen. Nicht zuletzt, weil die Bereitstellung und Prüfung der Antworten bislang sehr aufwändig ist.

Verschiebung des RED DA-Antragsdatums

Euralarm hat eine Erklärung zur Verschiebung des Anwendungsdatums der RED DA veröffentlicht

Die Europäische Kommission hat mit dem Erlass des delegierten Rechtsakts (DA) ((EU) 2022/30) für die Funkanlagenrichtlinie (RED) Maßnahmen ergriffen, um ihre Bürger vor Cyberangriffen und Datenschutzverletzungen zu schützen. Obwohl die CEN/CLC/JTC 13/WG 8 mit der extrem schnellen Entwicklung harmonisierter Normen zur Unterstützung der RED DA eine beispiellose Aufgabe bewältigt, ist Euralarm der Ansicht, dass das Anwendungsdatum der RED DA (derzeit August 2024) verschoben werden sollte. Das derzeitige Datum verhindert die Vermarktung einer beträchtlichen Anzahl bestehender und neuer Produkte mit potenziell großen Auswirkungen auf Unternehmen und Verbraucher. Euralarm fordert die europäischen Mitgliedsstaaten auf, mit der Kommission zusammenzuarbeiten, um die Fertigstellung von Normen besser auf das Datum der Anwendung abzustimmen.

Funkanlagenrichtlinie (RED)

Die Hersteller nutzen zunehmend neue Technologien und das Internet, um ihre Produkte zu verbessern; daher ist die Cybersicherheit heute von entscheidender Bedeutung. Um ein sicheres und geschütztes Online-Umfeld zu gewährleisten, hat die Europäische Kommission daher eine Reihe von neuen Vorschriften ausgearbeitet. Dazu gehören der Vorschlag für einen Cyber Resilience Act und die RED DA.

Letztere ist in Kraft getreten und deckt in Artikel 3 Absatz 3 Buchstaben d, e und f bestimmte Arten von Funkanlagen ab. Dazu gehören mit dem Internet verbundene Funkgeräte, tragbare Technologie oder tragbare Geräte mit einer Funkfunktion, Geräte für die Übertragung von Geld oder virtueller Währung und Kinderspielzeug mit einer Funkfunktion oder andere Kinderbetreuungsgeräte. Diese Ergänzung wird auch drahtlose Produkte für den Brandschutz und die Sicherheit umfassen.

Eine Expertenarbeitsgruppe aus ganz Europa (JTC13/WG8) entwickelt derzeit harmonisierte Normen zur Unterstützung der grundlegenden Anforderungen der RED DA. Diese harmonisierten Normen werden den Herstellern eine klare Anleitung geben, was von ihnen erwartet wird, wenn es um die Erfüllung der in der RED DA festgelegten Anforderungen geht. In Ermangelung von Normen, die im Amtsblatt der EU aufgeführt sind, müssen sich die Hersteller an eine ' Notified Body' wenden, um das Konformitätsbewertungsverfahren zu durchlaufen.

Verzögerung notwendig

Das Datum für die Anwendung der RED DA ist derzeit auf August 2024 festgelegt. Mit Blick auf den Prozess fordert Euralarm die Europäische Kommission und die Mitgliedsstaaten auf, dies zu berücksichtigen:

- Es ist sehr wahrscheinlich, dass die harmonisierten Standards nicht rechtzeitig erreicht werden. Trotz der bisherigen Fortschritte ist zu erwarten, dass die harmonisierten Normen von CEN-CENELEC bestenfalls 1 oder 2 Monate vor dem Anwendungsdatum angenommen werden.
- Der Bewertungs- und Zitierprozess wird sich nach der Verabschiedung weiter verzögern. Die Tatsache, dass kein HAS-Berater zur Verfügung steht, der die JTC13/WG8 bei der Ausarbeitung der Normen unterstützt, schafft zusätzliche Unsicherheit hinsichtlich der Wahrscheinlichkeit, dass die angenommenen Normen im Amtsblatt zitiert werden.
- Die Verzögerung wird die Hersteller daran hindern, eine rechtzeitige Selbstbewertung der Konfor- mität mit den neuen Anforderungen vorzunehmen.
- Es gibt nicht genügend 'Notified Bodies' (4 in 2 Ländern), um die erforderliche Konformitätsbewertung durchzuführen, so dass dies kein gangbarer Weg zur Einhaltung der Vorschriften ist. Obwohl ihre Zahl in den kommenden Monaten steigen dürfte, werden sie durch die Nachfrage überlastet sein, was bedeutet, dass die meisten Hersteller monatelang keine Gelegenheit haben werden, das Konformitätsbewertungsverfahren zu durchlaufen.
- Dies wird die Marktverfügbarkeit aller bestehenden und neuen Produkte, die unter die RED DA fallen, verzögern. Infolgedessen werden die Hersteller das Inverkehrbringen der von der RED DA erfassten Produkte in der EU bis zum Abschluss des Konformitätsbewertungsverfahrens einstellen. Zu diesen Produkten gehört eine breite Palette von Funkgeräten für den Geschäfts- und Privatkundenmarkt.
- Die zu installierenden Produkte werden nicht an Dienstleistungsunternehmen geliefert. Es wird klar sein, dass eine ordnungsgemäße Abstimmung des Datums für die Anwendung der RED DA einerseits und des Datums für die Bereitstellung der harmonisierten Normen, einschließlich der für die Bewertung, Prüfung und Bereitstellung auf dem Markt benötigten Zeit andererseits, von größter Bedeutung ist. Wenn diese nicht richtig aufeinander abgestimmt sind, wird sich dies negativ auf die Wirtschaftstätigkeit in den Mitgliedstaaten der Europäischen Union auswirken, sowohl für Unternehmen als auch für Verbraucherprodukte.

Gemeinsam mit den nationalen Industrieverbänden fordert Euralarm die Mitgliedstaaten und die Kommission daher dringend auf, das Datum des Inkrafttretens zu verschieben. Eine Verzögerung von 9 Monaten würde die ursprüngliche Reihenfolge zwischen der Annahme der Normen und dem Datum des Inkrafttretens wiederherstellen, wie sie im Normungsantrag M/585 festgelegt ist, aber eine Verzögerung von 12 bis 18 Monaten würde den Herstellern mehr Gelegenheit geben, ihre Produkte von einer ' Notified Body' bewerten zu lassen.

Telenot

Atruvia erteilt Freigabe für Zutrittskontrollsystem

Zutrittskontrollsystem hilock 5000 ZK besteht sicherheitstechnische Prüfung

Die Software compasZ 5500 dient der Verwaltung des Zutrittskontrollsystems hilock 5000 ZK von Telenot. Nun hat die Software die anspruchsvolle sicherheitstechnische Prüfung der Atruvia AG bestanden, Digitalisierungspartner der Volks- und Raiffeisenbanken. Diese Geldinstitute haben damit die Freigabe zum Einsatz des Systems für ihre Standorte.
Banken sind seit jeher Unternehmen, die in nahezu allen Bereichen ein erhöhtes Sicherheitsbedürfnis haben. Schließlich lagern in den Filialen zumeist erhebliche Geld-, Sachwerte und sensible Kundendaten, die es vor unbefugtem Zugriff und Diebstahl zu schützen gilt. Dem entsprechend hoch sind auch die Ansprüche, die von den Banken an die installierte Sicherheitstechnik gestellt werden. Bevor Banken die Produkte einsetzen dürfen, müssen diese eine eingehende sicherheitstechnische Prüfung bestehen.

Anfang Januar 2023 hat die Zutrittsverwaltungssoftware compasZ 5500 (ab Version 3.1.0.0.) von Telenot nach umfassenden Tests durch die Atruvia AG die Unbedenklichkeitsbestätigung bekommen.
Telenots Verwaltungssoftware compasZ 5500 hat bei dieser Prüfung das von der Atruvia geforderte Sicherheitsniveau deutlich überschritten. Die Software ist Teil des flexiblen und einfach skalierbaren Zutrittskontrollsystems hilock 5000 ZK. Das Zusammenspiel der Verwaltungssoftware mit dem Auswertesteuergerät hilock 5500 ermöglicht es Nutzern, wirtschaftliche Zutrittslösungen für jede Objektgröße und -art zu realisieren. Ganz einfach können dabei Funktionszeitmodelle beispielsweise zur Regelung der Öffnungszeiten jeder einzelnen Bankfiliale aufgestellt werden. Alle Zutrittsrechte lassen sich standortübergreifend koordinieren. Auch spezielle Routinen für Feiertage stellen für das System kein Problem dar.

„Die Freigabe belegt, dass unser Zutrittskontrollsystem als Ganzes allen relevanten technischen sowie sicherheitstechnischen Anforderungen entspricht und damit für den Einsatz im Umfeld von Finanzinstituten geeignet ist – und natürlich in allen anderen Bereichen, wo maximale Zuverlässigkeit gefragt ist", erklärt Julian Gring, Produktmanager Zutrittskontrolle.
Mit seiner Vielseitigkeit sowie der einfachen Bedienbarkeit reduziert compasZ 5500 den zeitlichen Verwaltungsaufwand deutlich und gewährleistet gleichzeitig höchste Sicherheit. Das hilock 5000 ZK bietet lizenzbasiert zudem unzählige Anwendungen wie Bereichswechselkontrolle, Zählfunktionen, Aufzugsteuerung, temporäre Zutrittsberechtigung, Toggle-Berechtigungen oder die Bildung von Organisationseinheiten und Gruppen. Höchste Verschlüsselungsstandards sorgen dabei für maximale Sicherheit – von der Verwaltungssoftware über das Auswerte- und Steuergerät hilock 5500, den RFID-(Schreib-)Lesern bis zum Transponder. Das vollumfängliche Programm an intelligenten Zutrittskontrolllesern, mechatronischen Schließelementen bis hin zu Smartphone-Accesslösungen ermöglicht Zutrittskontrolllösungen jeglicher Art.

Bildung notwendig

Studie: Cybersicherheit in Europa erfordert einheitliches Bildungsprogramm

- **Forscher der finnischen Aalto-Universität veröffentlichen Bericht über die gesellschaftlichen Fähigkeiten und Praktiken im Bereich Cybersicherheit aller europäischer Mitgliedsstaaten**
- **Es große Unterschiede bei der Entwicklung von Cyber-Kompetenzen innerhalb der EU gibt und ihre Bürger*innen von einem einheitlichen Ansatz profitieren würden**
- **Ziel der Cyber-Citizen-Initiative ist es, ein gemeinsames Verständnis und Lernmodell für Cyber-Bürgerkompetenzen in der EU zu entwickeln, um eine einheitliche Sicherheitskultur zu schaffen**

Die Zahl und Komplexität von Cyberangriffen und Cyberkriminalität nimmt in ganz Europa zu. Aus diesem Grund investieren die nationalen Regierungen in der gesamten EU bereits in Programme zur Aufklärung und Verbesserung der Bürgerkompetenz im Bereich der Cybersicherheit.

Das scheint jedoch nicht ausreichend zu sein, wie eine von der finnischen Aalto-Universität veröffentlichte Studie über die "Cyber-Citizen-Kompetenzen und ihre Entwicklung in der Europäischen Union" zeigt. Der Bericht wurde im Rahmen der von der EU finanzierten Cyber-Citizen-Initiative veröffentlicht.

Eine Initiative für Europäer*innen

Innerhalb der Untersuchung haben Forscher*innen festgestellt, dass es zwischen den EU-Ländern erhebliche Unterschiede in Bezug auf das Bewusstsein, die Bildung und Ausbildung im Bereich Cybersicherheit gibt. Obwohl diese eine länderübergreifende Bedrohung darstellt, gibt es derzeit kein einheitliches Modell für das Erlernen von Kompetenzen und auch keine gemeinsamen Praxis-Tools. Laut der bisherigen Erkenntnisse konzentriert sich die Cyber-Citizen-Kompetenz bisher weitestgehend auf die Technologie, anstatt auf das kollektive Know-how rund um diese gesellschaftliche Thematik.

Einheitliche Cyber-Citizen-Kompetenzen schaffen

Ziel der Initiative ist es, ein gemeinsames Verständnis und Lernmodell für Cyber-Bürgerkompetenzen in der EU zu entwickeln, um eine Sicherheitskultur in einem auf den Menschen ausgerichteten digitalen Umfeld zu schaffen. Dies stärkt die europäische Cybersicherheit und sorgt für eine einheitliche Vorgehensweise. Zu diesem Zweck wird ein digitales Lernportal eingerichtet. Eine breite Palette von E-Learning-Methoden inklusive eines Spiels vermitteln auf unterhaltsame Weise Informationen und vermitteln das allgemeine Verständnis im Bereich Cybersicherheit. Jarno Limnéll, Professor für Cybersicherheit an der Aalto-Universität und Leiter der Cyber-Bürger-Initiative, vergleicht diesen personenzentrierten Ansatz mit dem Verständnis der Verkehrsregeln beim Autofahren: "Die Cybersicherheit von Bürgern besteht aus ihrem Wissen, ihren Fähigkeiten und ihrer Einstellung. Die Beherrschung der Technik allein reicht nicht aus, um "cyber sicher" zu sein. Auch im Straßenverkehr ist es nicht ausreichend, nur ein Auto fahren zu können. Man muss auch die Regeln kennen und sich der anderen Verkehrsteilnehmer bewusst sein, um sich sicher zu bewegen. Cyber-Kenntnisse der Bürger sind nicht nur für deren eigenes, reibungsloses und geschütztes tägliches Leben notwendig, sondern auch für die Sicherheit und den wirtschaftlichen Erfolg der EU als Ganzes."

Bisherige Erfolge der Sensibilisierungskampagne in Deutschland

Auch in Deutschland ist die Zahl der Projekte im Bereich Cybersicherheit und Bildung in den letzten Jahren gestiegen. Das Bundesamt für Sicherheit in der Informationstechnik spielt eine wichtige Rolle bei der

Bereitstellung von Informationen für den privaten Sektor und die Öffentlichkeit. Zu den weiteren Bildungsinitiativen gehört unter anderem auch klicksafe. Eine Sensibilisierungskampagne zur Förderung der Medienkompetenz, die verschiedene Kurse und interaktive Materialien für Kinder, Jugendliche, Eltern, Lehrer und Experten anbietet, um diese beim kompetenten und kritischen Umgang mit dem Internet zu unterstützen. klicksafe ist das deutsche Awareness Centre der Europäischen Union und wird von der Medienanstalt Rheinland-Pfalz koordiniert und gemeinsam mit der Landesanstalt für Medien NRW umgesetzt. Deutschland sorgt dadurch national schon für mehr Kompetenz im Bereich Cybersicherheit und kann mit seinen bisherigen Erfahrungswerten einen erheblichen Beitrag für ein europäisches einheitliches Bildungsprogramm leisten.

Der Index-Überblick der Aalto-Studie veranschaulicht den aktuellen Kenntnisstand in der Europäischen Union und zeigt die Unterschiede im Bereich Cybersicherheit unter Berücksichtigung mehrerer Indizes: dem Global Cybersecurity Index (GCI), dem Nationalen Cybersicherheitsindex (NCSI) und dem Index für digitale Wirtschaft und Gesellschaft (DESI). Es können jeweils 100 Punkte und insgesamt höchstens 300 Punkte erreicht werden. Auch wenn alle Länder unter 250 Punkten liegen und damit noch deutliches Potenzial nach oben haben, siedelt sich Deutschland bereits im oberen Drittel an.

Die Vielfalt der verschiedenen Projekte und Praktiken in der EU zeigt, dass von jeder Ecke Europas aus etwas gelernt werden kann. Alle können etwas dazu beitragen, in der nächsten Phase der Cyber-Citizen-Initiative ein einheitliches europäisches Modell für den Erwerb von Cyber-Citizen-Kompetenzen zu entwickeln.

Machen Sie mit!

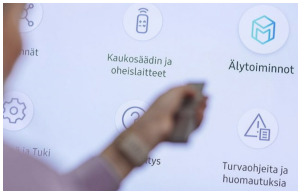
In der zweiten und dritten Phase der Cyber-Citizen-Initiative wird ein europaweites Kooperationsnetz geschaffen, in dem alle, die an der Entwicklung von Bürgerkompetenzen im Bereich Cybersicherheit interessiert sind, willkommen sind. Über die Website der Initiative können sich alle, die sich mit Cybersicherheit, Forschung und Bildung befassen oder generell etwas dazu beitragen können, melden: www.cyber-citizen.eu

Über die Cyber-Citizen-Initiative:

- Dauer: 2022-2024
- Finanzierung: Fünf Mio. Euro aus dem Aufbauinstrument der EU für einen Dreijahreszeitraum
- Beauftragter: Finnisches Ministerium für Verkehr und Kommunikation
- Ausführende Organisation: Aalto-Universität
- Projektleiter: Professor Jano Limnéll, Aalto Universität

Weitere Informationen:

- Cyber Citizen: Research report – Cyber citizen skills and their development in the European Union
- Finnland (Bild) schnürt ein Bildungspaket, um Cybersicherheit zu einer Bürgerkompetenz in der Europäischen Union zu machen



Digitale Prozesse verändern die Baubranche

Nachholbedarf bei BIM • Daten ermöglichen industrielle Fertigung und serielles Bauen • IoT, Virtual Reality und Künstliche Intelligenz auf der Baustelle

Branchen wie die Automobilindustrie oder der Maschinen- und Anlagenbau sind zwar noch ein gutes Stück voraus, doch auch im Bauwesen schreitet die digitale Transformation unaufhaltsam voran – in allen Phasen des Planungs- und Bauprozesses und bei allen Beteiligten. Die BAU 2023 widmet dem Thema einen eigenen Ausstellungsbereich. In Halle C5 präsentieren Unternehmen die neuesten Hard- und Softwarelösungen für die Planung und Ausführung. Im Forum C2 berichten Experten aus Planungs- und Ingenieurbüros am Freitag, 21. April, über die digitale Transformation und stellen anhand von Projektbeispielen aktuelle Lösungen vor.

Grundlage für die digitale Transformation ist die Cloud. Sie ermöglicht die Speicherung großer Datenmengen an zentraler Stelle. Für ein Bauprojekt geschieht das in der Regel in einem BIM-Modell, auf das alle Beteiligte Zugriff haben. In diesem digitalen Zwilling des realen Gebäudes werden alle Daten kontinuierlich erfasst und verwaltet. Änderungen lassen sich in Echtzeit verfolgen. So entsteht Transparenz, der Planungs- und Bauprozess wird verlässlicher, schneller und weniger anfällig für Fehler oder Missverständnisse. Ebenso wichtig wie ein nachvollziehbarer Planungs- und Bauprozess sind Zeitmanagement und Kostenkontrolle. Softwaretools, die anhand eines BIM-Modells Mengen ermitteln und daraus Kosten ableiten, schaffen be-

reits in der Planungsphase Verlässlichkeit. Bei Materialengpässen oder Preissteigerung lassen sich Ausführungsvarianten und Materialien miteinander vergleichen.

Nachholbedarf bei BIM

Obgleich die große Mehrheit der Branche den Mehrwert dieser Technologien erkennt, sieht sich weniger als die Hälfte der deutschen Planungs- und Bauunternehmen in Sachen Digitalisierung gut aufgestellt, wie aus einer Studie der Beratungsgesellschaft PwC vom Dezember 2020 hervorgeht. Bei BIM haben gar über zwei Drittel der Befragten noch Nachholbedarf. Das Bewusstsein für das Potenzial digitaler Instrumente ist also vorhanden, die Umsetzung scheitert aber oft an mangelnden Kenntnissen. Ein Grund dafür ist, dass digitale Lösungen von Bauherrn viel zu selten eingefordert werden. 80 Prozent der Studienteilnehmer berichten, dass das nur teilweise oder gar nicht der Fall ist.

Abhilfe schaffen soll u. a. das neue BIM-Portal des Bundes, das am 11. Oktober 2022 an den Start ging. Es stellt Informationen, Anwendungen und einheitliche Daten bereit, mit der die Digitalisierung von Bauvorhaben vorangebracht werden soll. Dazu zählen u. a. interaktive und webbasierte Werkzeuge, Datenbibliotheken sowie herstellerneutrale Bauteile-Informationen. Die Plattform soll ständig weiterentwickelt werden. Sie ist das Ergebnis eines Stufenplans, der bereits 2015 in Kraft trat und die schrittweise Einführung von BIM auf den Weg bringen sollte. Bis heute ist der Einsatz von BIM allerdings nur für die Ausschreibung öffentlicher Infrastrukturprojekte verpflichtend, nicht für den Hochbau allgemein.

Daten ermöglichen industrielle Fertigung und serielles Bauen

Ohne Digitalisierung keine industrielle Fertigung: Die Verfügbarkeit von Daten in BIM-Modellen, sowohl über Bauteile wie über das Gebäude selbst, ist die Voraussetzung für die standardisierte und automatisierte Fertigung in der Werkshalle, ohne die wiederum das serielle und modulare Bauen, oft als Allheilmittel gegen Wohnungsnot und Fachkräftemangel dargestellt, nicht vorankommt.

Aus den digitalen Daten werden standardisierte, aber frei kombinierbare Bausätze, die in der Fabrik vollautomatisch zusammengebaut werden, seien es Fenster, Wände oder ganze Fassaden. Auf der Baustelle werden ganze Wohnungen oder Teile davon dann nur noch zusammengesetzt, auf Basis standardisierter Grundrisse.

Die Vorteile dieser Art des Bauens liegen auf der Hand: geringere Bauzeit, Kosteneinsparungen, weniger Schutt auf der Baustelle, weniger Lärm vor Ort und weniger Baumängel aufgrund besserer Qualitäts- sicherung.

Auch auf der Baustelle: IoT, AR, VR, KI und Machine Learning

Digitale Werkzeuge kommen aber nicht nur in der Planung, sondern auch auf Baustellen zum Einsatz. Die grundlegende Technologie hierfür ist das Internet of Things (IoT). Es vernetzt Geräte und Baufahrzeuge und ermöglicht deren Interaktion und autonomen Betrieb. Das gilt auch für Roboter, die zunehmend auf Baustellen unterstützende Arbeiten verrichten, was mit Blick auf den Fachkräftemangel immer wichtiger wird. Dazu gehören auch 3-D-Druckverfahren, bei denen Roboterarme mittlerweile ganze Häuser aus schnell aushärtendem Beton fertigen. Künftig soll das auch mit Metallbaustoffen möglich sein.
Auch Technologien, die man eher vom Maschinen- und Anlagenbau kennt, halten langsam Einzug in die Bauindustrie. KI und Machine Learning zum Beispiel helfen bei der Projektsteuerung.

Sie erlauben Prognosen hinsichtlich Zeit- und Kostenvorgaben und schlagen Alarm, sobald etwas in die falsche Richtung läuft. Virtual Reality (VR) ermöglicht es Planern, in ihr CAD- oder BIM-Modell einzutauchen, und Augmented Reality (AR) kann ein wichtiges Hilfsmittel für die Erkennung von Risiken und die Vermeidung von Unfällen auf Baustellen sein. Schließlich gibt es auch immer mehr hilfreiche Apps rund um die Baustelle. Speziell Bauunternehmen und Handwerker nutzen sie gerne, etwa für die Erfassung von Maßen und Massen und auch für die Kommunikation mit Auftraggebern oder Bauleitern.

Die BAU 2023 zeigt, speziell im Ausstellungsbereich BAU IT, die neuesten Entwicklungen rund um die Digitalisierung des Planens und Bauens. Darüber hinaus bieten mit der digitalBAU (Februar 2024) sowie der digitalBAU conference & networking (4.-6. Juli 2023) zwei weitere Veranstaltungen die Möglichkeit, Chancen der digitalen Transformation live zu erleben.



Fraunhofer-Institut für Bauphysik

BAU 2023: Digitalisierung und Energieeinsparungen stehen im Mittelpunkt

Die Zeiten sind herausfordernd: Nicht nur sind die Baumaterialien im Jahr 2022 deutlich teurer geworden, auch ist die Zahl der Baugenehmigungen für Wohnungen um knapp sieben Prozent gesunken1. Veränderungen stehen der Baubranche zudem durch die zunehmende Digitalisierung sowie gestiegene Ansprüche an die Energieeffizienz von Gebäuden oder an deren Innenraumklima bevor. Neue Lösungen aus Industrie, Politik und Forschung sind daher dringend geboten. Auf der Messe BAU 2023, die vom 17. bis 22. April 2023 in München stattfindet, präsentiert das Fraunhofer IBP im Rahmen der Sonderschau »Bauen der Zukunft« auf dem Stand der Fraunhofer-Allianz Bau (Halle C2, Stand 528) innovative Produkte und Systemlösungen zu den Themeninseln Digitalisierung, Energie und Wärme, Zukunft des Wohnens und Arbeitens sowie Ressourcen und Recycling.

Lösungen für das Bauen der Zukunft, insbesondere für die Klimaneutralität und Kreislaufwirtschaft im Bau- und Wohnsektor, zeigt das Fraunhofer IBP mit zehn Exponaten. Präsentiert werden diese auf dem Messestand der Fraunhofer-Allianz Bau – genauer gesagt im und um den zweigeschossigen »Innovation Cube«. Dieser dient als symbolisches Gebäude, um neuartige Lösungen für die Gebäudehülle ebenso wie für den Innenraum zu demonstrieren. Die Exponate sind auf die vier Themeninseln Digitalisierung, Energie und Wärme, Zukunft des Wohnens und Arbeitens sowie Ressourcen und Recycling verteilt. Von Dienstag bis einschließlich Freitag gibt es zudem für alle interessierten Messebesucher zwischen 11 und 12 Uhr sowie ab 13.30 Uhr ein spannendes Vortragsprogramm.

Digitalisierung

Das Klima verändert sich, immer häufiger kommt es zu ausgedehnten Hitzeperioden oder starken Unwettern. Problematisch ist dies insbesondere in urbanen Räumen – sie reagieren hochsensibel auf diese Starkwetterereignisse. Städte müssen daher zunehmend auf den Klimawandel und dessen Auswirkungen reagieren. Leistungsfähige Stadtklimamodelle wie PALM-4U unterstützen dabei, denn sie lassen per Simulation das Stadtklima erlebbar werden: So ermöglichen sie klare Aussagen zu Klimaveränderungen und stadtklimatischen Zusammenhängen zu treffen. Kommunen, Planungsbeteiligte und Vorhabensträger können ihre planerischen Maßnahmen via PALM-4U auf deren klimatische Wirkung hin untersuchen und diese mittels Augmented-Reality-Anwendungen verständlich und immersiv an die Bürgerschaft kommunizieren.

Sinnvoll ist eine Digitalisierung auch, wenn es um Energiekennzahlen geht – schließlich klafft vielfach eine Lücke zwischen den vorab progno-

stizierten und den tatsächlich gemessenen Energiekennzahlen. Der Grund dafür: Es fehlen Daten zu Bedürfnissen und Verhalten der nutzenden Personen. Diesem Problem widmet sich das Projekt »DataFEE«: Die Prozesskette für die Datennutzung soll systematisch erschlossen und optimiert werden – auf diese Weise sollen die Prognosen für den Gebäudebetrieb verlässlicher und die Energieeffizienz besser werden. Die Forschenden erfassen die entsprechenden Daten, bereiten sie auf und stellen sie in Form von Modellen für Planungswerkzeuge und Systeme zur Betriebsführung zur Verfügung. Dabei helfen intelligente Sensorik, Data Mining, Machine Learning und Predictive Analytics. Auch der »Digitale Zwilling« soll als cyber-physisches Abbild der realen Geräte und Gebäude eine zentrale Rolle spielen. Aufbauend auf den Ergebnissen entwickeln die Forschenden Dienstleistungen für Gebäudenutzende und -betreibende.

Auf der Standfläche der Fraunhofer-Allianz Bau präsentiert sich auch in diesem Jahr einmal mehr das Mittelstand-Digital Zentrum Bau mit seinem Angebot für kleine und mittlere Unternehmen der Bau- und Immobilienwirtschaft. Der Fokus des Zentrums, das aus vier Konsortialpar- tnern aus Wissenschaft und Praxis gebildet und vom Fraunhofer IBP in Holzkirchen geleitet wird, liegt auf den fünf Themenbereichen Planungsprozess, Baustelle und Facility Management sowie in der Optimierung digitaler Geschäftsprozesse und der Entwicklung innovativer Transformationsstrategien. Hierzu bietet das Zentrum fundierte Informationsma- terialen, Veranstaltungen und Digitalisierungsprojekte mit zielorientierten Roadmaps für einen resilienten Mittelstand. Das Mittelstand-Digital Zentrum Bau gehört zum Mittelstand-Digital Netzwerk, mit dem das Bundesministerium für Wirtschaft und Klimaschutz die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk unterstützt.

Energie und Wärme

Soll die Energiewende gelingen, muss die Sanierungsquote im Gebäudesektor deutlich steigen – etwa über einen höheren Vorfertigungsgrad der Bauteile. Die Fraunhofer-Institute für Bauphysik IBP und für Energiewirtschaft und Energiesystemtechnik IEE haben eine Erneuerbare-Energien-Modulfassade entwickelt. Diese Fassade versorgt das Gebäude umwelt- freundlich mit Strom und beheizt, kühlt und lüftet die Räume. Herzstück des Moduls ist eine Photovoltaik-Anlage, kombiniert mit einer Wärmepumpe als Wärme- und Kälteer- zeuger, sowie ein dezentrales Lüftungsgerät mit Wärmerückgewinnung – die allesamt im Fassadenmodul untergebracht sind. Mit dem System lassen sich sowohl Bestandsfassaden sanieren als auch Neubauten nachhaltig und energieeffizient ausstatten. Die Fassade soll modular aufgebaut sein und kostengünstig produziert werden können.

Zukunft des Wohnens und Arbeitens

Wie lassen sich Baudenkmäler nachhaltig und energieeffizient erhalten? Mit dieser Fragestellung beschäftigt sich das Fraunhofer-Zentrum für energetische Altbausanierung und Denkmalpflege Benediktbeuern, indem es innovative und dauerhafte Lösungen erforscht. Dazu gehört auch die Weiterbildung »Fachplaner/in nachhaltige Instandsetzung historischer Bausubstanz« des Fraunhofer IRB unter der Marke »QualiBene – Lernen und Qualifizieren am Fraunhofer-Zentrum Benediktbeuern«. Die angehenden Fachplanerinnen und Fachplaner lernen und qualifizieren sich am Gebäude der Alten Schäfflerei, das denkmalgerecht und unter energetischen Gesichtspunkten instandgesetzt wurde und nun als Anschau- ungsobjekt im Sinne einer »Gläsernen Baustelle« dient. Auf der Website www.denkmalpflege.fraunhofer.de stehen ein virtueller Rundgang, aktuelle Ein- und Rückblicke in die energetische und denkmalgerechte Sanie- rung der Alten Schäfflerei sowie eine Vielzahl an aktuellen Inhalten zu Forschungsthemen bereit. Die neue Rubrik »Wissen sammeln & vermitteln« ermöglicht einen Zugang zu Baudatenbanken des Fraunhofer IRB.

Etwa drei Millionen Gebäude in Deutschland wurden in den 70-er und 80-er Jahren mit PCP- und Lindan-haltigen Holzschutzmitteln behandelt, um sie vor Schimmelbefall und Insektenfraß zu schützen. Beide Stoffe sind inzwischen verboten, schließlich zählen sie zu den krebserregenden und neurotoxischen Giften. Im Projekt CycloPlasma der Fraunhofer-Zukunftsstiftung untersuchen die Forschenden des Fraunhofer IBP, inwieweit sich das neuartige CycloPlasma-Verfahren zur Dekontamination nutzen lässt.

Dieses Verfahren kombiniert ein innovatives Adsorbermaterial mit der Plasmatechnologie. Das Ergebnis: Mit dem CycloPlasma-Verfahren können sowohl kontaminierte Hölzer als auch Innenräume behandelt werden – nachhaltig, rückstandslos und gesundheitlich unbedenklich. In einem Versuchsaufbau auf dem Gelände des Freilichtmuseums Glentleiten erprobt das Forscherteam den Ansatz prak-

tisch. Auch die Akustik spielt im Leben vieler Menschen eine wichtige Rolle – im Arbeitsumfeld wie auch in der Freizeit. Turnhallen fallen häufig durch eine extreme Halligkeit negativ auf – insbesondere Mittelhallen, die durch Trennvorhänge von den äußeren Hallenbereichen separiert werden. Dort ist es oft enorm laut und die Sprachverständlichkeit ist vielfach äußerst schlecht. Der neuartige Trennvorhang namens SportSAT, kurz für »Schall-Absorbierender Trennvorhang für Sporthallen«, entschärft die Situation. In Verbindung mit schallabsorbierenden Prallwänden und einer absorbierenden Decke sorgt der Trennvorhang für eine sehr gute Akustik in den Teilhallen und erfüllt damit die Anforderungen nach DIN 18041 sowie DIN 18032. Kurzum: Die Halligkeit wird verringert, es wird deutlich leiser und die Sprachverständlichkeit in den Sporthallen wird stark verbessert.

Bei der Berechnung solcher Nachhallzeiten hilft die neue online-basierte Software »reverberate« – insbesondere in Rechteckräumen mit ungleichmäßiger Absorberverteilung. Dazu kommt ein neues Rechenverfahren von Zhou et al. aus dem Jahr 2021 zum Einsatz. Nutzerinnen und Nutzer können dazu die Geometrie eines Rechteckraumes eingeben und die nötigen Anforderungswerte aus der DIN 18041 wählen. Zudem lassen sich alle Raumoberflächen unterteilen sowie mit absorbierenden Materialien belegen und damit die Nachhallzeit richtig berechnen.

Ressourcen und Recycling

Starkregen und damit einhergehende Überschwemmungen bestimmen zunehmend die Schlagzeilen. Verursachen sie Wasserschäden in Wohnungen, führte bisher kaum ein Weg an lärmenden und stromfressenden Bautrocknern vorbei, um Wände wieder trocken zu bekommen. Eine deutlich energiesparendere, schnellere Möglichkeit haben Forschende des Fraunhofer IBP mit »FastDry« entwickelt: Die Trocknungstechnologie benötigt nur etwa 15 Prozent der Energie, die Standard-Infrarotgeräte für den gleichen Vorgang brauchen. Die Arbeitstemperatur liegt typischerweise bei etwa 55° Celsius. Und, für die Bewohner besonders wichtig: Da weder Gebläse noch Kompressor im Einsatz sind, arbeiten die FastDry-Geräte lautlos. Das neuartige Trocknungsmodul besteht aus einer großen, rechteckigen und beidseitig kaschierten Dämmplatte aus handelsüblicher, nicht brennbarer Mineralwolle, die direkt an der feuchten Wand angebracht wird und die Wand mit einem integrierten Heizdraht erwärmt. Während die Wärme durch die Dämmung in der Wand bleibt, kann der Wasserdampf ungehindert durch das diffusionsoffene Modul entweichen.

Für eine schnelle Umsetzung der geforderten CO2-Emissioneneinsparung sind Dämmstoffe elementar: Vorausgesetzt, diese sind nachhaltig produziert und fallen auch am Ende ihres Lebenszyklus nicht aus dem Stoffkreislauf. Als besonders effizient gelten Schüttdämmungen: Eingesetzte Materialien müssen für diese Anwendung nur wenig vorverarbeitet werden und lassen sich auch gut in Produktionsprozessen integrieren. Ökologische Schüttdämmungen auf Basis von Lignocellulose-Materialien bieten hierbei ein Reihe von Vorteilen. Neben lokaler Verfügbarkeit aus Reststoffströmen können durch Adaptionen des Füllmaterials die Eigenschaften des Dämmstoffes für verschiedene Anwendungsszenarien optimiert werden: Über ein alkalisch aktiviertes Biokohlenkomposit wird das Steifigkeitsverhalten der Lignocellulose-Faser dauerhaft angepasst und zusätzlich mit einem Carbon-Capture-Effekt gepaart. Mit den Partnern Baufritz und CarbonInstead wurde die Idee bereits im Pilotmaßstab umgesetzt und mit dem vor Kurzem gestarteten Projekt SchüttliBi 2.0 soll die industrielle Umsetzung ausgearbeitet werden.

Hervorragende Wärmedämmeigenschaften hat auch Porenbeton, zudem punktet er mit einer langen Lebensdauer sowie guten akustischen Eigenschaften. Forschende des Fraunhofer IBP arbeiten daher daran, mehr alternative Rohstoffe für die Herstellung des Porenbetons zu nutzen und seine Recyclingfähigkeit zu erhöhen.

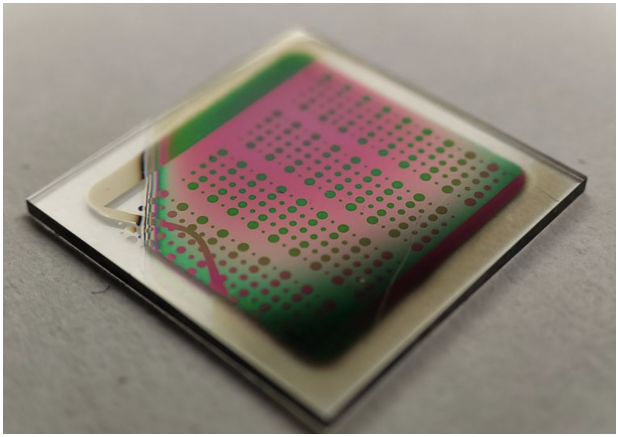
Im Fokus stehen dabei insbesondere primäre Rohstoffe, die eine hohe CO2-Last mit sich bringen, etwa Zement: Diese gilt es zu ersetzen, ohne die guten Dämmeigenschaften des Baumaterials negativ zu beeinflussen. Über computergestützte Modelle werden die Rezepturen für den klimafreundlichen Porenbeton systematisch optimiert. Auch verfügt das Fraunhofer IBP über die technische Ausstattung, um Porenbeton von der Rezepturerstellung bis hin zur Produktion im Pilotmaßstab weiterzuentwickeln.

1 Quelle: https://tinyurl.com/4erhac9f

www.tuwien.at

Sauerstoff-Ionen-Batterie für die Energiewende

Innovation von Forschern der Technischen Universität Wien kommt ohne seltene Elemente aus



Extrem langlebig, bauartbedingt vor Brand und Explosion geschützt und ohne den Einsatz von seltenen und damit teuren Materialien herstellbar, ist eine neuartige Batterie von Forschern der Technischen Universität Wien. Die Sauerstoff-Ionen-Batterie basiert auf Keramiken, die doppelt negativ geladene Sauerstoff-Ionen aufnehmen und abgeben können. Wird eine elektrische Spannung angelegt, wandern die Sauerstoff-Ionen von einem keramischen Material zum anderen, danach kann man sie wieder zurückwandern lassen und so elektrischen Strom abzapfen.

Von Brennstoffzellen zur Batterie

"Wir haben schon seit längerer Zeit viel Erfahrung mit keramischen Materialien gesammelt, die man für Brennstoffzellen verwenden kann. Das brachte uns auf die Idee zu untersuchen, ob solche Materialien vielleicht auch dafür geeignet sind, eine Batterie herzustellen", sagt Alexander Schmid vom Institut für Chemische Technologien und Analytik der TU Wien.

"Das Grundprinzip ähnelt stark dem der Lithium-Ionen-Batterie", ergänzt Jürgen Fleig, Professor für Technische Elektrochemie. "Aber unsere Materialien haben einige wichtige Vorteile." Brandunfälle, wie sie bei Lithium-Ionen-Batterien immer wieder vorkämen, seien ausgeschlossen, weil Keramik nicht brennt. Zudem komme man ohne seltene Elemente aus, die teuer sind oder nur auf umweltschädliche Weise gewonnen werden können.

Auch Lanthan soll ersetzt werden

"In diesem Punkt ist die Verwendung von keramischen Materialien ein großer Vorteil, weil sie sehr gut angepasst werden können. Man kann relativ problemlos Elemente, die nur schwer zu bekommen sind, durch andere ersetzen", so Tobias Huber, der zum Team gehört. Der Prototyp der Batterie verwendet noch Lanthan - ein zwar nicht seltenes, aber auch nicht alltägliches Element. Deshalb will das Team es ersetzen. Kobalt oder Nickel, die in vielen Batterien verwendet werden, sind bei der Sauerstoff-Ionen-Batterie überflüssig.

Der vielleicht wichtigste Vorteil der neuen Batterie ist ihre Langlebigkeit: "In vielen Batterien hat man das Problem, dass sich die Ladungsträger irgendwann nicht mehr bewegen können. Dann sinkt die Kapazität und letztlich wird der Stromspeicher unbrauchbar", meint Schmid. Die Sauerstoff-Ionen-Batterie lässt sich hingegen problemlos regenerieren: Wenn Sauerstoff durch Nebenreaktionen verloren geht, lässt sich der Schwund durch Sauerstoff aus der Umgebungsluft ausgleichen.
Für Smartphones und E-Autos ist das neue Batterie-Konzept nicht gedacht, denn die Sauerstoff-Ionen-Batterie erreicht gegenüber Lithium-Ionen-Batterien nur rund ein Drittel der Energiedichte. Außerdem liegt die Betriebstemperatur bei 200 bis 400 Grad Celsius. Höchst interessant aber ist die Technologie für die Energiewende. "Wenn man etwa einen großen Energiespeicher benötigt, um Solar- oder Windenergie zwischenzuspeichern, wäre die Sauerstoff-Ionen-Batterie eine hervorragende Lösung", glaubt Schmid.

ONVIF

25.000 konforme Produkte und 15-jähriges Jubiläum

ONVIF, die globale Standardisierungsinitiative für IP-basierte physische Sicherheitsprodukte, baut ihren Einfluss und ihre Wirkung auf den Markt für physische Sicherheit weiter aus und hat dabei zwei Meilensteine erreicht: Die Zahl der konformen Produkte hat die Marke von 25.000 überschritten, und ONVIF feiert sein 15-jähriges Bestehen als defacto-Branchenstandard für Interoperabilität. Seit der Gründung im Jahr 2008 ist die Zahl und der Umfang der Produkte, die mit den ONVIF-Profilen konform sind, stetig gewachsen. Angefangen hat es mit Kernprodukten wie IP-Kameras, Videomanagementsoftware und Netzwerk-Videoaufzeichnungslösungen. Die heutige Datenbank konformer Produkte umfasst nun auch Gegensprechanlagen, Kameras zur Nummernschilderkennung, Drohnen und Dienste wie Videoüberwachung als Service (VSaaS), was sowohl den wachsenden Wert von Video als auch die Vorteile der Nutzung von Cloud-Lö- sungen widerspiegelt. Die Liste der konformen Produkte ist nur auf onvif.org verfügbar. "ONVIF hat in den ersten 15 Jahren seines Bestehens eine Menge erreicht, aber unsere Arbeit ist noch lange nicht getan", sagte Leo Levit, Vorsitzender des ONVIF-Lenkungsausschusses. "Da die Branche weiterhin Videoanalyse, künstliche Intelligenz, Cloud und IoT einführt, wird die Rolle von ONVIF als Anbieter von standardisierten Schnittstellen in diesen Bereichen nur noch wichtiger werden." Zur Unterstützung der Branche in diesen Schlüsselbereichen der Videoanalyse und der Integration mit IoT— Systemen wurde die Spezifikation ONVIF Profile M entwickelt, die die Handhabung von Metadaten und Analyseereignissen standardisiert. Mit Hilfe des Profils können Systemintegratoren und Endanwender den Austausch von Metadaten zwischen Systemkomponenten verschiedener Hersteller, wie Kameras, Videomanagementsystemen und anderen Softwareplattformen, einfacher verwal- ten. Profil M bietet außerdem Kompatibilität mit IoT-Systemen durch die Unterstützung von JSON-formatierten Ereignissen über MQTT, ein gängiges Protokoll für IoT-Anwendungen. Insgesamt bietet ONVIF sieben Profile an, darunter das Profil S für Videostreaming, das Profil G für Videoaufzeichnung und -speicherung, das Profil C für physische Zugangskontrolle, das Profil A für eine breitere Konfiguration der Zugangskontrolle, das Profil T für erweitertes Videostreaming und das Profil D für Peripheriegeräte für die Zugangskontrolle. Produkte, die diesen Profilen entsprechen, werden nur von ONVIF-Mitgliedsunternehmen herge-stellt und müssen mindestens ein ONVIF-Profil unterstützen, können aber für zusätzliche Funktionen auch mehrere Profile unterstützen. Die Produkte müssen in der ONVIF-Liste der konformen Produkte registriert sein, um als konform zu gelten. **[www.onvif.org]**

Bitkom

Bund gibt Startschuss für europäisches Cloud-Projekt

Das Bundeswirtschaftsministerium den Förderstart für ein erstes Teil-Projekt des EU-Programms „IPCEI-CIS" angekündigt, mit dem Cloud- und Edge-Computing-Kapazitäten in der EU gestärkt werden sollen. Dazu erklärt Bitkom-Präsident Achim Berg: „Cloud- und Edge-Computing sind die Basis für Zukunftstechnologien wie Big Data und Künstliche Intelligenz. Der heutige Förderstart beim europäischen Gemeinschaftsprojekt IPCEI-CIS ist ein wichtiger industriepolitischer Impuls und markiert den Übergang von der Diskussion zum konkreten Handeln. Jetzt müssen aber zügig alle weiteren Teilprojekte in die Umsetzung kommen. Entscheidend ist, dass es uns gelingt, die dezentral und regional verteilten Anbieter von Cloud- und Edge-Lösungen in Europa besser zu vernetzen und offene und inklusive Standards voranzubringen. Für viele Anwendungen ist eine dezentrale Datenverarbeitung vorteilhaft oder unab- dingbar, etwa beim autonomen Fahren, bei der Datenanalyse in der Produktion oder der Dezentralisierung des Energiesystems. Die großen internationalen Cloud-Anbieter haben das dafür notwendige Edge Computing längst als wichtiges Zukunftsfeld ausgemacht und entsprechende Angebote entwickelt. Eine gemeinsame Antwort aller EU-Mitgliedstaaten über Landes- und Unternehmensgrenzen hinweg ist deshalb auch ein entscheidender Beitrag zu einer stärkeren europäischen digitalen Souveränität. Die deutsche und europäische Wirtschaft und insbesondere die Industrie benötigen hochperformante, sichere und vertrauenswürdige Technologien und Angebote im Bereich Cloud, Edge und Daten. IPCEI-CIS, aber auch Gaia-X und damit zusammenhängende Projekte leisten hier einen strategisch wichtigen Beitrag."

Qognify VMS

IP-Kameraserie von Pelco wird unterstützt

Qognify, ein Anbieter von Video- und Incident-Management-Lösungen für Unternehmen, hat heute eine bedeutende Erweiterung des Portfolios an Geräten bekannt gegeben, die von seiner Video-Management-Software Qognify VMS unterstützt werden. Die neueste IP-Kameraserie von Pelco, einem weltweit führenden Unternehmen im Bereich Design, Entwicklung und Herstellung von Videoüberwachungskameras, intelligenter Analytik und darauf abgestimmter Dienstleistungen, kann mit der fortschrittlichen Videolösung von Qognify für Firmen- und Unternehmensprojekte verwendet werden. Damit erhöht sich die Gesamtzahl der in Qognify VMS unterstützten Kameramodelle und Geräte von Drittanbietern auf mehr als 6.500.

Ermöglicht wird dies durch den revolutionären Smart Driver-Ansatz von Qognify, der auch einen Treiber für das ONVIF-Profil S/G/T enthält. Die einzigartige Architektur ermöglicht die Nutzung neuer Kameramodelle, ohne dass zusätzliche Treiberpakete heruntergeladen und installiert werden müssen. Dadurch erhalten die Kunden die Flexibilität, die neuesten Kameramodelle und -funktionen sofort zu nutzen, ohne Zeit und Geld darauf zu verwenden, dass der VMS-Hersteller aktualisierte Kameratreiber zur Verfügung stellt.

Philipp Kraft, Product Manager Cameras & Devices bei Qognify, erklärt: "Als herstellerunabhängiger Softwareanbieter wollen wir unseren Kunden und Partnern die Freiheit geben, das ideale Kamera-Portfolio für die spezifischen Anforderungen ihrer Videosicherheitsprojekte zu definieren. Pelco-Kameras genießen das Vertrauen von Kunden auf der ganzen Welt, und wir freuen uns, dass wir sie in die Reihe der von Qognify VMS unterstützten Geräte aufnehmen können. Da Pelco auf den ONVIF-Standard für die Integration von Drittanbietern setzt. Neben grundlegenden Videofunktionen wie der Übertragung von Videoströmen in H.264 und H.265 werden in Qognify VMS auch viele fortschrittliche Funktionen wie I/Os, kamerabasierte Bewegungserkennung und Videoanalyse oder Edge-basierte Aufzeichnung unterstützt, so dass Kunden das volle Potenzial ihrer Hardware-Investitionen ausschöpfen können."

Die Integration umfasst Pelcos Sarix Value, Sarix Pro 4 und Esprit Enhanced Series, weitere Kameras werden in den nächsten Monaten folgen. Der detaillierte Integrationsstatus der einzelnen Kameramodelle kann im Abschnitt "Unterstützte Geräte" auf der Qognify-Website eingesehen werden.

Hamish Dobson, Corporate Vice President, Enterprise Physical Security, Motorola Solutions, ist begeistert von der Zusammenarbeit: "Durch diese gemeinsame Initiative haben Qognify VMS-Kunden nun die Möglichkeit, ihre Projekte mit unseren erstklassigen Pelco-Kameras mit integrierter intelligenter Analytik zu planen und umzusetzen. Die Sarix- und Esprit-Kameras bieten eine breite Palette von Optionen, um die Anforderungen der Benutzer zu erfüllen, einschließlich einer verbesserten Bildqualität und robuster Designs, die für die rauesten Umgebungen ausgelegt sind.

IPS

Neue Software-Version des IPS VideoManagers

Videosicherheit ist intelligente Videoüberwachung mit IPS-Faktor

Der Sicherheitsexperte Securiton Deutschland bringt Version 14 seines IPS VideoManagers auf den Markt und unterstreicht damit einmal mehr die einzigartige Verschmelzung von Videomanagement und Videoanalyse aus einem Guss. Sowohl der IPS NextGen Client als auch die IPS NextGen VideoAnalytics sind mit neuen Funktionen ausgestattet, die für noch mehr Effizienz und leichtere Bedienung sorgen.

IPS NextGen Client mit ausgeklügelten Funktionen

Mit der neuen Exportfunktionalität auf der Recherche-Seite im IPS NextGen Client ist der Software-Entwicklung in München ein wahres Meisterstück gelungen: Der User kann direkt eine große Anzahl von ausgewählten Aufnahmen gesammelt exportieren. Vorbei die Zeiten, in denen jede Sequenz einzeln ausgewählt und exportiert werden musste. Der Zeitbereich zur Auswahl der betreffenden Sequenzen ist einfach und nutzerfreundlich einstellbar. Ein Export erfolgt als Archivdatei mit Passwortfunktion. Die Funktion eignet sich dazu, aufgenommenes Beweismaterial etwa der Polizei zu übergeben und die Strafverfolgung zu unterstützen. Das Material lässt sich je nach Berechtigung so maskieren, dass Zonen oder Objekte unkenntlich sind und der Datenschutz eingehalten werden kann.

Auch in den kleinen Alarmkarten der Übersichtsliste, die Alarmsituationen als Vorschaubild zeigen, ist der Schutz der Privatsphäre durch Maskierung gewährleistet. Bei der Verschleierung von Objekten und statischen Zonen hat sich ebenfalls einiges getan: Mit den entsprechenden Rechten lässt sich eine Maskierung auch wieder abschalten und alle Objekte und Zonen sind erkennbar – eine große Hilfe für Sicherheitsverantwortliche, Betriebsrat oder Polizei bei der Aufklärung.

Vereinfacht wurde auch die Systemkonfiguration: Mithilfe des neuen separaten Konfigurators, der als eigene Applikation verfügbar ist, lassen sich sowohl die System- als auch die Analysekonfiguration unabhängig vom IPS NextGen Client durchführen. Ein wahrer Gewinn für die nutzeroptimierte Anwendung des Videosicherheitssystems, da Client und Konfigurator gleichzeitig zur Verfügung stehen.

IPS NextGen VideoAnalytics für höchste Detektionsgenauigkeit

Auch bei den IPS NextGen VideoAnalytics gibt es Erweiterungen für noch mehr Videointelligenz. Die Anzahl der Regeln für eine individuelle Einrichtung der Videoanalyse erhöht sich von drei auf fünf. Das schafft mehr Flexibilität und die Anzahl möglicher Szenarien steigt. Zudem verbessert die Software-Entwicklung der Technologiemarke IPS die Detektionsqualität für kleine Objekte im hinteren Bildbereich: Die Analyse erfasst diesen Bereich präzise, mögliche Unregelmäßigkeiten und Gefahren werden im gesamten Videobild effektiv detektiert.

Weiterentwickelt wurde auch die Funktion „Loitering Detection", also das Detektieren von herumlungernden Personen. Bislang wird ein Alarm ausgelöst, wenn sich jemand zu lange in einer vordefinierten Zone aufhält.

In der neuen Version sendet die Analyse alternativ einen Alarm, wenn eine Person besonders lange an einer Stelle innerhalb einer Zone verweilt, zum Beispiel sich verdächtig lange am Zaun eines Fabrikgeländes aufhält und die maximal eingestellte Verweildauer überschrei- tet.

Die automatische Nummernschilderkennung mit dem IPS VideoManager verfügt jetzt über eine Erweiterung für die Kameramodelle des Herstellers Axis. So können beliebig viele Black- und White-Lists verwendet werden und der Operator kann auf nicht berechtigte Fahrzeuge spezifisch reagieren.
Auf die jeweiligen Kundenbedürfnisse angepasst, lassen sich im Ereignisfall zudem Alarmbilder darstellen, aufschalten und Verknüpfungen zu weiteren Workflows vornehmen.

Ausgewählte Kameras werden den verschiedenen Listen zugeordnet und abhängig davon Aktionen ausgelöst – beispielsweise bei der Zufahrtsberechtigung für Parkplätze durch das Steuern von Schranken und Toren.

Siedle Access Professional 7.0 bietet umfassende Concierge-Videofunktionen und bindet externe IP-Kameras ein. Beispielsweise kann die Concierge das Videobild der IP-Kamera im Empfangsbereich direkt an interne Teilnehmer weiterleiten. ©Siedle

SIEDLE ACCESS PROFESSIONAL 7.0

Komplettes Videoprogramm für die IP-Türkommunikation

Siedle optimiert sein IP-System Access Professional mit Fokus auf Video-Features. Das neue Major Release 7.0 bietet umfassende Concierge-Videofunktionen und bindet externe IP-Kameras ein. Außerdem vereinfacht ein neues Lizenzmodell die Integration zusätzlicher Systemfunktionen. Für Anwender wird das leistungsfähige System dadurch so flexibel wie nie zuvor.

Access Professional 7.0 bietet wesentliche Video-Features für mehr Sicherheit und Komfort in Wohnanlagen mit Concierge, in Industrie- und Gewerbekomplexen mit Pförtner sowie in Gebäuden mit sensiblen Bereichen, die videoüberwacht werden.

Concierge-Kamera

Die neue Funktion der Concierge-Kamera leitet das Videobild einer IP-Kamera im Empfangsbereich an interne Teilnehmer weiter.
Auf diese Weise können Bewohner ihre Besucher in Augenschein nehmen, bevor sie entscheiden, wen sie empfangen möchten.

Türvideo-Weiterleitung

Ebenfalls neu ist die Türvideo-Weiterleitung. Diese Funktion überträgt das Kamerabild einer Video-Türstation zu einem internen Teilnehmer, sobald der

Concierge diesen anruft. Der Bewohner spricht zunächst mit dem Concierge und sieht gleichzeitig bereits den Besucher vor der Sprechanlage. Wenn gewünscht, kann der Concierge die direkte Sprechverbindung herstellen. Die neuen Video-Features lassen sich auch kombinieren. Der Concierge steuert dann die Bildübertragung abhängig vom konkreten Auftenthaltsort eines Besuchers.
Beide Funktionen stellen Erweiterungen der Access-Software Concierge (ASC 170) dar und sind kostenfrei ohne zusätzliche Nutzerlizenzen einsetzbar.

Einbindung externer IP-Kameras

Mit dem neuen Release können neben der Concierge-Kamera auch IP-Kameras zur Überwachung sensibler oder sicherheitsrelevanter Bereiche eingesetzt werden, zum Beispiel in Tiefgaragen. Pro Siedle-Access-Server können bis zu zehn IP-Kameras mit Videostreams genutzt werden. Zur Überwachung lassen sich gezielt Streams auswählen, entweder im Live-Modus mit bis zu vier Streams auf einem Bildschirm gleichzeitig oder als Kamera-Scan mit automatisch wechselnder Bildfolge.

Neues Lizenzmodell

Als offenes IP-System ist Siedle Access Professional für praktisch alle denkbaren Einsatzzwecke konfigurierbar. Das Release 7.0 bietet auch ein neues Lizenzmodell: Damit lassen sich Systemfunktionen, die nicht zum Standardumfang von Access Professional zählen, so einfach und schnell wie nie zuvor ergänzen. Mit dem Erwerb von Anwendungslizenzen im Webshop können gewünschte Funktionsmodule sofort heruntergeladen und freigeschaltet werden, beispielsweise Rufspeicher, Aufzugsteuerung oder kundenspezifische Funktionen in Verbindung mit dem Access-Service-Center des Herstellers.
Upgrade für Access Professional 7.0
Die Upgrade-Lizenz für Version 7.0 ist kostenfrei erhältlich für alle Access-Professional-Systeme mit Siedle-Wartungsvertrag und für Systeme, deren Installation weniger als 12 Monate zurückliegt. Ältere Systeme lassen sich mit einem kostenpflichtigen Upgrade auf den neuesten Stand bringen. Siedle Access Professional 7.0 ist ab sofort verfügbar.

[www.siedle.de/access]

Komplettes Videoprogramm für die IP-Türkommunikation: Sie sind mit der Rezeption verbunden, zusätzlich gehen die Video-, Sprech- und Rufsignale über das Telefonnetz an zwei ISDN-Telefone in anderen Gebäudeteilen. Insgesamt acht Außenanlagen überwachen die Zufahrten und Eingänge. Bei der Gebäudekommunikation erfüllte Siedle Steel die hohen Ansprüche an edles Material, erstklassige Qualität, perfekte Funktion und elegantes Design. @Siedle

DOMERA Version E

Günstige Einstiegskameras in bewährter Dallmeier Qualität

Dallmeier, deutscher Hersteller von Videosicherheitstechnik, hat die „E" Version der bestehenden DOMERA® Kamerafamilie vorgestellt. Die Kameras eignen sich besonders für Projekte, bei denen eine hohe Bild- qualität zu einem niedrigen Preis im Vordergrund steht, aber z. B. bei der Videoanalyse keine KI-Unterstützung erforderlich ist.

Viel Bild für wenig Geld

Die im Jahr 2022 vorgestellten, modularen Kameras der Dallmeier „DOMERA"- Serie sind ab sofort auch als sogenannte „E–Version" erhältlich. Die beiden Kameras RDF5120DN (E) und RDF5140DN (E) bieten gewohnt hohe Bildqualität mit einer Auflösung von 2 MP bzw. 5 MP und damit auch in schwach beleuchteten Umgebungen detailreiche Aufnahmen. Die WDR-Funktion (Wide Dynamic Range) sorgt für eine optimale Aufnahme von Szenen mit sehr hellen und dunklen Bereichen. Darüber hinaus ermöglicht die optional integrierte, adaptive 180-Grad-IR-Beleuchtung der Kamera auch in völliger Dunkelheit klare Schwarz-Weiß-Bilder mit ausgezeichnetem Kontrast.

Die Anwender profitieren von den zahlreichen Vorteilen der DOMERA®-

Familie: Durch das modulare System mit verschiedenen Montagemöglichkeiten können Channel Partner und Errichter nicht nur Einsatzszenarien von Dome-Kameras abdecken, sondern auch Outdoor-, Box- und Bulletkameras ersetzen. Die Vorteile sind vielfältig, wie z. B. ein deutlich besserer Schutz vor Spinnen und eine bessere Belichtung durch die kameraeigene IR-Beleuchtung. Errichter und Channel Partner freuen sich zudem über den Dallmeier RPod (Remote Positioning Dome), mit dem sie das Objektiv aus der Ferne in drei Achsen justieren können. Damit können Techniker die Kamera unkompliziert installieren und die aufgenommene Szene schnell und einfach von überall aus anpassen, wenn sich die Anforderungen oder Kundenvorstellungen ändern. Das zeitaufwändige Feinjustieren des Objektivs auf der Leiter oder Hebebühne gehört damit der Vergangenheit an. Darüber hinaus unterstützen die Kameras die Videokompression H.264/H.265 und lassen sich dank der Unterstützung von ONVIF Profile S in zahlreiche Videomanagementsysteme (VMS) integrieren.

Kameras „Made in Germany" kurzfristig verfügbar

„Wir hören regelmäßig, dass unsere Kunden und Partner die Produkte von Dallmeier sehr schätzen. Leider gibt es im Markt aber auch die Wahrnehmung, dass Dallmeier vor allem im ‚Premiumsegment' der B2B-Videosicherheit positioniert sei, mit Produkten, die Features und Funktionalitäten bieten, die für bestimmte Anwendungen vielleicht gar nicht benötigt werden," so Thomas Dallmeier, CEO, Dallmeier electronic.

„Mit den Kameras der DOMERA® Version E bieten wir nun auch im Segment der B2B-Kameras mit einem Listenpreis von 600 bis 800 Euro Lösungen an, die zeigen, dass Qualität ‚Made in Germany' nicht immer teuer sein muss. Die Kameramodelle eignen sich hervorragend für Anwendungen, bei denen es in erster Linie auf ein erstklassiges Videobild ankommt, nicht aber auf Zusatzfunktionen wie KI-Analyse oder Audio."

Milestone

Fachkräftemangel an deutschen Flughäfen

In diesen Städten wird am dringendsten Personal im Sicherheitsbereich gesucht

An den Flughäfen in Deutschland herrscht ein großer Mangel an Fachkräften. Insbesondere Sicherheitspersonal wird nach der COVID-19-Pandemie dringend benötigt. Die Sicherheitskontrollen waren im Sommer 2022 oft unterbesetzt und überlastet. Das führte zu Chaos und dazu, dass viele Reisende ihre Flüge verpassten. Wenn modernste Videotechnologie verantwortungsvoll eingesetzt wird, kann das Sicherheitspersonal schnell und effektiv entlastet werden. Der Anbieter für Videomanagementsoftware Milestone Systems hat deshalb die zehn größten Flughäfen Deutschlands analysiert und herausgefunden, welche die meisten Stellenangebote im Bereich Sicherheit anbieten. Zusätzlich wurden entsprechende Gehälter und Arbeitsverhältnisse in die Recherche mit einbezogen. Der größte Fachkräftemangel herrscht in Frankfurt am Main und Berlin. Besonders viele Reisende mussten im vergangenen Jahr unter dem fehlenden Sicherheitspersonal leiden. Mit insgesamt 171 Stellenausschreibungen wird schnell deutlich, wie dringend die Suche nach qualifizierten Sicherheitskräften ist. Frankfurt am Main ist dabei Spitzenreiter. Der Flughafen in der hessischen Hauptstadt verzeichnete gleich 40 Ausschreibungen für Sicherheitsfachkräfte. Dicht dahinter folgt Berlin mit 33 unbesetzten Jobangeboten im Sicherheitsbereich. Unter den Top fünf reihen sich anschließend München mit 27, sowie Stuttgart und Köln mit jeweils 14 Stellenanzeigen ein.

Hannover Flughafen bezahlt am besten

Die am besten bezahlten Sicherheitsfachkräfte arbeiten in Hannover. Dort können Arbeitnehmende im Sicherheitsbereich bei einer 40-Stunden-Woche bis zu 3414 Euro brutto im Monat verdienen. Damit zahlt der niedersächsische Flughafen über 500 Euro mehr aus als der Durchschnittsverdienst aller untersuchten Flughäfen. Dieser liegt bei 2846 Euro. Hamburg und Düsseldorf reihen sich mit 3414 und 3261 Euro auf Platz zwei und drei ein. Die Stellenausschreibungen beziehen sich hierbei zu über 80 Prozent auf Vollzeitstellen und zu fünf Prozent auf Ausbildungsplätze. Jos Beernink, VP EMEA von Milestone Systems, kommentiert die Analyse: "Die Zahl der fehlenden Sicherheitskräfte ist erschreckend hoch. An kaum einem anderen Arbeitsplatz ist Sicherheit so wichtig, um etwaige Risiken so weit wie möglich zu minimieren. Dabei kann Videotechnologie zur Hilfe hinzugezogen werden, um vor allem Fachkräfte so schnell wie möglich entlasten zu können. Moderne Videosoftware kann dem Personal dabei helfen, alles zu überwachen und proaktive oder reaktive Maßnahmen schnell in die Wege zu leiten. Dies ermöglicht zum einen, Videomaterial zu filtern und zum anderen durch die Trackingfunktion einen einfacheren virtuellen Überblick zu behalten. Zusätzlich kann das Fachpersonal im Sicherheitsbereich durch Videotechnologien unterstützt und entlastet werden.

Lagebericht Security 2023

Cybersecurity-Vorfälle sorgen für mehr Datenschutzverletzungen und höhere Ausfallzeiten

Über die Hälfte der befragten Unternehmen erleiden Datenschutzverletzungen und sind monatlich von ungeplanten Ausfallzeiten betroffen

Splunk Inc., eines der führenden Unternehmen für Cybersicherheit und Observability, veröffentlichte in Zusammenarbeit mit der Enterprise Strategy Group den Lagebericht Security 2023, eine globale Studie, die jährlich die Sicherheitsprobleme moderner Unterneh- men untersucht. Für die diesjährige Studie wurden mehr als 1.500 Sicherheitsverantwortliche befragt. Es zeigt sich, dass die Zahl der Cyberangriffe und ungeplanter Ausfälle weiter zunimmt.

Über die Hälfte (52 %) der Unternehmen waren in den vergangenen zwei Jahren von einer Datenschutzverletzung betroffen (in 2022: 49 %; in 2021: 39 %). Darüber hinaus berichten 62 % der Befragten, dass ihre geschäftskritischen Anwendungen mindestens einmal im Monat aufgrund eines Cybersicherheitsvorfalls ungeplante Ausfallzeiten erleiden. Im Jahr 2022 sagten dies nur 54 % der Befragten.

Wichtige Erkenntnisse aus dem Bericht sind unter anderem:

- Böswillige Angreifer bleiben in Unternehmensnetzen über längere Zeiträume unbemerkt. Im Durchschnitt vergehen nach Angaben der Befragten über zwei Monate (2,24) zwischen dem Zugriff des Angreifers und dem Zeitpunkt, an dem die zuständigen Stellen davon erfahren.
- Die durchschnittliche Anzahl der Ausfälle, denen ein Unternehmen ausgesetzt ist, beträgt etwa 22 pro Jahr.
  Die Kosten für diese Ausfallzeiten verschlingen etwa 2,7 % des Jahresumsatzes. Laut dem aktuellen globalen Forschungsbericht von Splunk „Digitale Resilienz zahlt sich aus" können diese Ausfallzeiten Unternehmen rund 365.000 US-Dollar pro Stunde kosten.
- Sicherheitsvorfälle sind eine existenzielle Bedrohung. Mehr als ein Drittel (39 %) der Befragten gibt an, dass Sicherheitsvorfälle ihre Wettbewerbsposition direkt beeinträchtigen.
  Zudem geben 31 % an, dass Cybersecurity-Vorfälle den Unternehmenswert verringern.

Gerade da Unternehmen mit erheblichen Herausforderungen im Bereich der Cybersicherheit konfrontiert sind, ergreifen viele von ihnen bereits Maßnahmen, um diesen entgegenzuwirken:

- Die Sicherheitsteams wenden mehr Geld auf. 95 % der Befragten gehen davon aus, dass ihre Sicherheitsbudgets in den nächsten zwei Jahren steigen werden, wobei 56 % eine „erhebliche" Steigerung erwarten.
- Cybersicherheit ist ein Teamsport. 81 % der Unternehmen arbeiten daran, Aspekte ihres Sicherheits- und IT-Betriebs zusammenzuführen. Die Befragten sind der Ansicht, dass diese Zusammenführung dazu beiträgt, die Risiken in ihrer Umgebung besser sichtbar zu machen (58 %) und die Zusammenarbeit bei der Erkennung von Bedrohungen und deren Reaktion darauf zu verbessern (55 %).
- Unternehmen konzentrieren sich auf den Schutz ihrer Lieferkette. 95 % der Befragten geben an, dass

sie sich intensiver mit der Risikobewertungen von Dritten befassen.
- Daten sind die Antwort. 91 % der Befragten sind sich einig, dass eine bessere Erfassung und Analyse von Erkennungsdaten eines der wirksamsten Mittel zur Verhinderung erfolgreicher Ransomware-Angriffe sind.

„In den Unternehmen, mit denen wir zusammengearbeitet haben, war die Resilienz am stärksten, wenn ein kollaborativer Ansatz in allen Bereichen angewendet wurde: von der Softwareentwicklung über die Infrastrukturüberwachung bis hin zur Planung der Geschäftskontinuität", sagt Ryan Kovar, Distinguished Security Strategist bei Splunk und Leiter von SURGe, dem Cybersecurity-Research-Team von Splunk.

„Dieser Ansatz bezieht alle Beteiligten mit ein, einschließlich IT- und Sicherheitsverantwortliche sowie Geschäftsführung, damit sich alle auf den Schutz des Unternehmens konzentrieren können."

Weitere Erkenntnisse aus dem Lagebericht Security 2023 unter: https://tinyurl.com/y5p3d7f8

Methodik

Die Studie wurde weltweit von Mitte November 2022 bis Anfang Januar 2023 in Zusammenarbeit mit der Enterprise Strategy Group durchgeführt. Bei den 1.520 Befragten handelt es sich um IT- und Sicherheitsverantwortliche sowie Fachleute, die mehr als die Hälfte ihrer Zeit mit Sicherheitsfragen verbringen. Sie kommen aus zehn Ländern: Australien, Kanada, Frankreich, Deutschland, Indien, Japan, Neuseeland, Singapur, dem Vereinigten Königreich und den USA.

German Stevie Award 2023

Delinea Secret Server gewinnt German Stevie Award 2023

Höchst benutzerfreundliche PAM-Lösung mit herausragender Time-to-Value überzeugt Fachjury

Delinea, der Spezialist für erweiterte nahtlose Privileged-Access Management (PAM)-Lösungen, wurde bei den diesjährigen German Stevie Awards für seinen Secret Server mit einem Gold Stevie in der Kategorie „Business Technology Solution – Identity & Access-Sicherheitslösungen" ausgezeichnet. Mit Delinea Secret Server profitieren Unternehmen von einer sofort einsatzbereiten, benutzerfreundlichen und skalierbaren Enterprise-PAM-Lösung, die Security- und IT-Operations-Teams in die Lage versetzt, alle Arten von privilegierten Accounts automatisiert zu verwalten und abzusichern.

Laut dem IBM Cost of a Data Breach Report 2022 belaufen sich die durchschnittlichen Gesamtkosten einer Datenpanne auf 4,35 Millionen US-Dollar. Bedenkt man, dass 80 Prozent aller Cybervorfälle mittlerweile auf kompromittierte Zugangsdaten zurückzuführen sind, bedeutet jeder Tag, an dem Unternehmen keine angemessenes PAM-Lösung im Einsatz haben, ein enormes finanzielles Risiko.

Secret Server unterstützt IT-Abteilungen dabei, privilegierte Berechtigungen und Konten proaktiv vor Missbrauch durch Hacker und Insider-Angreifer zu schützen, indem er eine effiziente Administration aller privilegierten Zugriffe inkl. der Durchsetzung einer Zero-Trust-Strategie ermöglicht. Automatisierte Prozesse bei der Identifizierung von privilegierten Accounts und eine vollständige Transparenz aller Sitzungen entlasten die IT-Teams nachhaltig, was den Unternehmen wertvolle Zeit und Ressourcen einspart. Dabei bietet Secret Server die schnellste Time-to-Value aller führenden PAM-Produkte und ist zudem die skalierbarste Enterprise-Lösung mit den geringsten FTE- und Professional Services-Anforderungen. „Die Ausweitung privilegierter Zugriffskontrollen auf sämtliche Identitäten in der Unternehmenslandschaft war noch nie so wichtig wie heute", so Andreas Müller, Vice President Sales DACH von Delinea. „Aus diesem Grund arbeiten wir unermüdlich daran, unseren Kunden nahtlose PAM-Lösungen mit den fortschrittlichen Funktionen zur Verfügung zu stellen, die für die Absicherung moderner Infrastrukturen mit einer maximierten Anzahl menschlicher und maschineller Identitäten heute unerlässlich sind. Dass unser bewährter Secret Server nun mit einem Gold Stevie ausgezeichnet wurde, ehrt uns sehr."
Erst jüngst hat das Unternehmen mit der Delinea-Plattform eine neue Cloud-native Grundlage für seine branchenweit anerkannten PAM-Lösungen vorgestellt, die Unternehmen eine einzigartige End-to-End-Transparenz, dynamische Berechtigungskontrollen sowie adaptive Sicherheit ermöglicht. Secret Server Cloud ist dabei eines der ersten Delinea-Produkte, das die Plattform unterstützt.

In ihrer neunten Ausgabe nach dem erfolgreichen Debüt im Jahr 2015 haben die German Stevie Awards erneut herausragende Leistungen in der Arbeitswelt ausgezeichnet. Sie sind eines der acht Stevie® Awards Programme, die zu den international anerkanntesten Wirtschaftspreisprogrammen zählen. Über 400 Bewerbungen sind in diesem Jahr bei den German Stevie Awards in Kategorien wie beispielsweise „Unternehmen des Jahres", „Manager:in des Jahres" und „Bestes neues Produkt des Jahres" eingegangen und wurden von über 50 Führungskräften bewertet. Geehrt werden die Preisträgerinnen und Preisträger in diesem Jahr am 13. Oktober in Rom im Rahmen des Galabanketts der 20. International Business Awards.

Maggie Gallagher, Präsidentin der Stevie Awards, gratuliert allen Gewinnern der Goldenen, Silbernen und Bronzenen Trophäen zu ihren Erfolgen: „Wir freuen uns, dass wir im Rahmen der German Stevie® Awards auch in diesem Jahr wieder tolle und vor allem innovative Preisträgerinnen und Preisträger auszeichnen dürfen."

Fünf Tipps

So haben Hacker keine Chance

In Zeiten zunehmender Cyber-Krim nalität stellt sich zwingend die Frage, wie sich Unternehmen gegen Angriffe auf ihre IT-Landschaft schützen können. Denn gerade Ransomware-Attakken auf die SAP-Systeme und Betriebstechnologie (Operational Technology, OT) können verheerende Folgen haben. Legt ein Hacker das SAP-System lahm, dann steht mitunter die komplette Produktion still. Doch Fertigungslinien sind zumeist unverzichtbare Bestandteile komplexer Lieferketten. Sind diese gestört, kann das die Existenz der betroffenen Firmen gefährden. Bei Attacken auf kritische Infrastrukturen (KRITIS) – wie etwa Wasserleitungen von Energieversorgern – sind die Auswirkungen noch gravierender, da sie auch die Gesundheit von Menschen betreffen können. Die nachfolgenden 5 Tipps sollen Unternehmen dabei helfen, ihre SAP- und OT-Systeme besser vor Hackerangriffen zu schützen.

1 SAP- und OT-Sicherheit als Geschäftsprozess verstehen

Die meisten Unternehmen sind sich zwar der permanenten Gefahr von Angriffen bewusst und setzen auf die Expertise von Compliance Managern, Security-Experten und Hacker Nerds, um sich zu schützen. Das Problem ist jedoch: Die Experten beschäftigen sich auf einer eher theoretischen Ebene mit dem Thema und sie agieren losgelöst von anderen, relevanten Prozessen und Teams im Unternehmen.
Doch um das eigene Geschäft wirkungsvoll abzusichern, müssen Unternehmen SAP- und OT-Sicherheit als Geschäftsprozess verstehen, der alle relevanten Personengruppen im Unternehmen einbezieht.

Nur so lassen sich Strategien entwickeln und daraus geeignete praktische Maßnahmen ableiten – wie etwa die passende Security-Technologie einzusetzen.

Wird Cyber Security als kritischer Geschäftsprozess verstanden, dann ist dieser Ablauf mit Bedacht zu modellieren, mit Metriken zu steuern, mit Tools zu überwachen und kontinuierlich zu optimieren.

2 Dialog zwischen Management, IT und Produktion

iOT- und SAP-Sicherheit prozessorientiert zu verstehen bedeutet auch, dass alle relevanten Teams in einen Dialog treten. Das gilt vor allem für Management, IT und Produktion. Denn manchmal fehlt dem Management die genaue Vorstellung davon, wie wichtig SAP- und OT-Sicherheit für einen reibungslosen Geschäftsbetrieb sind. Die IT-Abteilung kann dabei helfen, dieses Verständnis zu vermitteln. In den Dialog einbezogen sein sollten unbedingt auch die Blue Collar Wor-

ker, die Mitarbeitenden in der Produktion. Denn diese wissen ganz genau, wie sich ein möglicher Stillstand von Maschine A auf Fertigungslinie B auswirkt.

3 Systemübergreifende Detection anstatt Netzwerkanalyse

Neben einem prozessualen Verständnis des Themas OT- und SAP-Sicherheit sowie einem fachbereichsübergreifenden Dialog braucht es leistungsstarke Security-Lösungen.
Dazu zählt auch die zeitgemäße, systemübergreifende Detec- tion, die sich aus der älteren Netzwerkanalyse weiterentwickelt hat. Um sensorische Daten aus unterschiedlichen Quellen zu verarbeiten, haben sich mit Endpoint Detection and Response (EDR) und Extended Detection and Response (XDR) zwei neue Methoden etabliert.
Mit einem EDR-Tool lassen sich Ereignisse, wie etwa eine Nutzeranmeldung, das Öffnen einer Datei und aufgebaute Netzwerkverbindungen, auf Endgeräten wie PCs, Notebooks, Tablets und Smartphones aufzeichnen. Darüber hinaus erlaubt XDR, Daten über mehrere Angriffsvektoren hinweg, wie etwa E-Mails, Identitäten, Geräte, Server, Cloud-Workloads und Netzwerke, automatisch zu erfassen und zu verknüpfen.

4 Auf Plattform-Lösungen von Hyperscalern setzen

Eine weitere Säule zeitgemäßer Security-Lösungen ist die Plattform-Sicherheit. Als Plattformen haben sich die Lösungen der etablierten Hyperscaler bewährt. Insbesondere Microsoft bietet eine vollumfängliche Security-Produktpalette mit einer Vielzahl an vorgefertigten Komponenten, die sich einfach in Betrieb nehmen und für individuelle Unternehmenszwecke bedarfsgerecht konfigurieren lassen: vom Schutz der Anwender (PCs, Identitäten und E-Mails) über die Absicherung verschiedener Betriebsszenarien (eigene Server, On-Premises im Rechenzentrum sowie Azure-, Google oder AWS-Cloud) bis hin zu speziellen Anwendungsfällen wie OT- und SAP-Sicherheit. Hinzu kommt: Solche Plattformen sind sehr viel effizienter zu integrieren als Einzellösungen.

5 Daten in zentralem System bereitstellen

Unternehmen haben also keine andere Wahl, als die Sensorik systemübergreifend zu verknüpfen und Alerts rund um die Uhr zu überwachen. Alternativ können sie die Managed Detection & Response Services eines spezialisierten Cyber Security Defense Centers (CSDC) beziehen.
Im Zentrum steht das Microsoft Threat Monitoring for SAP. Über einen Sensor lassen sich Daten aus komplexen SAP-Landschaften konsolidieren, sodass sie im cloudnativen SIEM-System Microsoft Sentinel für die weitere Verarbeitung bereitstehen.

Nachdem der Sensor mit verschiedenen SAP-Log-Quellen verbunden ist, erfasst er alle Daten, die über eine API zwecks Korrelation und Auswertung in Sentinel fließen. Erkennt das Tool eine Bedrohung, generiert es entsprechende Alerts. Dabei bilden standardisierte Regeln die Grundlage für (teil-)automatisierte SOAR-Prozesse (Security Orchestration, Automation and Response): Geht ein Alarm ein, erfolgt eine KI-basierte Analyse der erfassten Ereignisdaten. Je nach Art des Angriffs setzen sich dann vorab definierte Response-Maßnahmen in Gang.

Fazit

Cyber Crime ist ein lukratives Business, das nicht nur Auswirkungen auf die wirtschaftliche Situation von Unternehmen haben kann, sondern auch eine Gefährdung für kritische Infrastrukturen des öffentlichen Lebens darstellt.

Um Hackern keine Chance zu geben, müssen Unternehmen besser gewappnet sein. Das kann nur gelingen, wenn sie IT-Sicherheit als Geschäftsprozess verstehen und nicht als ein vom Business losgelöstes Thema. Vielmehr gilt es, den praktischen Bezug ihrer IT sowie OT zu verinnerlichen, daraus konkrete Schutzziele abzuleiten und Maßnahmen zu ergreifen wie etwa eine zeitgemäße, leistungsfähige Security- Lösung zu implementieren.

Falls Sie mehr Informationen rund um das Thema Cyber Security benötigen, dann können Sie sich auch das Whitepaper „Cyber Security – die digitale Transformation sicher gestalten" herunterladen.

Autor: Andreas Nolte, Head of Cyber Security bei Arvato Systems

Fraunhofer AISEC

Krypto-Protokoll für quantensicheren Pass

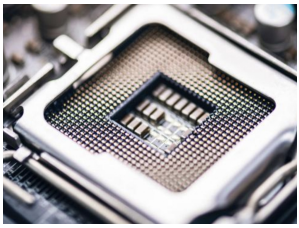
Quantensicherer Chip für Ausweis-Dokumente: Das Fraunhofer AISEC hat die dafür notwendigen Krypto-Protokolle entwickelt.

Der Sicherheitschip auf unseren Personalausweisen und Reisepässen ist durch Quantencomputer bedroht. Das Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC hat im Forschungsprojekt PoQuID jetzt Krypto-Protokolle entwickelt, die auch Angriffen durch Quantencomputer standhalten. Partner waren dabei Infineon und die Bundesdruckerei.

Seit 2005 sichert ein elektronischer Chip die deutschen EU-Reisepässe und seit 2010 die deutschen Personalausweise, mit denen sich Bürgerinnen und Bürger auch online authentisieren können (die Online-Ausweisfunktion). Im Chip sind die personenbezogenen Daten und biometrische Merkmale wie das Passbild und zwei Fingerabdrücke gespeichert. Der Chip ist zudem mit einem Echtheitsnachweis versehen. Angriffen durch ausreichend leistungsstarke Quantencomputer, die in den kommenden zehn bis 15 Jahren erwartet werden, hält die dort eingesetzte Kryptografie jedoch nicht stand: Es wird davon ausgegangen, dass diese die dahinterliegenden mathematischen Problemstellungen in viel kürzerer Zeit lösen können als heutige Computer. Der Chip könnte dann als Sicherheitsmerkmal nicht weiter genutzt werden.

Zwei Sekunden für den Sicherheitscheck

Das Fraunhofer AISEC hat den Chip im Forschungsprojekt PoQuID deshalb quantensicher gemacht. Partner des, vom Bundesministerium für Wirtschaft und Klimaschutz BMWK geförderten, Projekts waren Infineon



und die Bundesdruckerei. »Wir haben das für Reisepässe geltende kryptografische Standard-Protokoll ›Extended Access Control (EAC)‹ so angepasst und weiterentwickelt, dass es quantenresistent ist und auch mit den beschränkten Ressourcen des Sicherheitschips performant läuft«, sagt Prof. Dr. Marian Margraf, Abteilungsleiter »Secure Systems Engineering« am Fraunhofer AISEC in Berlin und Leiter des Forschungsprojekts. »Wir haben in unseren Forschungsarbeiten nachgewiesen, dass das neue Protokoll dieselben Sicherheitsfunktionen umsetzt wie das Bisherige. Es benötigt für die Berechnung lediglich zwei Sekunden, um das Sicherheitsmerkmal zu überprüfen und ist damit sowohl für die Grenzkontrolle von elektronischen Pässen geeignet als auch als Online-Ausweisfunktion.«

Zwei PQC-Standards der NIST miteinander kombiniert

Das Fraunhofer AISEC hat dafür zwei Krypto-Verfahren aus dem Standardisierungsprozess des National Institute of Standards and Technology (NIST) für Post-Quanten-Kryptografie miteinander kombiniert: Kyber und Dilithium. »Die NIST standardisiert ›kryptografische Primitive‹. Das sind Bausteine, die man zum Aufbau von kryptografischen Protokollen nutzen kann«, schildert Margraf. Dilithium ist ein asymmetrisches Verfahren*, das für elektronische Signaturen verwendet werden kann. Bei Kyber handelt es sich um ein asymmetrisches Verfahren zum Austausch kryptografischer Schlüssel.

»Das Forschungsprojekt hat die Grundlagen geschaffen, die Sicherheit elektronischer Ausweis-Dokumente fit fürs QC-Zeitalter zu machen. Bei der Markteinführung muss es jetzt schnell gehen«, sagt Margraf. Der Forscher rechnet mit einem internationalen Standardisierungsprozess von mindestens fünf Jahren. »Für Ausweis-Dokumente zuständige Behörden bzw. die Hersteller der Sicherheitschips müssen außerdem berücksichtigen, dass Ausweis-Dokumente bis zu zehn Jahre gültig sein können und erste, leistungsfähige Quantencomputer bereits für Anfang der 2030er Jahre prognostiziert sind.«

*Die asymmetrische Verschlüsselung verwendet zwei Schlüssel, einen zum Verschlüsseln und einen zum Entschlüsseln. Symmetrische Verfahren verwenden nur einen Schlüssel.

Klüh

Facility-Services-Anbieter: Geschäftsbericht 2022

Klüh mit 923 Mio. Euro Gesamtumsatz auf Wachstumskurs

Es ist der höchste Umsatz in der über 111-jährigen Unternehmensgeschichte, den die Klüh Service Management GmbH in ihrem Geschäftsbericht für das Jahr 2022 veröffentlicht hat: 923 Mio. Euro.

Damit hat die internationale Klüh-Gruppe ihren Umsatz um 13,4 % im Vergleich zum Vorjahr gesteigert. Zu diesem Wachstum trugen im Wesentlichen die Fachbereiche Cleaning (plus 44,8 Mio. Euro), Catering (plus 24 Mio. Euro) und Clinic Service (plus 22 Mio. Euro) bei.

Aber auch der Fachbereich Security verzeichnete mit über 6 Mio. Euro Umsatzplus ein gutes Ergebnis, das einem Zuwachs von 3,7 % im Vergleich zu 2021 entspricht.

Smart und nachhaltig zum Erfolg

Frank Theobald, Sprecher der Geschäftsführung: „Es ist uns 2022 gelungen, unsere Top-Performance als Anbieter für Qualitätsdienstleistungen im Bereich infrastrukturelle Dienstleistungen weiter auszubauen. Dafür haben wir die transformative Kraft von Digitalisierung und Nachhaltigkeit im Zusammenspiel genutzt.

Als agiles Unternehmen haben wir zudem bewiesen, dass wir mit Veränderungen Schritt halten und Innovationen vorantreiben." Innovative Entwicklungen ziehen sich durch alle

©Klüh Service Management GmbH

Fachbereiche von Klüh, dabei fördert eine neue Business-Development-Strategie die Klüh-Innovationskultur. Erklärtes Ziel ist es, neue Geschäftsmodelle zu projektieren und bei Kunden zu pilotieren sowie die bestehende Dienstleistungspalette zu erweitern.

Des Weiteren hat sich das Unternehmen auf einen strukturierten Nachhaltigkeitspfad begeben. „Wir haben eine neue Einheit gegründet, die dafür sorgt, dass unsere Nachhaltigkeitsstrategie umgesetzt wird", sagt Holding-Geschäftsführer Christian Frank.

„Dazu gehören Kompetenzteams aus Cleaning, Catering, Security, Einkauf, Verwaltung und Marketing sowie die Abteilung Qualitätsmanagement." Der Klüh-Nachhaltigkeitspfad wird gesäumt von einem unternehmensweit implementierten Sustainability Management in Form von Leitlinien, nachhaltiger Unternehmensführung sowie konkreten Zielen und Maßnahmen.

Erfolgreiche Klüh-Auslandsgesellschaften

Mit über 235 Mio. Euro betrug der Anteil des Auslandsgeschäftes 25,5 % vom Gesamtumsatz der Klüh-Gruppe und konnte im Vergleich zu 2021 von 194 Mio. Euro um 21,3 % gesteigert werden. In den Bereichen Personaldienstleistungen, Security, Hygieneservices und Infrastrukturdienstleistungen lassen sich Umsatzsteigerungen auf höhere Service Level Agreements zurückführen.

Geschäftsjahr 2022 von Klüh unter https://tinyurl.com/3wpr74f4

v.l.n.r.: Thorsten Braun, Director Global Operations Scheidt & Bachmann Parking Solutions GmbH, Martin Kammler, Managing Director Scheidt & Bachmann Parking Solutions GmbH Thomas Herling, Lead Global Business Owner ecosystems dormakaba, Juan Andres Arias Maestro, Senior Vice President Global Access Control Solutions dormakaba

dormakaba/Scheidt & Bachmann

Kooperation im Bereich Parkraum- und Gebäudezutrittsmanagement

dormakaba gibt den Abschluss einer Kooperation mit Scheidt & Bachmann bekannt. Scheidt & Bachmann ist ein weltweiter Anbieter von Systemlösungen für intelligente Mobilität und mit seinem Geschäftsbereich Parking Solutions führend bei zukunftsweisenden Parkraummanagement-Lösungen. Im Rahmen der vereinbarten Kooperation werden dormakaba und Scheidt & Bachmann eine Komplettlösung für Parkraum- und Gebäudezutrittsmanagement entwickeln.
Die Zusammenarbeit sieht die Integration der Scheidt & Bachmann Zufahrtslösung „parkoneer" in die dormakaba Zutrittssysteme „exos" und „MATRIX" vor. Die Kooperation ist seit dem 6. März 2023 offiziell in Kraft.

Die moderne Arbeitswelt benötigt zunehmend flexible Arbeitsplätze, damit einher geht ein unstetiges Mobilitätsverhalten und das Bestreben nach Selbstorganisation der Mitarbeitenden. Diese gesellschaftlichen Veränderungen berücksichtigen dormakaba und Scheidt & Bachmann mit einer integrierten Lösung von Access-Systemen, die Mitarbeitenden den nahtlosen Zutritt vom Parkplatz bis zum jeweiligen Arbeitsplatz ermöglicht. „Gebäude und deren Peripherie wie Parkplätze werden bislang noch häufig getrennt voneinander betrachtet und bewirtschaftet. Dies wird aber der neuen Arbeitswelt nicht gerecht", sagt Thomas Herling, Lead Global Business Owner Ecosystem bei dormakaba.

Als führende Unternehmen für Zutrittssysteme bzw. Parkraummanagementsysteme sind dormakaba und Scheidt & Bachmann bestrebt, durch die Vernetzung ihrer vorhandenen Technologien diese Trennung aufzuheben und durch einen ganzheitlichen Ansatz Mehrwert für die dynamische Nutzung von Smart Buildings zu schaffen. Herling ergänzt: „Scheidt & Bachmann bietet als führender Smart-Parking-Anbieter mit seiner zukunftsweisenden parkoneer Lösung genau das Property-Management-Systemmodul im Bereich Car Access an, das im Verbund mit unseren Zutrittssystemen für Kundinnen und Kunden ein einzelnes, integriertes System schafft. Darüber können alle Zufahrts- und Zutrittsvorgänge gemeinsam verwaltet werden. Zudem bietet es bedarfsgerechte Nutzungsmöglichkeiten in Echtzeit."

Die Digitalisierung und Dynamisierung des Parkens

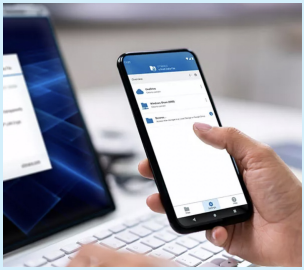
Die parkoneer Lösung vereint die Scheidt & Bachmann Hardware in einem kompakten Setup, bestehend aus Schranke, Kamera und einem Steuergerät mit QR-Code Scanner und Sprechstelle. Die Zufahrt erfolgt für vorab registrierte Nutzende per Kennzeichenerkennung. Über die parkoneer Software werden intuitiv alle Parkvorgänge verwaltet – rein webbasiert und auf jedem Endgerät. Schlanke, digitale Prozesse verringern den Verwaltungsaufwand. Zudem ermöglicht parkoneer eine dynamische Vergabe von Stellplätzen und minimiert so Auslastungsschwankungen.

parkoneer wird als Ergänzung im Property Management System per Software-Konnektor in die dormakaba Access Control Systeme „exos" und „MATRIX" integriert. So agieren Nutzerinnen und Nutzer auf einer digitalen Plattform und die Parkraum- und Gebäudezutrittsverwaltung erfolgt reibungslos. „Die Vorteile sind zahlreich und liegen auf der Hand", so Thorsten Braun, Director Global Operations Scheidt & Bachmann Parking Solutions GmbH. „Die flexible Selbstorganisation und der nahtlose Zugang zum Parkplatz, zu Gebäuden sowie Räumlichkeiten sind offensichtliche Faktoren. Hinzu kommt die erheblich vereinfachte Verwaltung des Zutritts- & Parkraummanagements, Auslastungssteigerungen der Parkfläche sowie eine optimierte Kosteneffizienz und nicht zuletzt eine Erhöhung der Zufriedenheit von Mitarbeitenden."

Utimaco

Conpal GmbH übernommen

Strategischer Ausbau des Lösungsportfolios vorangetrieben



Utimaco, internationaler Anbieter von IT-Sicherheitslösungen, hat zum 31. März 2023 die conpal GmbH, einen Anbieter von IT-Security-Lösungen zum Schutz vertraulicher Daten durch Verschlüsselung und Authentisierung, übernommen. Die beiden Unternehmen pflegten bereits vor der Übernahme eine konstruktive Partnerschaft und conpal-Produkte waren auch unter Utimaco-Branding erhältlich. Durch die nun erfolgte Integration kann Utimaco seinen Kunden ein vollständiges Lösungsport- folio für die IT-Sicherheit in den Bereichen Datenverschlüsselung, Hardware-Sicherheitsmodule, Schlüsselmanagement und Public Key Infrastruktur (PKI) in hochregulierten Bereichen aus einer Hand anbieten. Gleichzeitig markiert die Übernahme einen weiteren Meilenstein in der strategischen Entwicklung vom Produkt- zum Lösungsanbieter.

LAN Crypt, das bisherige Flagship-Produkt von conpal, wird zukünftig unter dem Namen u.trust Data File erhältlich sein. Die Kontinuität bleibt dennoch gewahrt, da Utimaco alle bisherigen Mitarbeiter übernimmt und die Standorte in Neu Isenburg und Linz erhalten wird. Die Marke „conpal" soll zwar in Zukunft innerhalb des Utimaco-Portfolios nicht mehr geführt werden, die „conpal GmbH" als Rechtssubjekt wird hingegen fortbestehen.

u. trust Data File gewährleistet den rechtssicheren Umgang mit sensiblen Daten in Übereinstimmung mit Datenschutzbestimmungen wie DSGVO, CCPA, PDPA usw. Gleichzeitig ist die Lösung benutzerfreundlich – ein entscheidender Faktor für die Akzeptanz von Sicherheitsmaßnahmen seitens der Belegschaft.

„Wir als Utimaco wollen uns als der präferierte Partner für Cybersicherheit und Compliance in hochregulierten und anspruchsvollen Branchen profilieren. Tiefe Integration, von der Hardware über verschiedene Software-Systeme bis in die Cloud, spielt dabei für uns eine entscheidende Rolle", sagt Stefan Auerbach, CEO von Utimaco. „Mit conpal gewinnen wir nun ein weiteres erstklassiges Produkt hinzu, das sich nahtlos in unser Ökosystem einfügt."

„Uns bei conpal verbindet eine langjährige Geschäftsbeziehung mit Utimaco. Wir kennen einander sehr gut und haben bereits gemeinsam an Projekten gearbeitet. So haben wir erkannt, dass wir ähnliche Ziele und Werte haben und unsere Unternehmenskulturen sehr gut zusammenpassen. Durch die Integration in Utimaco können wir nun unsere Kräfte bündeln und noch besser gemeinsam am Markt agieren. Unsere Bestandskunden können selbstverständlich auch weiterhin die Qualität und den Service erwarten, die sie von uns gewohnt sind", so Rolf Wassermann und Ralf Engers, bisherige und neue Geschäftsführer der conpal GmbH.

Mobotix

Neuer CTO startet zum 01. April 2023

Christian Cabirol hat seine Position als Chief Technology Officer (CTO) der MOBOTIX AG bereits zum 01. April 2023 angetreten. Wie bereits am 06. Februar 2023 verkündet, wird Christian Cabirol alle F&E-Schwerpunkte und Tech- nologiepartnerschaften als Schlüsselelemente der lösungsorientierten Strategie verantworten.

„Es ist mir wichtig, dass wir die Werte, die uns stark gemacht haben, weiter in den Vordergrund rücken. Qualität „Made in Germany" mit den sorgfältig von Hand montierten Kameras an unserm Standort Langmeil sind ein echtes Unterscheidungsmerkmal. Unsere Flexibilität und höchste Cybersicherheit unserer Videosysteme, mit ihrer dezentralen Architektur sind fest in der MOBOTIX DNA verankert. Dazu braucht es die stetige Neugier und unbedingte Bereitschaft, wegweisende, effektive und passende Lösungen für die Bedürfnisse unserer Kunden zu entwickeln. Wir möchten für die von uns bedienten Kernbranchen, gemeinsam mit unseren Partnern, greifbare Vorteile liefern. Dafür werde ich mich mit ganzer Kraft einsetzen", betont Christian Cabirol.

Mehr als Sicherheit – Prozesse verbessern, Erträge generieren

Ein Schwerpunkt der kommenden Jahre wird auf der Sammlung, Kombination und Analyse von Daten liegen, die rund um die Videotechnologie erzeugt werden. Die Zusammenführung der Daten, beispielweise über SCADA-Systeme in der Industrie, eröffnen nahezu unbegrenzte Möglichkeiten für individuelle Anforderungen.

„Mit den intelligenten MOBOTIX Videosystemen lassen sich Prozesse verbessern und Erträge erhöhen. Zudem können sie Menschen entlasten und machen ihnen das Leben einfacher" ergänzt Christian Cabirol.

„Intelligente Videotechnik bietet inzwischen viel mehr als nur Sicherheit. Unsere Kunden erwarten einen attraktiven Return on Investment (ROI).

Das wir das leisten können, belegt eindrucksvoll das Beispiel eines Gießereiprojekts. Dort haben sich unsere Videosysteme in der Prozessüberwachung bereits innerhalb von zwei Monaten amortisiert und tragen seitdem maßgeblich zum Ertrag bei. So etwas können wir in vielen Bereichen schaffen."

PMeV

Mitgliederversammlung bestätigt Vorstand

Bernhard Klinger führt den Verband auch in den kommenden zwei Jahren

Die Mitgliederversammlung des Bundesverbandes Professioneller Mobilfunk (PMeV) – Netzwerk sichere Kommunikation hat den Vorstand des Verbandes für die kommenden zwei Jahre bestätigt. Bernhard Klinger (HMF Smart Solutions GmbH), 2019 erstmals zum Vorsitzenden des Vorstands gewählt, führt den PMeV somit weiter an. Stellvertretender Vorsitzender und Finanzvorstand ist Konstantin König (Airbus Secure Land Communications GmbH). Neben König amtiert auch Volker Hartwein (Frequentis Deutschland GmbH) als stellvertretender Vorsitzender. Darüber hinaus gehören dem PMeV-Vorstand an: Thorsten Altemöller (telent GmbH), Helmut Gaschler (Motorola Solutions Germany GmbH), und Marcel Petruzzelli (Seamcom GmbH & Co.KG). Somit setzt der PMeV die Kontinuität seiner Vorstandsarbeit auch nach der Mitgliederversammlung 2023 fort.

Zur Bedeutung einer sicheren hochverfügbaren Kommunikation – dem Kernanliegen des PMeV – erklärte Bernhard Klinger in der Mitgliederversammlung: „Der Angriffskrieg Russlands auf die Ukraine führt uns vor Augen, dass gezielte Angriffe auf Kritische Infrastrukturen und Unternehmen keine theoretischen Gedankenspiele mehr sind. Generell gilt: In der konventionellen Sabotage liegt ebenso eine Gefahr wie in der Cyberkriminalität." Im Hinblick auf die Entwicklung des PMR-Marktes betonte Klinger die Bedeutung einer sicheren Kommunikation für die fortschreitende Digitalisierung. Hierin liege eine Chance für PMeV-Mitgliedsunternehmen, bestehende Märkte auszubauen und neue Märkte zu entwickeln. Der PMeV werde mit dem Netzwerk seiner Mitglieder die Entwicklung der Märkte für sichere Kommunikation auch in Zukunft mitge- stalten.

Hauptstadtbüro in Berlin eröffnet

„Die aktuellen Entwicklungen in Politik, Wirtschaft und dem Markt für sicherheitskritische Kommunikation stellen die Verbandsarbeit vor vielfältige Herausforderungen. Dabei kommt die persönliche Ansprache und dem Dialog mit Stakeholder aus Politik und Anwenderverbänden eine immense Bedeutung zu", so Bernhard Klinger weiter. Daher hat der PMeV zur Stärkung seiner Vernetzung in Berlin im Oktober 2022 ein Hauptstadtbüro eröffnet, in dem die Geschäftsführung angesiedelt ist.

Azkoyen Group

Struktureller Wechsel in der Organisation

Neue Doppelspitze führt primion in die Zukunft . Darío Vicario Ramírez übernimmt zum 1. April 2023 die Funktion als CEO / Wachstumsstrategie intensivieren

Darío Vicario Ramírez (links) und Jorge Pons Vorberg (rechts) ©Azkoyen Group

Mit Wirkung zum 1. April 2023 übernimmt Darío Vicario Ramírez als CEO die Leitung der T&S Division mit der primion Technology GmbH in Deutschland, der GET n.v. in Belgien und den Niederlanden, der primion DIGITEK SLU in Spanien, der primion SAS in Frankreich und der Opertis GmbH in Deutschland. Gleichzeitig bleibt er weiterhin CEO der Azkoyen Group. Jorge Pons Vorberg wird als Managing Director Finance Teil der Doppelspitze in der T&S Division sein. Die Einrichtung einer Doppelspitze wird maßgeblich dazu beitragen, die Wachstumsstrategie der T&S Division zu intensivieren.
Die Aufteilung der komplexen und intensiven Aufgaben im Management auf zwei Geschäftsführer sorgt außerdem für einen noch besseren Fokus und die maximale Effektivität. Darío Vicario Ramírez verantwortet künftig die Bereiche Sales & Operation, Forschung & Entwicklung, Produktmanagement sowie Marketing.
Jorge Pons Vorberg wird für die Bereiche Finanzen, Personal, die IT und die Supply Chain verantwortlich sein.

Darío Vicario Ramírez: „Wir sind der festen Überzeugung, dass diese organisatorische Änderung maßgeblich dazu beitragen wird, die T&S Division weiter zu stärken um anstehenden Herausforderungen zu begegnen und die Zukunft des Unternehmens aktiv zu gestalten".

Acre

Übernahme von Premisys von Identicard beendet

Acre hat die Übernahme des Software- und Hardwareportfolios von Premisys sowie der Vermögenswerte von Identicard abgeschlossen. Das Unternehmen setzt damit seine Strategie fort, die Konsolidierung voranzutreiben und Technologien zu erwerben, die sein Portfolio erweitern und den wachsenden Anforderungen seines Kundenstamms gerecht werden.
Die Technologien von Premisys ermöglichen es Unternehmen, den Zugang zu Türen selbst zu verwalten, integrierte Videobilder anzuzeigen und Einrichtungen abzuschließen. Die Übernahme erweitert auch die Möglichkeiten von Acre in den Bereichen Gesundheitswesen, Bildung, Rechenzentren und Senioreneinrichtungen.
"Seit seiner Gründung war es das übergeordnete Ziel von Acre, Zutrittskontrolle und Kunden unter einem Dach zu vereinen", sagt Darren Learmonth, CTO von Acre. "Diese Akquisition ist ein weiterer wichtiger Schritt in der Transformation von Acre und festigt die Position des Unternehmens als Marktführer im schnell wachsenden Markt für Zutrittskontrolle."
Dieser Deal folgt auf eine Geschichte des akquisitorischen Wachstums von Acre. Im Jahr 2021 kaufte das Unternehmen Feenics und Matrix, um die sich entwickelnden Kundenanforderungen im Cloud- und Unternehmenssegment zu erfüllen, und fügte 2022 Sisco zu seiner wachsenden Markenfamilie hinzu.
Die finanziellen Details der Transaktion wurden nicht bekannt gegeben.

CEPOL

EU-Agenturen für Justiz und Inneres präsentieren dem Europäischen Parlament das Ergebnis für 2022 und skizzieren die wichtigsten Prioritäten für 2023

Die Exekutivdirektorin der EU-Agentur für die Aus- und Fortbildung von Strafverfolgungsbehörden (CEPOL), Montserrat Marin Lopez, und die Exekutivdirektorin der EU-Agentur für Asylfragen (EUAA), Nina Gregori, sind heute im Europäischen Parlament, wo sie die Höhepunkte und Prioritäten des scheidenden und des kommenden Vorsitzes des Netzwerks der EU-Agenturen für Justiz und Inneres (JHAAN) vorstellen werden. Die EUAA hat am 1. Januar 2023 die Präsidentschaft des Netzwerks von der EPA übernommen.

Das Netz der JI-Agenturen spielt eine wichtige Rolle in Europa. Es verbindet die EU-Agenturen zum Schutz des Raums der Freiheit, der Sicherheit und des Rechts. Gemeinsam tragen die neun JI-Agenturen zur Umsetzung der EU-Ziele in den Bereichen Migration, Asyl und Verwaltung der Außengrenzen, Bekämpfung der organisierten Kriminalität, des Drogenhandels und des Terrorismus, Gleichstellung der Geschlechter und Achtung der Grundrechte bei. Sie erleichtern auch das Funktionieren der einschlägigen IT-Systeme der EU, tragen zu den EU-Maßnahmen gegen Drogen und Drogensucht bei und erleichtern die Ausbildung der Strafverfolgungsbehörden.

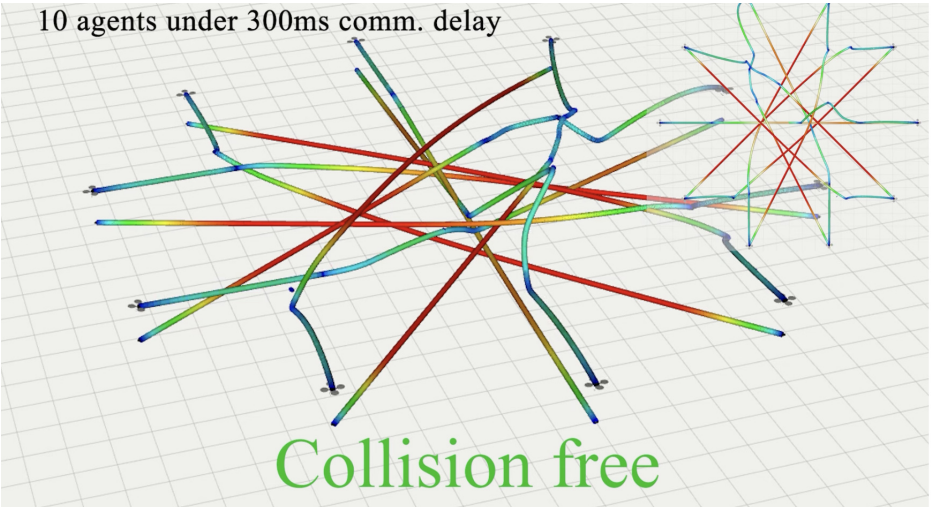
Im Jahr 2022 stand die technische Unterstützung der Mitgliedstaaten und EU-Institutionen bei der Reaktion auf die militärische Aggression Russlands gegen die Ukraine im Mittelpunkt der Aktivitäten des Netzwerks. Das ganze Jahr über fanden Sitzungen statt, um die Situation zu beobachten und sicherzustellen, dass die kollektive Reaktion Europas den sich ändernden Bedürfnissen entspricht. In diesem Zusammenhang leisteten mehrere JI-Agenturen auch Unterstützung für die Republik Moldau. Neben der laufenden Unterstützung der Mitgliedstaaten bei der Bewältigung der Herausforderungen, die sich aus der russischen Aggression gegen die Ukraine ergeben, waren die Digitalisierung, die Zusammenarbeit mit Nicht-EU-Ländern, die Ausbildung und die Umsetzung der Grundsätze des Europäischen Green Deal die wichtigsten Prioritäten des Netzwerks im vergangenen Jahr unter dem EPA-Vorsitz.

Das Format der Dreierpräsidentschaft, das im vergangenen Jahr zum ersten

Mal angewandt wurde, gewährleistet einen reibungslosen Übergang von einem Vorsitz zum nächsten. Daher werden die gemeinsamen Bemühungen der JI-Agenturen auch 2023 fortgesetzt. Unter den von der EUAA für dieses Jahr festgelegten vorrangigen Themen bleibt die Digitalisierung ein Schlüsselelement des Arbeitsprogramms des Netzwerks, zusammen mit der Umsetzung des EU Green Deal, der Cybersicherheit und der Bereitstellung von Informationen in gemischten Migrationssituationen, die ebenfalls oberste Priorität haben. Die EUAA wird den Vorsitz des Netzwerks der JI-Agenturen bis zum 31. Dezember 2023 innehaben und ihn dann 2024 an eu-LISA abgeben.

Die Ergebnisse des Netzwerks im Jahr 2022 wurden am 22. Februar dem Ständigen Ausschuss für die operative Zusammenarbeit im Bereich der inneren Sicherheit (COSI) des Rates vorgestellt.

https://euro-security.de/wp-content/uploads/2023/04/cepol-european-law-enforcement-research-bulletin-issue-22.pdf



MADER

Drohnenkollisionen können vermieden werden

Neues System des Massachusetts Institute of Technology setzt gezielt auf Verzögerungstaktik

Die neue Software MADER von Forschern des Massachusetts Institute of Technology (https://www.mit.edu) (MIT) verhindert in Kombination mit einem Navigations- und Kommunikationssystem effektiv unbeabsichtigte Zusammenstöße zwischen Drohnen. Jedes im Schwarm operierende Fluggerät informiert die anderen Mitglieder ständig über den Kurs, der gerade eingeschlagen wurde.

Fehler bei der Kommunikation

Heute funktioniert das System, das anfangs nur für Frust sorgte. Als Jonathan P. Wie MADER mit seinem Team vor knapp drei Jahren entwickelt hat, war die Enttäuschung groß, als der Schwarm erstmals auf die Reise geschickt wurde. Immer wieder kam es zu Kollisionen. "Wir merkten ziemlich schnell, dass daran Verzögerungen bei der Kommunikation schuld waren", sagt der zum Team gehörende MIT-Student Kota Kondo.

Bei "Robust MADER", wie die jetzt vorgestellte Weiterentwicklung heißt, passiert das nicht. Der neue Algorithmus ist so ausgelegt, dass er mögliche Verzögerungen bei der Kommunikation einbezieht. Die Idee dahinter ist einfach, auch wenn die Realisierung lange gedauert hat.

Eine Drohne wartet eine bestimmte Zeit mit einem Kurswechsel, wenn sie eine neue Flugbahn ausgewählt und diese den anderen Drohnen mitgeteilt hat. Erhält sie während dieser Verzögerung zusätzliche Flugbahninfos anderer Drohnen, kann sie ihre neue Flugbahn aufgeben und den Optimierungsprozess von vorne beginnen.

100-prozentige Erfolgsquote

Als Kondo und seine Kollegen Robust MADER sowohl in Simulationen als auch in Flugexperimenten mit echten Drohnen testeten, ergab es eine 100-prozentige Erfolgsquote bei der Vermeidung von Kollisionen. Der Schwarm agierte lediglich ein wenig langsamer. "Wenn man sicherer fliegen will, ist Vorsicht angebracht. Daher ist es vernünftig, dass wir mehr Zeit einplanen, denn wenn die Drohnen kollidieren, erreichen sie ihr Ziel nie", so Kondo.

Video: https://www.youtube.com /watch?v=i1d8di2Nrbs

Auf Augenhöhe

Friedrich P. Kötter im „Dialog mit der Jugend" • Familienunternehmer stellt sich den Fragen von Oberstufenschülern• Top 10-Gebäudedienstleister bietet Ausbildungsplätze

Unternehmenslenker Friedrich P. Kötter traf sich gestern zum persönlichen Austausch mit 20 Schülerinnen und Schülern der Gesamtschule Mülheim-Saarn. Erneut beteiligte sich das Familienunternehmen an der Gesprächsreihe der Stiftung TalentMetropole Ruhr und gab Jugendlichen die Möglichkeit, sich über die regionale Wirtschaft, Berufe und Arbeitswelt zu informieren – und sich bei Interesse direkt für eine Ausbildung zu bewerben.

Der „Dialog mit der Jugend" bringt Oberstufenschülerinnen und -schüler mit Top-Managern aus der Region zu einem Gespräch auf Augenhöhe zusammen. Seit über zwei Jahrzehnten ist die Wirtschaftreihe festes Projekt der Bildungsarbeit der Stiftung TalentMetropole Ruhr. Nach digitalen Veranstaltungen in den vergangenen beiden Jahren freute sich Unternehmenslenker Friedrich P. Kötter umso mehr, 20 Schülerinnen und Schüler am Essener Stammsitz der KÖTTER Unternehmensgruppe begrüßen zu dürfen.

Der Familienunternehmer zeigte auf, dass es dem bundesweit tätigen Familienunternehmen auch in einem schwierigen wirtschaftlichen Umfeld gelungen ist, sich weiter erfolgreich am Markt zu behaupten und den Umsatz um zwei Prozent auf jetzt 601 Millionen Euro zu steigern. Dies gelang durch innovative Lösungen in den Sicherheits-, Reinigungs- und Personaldienstleistungen und ins-

besondere durch eine herausragende Leistung von qualifizierten Mitarbeiterinnen und Mitarbeitern. Den klaren Fokus auf Qualität und Qualifikation verdeutlicht auch diese beeindruckende Zahl: 650.000 Stunden Aus- und Weiterbildung wurden im vergangenen Jahr 2022 durchgeführt. Friedrich P. Kötter: „Damit investieren wir in die Zukunft unserer Teams. Und es lohnt sich: Denn nur mit gut aus- und fortgebildeten Mitarbeiterinnen und Mitarbeitern können wir unsere Leistungsstärke bei all unseren Kunden jeden Tag aufs Neue beweisen.“

Praktische Einblicke in die Arbeitswelt

Nach der Gesprächsrunde konnten die Schülerinnen und Schüler an drei Praxisstationen verschiedene Fachbereich des Top 10-Gebäudedienstleisters kennenlernen. Dazu gehörten die KÖTTER Notruf- und Serviceleitstelle, mit ihrer Hightech-Ausstattung und dem Hochsicherheitsbereich eine der modernsten Leitstellen Europas, sowie die KÖTTER Akademie, die ihre Schulungsangebote am Beispiel von Brandschutz und Brandbekämpfung vorstellte. In der unternehmenseigenen Kfz-Werkstatt stand u. a. die E-Mobilität im Vordergrund, die das Familienunternehmen als wesentlichen Faktor ihrer Nachhaltigkeitsstrategie vorantreibt. So schaffte die KÖTTER Unternehmensgruppe 2022 einen Sprung von 50 auf jetzt deutlich über 100 elektrobetriebene Fahrzeuge in ihrer Flotte, die eine Einsparung von knapp 400 Tonnen CO_2 erzielen.

Friedrich P. Kötter: „Als Familienunternehmen sehen wir uns besonders in der Verantwortung für kommende Generationen und machen uns stark für Mensch und Natur. Deshalb setzten wir auf eine nachhaltige Unternehmensführung. Das betrifft den Umweltschutz genauso wie unser wirtschaftliches Handeln, bei dem wir großen Wert auf langfristige Miarbeiter- und Kundenbeziehungen legen.“

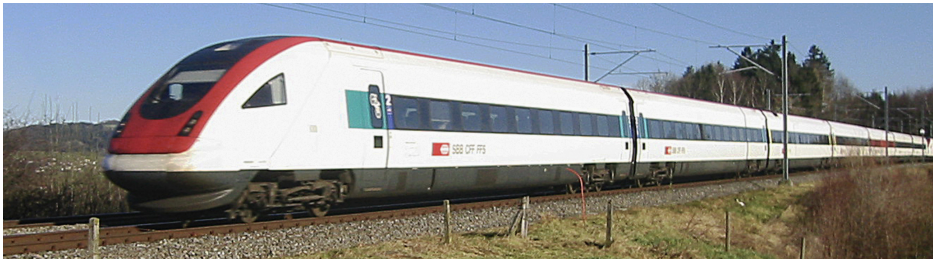
Freie Ausbildungsplätze – jetzt bewerben!

Insgesamt beschäftigt das Familienunternehmen bundesweit aktuell rund 250 Auszubildende in zehn Berufsfeldern. Für das im Sommer bzw. Herbst 2023 startende Ausbildungsjahr sind weitere ca. 120 Neueinstellungen geplant. Bundesweit freie Ausbildungsplätze gibt in den folgenden Berufen: Kaufleute für Büromanagement (m/w/d), Personaldienst- leistungskaufleute (m/w/d), IT-Systemelektroniker (m/w/d), Elektroniker für Informations- und Kommunikationstechnik (m/w/d), Fachkraft für Schutz und Sicherheit (m/w/d), Servicekraft für Schutz und Sicherheit (m/w/d) sowie Gebäudereiniger (m/w/d).

[www.koetter.de/ausbildung]

Schweizerische Bundesbahnen

RFID -Fahrzeugidentifikation die Digitalisierung relevanter Prozesse



Der einwandfreie Zustand aller Schienenfahrzeuge dient nicht nur der Fahrgastsicherheit, er verhindert auch potenzielle Schäden an der Infrastruktur, wie Schiene, Oberleitung oder Zugkomponenten. Um ein durchgängiges Zustands-Monitoring überhaupt erst etablieren zu können, kennzeichnete die Schweizerische Bundesbahnen (SBB) ihre Schienenfahrzeuge über RFID. Ziel war es, diese zu identifizieren, um sie exakt zu lokalisieren und automatisiert Daten über deren Zustand zu erhalten.

Kritische Entwicklungen frühzeitig erkennen

Die SBB Infrastruktur ist die Betreiberin der Zugkontrolleinrichtungen. Ziel der Infrastrukturbetreiberin ist es, schadhafte Fahrzeuge frühzeitig zu erkennen und durch gezielte Maßnahmen bestimmte Ereignisse präventiv zu verhindern. Damit es nicht zu Betriebsbeeinträchtigungen kommt, wird die Infrastruktur und alle darauf verkehrenden Fahrzeuge permanent überwacht. Unerwartete Reparaturen an

"Fahrzeugidentifikation mittels RFID in Rail betrachten wir als eine Enabler-Technologie, mit der alle Prozesse, die auf eine Fahrzeug-ID angewiesen sind, digitalisiert werden."

Stefan Koller, Leiter Zugkontrolleinrichtungen, SBB AG

Schienenfahrzeugen im Personen- oder Güterverkehr wollte die SBB aus Sicherheits- und Kostengründen vermeiden. Zudem sollte der plötzliche Ausfall von Zügen verhindert werden, damit es nicht zu ungeplanten Reparatureinsätzen kommt. Eine proaktive Instandhaltung ist ein wichtiger Prozess für einen reibungslosen, zuverlässigen Fahrplan.

Nicht digitalisiert, nicht transparent

Warum sich die SBB für eine zuverlässige Fahrzeugidentifikation mit RFID entschied? Man suchte nach einer Lösung für Echtzeit-Transparenz. Bislang konnte zwar festgestellt werden, dass ein Fahrzeug defekt war, aber nicht welches. Die genaue Fahrzeugnummer konnte nicht ermittelt werden. Ohne zuverlässige Fahrzeugidentifikation konnten die Messdaten über den Fahrzeugzustand auch nicht an die verantwortlichen Fahrzeughalter übergeben werden. Diese konnten somit nicht von Daten profitieren, die wichtige Informationen über den Zustand von Komponenten lieferten. Sie hatten nicht die Möglichkeit, auffällige Probleme frühzeitig zu beheben, bevor sie ein kritisches Ausmaß erreichten.

Der Dominoeffekt

Im bisherigen Prozess konnte man zwar schadhafte Fahrzeuge bei Erreichen einer Interventionsschwelle rechtzeitig ausmachen, um einen Serviceeinsatz durchzuführen. Allerdings führten diese ungeplanten Interventionen zu Beeinträchtigungen der Transportkette sowie des übrigen Verkehrs und hatten somit Auswirkungen auf ganz unterschiedliche Kunden – sowohl im Cargo als auch im Personenverkehr. Diese unerwünschte Kettenreaktion wollte man zukünftig unterbinden.

Der Anfang: Kennzeichnung mit RFID

Die Basis für die gewünschten qualitäts-

sichernden Maßnahmen war zunächst die Fahrzeugidentifika- tion über RFID-Transponder, die eine achsscharfe Zuordnung der Daten zu einem Fahrzeug ermöglichte. Nur so kann der Fahrzeugzustand zuverlässig über mehrere Zugkontrolleinrichtungen verfolgt und kritische Entwicklungen frühzeitig erkannt werden.

Monitoring von Infrastruktur und Fahrzeugen

Die Erfassung von Fahrzeugachsen wurde über Schienenkontakte, die am Gleis verbaut sind, sichergestellt. Durch Verknüpfung dieser Daten mit den RFIDIdentifikationsdaten, war man in der Lage ein selbstsprechendes Businessevent zu erzeugen, das Auskunft über Zustand und Fahrzeugindividualdaten gab. Das Ergebnis: Echtzeittransparenz über den Zustand der Schienenfahrzeuge. Zur benutzerfreundlichen Visualisierung hat KATHREIN Solutions dafür eine auf die SBB zugeschnittene App entwickelt, um die ermittelten Fahrzeugdaten (Präsenz, Fahrzeugnummer, Achsen) auf mobilen Endgeräten anzuzeigen. Diese Visualisierung bildet jedes Fahrzeug mit jeder einzelnen Achse ab und vermittelt einen sofortigen Überblick bzw. Transparenz pro erfasstem Schienenfahrzeug.

Installierte RFID Hardware und Leseprozesse

Die RFID-Transponder an den Zügen sowie die am Gleisbett verbauten RFID-Reader erfordern eine besondere Robustheit, die jeder Witterung standhält. Der KATHREIN Reader ARU 3500 ist speziell für raue Umgebungen konzipiert und daher optimal für diese Bedingungen geeignet. Die Hardware-Kosten hielten sich durch die interne Antenne des ARU 3500 bei einer Eingleis-Anwendung in Grenzen. Bei einer Zweigleis-Anwendung wurde ein zusätzlicher ARU 3500 als Slave angebunden. Durch die konfigurierten IDs (Master und Slave) am Haupt-Reader kann jede Erfassung dann entsprechend dem Gleis zugeordnet werden. KATHREIN rüstete außerdem sämtliche Zugkontrolleinrichtungen (ca. 70 Standorte) mit RFID-Lesegeräten aus und kennzeichnete die Schienenfahrzeuge mit einem RFID-Tag, gemäß DIN Norm EN17230.

Datenerfassung bei 180 km/h, Schnee oder Starkregen

Die Leseanforderungen der RFID-Transponder an den Fahrzeugen beinhalteten Fahrzeugnummer und Gleisnummer. Außerdem mussten die Daten-Erfassungen in einer Range von 5 km/h bis 180 km/h zuverlässig erfolgen. Da die Witterungsbedingungen gerade im Winter in der Schweiz extrem sein können, war eine Installationsart notwendig, die auch unter schwierigen Witterungsbedingungen einwandfrei funktioniert.
Dazu wurden 68 Erfassungspunkte über das Schweizer Schienennetz verteilt. 14 kommen bei eingleisigen Erfassungen mit einem einzigen ARU 3500 zum Einsatz. Für die zweigleisigen Erfassungen verwendete man einen Master-Slave Prozess mit zwei ARU 3500 Readern.

Daten aufnehmen und intelligent aufbereiten

Nachdem die RFID Reader die Daten aufgenommen haben, werden diese über die KATHREIN CrossTalk Software an die speziell für die SBB entwickelte APP übergeben. Dabei sendet jede Lesestelle die Daten an drei Server:

- Einen Produktiv Server
- Einen Backup Server
- Einen Test Server

Das Monitoring der RFID-Hardware findet zentral über ein SBB internes System statt, das via KATHREIN CrossTalk Agent und dem CrossTalk Server die Reader-Statusdaten erhält. KATHREIN CrossTalk ermöglicht auch die Integration der RFID-Hardware in das führende System der SBB. Dabei wird der KATHREIN RFID-Reader mittels des CrossTalk Agents intelligent gemacht, sodass diese ihre Zustandsdaten an das SBB System zur Verfügung stellen.

Der Projekterfolg

Was mit einer reinen RFID-basierten Identifikation für mehr Transparenz begann, führte zu einem neuen Qualitätsmanagement in der Instandhaltung der Infrastruktur. Die neu gewonnene Transparenz gibt in Echtzeit Auskunft über den Zustand von Komponenten, sowie deren beginnenden Verschleiß und warnt frühzeitig vor auftretenden Reparaturen. Wartungseinsätze können nun noch gezielter geplant werden, ohne Fahrpläne zu gefährden. Das ist ein riesiger Pluspunkt für die Kundenzufriedenheit, sowohl im Güter- als auch im Personenverkehr. Die digitalisierten Informationen werden auf einem Terminal visualisiert, das exakt anzeigt, an welchem Schienenfahrzeug ein Problem aufgetreten ist, ohne dass eine personalintensive Suche dafür gestartet wird. Die Kennzeichnung mit RFID nutzte die SBB intelligent für die digitale Transformation zentraler Bereiche. Sind die Daten erst einmal erfasst, können sie vielfältig genutzt werden. Es bleibt abzuwarten, wo die Reise in der schönen Schweiz diesbezüglich noch hinführt.

Kathrein Produkte
KATHREIN Reader ARU 3500
Kathrein Benefits

- Predictive Maintenance (Vorausschauende Instandhaltung)
- Digitales Frühwarnsystem
- Fahrgastsicherheit
- investitionsschutz der Infrastruktur
- Pünktliche Einhaltung des Fahrplans
- Kostenreduktion durch Vermeidung von ungeplanten und unnötig teuren Reparatureinsätzen

Investitionen in IT-Strukturen

SITA Airport Management-Lösung strafft die Organisation am internationalen Flughafen Nursultan Nasarbajew - Flughafen Nursultan Nazarbayev unterzeichnet umfassendes IT-Investitionsprogramm mit SITA

Der internationale Flughafen Nursultan Nasarbajew in Kasachstan hat sich an SITA gewandt, um neue digitale Lösungen zur Senkung der Betriebskosten und zur Verbesserung der Abfertigungsleistung von Flugzeugen zu liefern. Dazu gehört, dass SITA alle wichtigen Passagier-, Gepäck- und Betriebs-IT-Systeme bereitstellt.

Ein Hauptaugenmerk des Flughafens liegt auf der Rationalisierung der luftseitigen Abläufe. Mit der Airport Management-Lösung von SITA kann der Flughafen den Betrieb auf dem gesamten Flugplatz besser vorhersagen und verwalten. Durch den Austausch von Ereignismeilensteinen mit Partnern wie z. B. Fluggesellschaften haben die Betriebsteams einen genauen Überblick darüber, wie verschiedene Aktivitäten auf dem Flughafen integriert sind und sich auf den Gesamtbetrieb auswirken können. Bodenpersonal kann seine Aktivitäten effizienter und proaktiver planen, von der Zuweisung von Teamzuweisungen bis hin zur Verwaltung von Flugzeugparkplätzen, Gates und anderen Ressourcen. Dies wird den Flughafen-

betrieb digitalisieren, die Pünktlichkeit verbessern und unnötige Flugverspätungen vermeiden. Der Flughafen geht davon aus, dass die Implementierung von SITA Airport Management zu einer Kostenreduzierung von 15-20 % führen kann und damit die Grundlage für eine kollaborative Entscheidungsfindung (Airport Collaborative Decision-Making, A-CDM) schafft.

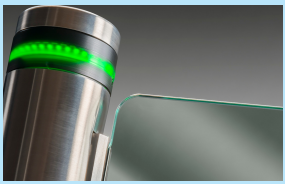
Als Eckpfeiler des Passagierservices wird SITA neue Smart Path Check-in-Kioske und Gepäckabgabestationen bereitstellen, die den Passagieren nahtlose Selbstbedienungsoptionen von der Bordsteinkante bis zum Gate bieten. Diese Touchpoints ebnen den Weg für eine zukünftige biometrische Reise im Einklang mit dem One-ID-Programm der IATA. Künftig werden die Gesichter der Passagiere zu ihren Bordkarten, und die Passagiere werden schnell identifiziert, wenn sie sich einer Kamera an jedem Touchpoint nähern.

Daulet Hamzin, Vorstandsvorsitzender des Internationalen Flughafens Nursultan Nasarbajew, sagte: "Der internationale Flughafen Nursultan Nasarbajew beschleunigt ein umfangreiches Entwicklungsprogramm, um das Wachstumspotenzial des kasachischen Luftverkehrsmarktes zu unterstützen. Wir haben angekündigt, dass das Jahr 2023 ganz im Zeichen der Digitalisierung des Flughafens stehen wird. Wir sind der festen Überzeugung, dass Technologie eine Schlüsselrolle bei der Bewältigung dieses rasanten Wachstums, der Rationalisierung der luftseitigen Abläufe und der Verbesserung des Kundenerlebnisses spielt. Wir freuen uns sehr, mit SITA zusammenzuarbeiten, um mehrere regionale digitale Initiativen voranzutreiben."

Sergio Colella, SITA-Präsident für Europa, sagte: "Der internationale Flughafen Nursultan Nasarbajew ist Vorreiter bei der Digitalisierung seines Betriebs und positioniert sich als einer der führenden Flughäfen der Region. Wir freuen uns, mit dem Flughafen zusammenzuarbeiten und die Vorteile der Automatisierung und Digitalisierung voll auszuschöpfen."

Boon Edam

Rahmenlose Zugangsschranke Winglock Swing



Boon Edam hat seine schmalste Zugangsschranke Winglock Swing um Funktionen erweitert. Die Eingangslösung bietet jetzt noch mehr Sicherheit und Vielseitigkeit für Zugänge mit größerer Durchgangsbreite. Mit immer größeren Gebäuden und wachsenden Besucherströmen gewinnt die Kontrolle des Personenaufkommens zunehmend an Bedeutung. Die Zugangsschranke Winglock Swing ist die ideale Eingangslösung, wenn ein sicherer Zugang bei großer Durchgangsbreite gefragt ist, zum Beispiel für sperrige Güter oder Personengruppen. Das aus hochwertigem Edelstahl und einer durchgängigen Glasscheibe gefertigte Original, die Zugangsschranke Winglock Swing, ist äußerst elegant und benutzerfreundlich. Dank ihres schlichten Designs fügt sie sich nahtlos in jede Umgebung ein. Die aktuelle Funktionserweiterung bietet nun noch mehr Möglichkeiten als die klassische Version. Die Winglock Swing gibt den Nutzern ein Gefühl von Sicherheit. Zur besseren Anpassung an die allgemeine Designästhetik von Gebäuden und Einrichtungen kann sie jedoch noch feiner abgestimmt werden. Designelemente wie die LED-Leuchten zur intuitiven Benutzerführung und ihr ergonomisches Design sorgen für einen hochmodernen Sicherheitseingang mit geringem Platzbedarf. Im Zusammenspiel mit der häufig von Planern eingesetzten Serie Lifeline Speedlane von Boon Edam stellt sie die beste Wahl für Einsatzorte mit geringem Platzangebot dar.Boon Edam bietet nun eine Seitenschranke mit hohen Glasscheiben (bis zu 1800 mm Höhe) oder auch in Doppelglasausführung (mit bis zu 1400 mm Durchgangsbreite) an. Außerdem wurde die Geschwindigkeitskurve der Winglock Swing besser abgestimmt, um eine Stoßkraft von weniger als 400 N zu gewährleisten. Die beiden neuen Funktionen sind in der Sicherheitsnorm EN 17352 vorgeschrieben, um einen möglichst sicheren Durchgang für alle Benutzer zu gewährleisten.

Hälfte aller Phishing-Websites imitieren Finanzinstitute

Dr. Martin J. Krämer, Security Awareness Advocate bei KnowBe4

Phishing-Angriffe zielen zwar vor allem auf den Diebstahl von Zugangsdaten ab, Bankbetrug ist jedoch weiterhin eine große Bedrohung für Privatpersonen wie Unternehmen. Hinter jedem Cyberangriff steht das Motiv, den Angriff so schnell wie möglich zu Geld zu machen. Und einer der schnellsten Wege ist es, sich einfach die Bankdaten des Opfers zu beschaffen.

Nach neuen Daten des Cybersecurity-Anbieters Fortra wurde der Finanzdienstleistungssektor im vierten Quartal des vergangenen Jahres am häufigsten Opfer von Cyberangriffen und machte 55 Prozent aller angegriffenen Geschäftsbereiche aus. Mit einem Anstieg von nur drei Prozent gegenüber dem vorangegangenen Quartal bietet der Finanzdienstleistungssektor Bedrohungsakteuren weiterhin eine einfache Möglichkeit, Opfer dazu zu bringen, direkten Zugang zu ihrem Geld, ihren Kreditkarten, Kreditlinien und mehr zu gewähren.

Ein solcher Diebstahl von Zugangsdaten erfolgt in erster Linie ohne Kosten für den Angreifer; laut dem Anbieter wurden drei Viertel der Phishing-Seiten durch kostenlose Methoden wie die Kompromittierung einer bestehenden Website oder den Missbrauch eines kostenlosen Web-Tools oder -Dienstes inszeniert. Bei fast 60 Prozent der Angriffe wurde ein alter globaler Top-Level-Domain-Name (z. B. .com und .org) verwendet, um den Angriffen Legitimität zu verleihen. Dem Bericht zufolge ahmen die Bedrohungsakteure Unternehmen aus dem Finanzsektor nach, darunter nationale und regionale Banken, Kreditgenossenschaften und andere verwandte Unternehmen.

In Deutschland werden Sparkassen-Kunden besonders ins Visier genommen

So wird in Phishing-Mails beispielsweise mit Betreffen wie „Bitte umgehend bearbeiten" auf die Opfer Druck ausgeübt; es liege eine Aktivität auf unbekannten Geräten vor, heißt es dann in der E-Mail. Auch in angeblichen E-Mails der ING DIBA ist von solchen verdächtigen Aktivitäten die Rede. Der Kunde solle nun im nächsten Schritt sensible Bankinformationen eingeben, um die Aktivität zu überprüfen.

In vermeintlichen E-Mails der Deutschen Kreditbank (DKS) wird auf ein angebliches Auslaufdatum der Kredit- und Debitkarten hingewiesen. Um eine Kontosperrung zu verhindern, müssten persönliche Daten aktualisiert werden. Es kursieren außerdem Phishing-Mails, die behaupten, der DKS-Kunde hätte Daten nicht bestätigt. Das angeblich gesperrte Konto könne man nur über den beigefügten Link freigeben. Aufgrund der P2D2-Richtlinie werden Bankkunden außerdem scheinbar von Volksbanken Raiffeisenbanken oder der Bundesregierung bzw. EU-Kommission aufgefordert, unverzüglich eine Verifizierung durchzuführen. In Wahrheit werden die Kunden nie aktiv diesbezüglich kontaktiert, denn die Richtlinie bewirkt nur alle 90 Tage im Online-Banking eine zusätzliche TAN-Eingabe.

Phishing-E-Mails von angeblichen Banken erkennen

Der erste, seriöse Eindruck einer E-Mail kann trügen: Daher kann zwar das Design realitätsnah sein, der Text aber Rechtschreibfehler und weitere Mängel beinhalten. Außerdem ist es ratsam, nicht direkt auf die Links der E-Mail zu klicken, sondern zunächst auf der Webseite der Bank nach weiteren Informationen zu suchen.

Es hat sich gezeigt, dass Bankbetrügereien sehr gut funktionieren und sowohl Privatpersonen als auch Unternehmen einem finanziellen Risiko aussetzen – alles, was es braucht, sind die richtigen Bankdaten, und die Konten der Opfer können innerhalb weniger Minuten komplett leergeräumtwerden.

Diese Angriffe beginnen alle mit einer Phishing-Methode, deshalb sollten Unternehmen Benutzern ein kontinuierliches Security-Awareness-Training ermöglichen. So können sie sicherzustellen, dass sie über die neuesten Phishing-Betrügereien und Social-Engineering-Taktiken informiert sind.

Herrmann zum Lagebild Cybercrime Bayern

Bayerns Innenminister Joachim Herrmann zum Lagebild Cybercrime Bayern 2022: Neuer Höchststand bei der Internetkriminalität - Deutliche Verstärkung der Cybercrimebekämpfung - Mehr IT-Spezialisten

Bayerns Innenminister Joachim Herrmann hat heute in Nürnberg das Lagebild Cybercrime Bayern 2022 vorgestellt. "Das Risiko, in der digitalen Welt Opfer einer Straftat zu werden, ist so groß wie nie zuvor", warnte Herrmann. Die Zahl der Straftaten mit dem Internet als Tatmittel habe 2022 mit 45.065 Fällen in Bayern einen neuen Höchststand erreicht, im Vergleich zum letzten Vor-Corona-Jahr 2019 ein Anstieg um 51,6 Prozent (2019: 29.717 Fälle; 2021: 39.469 Fälle). Darunter fallen beispielsweise Beleidigungen in Sozialen Medien oder Betrugsdelikte auf Auktionsplattformen. Einen nennenswerten Anstieg gab es auch bei der Cybercrime im engeren Sinne, also beim Ausspähen von Daten, Schadsoftware und Computersabotage. Hier verzeichnete die Kriminalstatistik in Bayern von 2019 auf 2022 ein Plus von 10,2 Prozent auf 15.889 Straftaten (2019: 14.420 Fälle, 2021: 15.344 Fälle). Für den Innenminister steht fest: "Wir werden die Cybercrime-Bekämpfung in Bayern deutlich verstärken!"

Gute Nachrichten hatte Herrmann bei der Zahl der aufgeklärten Fälle. Die Aufklärungsquote betrug 2022 bei Fällen mit Tatmittel Internet 52,5 Pro-

Cybercrime Bayern 2022

zent (2019: 49,1 Prozent; 2021: 52,3 Prozent). "In den vergangenen zehn Jahren konnte die Bayerische Polizei die Aufklärungsquote hier um rund zehn Prozentpunkte steigern", so Herrmann (2013: 42,7 Prozent). Die Aufklärungsquote im Bereich von Cybercrime im engeren Sinne lag im vergangenen Jahr bei 31,9 Prozent und damit im längerfristigen Vergleich im Mittelfeld.

Laut Herrmann hat Bayern in den letzten Jahren eine schlagkräftige Cybersicherheitsarchitektur aufgebaut und die Kompetenzen der operativen Behörden und Einrichtungen mit Cybersicherheitsaufgaben in der 2020 geschaffenen 'Cyberabwehr Bayern' gebündelt. Dadurch wird ein regelmäßiger Austausch zu relevanten Cybersicherheitsvorfällen in Bayern und ein abgestimmtes Vorgehen im Angriffsfall sichergestellt. Teilnehmer sind neben der Zentralen Ansprechstelle Cybercrime beim Bayerischen Landeskriminalamt auch das Cyber-Allianz-Zentrum Bayern beim Bayerischen Landesamt für Verfassungsschutz, die Zentralstelle Cybercrime Bayern bei der Generalstaatsanwaltschaft Bamberg, das Landesamt für Datenschutzaufsicht, der Landesbeauftragte für den Datenschutz sowie das Landesamt für Sicherheit in der Informationstechnik.

"Insbesondere bei der Bayerischen Polizei haben wir in den letzten Jahren die Cybercrimebekämpfung deutlich verstärkt", hob der Innenminister hervor. "Aktuell haben wir dort mehr als 400 IT-Spezialisten eingesetzt." Dabei handelt es sich um rund 300 speziell aus- und fortgebildete Ermittler sowie um rund 100 IT-Forensiker, die durch Sicherung und Aufbereitung der digitalen Spuren die Ermittlungen

unterstützen. "Noch in diesem Jahr wollen wir weitere 20 IT-Kriminalisten einstellen", kündigte Herrmann an. Außerdem verwies der Innenminister darauf, dass mittlerweile jede Kriminalpolizeiinspektion über eigene Kommissariate zur Verfolgung schwerwiegender Cybercrime-Delikte verfügt. "Zudem haben wir bei allen Landespolizeipräsidien und dem Landeskriminalamt sogenannte 'Quick-Reaction- Teams' eingerichtet, um schnellstmöglich am Einsatzort digitale Spuren zu sichern", ergänzte Herrmann. Außerdem erprobe derzeit das Polizeipräsidium Oberfranken bundesweit erstmalig den mobilen Einsatz eines vollwertigen IT-Forensiklabors. Dieses beinhaltet alle Geräte zur digitalen Beweissicherung sowie spezielle Arbeitsplätze zum Sichten und Sichern digitaler Beweise, Kostenpunkt 300.000 Euro.

Lagebild Cybercrime Bayern: https://tinyurl.com/5n83kcvc

Kurznachrichten

Tesla

Keine Werbung für Wächter-Modus

Vom Verbraucherzentrale Bundesverband geforderte Untererlassungserklärung abgegeben

Der Autohersteller Tesla (tesla.com) bekennt sich zu irreführender Werbung in Bezug auf die Funktion des "Wächter-Modus", eine Kameraüberwachung beim Parken seiner Fahrzeuge, und hat vor dem Landgericht Berlin eine vom Verbraucherzentrale Bundesverband (vzbv.de) geforderte Untererlassungserklärung abgegeben.

Datenschutzrecht verletzt

Nach Ansicht des vzbv verstößt die kritisierte Nutzung der Funktion im öffentlichen Raum gegen das geltende Datenschutzrecht in Deutschland. "Kameraüberwachung von Dritten ohne deren Wissen, das geht nicht. Verbraucher konnten den Wächter-Modus von Tesla nicht ohne massive Datenschutzverstöße nutzen", sagt vzbv-Vorstand Ramona Pop.

Der Expertein nach riskierten Nutzer ein Bußgeld, wenn der Modus aktiviert war. Diese Info habe in der Werbung für den Wächter-Modus allerdings gefehlt. "Tesla hat nun nach der mündlichen Verhandlung vor dem Landgericht Berlin eine Unterlassungserklärung abgegeben und darf so nicht mehr werben. Das Verfahren zum Wächter-Modus ist damit beendet", so Pop.

Österreich

Unzumutbare Gehwegsicherheit an Wiener Baustellen: „Keine einheitli- chen Standards wie in anderen Ländern“

Bmst Ing. Thomas Korol: "Aktuelle Zeitungsartikel haben mich auf Problem aufmerksam gemacht"

Aktuell sind die Zeitungen voll mit Klagen von Bürgern über fehlende oder schlechte beschilderte Gehsteige bei aktuellen Bauprojekten in Wien. Grundsätzlich gibt es in der STVO §89 + §90 nur sehr unzureichende und nicht verbindliche Vorgaben zu Baustellenabsicherung, um Fußgänger:innen zu schützen. "Ich kenne die Branche und weiß, es wird sich nichts ändern, wenn es nicht zu verpflichtenden Sicherheitsmaßnahmen kommt. Derzeit wird nur nachträglich kontrolliert, wenn tatsächlich ein Unfall passiert ist und Menschen zu Schaden gekommen sind. Kurz gesagt, herrscht an Baustellen in Wien eine unzumutbare Sicherheitslage für Fußgänger und Passanten, weil es keine einheitlichen Baustellensicherheitsstandards wie in Nachbarländern wie Deutschland oder Italien gibt", so der Wiener Baumeister Ing. Thomas Korol.

Schlechte Beschilderung, fehlende Gehwegbrücken, wackelige Holzbalken und Chaos pur

In Wien müssen Fußgängerinnen und Fußgänger an Baustellen unzumutbare Sicherheitsrisiken in Kauf nehmen. Es gibt keine anerkannten Richtlinien, wie Gehwege vor Bauarbeiten gesichert werden müssen. Eine Änderung dieser Situation ist dringend notwendig. Auch der Verkehrsclub Österreich (VCÖ) fordert eine einheitliche und verbindliche Baustellenabsicherungen, um Passanten besser zu schützen. "Fakt ist, sehr oft sind die Baustellen direkt auf einem Gehweg und sehr nachlässig gekennzeichnet und die Gehwege daher nur schlecht gesichert. Kein Wunder, Beschilderungen kosten Geld, also wird da gerne gespart. Dabei wäre eine vernünftige Baustellenabsicherung für die jeweiligen Baufirmen sogar Selbstschutz. Wenn es nämlich zu einem Unfall kommt, dann kann es richtig teuer werden und bei Personenschaden droht den für die Sicherheit Verantwortlichen sogar Gefängnis. Daher sollte das Thema Gehweg-Sicherheit an Baustellen einen höheren Stellenwert bekommen als bisher", so Ing. Korol.

Forderung nach einheitlichen Sicherheitsvorgaben, an die sich alle halten können und müssen

Es ist meist nicht einmal Sparsamkeit oder Mutwilligkeit, wenn die Baustellenbeschilderung und Absicherung an Gehwegen schlecht ist. "Es gibt schlicht keine verbindliche Vorgabe in der STVO, die jeder Baufirma eine klare Auflistung der notwendigen Beschilderungen, Bauzäune und Absicherungsmaßnahmen geben würde, an die sie sich halten könnte. Daher passiert, was eben seit Jahren passiert: Jeder macht, was gerade noch vertretbar ist. Mehr aber auch nicht! Da sollte sich dringend etwas ändern. Auch weil es dann für die Baufirmen mehr Planungssicherheit und auch Rechtssicherheit gäbe. In Deutschland gibt es schon lange einheitliche Richtlinien, die die Sicherheit von Passanten an Baustellen gewährleisten. Das muss sich auch in Wien ändern", so Ing. Thomas Korol.

FH St. Pölten

Größere Reichweite für drahtlose Sensoren

Projekt der FH St. Pölten untersucht mögliche Anwendungen in Smart Homes und Industrie

Smart Homes, Häuser mit unterstützender Technik, verwenden eine Vielzahl an Sensoren für unterschiedlichste Aufgaben. So manche beabsichtigte Funktion scheitert aber an der Reichweite der verwendeten drahtlosen Sensoren. Ein Forschungsprojekt der Fachhochschule St. Pölten arbeitet an einer Technik, um die Reichweiten zu erhöhen. Bewegungs- und Temperatursensoren übernehmen in Smart Homes eine Reihe an Aufgaben, um Geräte zu steuern oder Besitzer*innen zu informieren. Die gängigen Funksensoren haben jedoch nur geringe Reichweiten und können daher nicht überall eingesetzt werden.
Henri Ruotsalainen vom Institut für IT-Sicherheitsforschung der FH St. Pölten arbeitet derzeit an einer Methode, um die Reichweiten der Sensoren zu erhöhen. "Für Anwendungsfälle, bei denen Daten von mehreren lokal montierten Sensoren drahtlos über größere Entfernungen übertragen werden müssen, gibt es derzeit keine brauchbare Technologie. In unserem Projekt LoRaBridge entwickelten wir eine Datenbrücke, mit der Daten von lokalen Sensoren über größere Entfernungen an einen Server gesendet werden können", sagt Ruotsalainen.

Eine der Zielgruppen sind Privatpersonen, die gerne Sensoren oder Smart-Home-Komponenten im Keller,

am Dachboden oder im Garten montieren möchten, aber daran scheitern, dass die Reichweite einer Funkverbindung nicht groß genug ist, um Daten über solche Distanzen abrufen zu können. Ruotsalainen hat die Technologie sowohl in Innenräumen eines großen Bürogebäudes als auch im Freien umfassend getestet: "Unsere Messkampagne in Langenlois hat gezeigt, dass die kostengünstigen Sensoren auch für die Frosterkennung in Weinfeldern eingesetzt werden können".

Einsatz in der Industrie

"Derzeit ist der Chipmangel ein großes Problem. Hardware ist oft teuer. Mit unserer Lösung können wir günstige Sensoren mit niedriger Reichweite in solche mit langer Reichweite umwandeln", erklärt Ruotsalainen.
Auch Anwendungen in der Industrie sind denkbar. Dazu will Ruotsalainen die Technik mit anderen Sensoren und mit Drittanbieter*innen untersuchen und weiterentwickeln. Beispiele für mögliche Anwendungsfälle sind Füllstandserfassung von Mülltonnen, Monitoring von Parkplätzen oder Waldbrandfrüherkennung. "Unsere Datenbrücke achtet auf Sicherheit, Flexibilität, modulare Einsätze und kann an verschiedene Bedürfnisse angepasst werden. Die Technik steht als Open Source allen Interessierten zur Verfügung", so Ruotsalainen. Das Projekt wurde von der Initiative NetIdee gefördert.
[https://tinyurl.com/2p8hb79c]

Über die Fachhochschule St. Pölten

Die Fachhochschule St. Pölten ist Anbieterin praxisbezogener und leistungsorientierter Hochschulausbildung zu den Themen Medien, Kommunikation, Management, Digitale Technologien, Informatik, Security, Bahntechnologie, Gesundheit und Soziales. In 6 Departments bieten 26 Studiengänge und zahlreiche Weiterbildungslehrgänge ca. 3.700 Studierenden eine zukunftsweisende Ausbildung. Hierbei werden Lehre und Forschung eng verzahnt. Als European University leitet die FH St. Pölten die europäische Hochschulallianz E³UDRES² (Engaged and Entrepreneurial European University as Driver for European Smart and Sustainable Regions) und arbeitet mit Hochschulen aus 9 Partnerländern an Konzepten für die Hochschule der Zukunft sowie an der Entwicklung smarter und nachhaltiger europäischer Regionen.

Universität Tokio

Emoji-User verbergen eigenen Gemütszustand

Wissenschaftlerin der Universität Tokio warnt vor Verlust authentischer Emotionen im Internet

Wer anderen auf elektronischen Weg bittere Wahr- oder Unwahrheiten an den Kopf wirft, garniert sie gern mit einem versöhnlich wirkenden Emoji. "Da Online-Sozialisierung immer häufiger wird, haben sich die Menschen daran gewöhnt, ihre Ausdrücke zu verschönern und die Angemessenheit ihrer Kommunikation zu überprüfen", sagt Moyu Liu von der Uni- versität Tokio*, die sich wissenschaftlich intensiv mit der Emoji-Vergabe befasst hat. "Mir wurde dabei klar, dass wir dadurch den Kontakt zu unseren authentischen Emotionen verlieren können."

Emotionale Erschöpfung droht

Liu hat 1.289 Teilnehmer rekrutiert, alle Benutzer von Simeji, der am häufigsten heruntergeladenen Emoji-Tastatur in Japan. Damit sollte untersucht werden, wie User Emojis verwenden. Sie können Emotionen ausdrücken oder sie vertuschen. Frühere Forschungen hatten gezeigt, dass Menschen Emojis als funktionale Äquivalente von Gesichtsausdrücken verwenden, aber nicht die Beziehungen zwischen wirklichen und kaschierten Emotionen."Wenn die Diskrepanz zwischen den Emotionen, die Sie erleben, und den Emotionen, die Sie ausdrücken, zu groß ist, kann sich emotionale Erschöpfung entwickeln", warnt Liu. Die Teilnehmer haben zudem demografische Daten preisgegeben, Fragen zu ihrem subjektiven Wohlbefinden beantwortet und angegeben, wie oft sie Emojis nutzen. Sie erhielten Botschaften mit unterschiedlichen sozialen Kontexten, reagierten wie gewohnt darauf und bewerteten die Intensität des Ausdrucks ihrer Emotionen.

Echte Emotionen nur für Freunde

Laut Liu geben Menschen Emotionen mit Emojis wahrheitsgemäß eher im privaten Kontext mit engen Freunden preis. Die Befragten haben die geringsten Emotionen gegenüber Personen mit höherem Status gezeigt. Intensive Gefühlsausdrücke kamen mit passenden Emojis, es sei denn, die Menschen hatten das Bedürfnis, ihre wahren Emotionen zu maskieren, indem sie lächelnde Emojis verwendeten. Negative Emojis wurden nur dort verwendet, wo sehr starke negative Gefühle ins Spiel kamen. Das Aus- drücken von Emotionen mit Emojis war mit einem höheren subjektiven Wohlbefinden verbunden als das Verstecken von Emotionen. "Da Online-Sozialisierung immer häufiger wird, ist es wichtig zu überlegen, ob wir uns dadurch mehr von unseren wahren Emotionen lösen", so Liu abschließend. * (www.u-tokyo.ac.jp/en)

University of Sheffield

Kamera sagt Vulkanausbrüche sicher vorher

Ohne großen Personalaufwand betriebenes Gerät registriert mit Schwefeldioxid die Vorboten +

Mit einer neuen, relativ kostengünstigen Kamera von Forschern der University of Sheffield* kommen Vulkanologen der Vorhersage katastrophaler Ausbrüche ein gutes Stück näher. Sie soll mit einem Preis von 5.000 Dollar deutlich billiger sein als die bisher genutzten Kameras, die schnell 20.000 Dollar und mehr kosten. Damit wird die dauerhafte Überwachung von Vulkanen an deutlich mehr Standorten möglich als bisher, heißt es.

Sensor wie im Smartphone

Die Kamera kann Schwefeldioxid (SO_2) detektieren, auch in kleinen Mengen. Dieses ätzende Gas ist oft Vorbote eines Ausbruchs. "Unser Instrument verwendet einen Sensor, der dem in Smartphones nicht unähnlich ist. Wir haben den Sensor modifiziert, um ihn für ultraviolettes Licht empfindlich zu machen, wodurch der Nachweis von SO_2 möglich wird", sagt Geowissenschaftler Thomas Wilkes. "Wo immer es ging, haben wir Teile der Kamera im 3D-Druck hergestellt, um die Kosten niedrig zu halten. Außerdem setzen wir eine benutzerfreundliche, frei verfügbare Software ein, mit der das Gerät gesteuert und die erfassten Daten robust verarbeitet werden können", so Wilkes. Der Stromverbrauch sei bei einer Leistungsaufnahme von 3,75 Watt so gering, dass er von einem kleinen Solarmodul gedeckt werden kann, das neben den Koffer mit der Kamera platziert wird.

Kamera arbeitet autonom

Gasemissionen sind Manifestationen von Aktivitäten unter der Oberfläche eines Vulkans. Durch deren Messung können Forscher quasi in den Vulkan

hineinschauen. Das ist entscheidend für die Vorhersage von Ausbrüchen. Seit Mitte der 2000er-Jahre sind SO2-Kameras zu wichtigen Instrumenten für diese Messung geworden. Doch abgesehen von den hohen Kosten für diese Geräte können sie nicht zur Langzeitüberwachung eingesetzt werden, weil Personal zur Bedienung unumgänglich ist. Die neue Kamera arbeitet dagegen vollkommen autonom.Wilkes und sein Team haben die neue Kamera bisher an den Vulkanen Lascar in Chile, und Kilauea auf der zu Hawaii gehörenden Insel Big Island getestet. Obwohl die Ergebnisse zufriedenstellend waren, sehen die Forscher noch weiteren Entwicklungsbedarf. Die Qualität der Daten hänge stark von den meteorologischen Verhältnissen ab. "Sie funktio-

niert am besten bei strahlend blauem Himmel und wenn die vulkanische Gaswolke sich in einem 90-Grad-Winkel zur Blickrichtung der Kamera bewegt", schließt Wilkes.

* www.sheffield.ac.uk

Cricket Wireless

Mobile Apps läuten Ende von Webseiten ein

70 Prozent der US-Bürger sehen Laptops oder klassische Standgeräte mehr und mehr aussterben

Apps auf Smartphones werden in den nächsten Jahren klassische Webseiten ersetzen. Das sagen 70 Prozent der erwachsenen US-Bürger in einer neuen OnePoll*-Umfrage unter 2.000 Personen im Auftrag des Prepaid-Mobilfunkanbieters Cricket Wireless**. Das Smartphone tritt demnach an die Stelle von PC und Laptop. 26 Prozent der Befragten können sich bereits vorstellen, wenigstens ein Jahr lang ganz auf einen Standard-Computer-Browser zu verzichten.

Tagespensum per Smartphone

Während 69 Prozent ihr Smartphone täglich nutzen, sind es bei Desktop oder Laptop nur 44 Prozent. 46 Prozent erledigen ihr Tagespensum sogar vollständig von ihrem Smartphone aus.

Die Umfrage zeigt auch, dass sich 59 Prozent für ihr Telefon entscheiden würden, wenn sie gezwungen wären, zwischen einem Smartphone und einem Computer zu wählen. 36 Prozent sagen, dass sie nicht einmal einen einzigen Tag ohne ihr Smartphone auskommen könnten.

Andererseits behaupten 34 Prozent der iPhone-Nutzer, dass sie eine Woche lang telefonlos überleben könnten. In der Andorid-Riege sind es nur 21 Prozent. Unterhaltungs- (67 Prozent) und Kommunikations-Apps (66 Prozent) werden am meisten genutzt. Doch weit mehr Befragte haben eine Finanz-App (59 Prozent), während es bei Nachrichten-/Zeitschriften-Apps nur 28 Prozent sind.

Lebensmittel und Kleiderkauf

"Ob Arbeit oder Spielen: Menschen nehmen den Komfort von Apps in allen Lebensbereichen an. Apps können auch eine großartige Möglichkeit sein, alternative Dienste auszuprobieren, bevor Sie sich verpflichten", sagt Tony Mokry, Vice President & Chief Marketing Officer bei Cricket Wireless. 52 Prozent verlassen sich auf zudem Apps, um ihre Steuern einzureichen, verglichen mit 36 Prozent, die es "zu Fuß" erledigen. 51 Prozent managen den Einkauf von Lebensmitteln ausschließlich per App. Beim Fotografieren und Aufnehmen von Videos sind es ebenfalls 51 Prozent, beim Kleiderkauf 47 Prozent. Beim Lesen von Büchern und Zeitschriften sind es 38 Prozent.

* www.onepoll.com
** www.cricketwireless.com

University of California

Handy-Eltern: Emotionale Intelligenz leidet

Kinder suchen die Aufmerksamkeit von Erwachsenen und sollten dabei nicht enttäuscht werden

Die emotionale Intelligenz von Kindern wird durch die Smartphone-Nutzung ihrer Eltern beeinträchtigt, wenn sie auf das Display starren, während ihr Kind in der Nähe ihre Aufmerksamkeit sucht. Das zeigt eine Untersuchung von Robin Nabi von der University of California, Santa Barbara (www.ucsb.edu).

Lernen, üben, weiterentwickeln

Emotionale Intelligenz ist eine Reihe von mentalen Fähigkeiten, die es einer Person ermöglichen, ihre emotionalen Zustände zu erkennen, zu verstehen und zu verwalten. Laut Nabi werden Babys mit einem gewissen Maß an emotionaler Intelligenz geboren. Aber es ist auch eine Fähigkeit, die erlernt, geübt und entwickelt werden kann, und sie variiert von Person zu Person, so die Kommunikationswissenschaftlerin.

"Manche Menschen sind sehr gut darin, Emotionen wie Angst oder Wut zu beherrschen, andere nicht", verdeutlicht Rabin. Menschen mit höher entwickelter emotionaler Intelligenz würden dazu neigen, befriedigendere persönliche Beziehungen und mehr Erfolg in ihrem Arbeitsleben zu haben. Im Allgemeinen können sie sich auch über ein höheres Wohlbefinden freuen.
"Wir wissen, dass die Art und Weise, wie Eltern Emotionen ausdrücken, reflektieren und mit ihren Kindern darüber sprechen, deren Entwicklung der emotionalen Intelligenz beeinflusst.

Und wir wissen auch, dass Eltern oft in ihre Telefone vertieft sind, was die Interaktion und das Feedback, das sie ihren Kindern geben, einschränken könnte", betont die Forscherin.

400 Eltern zielgerichtet befragt

Nabi und ihr Team haben 400 Eltern von Kindern im Alter von fünf bis zwölf Jahren befragt. Unter anderem sollten sie die emotionale Intelligenz ihrer Kinder und deren Sorge um andere bewerten.
Sie berichten auch über deren Nutzung von Medien wie Fernsehen, Computer, Spielkonsolen, Tablets und Smartphones, und darüber, wie oft ihre Kinder Aktivitäten wie Lesen, Musik hören und Spielen im Freien und in Innenräumen nachgehen. Andererseits berichten die Eltern über die Zeit, die sie sie selbst in Anwesenheit ihrer Kinder mit digitalen Geräten verbringen und wie oft sie dabei Gespräche mit ihren Kindern angefangen haben.

Es stellte sich heraus, dass allein die Smartphone-Nutzung einen Einfluss auf die Entwicklung der emotionalen Entwicklung der Kinder hat. "Telefone können uns helfen, uns zu entspannen, mit der Familie Kontakte zu pflegen und interessante Dinge über die Welt zu lernen. Sie können aber auch problematisch sein, je nachdem, wie wir sie verwenden. Dazwischen muss die Balance gefunden werden", schließt Nabi.

Proxyjacking ist dem Chat beigetreten

Eine neue Einnahmequelle für Angreifer gewinnt an Bedeutung - Von Crystal Morin

Wussten Sie, dass Sie mühelos ein kleines passives Einkommen erzielen können, indem Sie einfach eine Anwendung auf Ihren Heimcomputern und Mobiltelefonen laufen lassen? Sie ermöglicht es anderen, die eine Gebühr an einen Proxy-Dienstanbieter zahlen, sich Ihre IP-Adresse zu leihen, um z. B. ein YouTube-Video anzusehen, das in ihrer Region nicht verfügbar ist, uneingeschränkt im Internet zu surfen oder dubiose Websites zu besuchen, ohne dass die Aktivitäten ihrer eigenen IP-Adresse zugeordnet werden. Wie bei allen Dingen können böswillige Akteure einen Vorteil daraus ziehen. In dieser Situation können sie in Ihrem Namen – ohne Ihr Wissen – Bandbreite verkaufen, um bis zu 10 US-Dollar pro Monat für jedes kompromittierte Gerät zu verdienen und Sie gleichzeitig zusätzlichen Kosten und Risiken auszusetzen.

Das Threat Research Team von Sysdig (Sysdig TRT) entdeckte einen neuen Angriff, der als Proxyjacking bezeichnet wird und die Log4j-Schwachstelle für den Erstzugang ausnutzt. Anschließend verkaufen die Angreifer die IP-Adressen der Opfer gewinnbringend an Proxyware-Dienste. Während Log4j-Angriffe häufig vorkommen, war die in diesem Fall verwendete Nutzlast ungewöhnlich. Anstelle des typischen Cryptojakking- oder Backdoor-Payloads installierte der Angreifer einen Agenten, der das kompromittierte Konto in einen Proxy-Server verwandelte und es dem Angreifer ermöglichte, die IP-Adresse an einen Proxyware-Dienst zu verkaufen und den Gewinn einzustreichen.

Was ist Proxyjacking?

Es ist ein neues Phänomen, das durch die Zunahme und Nutzung von Proxyware-Diensten in den letzten Jahren entstanden ist. Ein Proxyware-Dienst ist eine völlig legitime und nicht bösartige Anwendung oder Software, die Sie auf Ihren mit dem Internet verbundenen Geräten installieren können und mit der Sie Ihre Internet-Bandbreite mit anderen

teilen, die für die Nutzung Ihrer IP-Adresse bezahlen. Diese Dienste, wie z. B. IPRoyal, Honeygain, Peer2Profit und andere, bezahlen Sie für jede IP-Adresse, die Sie freigeben, auf der Grundlage der Anzahl der Stunden, in denen Sie die Anwendung ausführen. Diese Dienste wurden bei Adware-Angriffen eingesetzt, über die die Cisco Talos Intelligence Group und das AhnLab Security Response Center (ASEC) bereits berichtet haben. Proxyware- Dienste ermöglichen es einem Benutzer, Geld zu verdienen, indem er seine Internetverbindung mit anderen teilt. Wie Talos in ihrem Blog-Post erklärt, nutzen Angreifer diese Plattformen, um die Internet-Bandbreite der Opfer zu monetarisieren, ähnlich wie bösartiges Cryptocurrency-Mining versucht, die CPU-Zyklen infizierter Systeme zu monetarisieren.

Das Verdienstpotenzial von Proxyjacking

Auf breiter Ebene könnte diese Kampagne den Angreifern ein lukratives Einkommen verschaffen. Laut der Gewinnskala von pawns[.]app bringt eine 24-stündige Aktivität für eine IP-Adresse 9,60 US-Dollar pro Monat ein. Während Pawns Kontrollen durchführt, um sicherzustellen, dass der Nutzer keine Cloud-Instanz wie EC2 verkauft, gelten für Peer2Profit nicht dieselben Einschränkungen. Wie bereits erwähnt wurde, geschah der erste Zugang in unserem Honeypot durch Ausnutzung einer Log4j-Schwachstelle. Millionen von Systemen laufen immer noch mit anfälligen Versionen von Log4j und laut Censyssind mehr als 23.000 davon über das Internet erreichbar. Log4j ist nicht der einzige Angriffsvektor für die Verbreitung von Proxyjacking-Malware, aber allein diese Schwachstelle könnte theoretisch mehr als 220.000 Dollar Gewinn pro Monat einbringen. Konservativer ausgedrückt: Eine bescheidene Kompromittierung von 100 IPs bringt ein passives Einkommen von fast 1.000 Dollar pro Monat.

Kryptomining und Proxyjacking

Cryptojacking ist die unbefugte Nutzung eines Computers oder Geräts zum Mining von Kryptowährungen. In der häufigsten Form installieren Angreifer CPU-basierte Miner, um den maximalen Wert aus den kompromittierten Systemen zu ziehen (die nur sehr selten über GPUs verfügen, wodurch die häufigeren GPU-basierten Miner obsolet werden). Proxyjacking, wie es in diesem Beitrag definiert wird, kann als Gegenstück zu Cryptojacking betrachtet werden, da es hauptsächlich darauf abzielt, Netzwerkressourcen zu nutzen und dabei nur einen minimalen CPU-Fußabdruck zu hinterlassen. Sowohl Kryptojacking als auch Proxyjacking können einem Angreifer monatlich etwa den gleichen Geldbetrag einbringen – Proxyjacking könnte bei den aktuellen Kryptowährungskursen und Proxyware-Auszahlungen sogar profitabler sein. Proxyjacking ist jedoch in Systemüberwachungssoftware nicht annähernd so sichtbar wie Kryptojakking. Fast jede Überwachungssoftware hat die CPU-Auslastung als eine der ersten (und zu Recht wichtigsten) Messgrößen. Die Auswirkungen von Proxyjacking auf das System sind jedoch marginal – 1 GB Netzwerkverkehr, verteilt über einen Monat, sind einige MB pro Tag, die sehr wahrscheinlich unbemerkt bleiben.

Auswirkungen

Ein Proxyjacking-Angriff kann als lästige Malware und nicht als ernsthafte Bedrohung unterschätzt werden, wie es beim Cryptomining häufig der Fall ist. Auch wenn diese Art von Angriff nicht direkt zur Zerstörung von Daten oder zum Diebstahl von geistigem Eigentum führt, könnte dies eine indirekte Folge sein, wie in der SCARLETEEL-Analyse berichtet wurde. Ein Proxyjacking-Angriff kann sich auf zwei Arten negativ auf ein Unternehmen auswirken:

1. Finanzielle Folgen

Proxyjacking verursacht, ähnlich wie Kryptojacking, finanzielle Kosten für die Opfer. Im Falle von Diensten, die bei einem Cloud-Service-Anbieter (CSP) laufen, könnten diese gemessen werden. AWS beispielsweise erhebt Gebühren auf der Grundlage der Menge des Datenverkehrs, der über das Internet nach außen geleitet wird. Proxyjacking-IP-Verkehr geht für jede Instanz, auf der der Agent läuft, sowohl ein- als auch auswärts. Der Agent verbraucht auch CPU und Speicher, was die Kosten für das Opfer weiter erhöht.

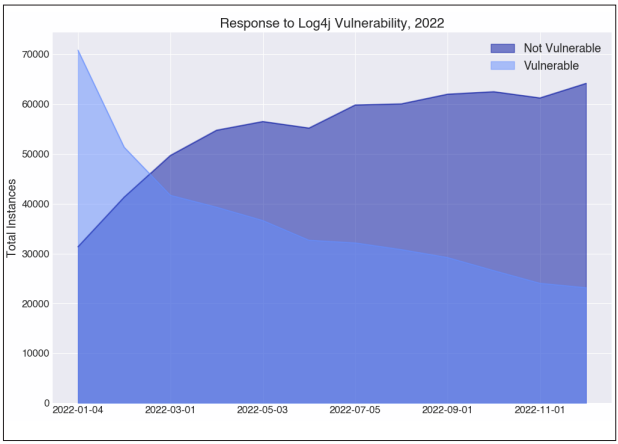
Da jeder CSP eine andere Abrechnungsmethode hat, ist es wichtig zu verstehen, wie man bei einem solchen Vorfall betroffen sein könnte. Es ist zwar bekannt, dass CSPs die durch Malware entstandenen Kosten verzeihen, aber es gibt keine Garantie dafür, dass diese Praxis auch in Zukunft beibehalten wird. Ein solcher Angriff könnte, vor allem wenn er sich in interner Infrastruktur ausbreitet, zu einer erheblichen finanziellen Belastung führen.

2. Reputation/ Rechtliche Folgen

Wenn wissentlich oder unwissentlich Internet-Bandbreite an einen Proxyware-Dienst verkauft wird, gibt es keine Garantie, dass diese nicht für böswillige oder illegale Aktivitäten genutzt wird.

Ein Akteur kann genauso leicht ein gemeinsam genutztes Internet kaufen und für einen Angriff nutzen. Viele böswillige Angreifer verwenden Proxys, um ihre Befehls- und Steuerungsaktivitäten und Identifizierungsinformationen zu verschleiern.

Laut Vista Criminal Law ist eine IP-Adresse häufig der Ausgangspunkt für Ermittlungen, und der Haupteigentümer oder -nutzer der IP ist in der Regel nicht an der illegalen Aktivität beteiligt. Mit der Verschleierung durch den Proxyware-Dienst scheint der Angriff nun von einem ihrem Netzwerk auszugehen; Sie und Ihr Netzwerk sind nun potenziell in die Ermittlungen der Strafverfolgungsbehörden verwickelt.



Zusammenfassung

Proxyjacking ist ein Angriff mit geringem Aufwand und hohem Gewinn für die Bedrohungsakteure, der weitreichende Folgen haben kann. Die Liste der Proxyware-Dienste, von denen berichtet wird, dass sie für Proxyjacking genutzt werden, ist im Moment noch klein, aber mit der Zeit werden die Angreifer einen Weg finden und die Verteidiger werden weitere ruchlose Aktivitäten aufdecken. Das Sysdig TRT empfiehlt die Einrichtung von Abrechnungsgrenzen und Warnmeldungen beim CSP, um den Erhalt von möglicherweise schockierenden Rechnungen zu vermeiden. Außerdem sollten Regeln für die Erkennung von Bedrohungen eingerichtet werden, um bei den ersten Zugriffs- und Nutzdatenaktivitäten vor der Installation einer Proxyware-Anwendung im Netzwerk Alarm zu schlagen. Bei dem von Sysdig TRT entdeckten Proxyjacking-Angriff zielten die Angreifer auf Kubernetes-Infrastruktur ab, insbesondere auf einen ungepatchten Apache Solr-Dienst, um die Kontrolle über den Container zu übernehmen und ihre Aktivitäten fortzusetzen.

Crystal Morin: Threat Research Engineer

Crystal ist Threat Research Engineer bei Sysdig und beschäftigt sich mit der Entdeckung und Analyse von Cyber-Bedrohungsakteuren in Cloud- und Container-Umgebungen. Crystal begann ihre Karriere als Linguistin und Geheimdienstanalystin bei der United States Air Force. Bevor sie zu Sysdig kam, war sie vier Jahre lang als Auftragnehmerin für Booz Allen Hamilton tätig, wo sie über Terrorismus und Cyberbedrohungen forschte und berichtete. Crystal war für die Bildung und Weiterentwicklung von Booz Allens Cyber-Bedrohungsintelligenz Community und Fähigkeiten zur Bedrohungsjagd verantwortlich.

Sysdig: Das Untermehmen

Sysdig treibt den Standard für Cloud- und Containersicherheit voran. Mit unserer Plattform können Sie Software-Schwachstellen finden und priorisieren, Bedrohungen und Anomalien erkennen und darauf reagieren sowie Cloud-Konfigurationen, Berechtigungen und Compliance verwalten.
Sie erhalten eine zentrale Ansicht des Risikos vom Sourcecode bis zum Betrieb - ohne blinde Flecken und ohne Blackboxes. Mit Falco haben wir den den Open-Source-Standard für Cloud-native Bedrohungserkennung entwickelt. Die größten Unternehmen der Welt vertrauen auf Sysdig

Eine Frage der Ethik

„Zeit für die Industrie, sich zu engagieren", denn die Nutzer von Sicherheitskameras wenden sich von unethischen Marken ab

Eine neue, von Hanwha Techwin in Auftrag gegebene Studie zeigt, wie sehr die Nutzer darauf achten, dass die ihnen zur Verfügung stehenden Videokameras von einem seriösen Hersteller produziert und verantwortungsvoll eingesetzt werden.

Fast drei Viertel (73 %) der europäischen Sicherheitsmanager sind der Meinung, dass es wichtig ist, ihre Kameras von Herstellern zu beziehen, die den verantwortungsvollen Einsatz von Sicherheitstechnologie unterstützen, während fast 9 von 10 (89 %) deutschen Sicherheitsmanagern der Meinung sind, dass Überwachungstechno- logie, wie z. B. Videokameras, verantwortungsvoll eingesetzt werden sollte.

Die Umfrage unter mehr als 600 Sicherheitsverantwortlichen mittlerer bis großer Organisationen in Deutschland, Großbritannien, den Niederlanden, Frankreich und Italien wurde von Research Without Barriers im Dezember 2022 für den südkoreanischen Videoanbieter Hanwha Techwin durchgeführt.

„Genauso wie wir es auf den Märkten für Verbrauchertechnologie gesehen haben, suchen kommerzielle Videokameranutzer mehr als nur niedrige Kosten: Sie wollen mit Marken zusammenarbeiten, die verantwortungsvolle Nutzung, Datensicherheit und ethische Herstellung in den Mittelpunkt stellen", sagt Uri Guterman, Head of Product & Marketing von Hanwha Techwin Europe.

Die europäischen Behörden haben vor den Risiken gewarnt, die mit dem Einsatz von Videoüberwachungsanlagen bestimmter Hersteller verbunden sind, da sie befürchten, dass die Technologie ein Sicherheitsrisiko darstellt und die Kameras auf unethische Weise eingesetzt werden. Im Jahr 2021 stimmte das EU-Parlament dafür, die Kameras eines Herstellers aus den Parlamentsgebäuden zu entfernen, da es immer wieder Behauptungen über den unethischen Einsatz der Kameras dieses Herstellers gab.

Möglicherweise als Reaktion auf diese Befürchtungen hat die Studie ergeben, dass mehr als jeder zweite deutsche Sicherheitsmanager (51 %) davon ausgeht, dass eine ähnliche Gesetzgebung wie der NDAA (National Defense Authorization Act) der USA, der den Verkauf und die Verwendung von Videotechnologie bestimmter Hersteller einschränkt, irgendwann auch in Deutschland Gesetz wird. In der Tat würde jeder zweite (50 %) deutsche Sicherheitsverantwortliche die Einführung einer Version des NDAA in seinem Land unterstützen.

Die Studie zeigt auch, dass mehr als einer von zwei (52 %) deutschen Sicherheitsverantwortlichen in der Lage ist, zwischen Sicherheitsanbietern und -herstellern zu unterscheiden, wenn es um den ethischen Einsatz von Überwachungstechnologie geht. Dies scheint alle Versuche unseriöser Marken zu untergraben, die Sicherheitsbedrohungen und den unethischen Gebrauch ihrer Kameras herunterzuspielen.

„Wie in anderen Technologiebereichen weht auch in der Videoüberwachungsbranche ein frischer Wind", sagt Guterman. „Unsere Untersuchung zeigt deutlich, dass Entwicklungen wie KI am Rande des Systems die Videokamerasysteme zwar leistungsfähiger machen, die Nutzer aber die größeren Einblicke und die Kontrolle, die sie durch diese Technologie gewinnen, mit der Gewissheit in Einklang bringen wollen, dass sie auf verantwortungsvolle Weise genutzt und geliefert wird."

Mit Blick auf das starke Gefühl, das die Sicherheitsmanager in der Studie zum Ausdruck brachten, ruft Guterman die gesamte Branche dazu auf, die Anforderungen der Nutzer zu erfüllen: „Das Wachstum der europäischen Sicherheitsbranche – und die erfolgreiche Ausweitung der Videotechnologie über die typischen Sicherheitsanwendungen hinaus zur Erzielung größerer Geschäftseffizienzen – hängt davon ab, dass Hersteller und Errichter gleichermaßen die Forderungen der Nutzer nach einer verantwortungsvollen Nutzung in den Mittelpunkt ihres Handelns stellen. Es ist an der Zeit, dass die Industrie einen Schritt nach vorne macht.

Report: tinyurl.com/5n6fmzsj

The Industry Report:
2023 State of Security and Identity

HID-Umfrage: Trends und Sorgen der Sicherheitsbranche

HID, internationaler Anbieter von vertrauenswürdigen Identitätslösungen, veröffentlicht seinen neuen „State of the Security Industry Report". Der Branchenbericht enthält die Ergebnisse einer Umfrage unter 2.700 internationalen Partnern, Endanwendern sowie Sicherheits- und IT-Mitarbeitern.

Im Mittelpunkt der Untersuchung stehen branchentypische Innovationen und Technologien, aber auch aktuelle Herausforderungen. Die Umfrageergebnisse aus dem Herbst 2022 zeigen folgende fünf große Themen:

1. Nachhaltigkeit

87 % der Befragten gaben an, dass Nachhaltigkeit für ihre Kunden „wichtig bis sehr wichtig" ist. Sie beobachteten, dass Endverbraucher zuneh- mend Transparenz in Bezug auf Betriebsabläufe, Produktbeschaffung sowie Forschungs- und Entwicklungspraktiken von Unternehmen verlangen. Um dieser wachsenden Nach- frage gerecht zu werden, nutzten Sicherheitsteams verstärkt die Cloud und IoT, um Prozesse zu optimieren und Ressourcen zu schonen. Darüber hinaus werden neue Produkte und Lösungen strategisch entwickelt, um eine bewusste Energienutzung, Abfallreduzierung und Ressourcenoptimierung zu erreichen.

2. Hybrid Work

Hybrid Work hat sich durchgesetzt: 81

% der Umfrageteilnehmer gaben an, dass sie ihren Angestellten ermöglichen, im Büro und auch dezentral zu arbeiten.
Um sicheren Zugriff bei der Remote-Arbeit zu garantieren, schätzten 67 % Multifaktor-Authentifizierung und passwortlose Authentifizierung als die wichtigsten Methoden ein, während 48 % auf die Bedeutung mobiler und digitaler IDs hinwiesen. Allerdings zeigt die Umfrage auch, dass fast die Hälfte der befragten Unternehmen noch nicht bereit ist, eine umfassende Identity-as-a-Service-Strategie zu implementieren. Solche Tools wären aber die Basis, um die Sicherheit zu erhöhen und die Kosten zu senken.

3. Digitale IDs

Identifizierung und Authentifizierung erfolgen immer häufiger über mobile Geräte wie Smartphones und Wearables. Die wachsende Beliebtheit digitaler Geldbörsen von Anbietern wie Google, Apple und Amazon ist einer der Hauptgründe für diesen Trend. Dank erweiterter Funktionen können Smartphone-Nutzer zum Beispiel Schlüssel, Ausweise und digitale Dokumente direkt in einer Wallet-App aufbewahren. Dazu gehören, je nach Land, etwa COVID-19-Impfinformationen, Mitarbeiterausweise, Studentenausweise, Hotelzimmerschlüssel und Führerscheine.
Gewerbliche Immobilienunternehmen (40 %) lagen bei den digitalen IDs vorn, da große Immobilienfirmen den mobilen Zugang als Teil ihrer Mieter-Apps nutzen, ergab die HID-Umfrage.

4. Biometrie

Immer mehr biometrische Identitätsmanagementlösungen ergänzen oder lösen konventionelle Zugangskontrollsysteme ab. Das Verwenden biometrischer Daten wie Finger-

IDC: Ausgaben für Sicherheit in Europa wachsen 2023 um 10,6 %, an getrieben vom Finanzsektor

Wachsende Sicherheitsbedürfnisse, neue Vorschriften und das zunehmende Risiko von Ransomware-Angriffen aufgrund der aktuellen geopolitischen Lage treiben die europäischen Sicherheitsausgaben weiter an. Laut dem Worldwide Security Spending Guide von IDC werden die Gesamtausgaben in Europa bis 2023 um 10,6 % steigen. Die Ausgaben in der Region werden im Prognosezeitraum weiterhin fast zweistellig wachsen und im Jahr 2026 insgesamt 71 Milliarden US-Dollar erreichen.

Großbritannien, Deutschland und Frankreich sind die Spitzenreiter bei den Ausgaben für Sicherheit und machen zusammen mehr als die Hälfte des europäischen Sicherheitsmarktes aus. In Mittel- und Osteuropa wird die Tschechische Republik im Jahr 2023 mit über 12 % das schnellste Wachstum aufweisen.

"Die IDC-Studie zeigt, dass anhaltende Störungen und eine dynamische Bedrohungslandschaft europäische Unternehmen dazu veranlasst haben, ihre Cyber-Resilienz zu überdenken und proaktiv sicherzustellen, dass ihre Organisation eine gute Cyber-Hygiene aufrechterhält", sagte Romain Fouchereau, Research Manager, IDC European Security.
"Die Einführung von Zero-Trust-Prinzipien, um Sicherheitsmaßnahmen zu verstärken und sichere Zugangskontrollen über Netzwerke, Anwendungen und Geräte hinweg zu imple- mentieren, hat oberste Priorität, wobei eine definierte Strategie und die Unterstützung der Geschäftsleitung für neue Investitionen und Initiativen erforderlich sind."

abdruck oder Gesicht als zusätzlichen Authentifizierungsfaktor hilft Unternehmen dabei, unbefugten Zugang und Betrug zu verhindern.

Die Bedeutung dieses Trends wird durch die Umfragedaten veranschaulicht, aus denen hervorgeht, dass 59 % der Befragten derzeit biometrische Technologien einsetzen, deren Implementierung planen oder zumindest in naher Zukunft testen möchten.

5. Versorgungsprobleme

Probleme in der Lieferkette sind nach wie vor ein besorgniserregender Faktor, aber die Befragten zeigten sich auch optimistisch. 71 % denken, dass dieses Thema die Branche auch 2023 beschäftigen wird; 74 % waren im Jahr 2022 selbst von Problemen in der Lieferkette betroffen. Es zeichnet sich auch Zuversicht ab, denn die Hälfte aller Befragten schätzt, dass sich die Bedingungen in diesem Jahr verbessern werden. Am stärksten betroffen sind gewerbliche Immobilienunternehmen: Für 78 % sind Probleme in der Lieferkette die größte Sorge.

„Gesellschaftliche und wirtschaftliche Trends von großer Tragweite haben unser Business as usual verändert", betont Matt Winn, Senior Director, Public Relations and Corporate Communications bei HID. „Die Sicherheitsbranche steht also vor der Herausforderung, die Grundlagen bis hin zum ganzen Konzept der Identität zu überdenken.

Für diesen Umbruch nutzen wir neue Technologien, um Sicherheitslösungen intelligenter zu gestalten. Die Ergebnisse unserer Studie zeigen, in welche Richtung sich die Branche entwickelt, und geben wichtige Impulse, um außergewöhnliche digitale und physische Erlebnisse zu bieten."

Umfrage in englischer Sprache: https://tinyurl.com/bdzdx6mx

Die europäischen Ausgaben für Software werden im Jahr 2023 mit einem Wachstum von ca. 11 % im Vergleich zum Vorjahr an der Spitze stehen, aber Sicherheitsdienstleistungen werden im Jahr 2023 die größten Ausgaben verzeichnen, was ihre Schlüsselrolle für europäische Unternehmen aller Branchen widerspiegelt.

"Wir stellen fest, dass europäische Unternehmen neben Software und Hardware auch einen sehr realen Bedarf an Sicherheitsdienstleistungen haben, um ihren kontinuierlichen Betrieb und die Einhaltung von Vorschriften zu gewährleisten", sagt Vladimir Zivadinovic, Senior Research Analyst, IDC European Data and Analytics.

"Dies gilt insbesondere für Unternehmen mit begrenzten Kompetenzen im Bereich Sicherheit, vor allem für KMUs in weniger digital ausgereiften Branchen wie Medien, Fertigung und Gesundheitswesen."

Im Jahr 2023 wird der Finanzsektor die höchsten Ausgaben in Europa haben, getrieben von der Notwendigkeit des Datenschutzes und der Einhaltung von Vorschriften. Gleichzeitig zwingt die Marktdynamik die Finanzinstitute dazu, ihre Reaktionsfähigkeit und Agilität zu erhöhen.

Sicherheitsdienste werden entscheidend sein, um das volle Potenzial ihrer internen IT-Teams freizusetzen, damit sie sich auf neue Dienstleistungen und ein besseres Kundenerlebnis konzentrieren können.

Die Finanzbranche wird dicht gefolgt von der Fertigungsindustrie, wobei der Regierungssektor im Jahr 2023 die drittgrößten Ausgaben tätigen wird. Das verarbeitende Gewerbe wird sich weiterhin auf den Schutz seiner Industrieanlagen konzentrieren, die zunehmend mit dem IT-Netzwerk des Unternehmens verbunden sein werden.

Der öffentliche Sektor wird weiterhin in den Datenschutz und in die Umsetzung seiner Initiativen zur digitalen Transformation investieren, die von immer raffinierteren Ransomware-Angriffen betroffen sind.

Grafische Benutzeroberfläche, AnwendungBeschreibung automatisch generiert

Der Worldwide Security Spending Guide von IDC quantifiziert die globalen Umsatzchancen für Sicherheitseinkäufe der ersten und der nächsten Generation mit detaillierten Prognosedaten für die Sicherheitsausgaben von 20 Branchen in neun Regionen und 44 Ländern.

[https://tinyurl.com/2kn6udbj]

Nürnberg, Germany
21.–22.6.2023

FeuerTrutz 2023

Internationale Fachmesse mit Kongress für vorbeugenden Brandschutz
International Trade Fair with Congress for Preventive Fire Protection

FeuerTrutz
Eine Marke von
RM Rudolf Müller Medien

feuertrutz-messe.de

NÜRNBERG MESSE

FT23_Poster_General_594x841mm_DE-EN